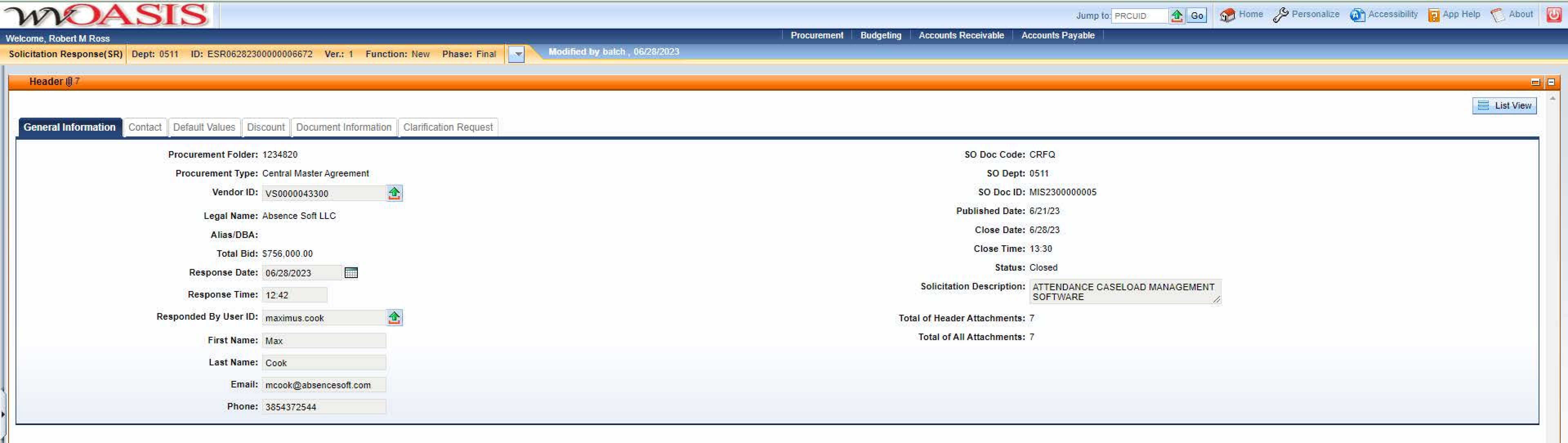
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Welcome, Robert M Ross

Solicitation Response(SR) Dept: 0511 ID: ESR06282300000006672 Ver.: 1 Function: New Phase: Final

Modified by batch , 06/28/2023

Header 7

Procurement Folder:	1234820
Procurement Type:	Central Master Agreement
Vendor ID:	VS0000043300
Legal Name:	Absence Soft LLC
Alias/DBA:	
Total Bid:	$756,000.00
Response Date:	06/28/2023
Response Time:	12:42
Responded By User ID:	maximus.cook
First Name:	Max
Last Name:	Cook
Email:	mcook@absencesoft.com
Phone:	3854372544

SO Doc Code:	CRFQ
SO Dept:	0511
SO Doc ID:	MIS2300000005
Published Date:	6/21/23
Close Date:	6/28/23
Close Time:	13:30
Status:	Closed
Solicitation Description:	ATTENDANCE CASELOAD MANAGEMENT SOFTWARE
Total of Header Attachments:	7
Total of All Attachments:	7

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder:	1234820
Solicitation Description:	ATTENDANCE CASELOAD MANAGEMENT SOFTWARE
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2023-06-28 13:30	SR 0511 ESR06282300000006672	1

VENDOR

VS0000043300
Absence Soft LLC

Solicitation Number: CRFQ 0511 MIS2300000005

Total Bid: 756000 **Response Date:** 2023-06-28 **Response Time:** 12:42:20

Comments: 35% government discount is already factored into current cost.
7% additional discount if paid within 30 days

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor
Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Attendance Caseload Management Software (FMLA/FLOA/PLA)	9.00000	EA	63000.000000	567000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: $63,000 is the annual price for our off the shelf core solution.
Additional scoping may be required for first year implementation (see pricing and implementation slide for reference).
Price is by number of employees. 3-9 admins are included in that price.

Extended Description:

3.1.2 Attendance Caseload Management Software (FMLA/FLOA/PLA)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Year One Optional Renewal				63000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: First year implementation drops off at renewal. Only subscription cost from there on out.

Extended Description:

Optional Renewal Year One

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Year Two Optional Renewal				63000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: We anticipate 5% year over year increase

Extended Description:

Optional Renewal Year Two

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Year Three Optional Renewal				63000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: We anticipate 5% year over year increase

Extended Description:

Optional Renewal Year Three

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	Additional Users/Licenses	1.00000	EA	0.000000	0.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: Price is by number of employees. 3-9 users is already built into cost

Extended Description:

3.1.2.21 Additional Users/Licenses- each add on user/license (9 used for bidding scenario only, quantity could increase or decrease during life of contract)

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	Online Training for Licenses Holders				0.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments: On demand training is free. AbsenceSoft University can be accessed by any mobile device.

Extended Description:

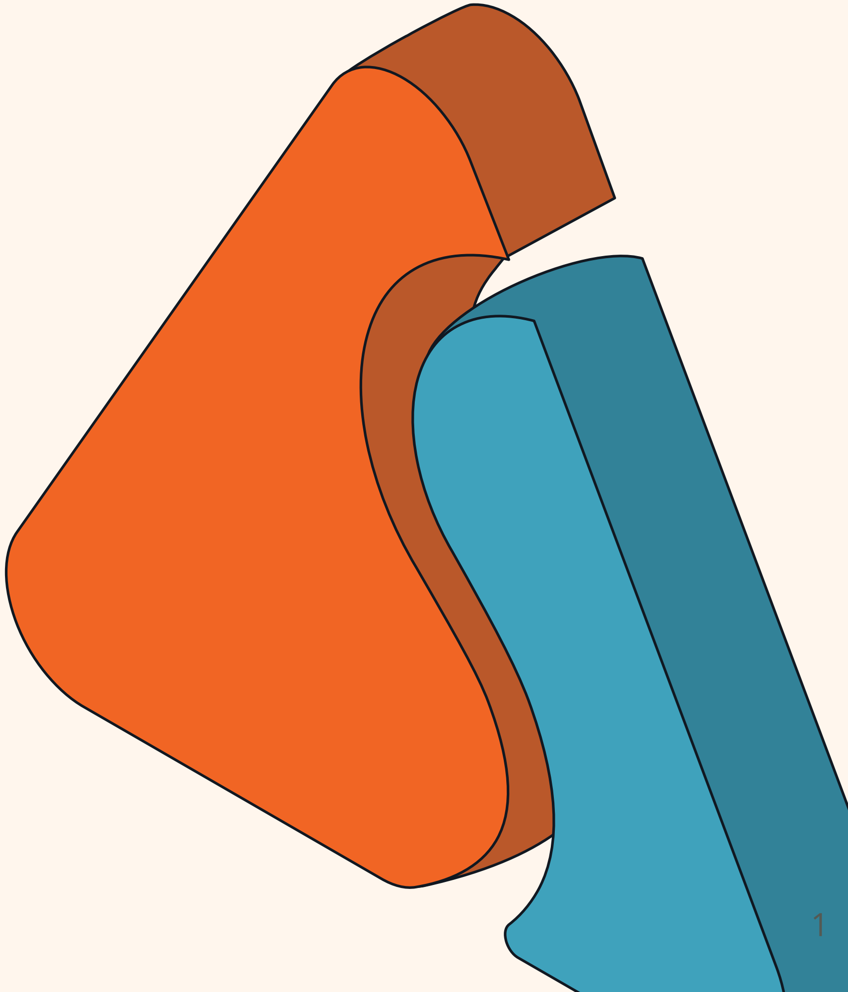
3.1.2.22 Must provide online training for license holders at no cost. System upgrades, enhancements, and error corrections must be at no additional cost/charge when such upgrades, enhancements, and error corrections are generally made available to its other clients of similar systems at no additional cost/charge.

AbsenceSoft

West Virginia DHHR

Leave of Absence & Accommodations Pricing Proposal

June 2023



AbsenceSoft

Table of Contents

Executive Summary

West Virginia DHHR

West Virginia DHHR: Scope of Work

Your Background – The Basics:

- 5,000-6,000 Employees
- Average 6-15 leave requests per day and approx. 1,400-1,500 leave cases per year

Your Pain Points:

- Manual system isn't functioning to manage full leave and accommodation case load
- Out of compliance due to leave requests that fall through the cracks
- Decreased productivity while spending countless hours researching all eligibility requirements
- No employee self-service or easy way for department employees to request leaves or accommodations
- Current manual process does not provide prompt work restriction approvals, track, and notify when the length of leave is nearing 90 days; then automatically send out accommodation or leave paperwork

AbsenceSoft

We've heard you!

We understand your goals & know we can help.

Streamline & Automate Processes

Our software was built by leave professionals for leave professionals, it streamlines & automates the leave and accommodations processes at every step.

Our Proven Track Record

We've helped many public sector customer transition from manual leave & accommodations management to AbsenceSoft, saving them an average of 66% in administrative time.

Centralized, Single Source of Truth

With all requests and communications stored in our system, we keep you compliant by ensuring data security and provide you with a single source of truth.

Enhanced Compliance Engine

Our Internal Compliance Team Partners with Littler Mendelson to Track Legislation, keeping you up-to-date and compliant with federal and state leave laws.

White Glove Implementation

Everyone you'll speak with is a Certified Leave Management Specialist (CLMS), partnering with you to ensure we meet your specific business needs & goals.

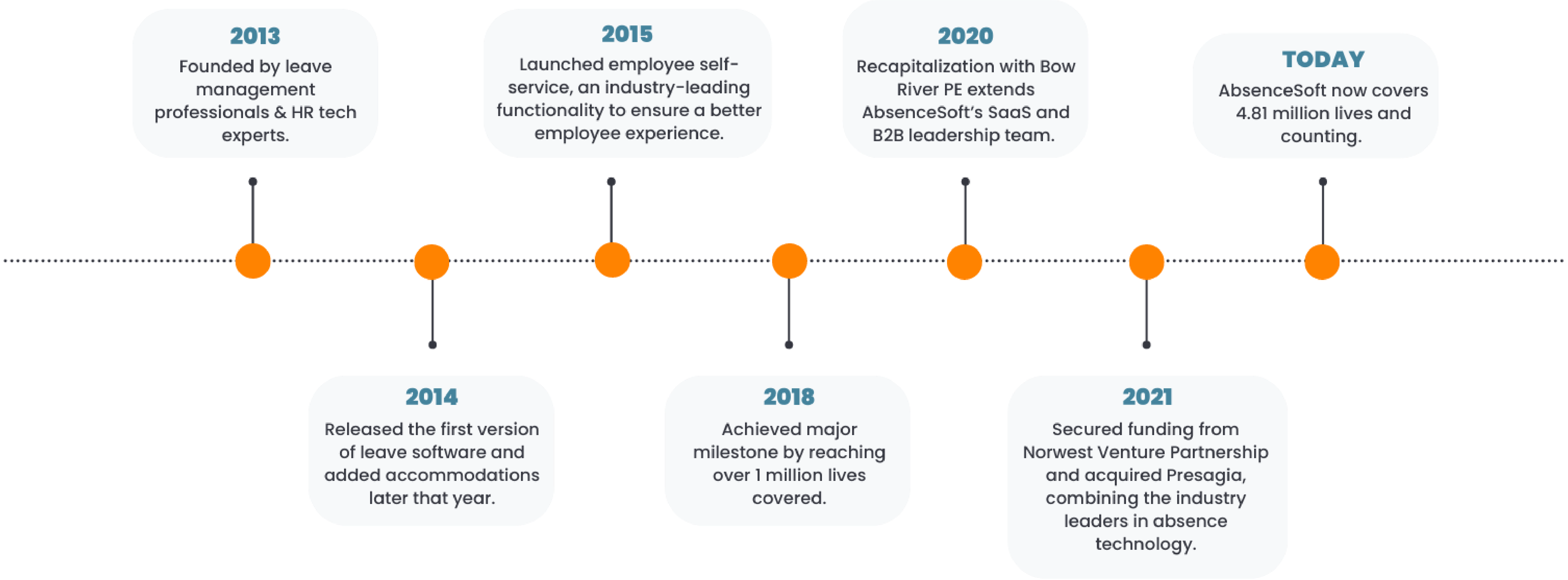
Employee Self-Service Portal

Our off-the-shelf Employee Self-Service Portal provides an easy way for employees to request a leave or accommodations, and keeps employees and people automatically up to date on leave request status.

Plus, a 99% customer retention rate.

Brief Introduction to AbsenceSoft

Our History



2013
Founded by leave management professionals & HR tech experts.

2014
Released the first version of leave software and added accommodations later that year.

2015
Launched employee self-service, an industry-leading functionality to ensure a better employee experience.

2018
Achieved major milestone by reaching over 1 million lives covered.

2020
Recapitalization with Bow River PE extends AbsenceSoft's SaaS and B2B leadership team.

2021
Secured funding from Norwest Venture Partnership and acquired Presagia, combining the industry leaders in absence technology.

TODAY
AbsenceSoft now covers 4.81 million lives and counting.

AbsenceSoft

Who Are We?

What Is AbsenceSoft?

- Leave of Absence & Accommodations management software
- Streamlines and automates your leave & accommodations processes, while ensuring compliance
- Created by HR Professionals, for HR Professionals

What Is Our Purpose?

We exist to help you…

- Enhance your employee experience & satisfaction
- Improve productivity & visibility
- Reduce time & costs
- Decrease compliance risk

AbsenceSoft

What Sets Us Apart?

We bring automation, order and transparency to a complex process.

Intelligent Automation

We automate the eligibility process of state, federal and company specific policies, which can trigger compliant letters, emails & texts notifying employees of the status of their requests.

Real-Time Compliance

As Federal & State regulations change, so does our software. We release new functionality weekly to ensure we're keeping you up to date as soon as new laws are enacted.

Employee Experience

Free up your HR team's time. Allow them to spend less time on administrative tasks and more time with your employees, improving your employee experience, satisfaction & retention.

Plus, a 99% customer retention rate.

AbsenceSoft

Let’s make your job fun & people focused again.

You no longer need to worry about....

Processing Leave Requests

Employees can input a request easily on their own in 4-clicks & get an automatic eligibility decision that fully complies with state, federal and your company-specific leave policies.

Missing Deadlines

AbsenceSoft helps you consolidate all of the required information and deadlines, presenting it in an easy-to-view dashboard so nothing is missed, and your work is streamlined.

Writing the same communications, over & over

Use customized, templated letters, emails & text messages that auto-fill employee and company information and ensure all pertinent information is sent without requiring a new letter to be created for each employee.

Compliance

Our dedicated internal compliance team updates our software regularly to include new and updated legislation, so you don’t have to keep up with it.

Scrambling for Information & Data

All historical information like tasks and communications are tracked in the software. You can pull standard reports or create your own with the click of a button, 24/7.

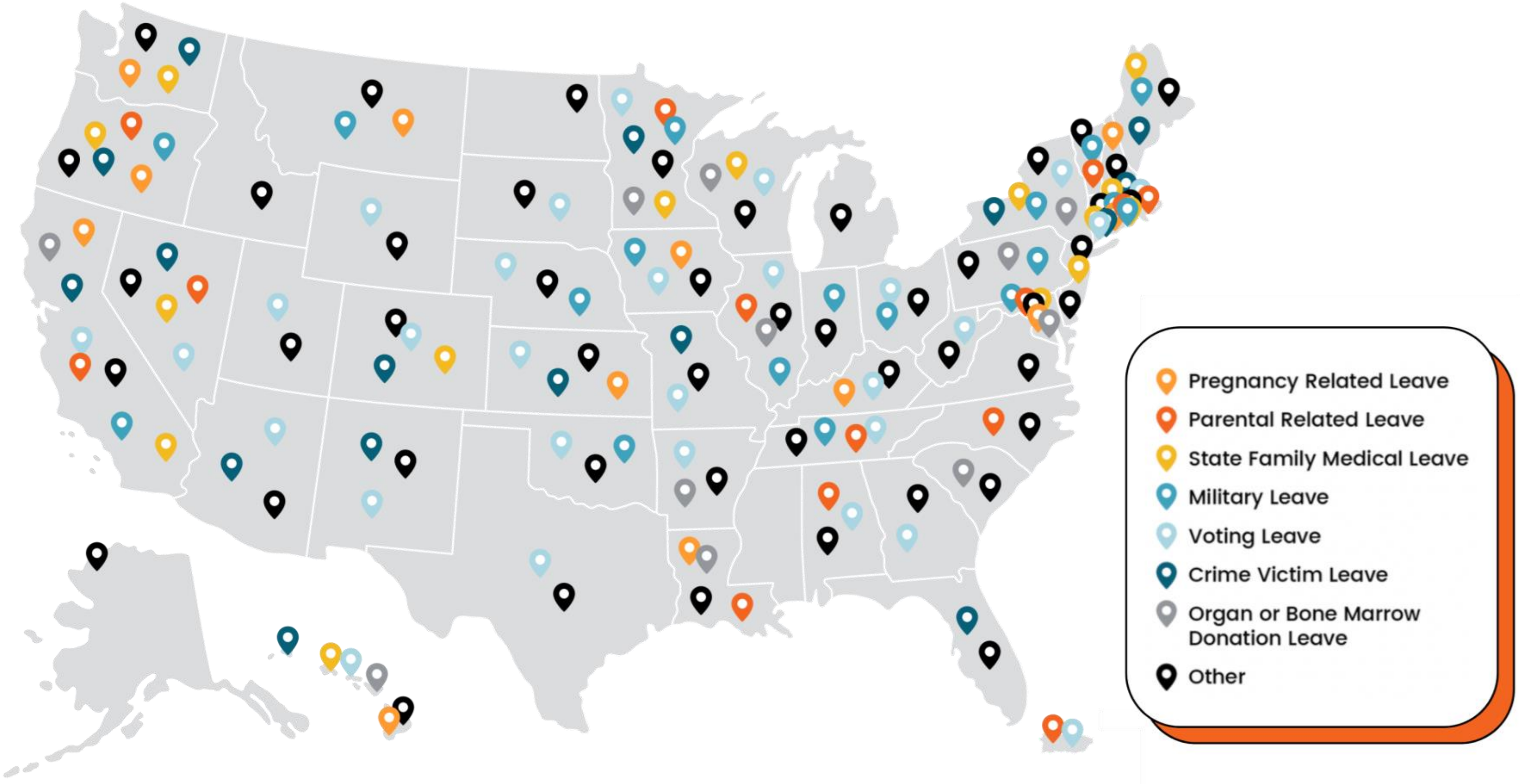
...spend the extra time supporting & building relationships with your employees.

AbsenceSoft

AbsenceSoft's Compliance Engine

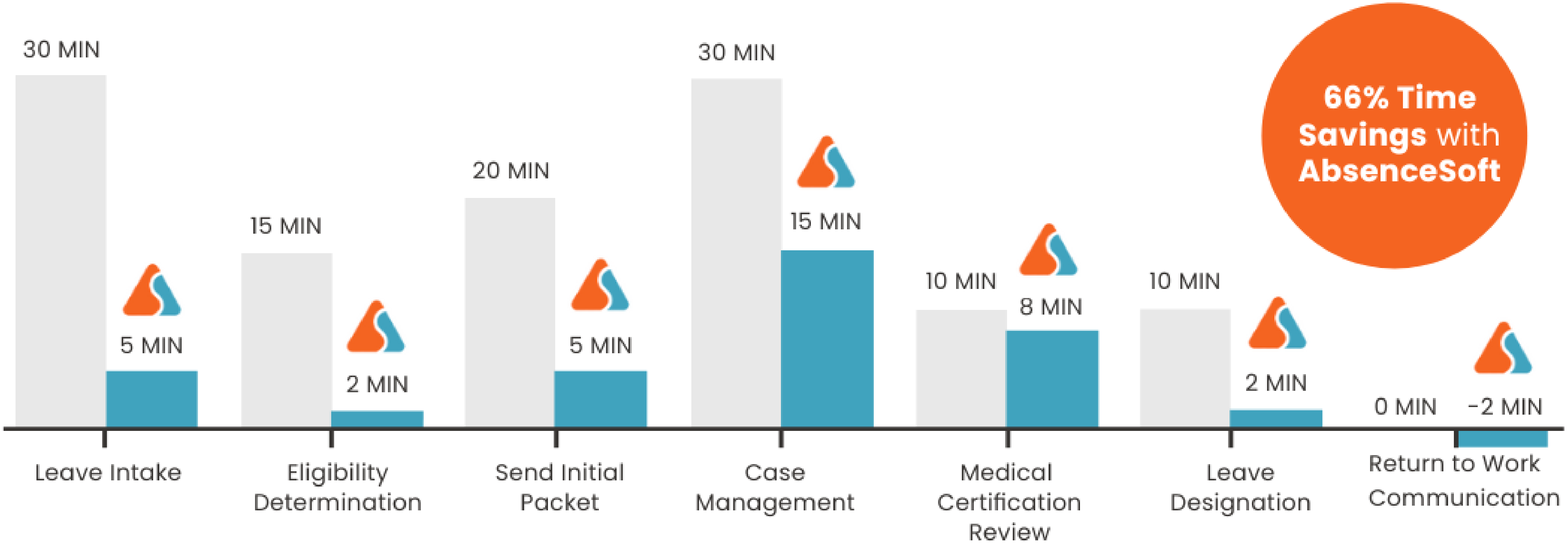
The current state of compliance.

- Our compliance engine powers all of our solutions
- Our compliance team manages 180+ U.S. leave rules



See the Difference

Manual Leave Case Management vs. AbsenceSoft



66% Time Savings with **AbsenceSoft**

Client Testimonials

Hear from our current clients.

“AbsenceSoft helps us stay compliant. When the attorneys and compliance teams call for case information, I can pull exactly what I need and quickly.”

Lisa Schwartzenburg
Director of Benefits & Wellness
Gonzaga University

“So worth the investment. We now spend time helping our people instead of focusing on the administration of our leave program.”

Rachel James
HR Director
Davis Wright Tremaine LLP

Want to hear from another client? Watch this 30-minute conversation with Pam Armstrong, *Sr. Manager of Absence Management at American Airlines*.

Nearly **5 million** lives covered and a **99%** customer retention rate.

Product Overview

AbsenceSoft

Our Product Suite

An easy-to-use leave & accommodations automation platform

Main Modules

- Leave of Absences: FMLA, Federal & State Leaves
- Accommodations: ADA & PWFA

Optional Features

- Text Messaging
- Faxing & Barcoding
- Insights Advanced
- Employee Self-Service
- Batch Fulfillment

AbsenceSoft

AbsenceSoft Modules & Features

Let’s decide what makes sense for you.

Leave of Absence & FMLA	ADA & Accommodations	Employee Self Service	Batch Fulfillment	Text Messaging	Faxing & Barcoding	Insights Advanced
• Tracking of all State, Federal & company specific policies • Automatic updates on all federal & state law changes • Automated email notifications & capabilities • Ad-hoc & custom insights • Unlimited email templates • Tracks work related absences • Compliant audit trail	• Tracking of all company specific ADA policies • EEOC compliant interactive process • Ad-hoc & custom insights • Automating email notifications & capabilities • Audit trail	Employee portal that allows for: • Employees able to enter their own leave requests & upload paperwork • Create notes in cases to communicate with leave team • Real-time access for employees into their cases • Audit trail	Batch out communication packets: • Ability to send all communications to external or internal print fulfillment center or vendor	Send text messages to your employees through our system: • Utilize a preferred method of communication • Easily send text reminders about needed documentation, return-to-work, etc.	Unique communication barcodes that: • Automatically routes documents to the appropriate case • Provide the ability to upload multiple documents at once	All the features of insights core with more powerful capabilities, enabling your team to: • · Customize core dashboards and reports • · Create entirely new, fully custom dashboards and reports • Share reports to team members with the click of a button • Stay up to date with regular or recurring report scheduling

AbsenceSoft

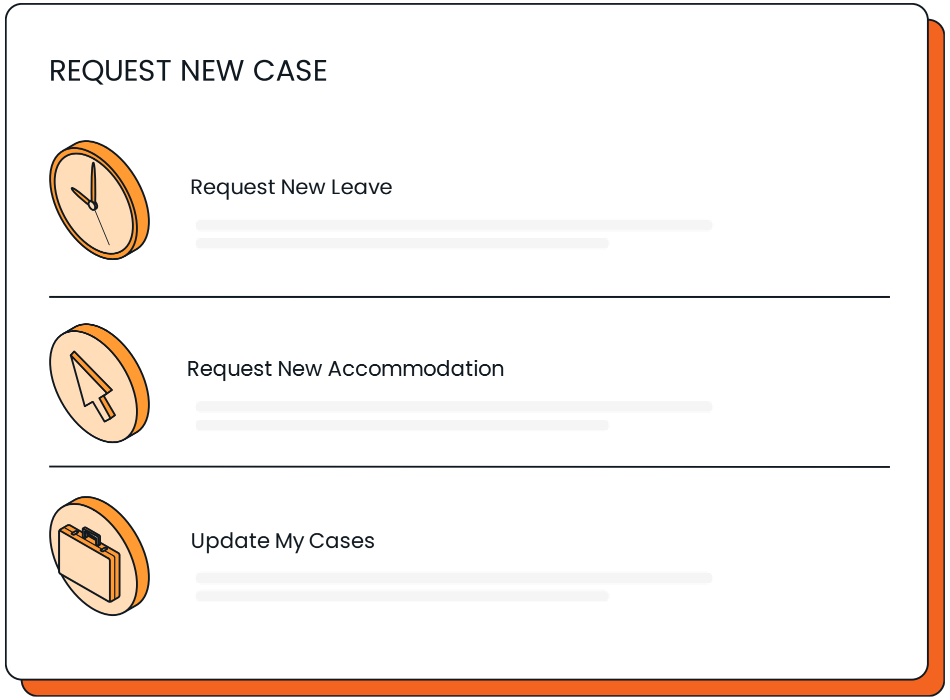
Employee Self-Service

What is it?

From initial leave requests to return to work, our Employee Self-Service feature closes the communication gap between HR and employees.

Key Features:

- ✓ Allows employees to complete their part of the leave process easily & hassle-free, without a phone call
- ✓ Leave intake and return-to-work documentation can be collected all in one platform
- ✓ Employees can easily view entitlement, eligibility and case status in real-time
- ✓ Automatically notify case manager and employee when tasks are due
- ✓ Access to case information in real-time by employees, supervisors, and the HR team
- ✓ Fully WCAG Compliant for maximum accessibility



REQUEST NEW CASE

Request New Leave

Request New Accommodation

Update My Cases

AbsenceSoft

Advanced Reporting

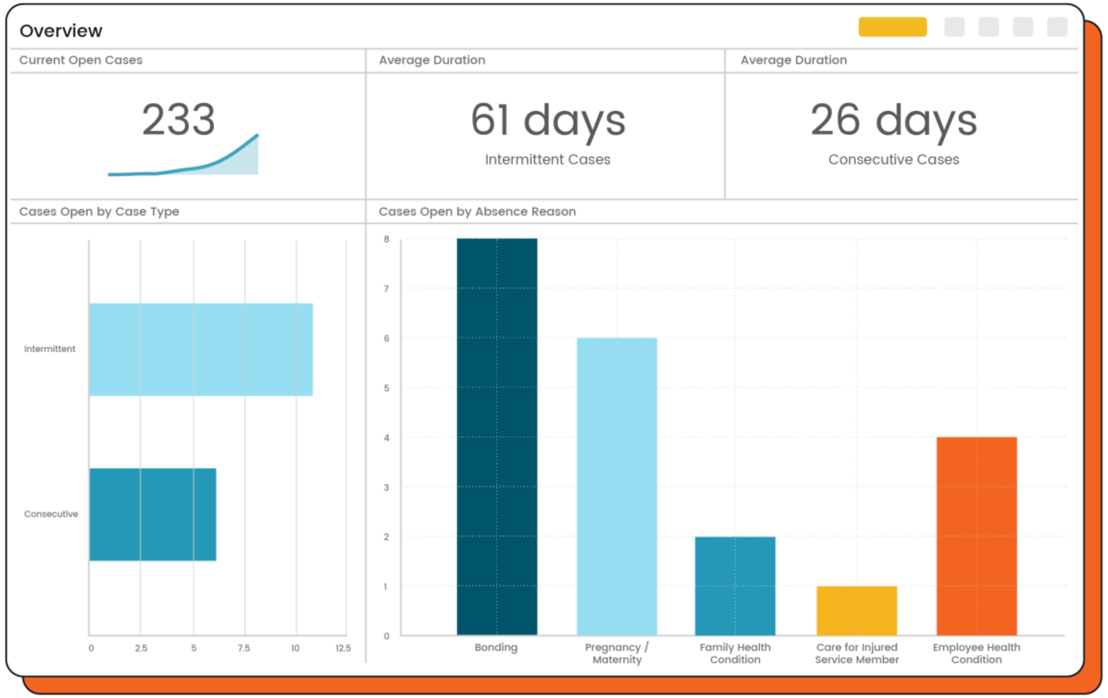
What is it?

Need to know how many of your employees are on leave at any given time?

Looking for insights into leave usage to inform policy decisions?

Our reporting tools give your leave team real-time insight into the current state of your leave and accommodations program.

- Easily pull consolidated, detailed, customizable, up-to-date reports about your entire workforce on-demand.
- Visual displays and dashboards help you quickly and easily analyze leave and accommodation data.



Overview

Current Open Cases: 233

Average Duration: 61 days, Intermittent Cases

Average Duration: 26 days, Consecutive Cases

Cases Open by Case Type

Cases Open by Absence Reason

> *I love AbsenceSoft's Advanced Reporting feature! The graphs tell a stronger story than numbers alone, so the visual in conjunction with the data helps me highlight cases and share trends with our directors and leadership team. It's much easier to drill down than any other leave or accommodations reporting I've seen!*

Erica Alves, MSHRM
Benefits Consultant, Leave Administration Team Lead
Occidental Petroleum

Pricing

AbsenceSoft

Pricing

Annual Subscription Fee

Our annual subscription fee is priced per module. Price is based on three modules RFQ mentions (highlighted in orange). Feel free to calculate any additional modules the agency would want to utilize.

Pricing below is calculated Per Employee Per Month, based on **5,000 employees**.

	Core FMLA/FLA/PLA	ADA	Employee Self-Service	Text Messaging	Fax Barcoding	Batch Print	Insights Advanced	**Total Annual Cost for In Scope Modules**
Price (PEPM)	$0.75	$0.20	$0.15	$0.10	$0.10	$0.10	$0.15	
	✓	✓	✓					**$63,000**

Pricing is subject to change.
This pricing is valid for 90 days from sent-by date.
Anticipated 5% increase YoY

Pricing

One-Time Implementation Fee

Our **one-time** implementation fee is based on the customizations needed & modules included.

What's Included?

- Implementation & customization of all modules selected
- Import of up to 2 years of historical data
- Standard FTP Employee Data Load from HRIS system
- Extensive admin training for your team
- Set-up of user and role-based visibility
- Operational, technical and ad-hoc calls with our CLMS Certified implementation teams

Implementation, Simplified

- We fix-bid our implementation costs and stand-by that number
- Only 4% of Implementations take 5 or more months
- Minimal IT involvement, integrate with all major HRIS & ERP systems
- 99% customer retention rate

Estimated Fee:

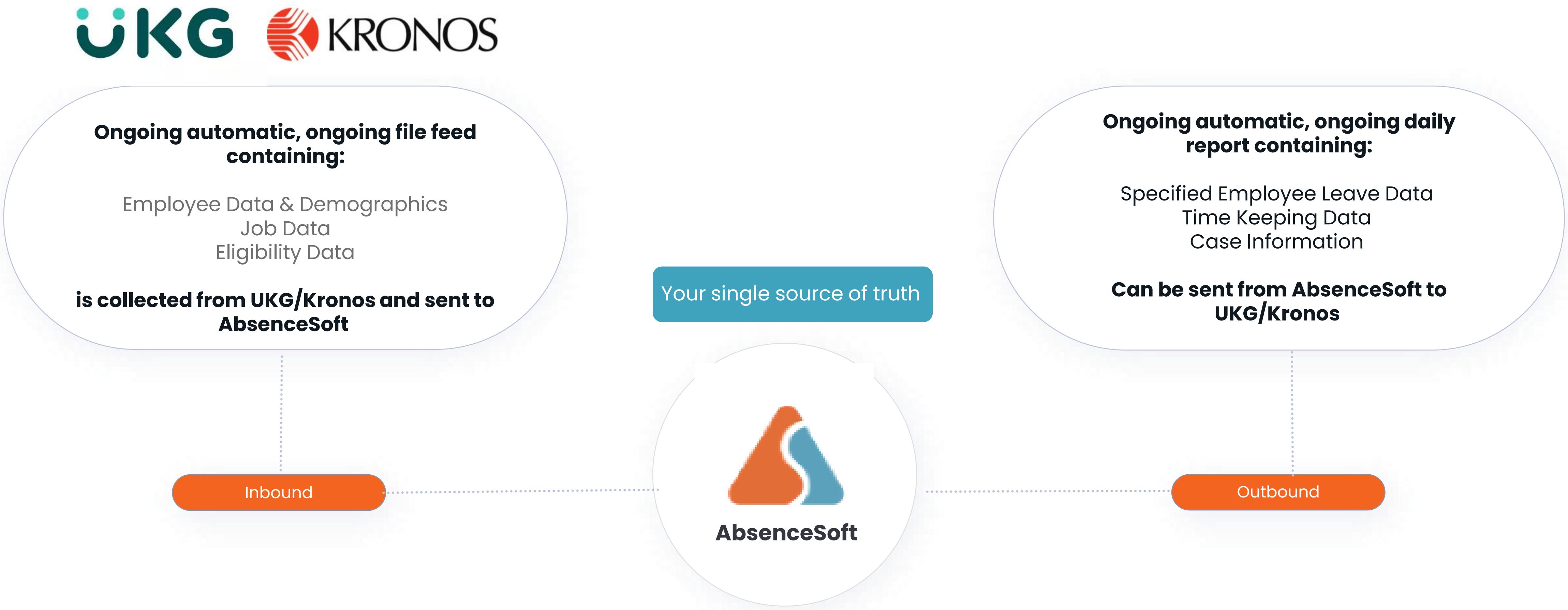
$45,000-$58,000

**Dependent on customization & modules*

Pricing is subject to change.
This pricing is valid for 90 days from sent-by date.

Integrations & Implementation

Streamlined Data Integration



UKG KRONOS

Ongoing automatic, ongoing file feed containing:

Employee Data & Demographics
Job Data
Eligibility Data

is collected from UKG/Kronos and sent to AbsenceSoft

Your single source of truth

Ongoing automatic, ongoing daily report containing:

Specified Employee Leave Data
Time Keeping Data
Case Information

Can be sent from AbsenceSoft to UKG/Kronos

Implementation Approach

Our four phases to get you to the finish line.

Time / Effort of Stage:

Discover

1-2 Weeks / 5-15 Hours

- Project Team Mobilization
- Project Planning
- Solution Definition
- Data Gathering
- Integration Planning/ Architecture
- Solution Review

Configure

3-6 Weeks / 15-30 Hours

- System Configuration
- Test Planning
- Data Migration
- Unit Testing
- Configuration Review
- User Review/Testing

Launch

1-2 Weeks / 5-15 Hours

- Cutover Preparation
- Training (Train the Trainer)
- Production Deployment
- Data Extraction/Load
- Data Validation
- Production Cutover

Complete

2 Weeks / 5-15 Hours

- Production Stabilization
- Project Completion
- Knowledge Transfer to Client Team
- Transition to Support
- Project Close

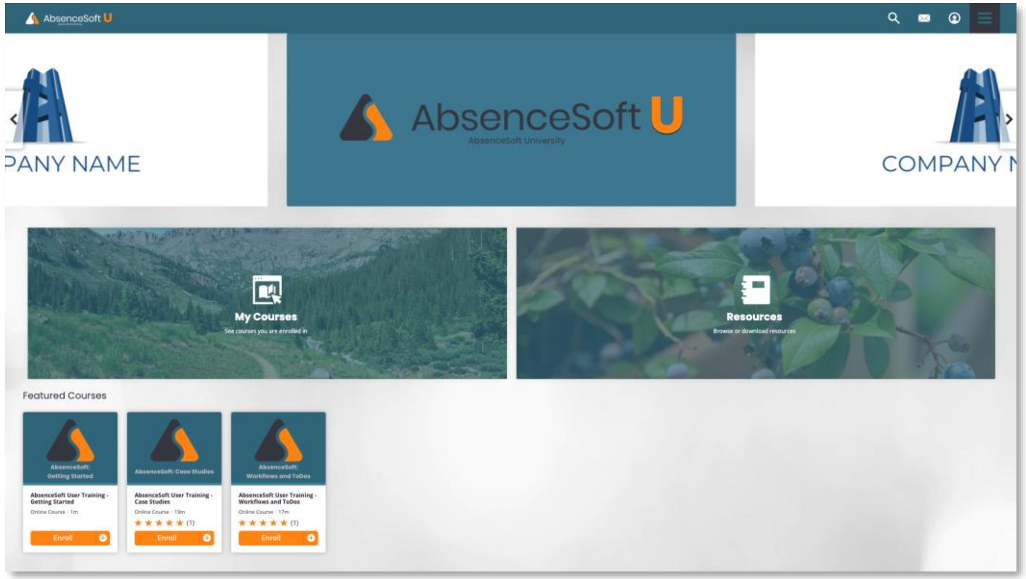
Total:
7-12 Weeks / 30-70 Hours

On-Demand Training

AbsenceSoft U

AbsenceSoft University

AbsenceSoft University is a self-paced learning platform that will assist you and your team in learning the AbsenceSoft Platform. Beginning with the fundamentals of getting around, you will see demonstrations of common leave case workflows and how to manage cases effectively and efficiently. Your *AbsenceSoft U* Portal is only viewable by you.



My Courses
See courses you are enrolled in

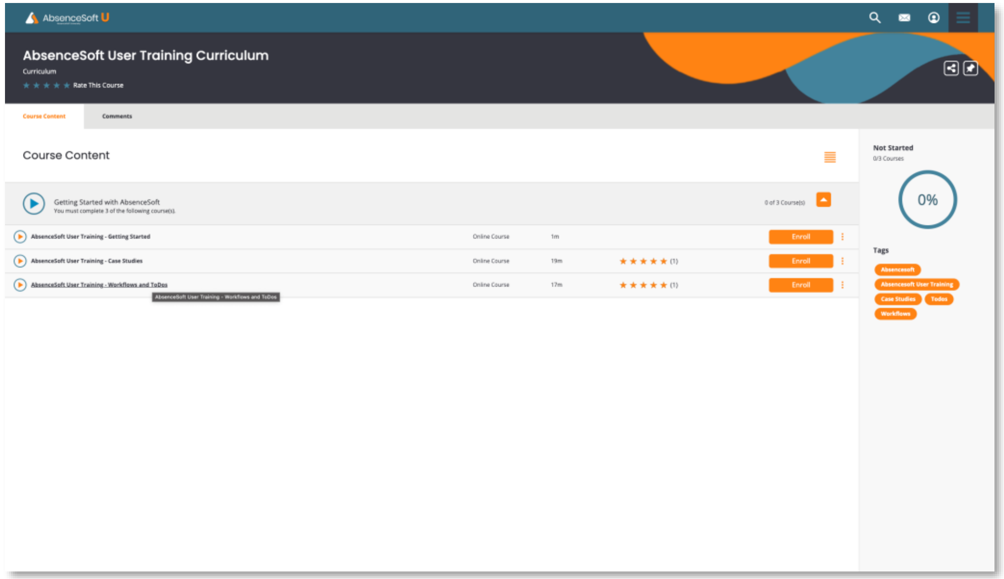
Resources
Browse or download resources

Featured Courses

AbsenceSoft: Getting Started
AbsenceSoft User Training - Getting Started
Online Course · 1m
Enroll

AbsenceSoft: Case Studies
AbsenceSoft User Training - Case Studies
Online Course · 19m
★★★★★ (1)
Enroll

AbsenceSoft: Workflows and ToDos
AbsenceSoft User Training - Workflows and ToDos
Online Course · 17m
★★★★★ (1)
Enroll



AbsenceSoft User Training Curriculum
Curriculum
★★★★★ Rate This Course

Course Content | Comments

Course Content

Getting Started with AbsenceSoft
You must complete 3 of the following course(s).
0 of 3 Course(s)

AbsenceSoft User Training - Getting Started	Online Course	1m		Enroll
AbsenceSoft User Training - Case Studies	Online Course	19m	★★★★★ (1)	Enroll
AbsenceSoft User Training - Workflows and ToDos	Online Course	17m	★★★★★ (1)	Enroll

AbsenceSoft User Training - Workflows and ToDos

Not Started
0/3 Courses
0%

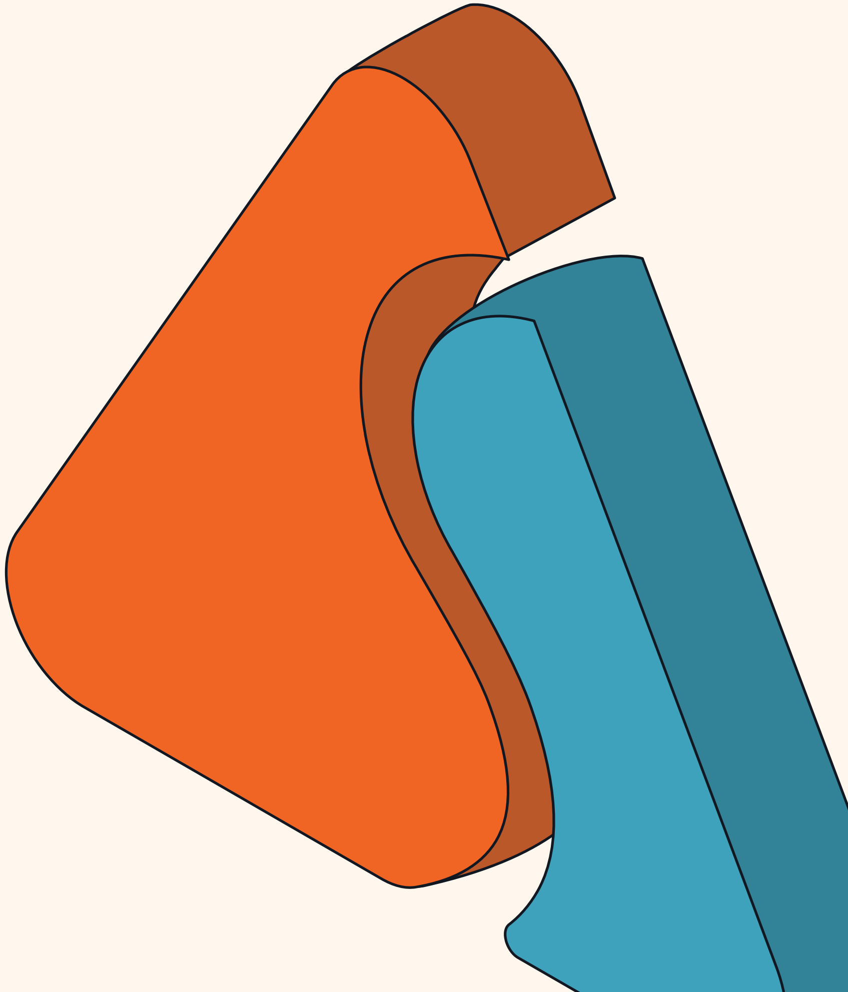
Tags
Absencesoft
Absencesoft User Training
Case Studies
Todos
Workflows

AbsenceSoft

Thank You

Max Cook

Public Sector Leave/Accommodation Specialist
mcook@absencesoft.com
385-437-2544



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Info Technology

Proc Folder: 1234820

Doc Description: ATTENDANCE CASELOAD MANAGEMENT SOFTWARE

Proc Type: CentralMasterAgreement

Reason for Modification:

Date Issued	Solicitation Closes	Solicitation No	Version
2023-06-07	2023-06-28 13:30	CRFQ 0511 MIS2300000005	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON STE
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name :

Address:

Street:

City:

State: **Country:** **Zip:**

Principal Contact :

Vendor Contact Phone: Extension:

FOR INFORMATION CONTACT THE **BUYER**
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor
Signature X FEIN# DATE

All **offers** subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, WEST VIRGINIA DEPARTMENT OF HEALTH AND HUMAN RESOURCES (DHHR), OFFICE OF MANAGEMENT INFORMATION SERVICES, IS SOLICITING BIDS TO ESTABLISH AN OPEN-END CONTRACT FOR ATTENDANCE CASELOAD MANAGEMENT SOFTWARE (FMLA/FLOA/PLA TRACKING) PER THE ATTACHED DOCUMENTS.

QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS

!INVOICE TO	jsHIPTO
HEALTH AND HUMAN RESOURCES	HEALTH AND HUMAN RESOURCES
OFFICE OF HUMAN RESOURCES MGMT	OFFICE OF HUMAN RESOURCES MGMT
ONE DAVIS SQUARE, STE 400	ONE DAVIS SQUARE, STE 400
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
	Attendance Caseload Management Software (FMLA/FLOA/PLA)	9.00000	EA		

Comm Code	Manufacturer	Specification	Model#
43230000			

Extended Description:

3.1.2 Attendance Caseload Management Software (FMLA/FLOA/PLA)

[INVOICE TO	!SHIP TO
HEALTH AND HUMAN RESOURCES	HEALTH AND HUMAN RESOURCES
OFFICE OF HUMAN RESOURCES MGMT	OFFICE OF HUMAN RESOURCES MGMT
ONE DAVIS SQUARE, STE 400	ONE DAVIS SQUARE, STE 400
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Year One Optional Renewal				

Comm Code	Manufacturer	Specification	Model#
43230000			

Extended Description:

Optional Renewal Year One

IINVOICETO

HEALTH AND HUMAN
RESOURCES
OFFICE OF HUMAN
RESOURCES MGMT
ONE DAVIS SQUARE, STE
400
CHARLESTON WV
US

IsHIPTO

HEALTH AND HUMAN
RESOURCES
OFFICE OF HUMAN
RESOURCES MGMT
ONE DAVIS SQUARE, STE
400
CHARLESTON WV
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Year Two Optional Renewal				

Comm Code	Manufacturer	Specification	Model#
43230000			

Extended Description:
Optional Renewal Year Two

j1NVOICETO

HEALTH AND HUMAN
RESOURCES
OFFICE OF HUMAN
RESOURCES MGMT
ONE DAVIS SQUARE, STE
400
CHARLESTON WV
US

IsHIPTO

HEALTH AND HUMAN
RESOURCES
OFFICE OF HUMAN
RESOURCES MGMT
ONE DAVIS SQUARE, STE
400
CHARLESTON WV
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Year Three Optional Renewal				

Comm Code	Manufacturer	Specification	Model#
43230000			

Extended Description:
Optional Renewal Year Three

IINVOICETO	IsHJP TO
HEALTH AND HUMAN RESOURCES	HEALTH AND HUMAN RESOURCES
OFFICE OF HUMAN RESOURCES MGMT	OFFICE OF HUMAN RESOURCES MGMT
ONE DAVIS SQUARE, STE 400	ONE DAVIS SQUARE, STE 400
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	Additional Users/Licenses	1.00000	EA		

Comm Code	Manufacturer	Specification	Model#
43230000			

Extended Description:

3.1.2.21 Additional Users/Licenses- each add on user/license (9 used for bidding scenario only, quantity could increase or decrease during life of contract)

IINVOICETO	IsHIPro
HEALTH AND HUMAN RESOURCES	HEALTH AND HUMAN RESOURCES
OFFICE OF HUMAN RESOURCES MGMT	OFFICE OF HUMAN RESOURCES MGMT
ONE DAVIS SQUARE, STE 400	ONE DAVIS SQUARE, STE 400
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	Online Training for Licenses Holders				

Comm Code	Manufacturer	Specification	Model#
43230000			

Extended Description:

3.1.2.22 Must provide online training for license holders at no cost. System upgrades, enhancements, and error corrections must be at no additional cost/charge when such upgrades, enhancements, and error corrections are generally made available to its other clients of similar systems at no additional cost/charge.

IscHEDULE oF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2023-06-15

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. REVIEW DOCUMENTS THOROUGHLY: The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

2. MANDATORY TERMS: The Solicitation may contain mandatory provisions identified by the use of the words "must," "wiJI," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

3. PREBID MEETING: The item identified below shall apply to this Solicitation.

1Z] A pre-bid meeting will not be held prior to bid opening

0 A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

4. VENDOR QUESTION DEADLINE: Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted emails should have the solicitation number in the subject line.

Question Submission Deadline: June 15, 2023 at 10:00 AM ET

Submit Questions to: Crystal Hustead, Senior Buyer
2019 Washington Street, East
Charleston, WV 25305
Fax: (304) 558-3970
Email: crystal.g.hustead@wv.gov

5. VERBAL COMMUNICATION: Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

6. BID SUBMISSION: All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through wvOASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronica1ly through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit bids through wvOASIS. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via email. Bids submitted in paper or facsimile form must contain a signature. Bids submitted in wvOASIS are deemed to be electronically signed.

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

For Request for Proposal ("RFP") Responses Only: Submission of a response to a Request for Proposal is not permitted in wvOASIS. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time identified in Section 7 below, plus _____ nl_a___________ __ convenience copies of each to the Purchasing Division at the address shown below. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

Bid Delivery Address and Fax Number:
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:
BUYER: Crystal Hustead, Senior Buyer
SOLICITATION NO.: CRFQ MIS2300000005
BID OPENING DATE: June 28, 2023
BID OPENING TIME: 1:30 PM ET
FAX NUMBER: 304-558-3970

7. **BID OPENING:** Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: June 28, 2023 at 1:30 PM ET

Bid Opening Location: Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

8. ADDENDUM ACKNOWLEDGEMENT: Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to ·acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

9. BID FORMATTING: Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

10. ALTERNATE MODEL OR BRAND: Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

D This Solicitation is based upon a standardized commodity established under W. Va. Code § SA-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

11. EXCEPTIONS AND CLARIFICATIONS: The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

12. COMMUNICATION LIMITATIONS: In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

13. REGISTRATION: Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable.

14. UNIT PRICE: Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

15. PREFERENCE: Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code§ SA-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

15A. RECIPROCAL PREFERENCE: The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrcNenpref.pdf.

16. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES: For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 and W. Va. CSR§ 148-22-9, any non-resident vendor certified as a small, women- owned, or minority-owned business under W. Va. CSR§ 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-. owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR§ 148-22-9.

17. WAIVER OF MINOR IRREGULARITIES: The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules§ 148-1-4.6.

18. ELECTRONIC FILE ACCESS RESTRICTIONS: Vendor must ensure that its submission in wvOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

19. NON-RESPONSIBLE: The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules§ 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance."

20. ACCEPTANCE/REJECTION: The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules§ 148-1-4.5. and§ 148-1-6.4.b."

21. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code§§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code§§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, *A* TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code§ 47-22-1 et seq. All submissions are subject to public disclosure without notice.

22. WITH THE BID REQUIREMENTS: In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR§ 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

23. EMAIL NOTIFICATION OF AWARD: The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor wvOASIS or the Purchasing Division's website to determine when a contract has been awarded.

24. ISRAEL BOYCOTT CERTIFICATION: Vendor's act of submitting a bid in response to this solicitation shall be deemed a certification from bidder to the State that bidder is not currently engaged in, and will not for the duration of the contract, engage in a boycott oflsrael. This certification is required by W. Va. Code§ SA-3-63.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. DEFINITIONS: As used in this Solicitation/Contract, the fo1lowing terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or **"Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or **"Proposal"** means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or **"Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

0 **Term Contract**

Initial Contract Term: The Initial Contract Term will be for a period of one (1) year _ _ _ _ _ _ _ _ _ _ _ _ _ _ . The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _________________________________ __,, and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

> D **Alternate Renewal Term -** This contract may be renewed for __________________ successive ___________year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

D **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _________________________days.

O **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _________________ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

D the contract will continue for _________________ years;

D the contract may be renewed for __________________successive _______ __ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

D **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

D **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _______________________________ _,, and continues until the project for which the vendor is providing oversight is complete.

O **Other:** Contract Term specified in ______________________ __

4. AUTHORITY TO PROCEED: Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

1Z] **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

D **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

D **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

D **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

0 **Construction:** This Contract is for construction activity more fully defined in the specifications.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

7. **REQUIRED DOCUMENTS:** All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

0 **LICENSE(S) /CERTIFICATIONS/ PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

□

□

□

□

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice df any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

It] **Commercial General Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

O **Automobile Liability Insurance** in at least an amount of: ___________ _,er occurrence.

D **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: _ _ _ _ _ _ _ _ _ _ er occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

D**Commercial Crime and Third Party Fidelity Insurance** in an amount of: _________________per occurrence.

D **Cyber Liability Insurance** in an amount of: ____________________________ per occurrence.

D **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

D **Pollution Insurance** in an amount of: __________________ per occurrence.

D **Aircraft Liability** in an amount of: _________________ per occurrence.

□

□

□

□

\

9. WORKERS' COMPENSATION INSURANCE: Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

10. VENUE: All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

□ ________________ for ________________________________

D Liquidated Damages Contained in the Specifications.

D Liquidated Damages Are Not Included in this Contract.

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

13. PRICING: The pricing set forth herein is firm for the life of the- Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

14. PAYMENT IN ARREARS: Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

15. PAYMENT MEIBODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is, exempt from federal and state taxes and will not pay or reimburse such taxes.

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July **1** of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

20. TIME: Time is of the essence regarding all matters oftime and performance in this Contract.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

> **SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in http://www.state.wv.us/admin/purchase/privacy/default.html.

31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code§§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-l-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-l-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code§ 47-22-1 et seq. All submissions are subject to public disclosure without notice.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

> **SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Documen from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

34. VENDOR NON-CONFLICT: Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

37. **NO DEBT CERTIFICATION:** In accordance with West Virginia Code§§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

38. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

39. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

D Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

DQuarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.2.ov.

40. BACKGROUND CHECK: In accordance with W. Va. Code§ 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code§ 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code§ 5A-3-56. As used in this section:

a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.

c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

    1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

    2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code§ 5-19-1 et seq., and W. Va. CSR§ 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code§ 6D-1-2 requires that for contracts with an actual or estimated value of at least $1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the forn1 referenced above.

44. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted **in** the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

45. VOID CONTRACT CLAUSES: This Contract is subject to the provisions of West Virginia Code§ SA-3-62, which automatically voids certain contract clauses that violate State law.

46. ISRAEL BOYCOTT: Bidder understands and agrees that, pursuant to **W.** Va. Code§ SA-3-63, it is prohibited from engaging in a boycott oflsrael during the term of this contract.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) ______________________________________ __

(Address) ____

(Phone Number)/ (Fax Number) ____________________________________

(Email address) ____

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

B signing below. I further certifv that I understand this Contract is subiect to the provisions o(West Virgi,nia Code § 5A-3-62, which automaticallv voids certain contract clauses that violate State law: and that pursuant to W. Va. Code 5A-3-63. the entiry entering into this contract is prohibited from engaging in a bovcott against Israel.

____
(Company)

____
(Signature of Authorized Representative)

____
(Printed Name and Title of Authorized Representative) (Date)

____
(Phone Number) (Fax Number)

____
(Email Address)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ MIS23ooooooos

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

0 Addendum No. I
D Addendum No. 2
D Addendum No. 3
D Addendum No. 4
D Addendum No. 5
D Addendum No. 6
D Addendum No. 7
D Addendum No. 8
D Addendum No. 9
0 Addendum No. I0

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

____
Company

____
Authorized Signature

____
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

SPECII◂'ICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Department of Health and Human Resources (DHHR) Office of Management Information Services for the WV DHHR Human Resources Management Office to establish an open-end contract for an Attendance Caseload Management Software (FMLNFLOA/PLA tracking).

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

2.1 **"Contract Item"** or **"Contract Items"** means the list of items identified in Section 3.1 below and on the Pricing Pages.

2.2 **"Pricing Pages"** means the schedule of prices, estimated order quantity, and totals contained in wvOASIS or attached hereto as Exhibit A, and used to evaluate the Solicitation responses.

2.3 **"Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.4 **"FMLA"** means Family Medical Leave Act.

2.5 **"FLOA"** means Family Leave of Absence.

2.6 **"PLA"** means Personal Leave of Absence.

3. **GENERAL REQUIREMENTS:**

3.1 **Contract Items and Mandatory Requirements:** Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below.

3.1.1 **General Operating Requirements**

3.1.1.1 Must be compatible with the West Virginia Office of Technology's current operating system, Windows 10.

Confirmed. AbsenceSoft is provided on a Software as a Service basis and supports the latest versions of the following browsers:
•Microsoft Edge
•Mozilla Firefox
•Google Chrome

•Safari

3.1.1.2 Must be compatible with WVOasis and UKG/Kronos.

Confirmed. AbsenceSoft can integrate with any third-party system that accepts file feeds. AbsenceSoft has many clients using UKG/Kronos and has integrated with these system so that they have a seamless experience using our purpose-built leave management platform.

3.1.2 Attendance Caseload Management Software (FMLA/FLOA/PLA)

3.1.2.1 Software must have automated FLMA/MLOA/PLA tracking.

Confirmed. AbsenceSoft is a purpose-built leave and accommodation management solutions provider, delivering scalable, easy-to-use, and configurable software to manage FMLA, ADA, disability, and many other forms of leave easily and efficiently. AbsenceSoft automates the entire leave process, including tasks for next steps, and templated & auto-filled communications. WV DHHR will be able to configure nearly any part of the workflow to meet their needs. The solution comes pre-built with leave rules, letter templates and workflows for federal and state leave laws, and we maintain compliance of these for our clients as laws change.

3.1.2.2 Software must assign tasks to caseworkers (rotating) and provide updates when items are due. When additional tasks come in for a previously handled employee, reassign to the same caseworker.

Confirmed. AbsenceSoft has completely configurable triage functionality, by which cases can be assigned by rotary, location, case type, or alpha-numerically, among other case assignment types.

AbsenceSoft automatically creates tasks for leave cases to remind users when next steps are due (i.e. determine eligibility, send eligibility notice, receive medical certifications, etc). There is a dashboard on the main page for each user; the view includes all tasks that need to be completed with associated due dates. This view can be sorted and filtered by due date of action item as well as by user and more. On the dashboard, Leave Managers will have the ability to toggle between their own tasks and cases as well as their team's tasks and cases. Leave Managers can also run reports on their teams case load and re-assign tasks and/or cases.

3.1.2.3 Software must be fully customizable.

Confirmed. While the core of the platform is off the shelf ready to go - AbsenceSoft is fully configurable through the UI for authorized users. West Virginia DHHR can configure the solution in multiple ways, including adding company policies, customizing communications, configuring workflows/tasks, adding custom fields, configuring case assignment rules, updating absence reasons, and more.

3.1.2.4 Software must offer recommendations based on state and federal employment and attendance regulations.

Confirmed. AbsenceSoft uses an employee's demographic details and eligibility criteria, such

as hours worked, work state, etc, to automatically calculate eligibility upon case intake for all state and federal policies in the United States.

3.1.2.5 Software must create automated reports (i.e., how many employees are on the different types of leave.)

Confirmed. Using AbsenceSoft's UI, West Virginia DHHR will have the ability to create/generate any report needed at a frequency, such as for how many employees are on each type of leave.

With AbsenceSoft's Advanced Insights module, WV DHHR will have the ability to build, schedule, and send monthly LOA reports at your fingertips inclusive of any graphs/charts needed. Your team will have a real-time look into the current state of all your programs. Easily pull consolidated, customizable, up-to-date reports about your entire workforce on-demand. Visual displays and dashboards help you quickly and easily analyze leave and accommodation data. Whether it's simple case reports or to fulfill complex audit requests, AbsenceSoft Insights are tailored to meet your specific needs.

3.1.2.6 Software must create automated letters of leave from templates that are emailed or mailed to employees.

Confirmed. All AbsenceSoft communications are template-based and dynamically generated based on leave/accommodation request type. When cases are created, automated packets are created using the employee demographic (name, address, etc.) and case details (date requested, reason for leave, accommodation type, etc.) that are pre-populated in the communication. Communications can have conditional text that is displayed based on leave/accommodation request types or employee demographic information (e.g. – union code) so that communications can be configured to WV DHHR's requirements. Communications can also include "attachments" such as medical certification and other forms. Finally, communications are also auto-generated at other steps in the leave process (e.g. - approval) or can be manually composed. Communications can be sent to a printer to mail or via email.

3.1.2.7 Software must assign case numbers to an employee's leave case to keep all appropriate documents linked to that specific employee's case number.

Confirmed. Once a case is created in AbsenceSoft, a unique case number is assigned where all communications, notes, attachments and tasks are housed. To assist with documentation, there is also a fax barcoding feature whereby barcodes are added to leave letters like medical certifications. When a healthcare provider faxes back the medical certification, the system will automatically attach it to the correct leave case.

3.1.2.8 Software must track FMLA/MLOA/PLA used by each employee.

Confirmed. The system can easily track FMLA, MLOA, and PLA leave used by each employee.

All leave cases are displayed within an employee profile page. This allows for streamlined visibility into an employee's leave history with the ability to view further details regarding cases on each case page. All eligible policies for a given case are visible with the ability to click in and

review all rules and requirements that were tested for eligibility criteria. Further, all time used vs. time available for each eligible policy is viewable in a time tracker as well as a calendar based visual that highlights each case date with the ability to view the status of each policy on that given date. AbsenceSoft's letters also include an aggregate of information pertaining to all policies in each letter, simplifying both the management process as well as breaking out the leave information in an intuitive way for employees and managers.

3.1.2.9 Software must allow HR personnel to input disciplinary information into most recent templates and submit it to the next appropriate approval authority, then to employee management, then when approved, email to the appropriate individuals. (Payroll, HR Director, and HR personnel completing discipline).

Confirmed. All communications in AbsenceSoft are driven from MS Word templates that West Virginia DHHR will have the ability to customize during implementation. They will also have the ability to customize a letter self-service post implementation. Further, when a user generates a communication in the product, given proper permission, they are able to edit before sending the letter on an ad-hoc basis. This allows case managers to reiterate conversations, include reminders, or leave a personal message for the employee in the communication.

A workflow can be configured to accommodate the process as described above.

3.1.2.10 Software must track disciplinary matters with weekly reminders of employees who are suspended pending investigation.

Confirmed. West Virginia DHHR can add a workflow to trigger weekly reminders for suspended employees who are pending investigation. Documentation, notes and communications can be housed in AbsenceSoft on a case or employee level.

3.1.2.11 Software must interact with UKG/Kronos and WVOasis to coordinate all pertinent information for all types of leaves per each employee.

Confirmed. AbsenceSoft can integrate with UKG/Kronos and any other third-party system like WVOasis via file feeds. Any data point housed in AbsenceSoft can be included in outbound file feed and the solution can accept any data point from an inbound file feed. We have many clients who use AbsenceSoft to complement their UKG/Kronos solutions with complete leave and ADA management.

3.1.2.12 Software must track ADA cases and prompt next steps to assigned HR personnel.

Confirmed. AbsenceSoft supports a fully compliant ADA Accommodations process that is configurable to meet WV DHHR's needs. Employees are able to submit their own ADA request via the Employee Self-Service module or a request can manually be entered by a Case Administrator. Accommodations can also be configured to be part of the Return to Work process as they are related to a leave. Request details, accommodation type and duration is all collected at case intake. From there, proper ADA communications are automatically generated including all necessary forms and paperwork. A fully configurable Interactive Process is available that includes the ability to write applicable notes. Requests can then be approved or denied and are fully reportable.

3.1.2.13 Software must track investigative report status, calculate due dates, and prompt investigator to updates daily.

Confirmed. With AbsenceSoft's configurable solution, custom fields, workflows, and communications can be added to track investigative report statuses, due dates, and provide daily task reminders.

3.1.2.14 Software must provide self-service access for employees.

Confirmed. AbsenceSoft provides an easy-to use self-service portal for employee to complete activities such as requesting leaves/accommodations, viewing leave/accommodation request statuses (approved, denied, pending), view time used vs time available, view who is assigned to the case, corresponding with case managers, view the expected return to work date, submit and view intermittent time off requests, and uploading documents. Managers can also have self-service access to see their team of employees and can have access to reports.

3.1.2.15 Software must track notes and emails associated with specific leave cases and employees.

Confirmed. AbsenceSoft supports free text notes on the case as well as employee-level. Each note can be categorized and are name, date, and time stamped. All notes are searchable within the "Notes Tab". Communications and attachments are all housed on a case-level and can be downloaded for use outside of AbsenceSoft at any time.

3.1.2.16 Software must allow employees, supervisors, HR personnel to send medical paperwork and identify paperwork if for ADA, FMLA, MLOA, LOA, or unknown.

Confirmed. Paperwork can be uploaded by the employee directly via the employee self service upload function. Further, paperwork can be uploaded via drag and drop functionality by an

administer directly to an employees case file. AbsenceSoft also has integrated fax and barcoding functionality. Every piece of communication generated in the platform would have its own QR code associated with it. As medical providers fax over paperwork, the platform is able to read the bar code and attach the paperwork to the appropriate case or direct the paperwork to a document admin inbox where it can be reviewed and manually attached from there.

3.1.2.17 Software must allow creation ofreports on productivity, time used, open cases, employee participation, etc. for caseload management.

Confirmed. Reports can be easily created to review productivity, time used, open cases, and employee participation for caseload management.

With AbsenceSoft's Advanced Insights module, WV DHHR will have the ability to build, schedule, and send monthly LOA reports at your fingertips inclusive of any graphs/charts needed. Your team will have a real-time look into the current state of all your programs. Easily pull consolidated, customizable, up-to-date reports about your entire workforce on-demand. Visual displays and dashboards help you quickly and easily analyze leave and accommodation data. Whether it's simple case reports or to fulfill complex audit requests, AbsenceSoft Insights are tailored to meet your specific needs.

3.1.2.18 Software must be compatible with Google Docs and Microsoft Office Suite.

Confirmed. AbsenceSoft is compatible with both.

3.1.2.19 Software must prompt donated leave approvals and autogenerate responses.

Confirmed. Through the automated workflow, AbsenceSoft can prompt users for leave approvals. Any communication in the solution can be set up to be automatically sent at the correct time in the case lifecycle.

3.1.2.20 Software must prompt restricted leave approvals, track and notify when length of leave time is nearing (90) ninety days, which will automatically send out ADA paperwork.

Confirmed. Through the automated workflow, AbsenceSoft can prompt users for leave approvals. When a leave policy is nearing the 90 day exhaustion date, the system can automatically send a communication packet with ADA paperwork to the employee notifying them of the upcoming exhaustion and communicating expectations for the ADA paperwork.

3.1.2.21 Additional Users/Licenses may be needed and added per set cost and per each license.

(9 licenses are being used for bidding scenario only, quantity could increase or decrease during life of contract)

Confirmed. AbsenceSoft subscriptions include an unlimited number of user licenses.

3.1.2.22 Must provide online training for license holders at no cost. System upgrades, enhancements, and error corrections must be at no additional cost/charge when such upgrades, enhancements, and error corrections are generally made available to its other clients of similar systems at no additional cost/charge.

Confirmed. AbsenceSoft's training model is a "train the trainer" and will consist of core sessions that are offered remotely but could be onsite if West Virginia DHHR prefers. Each training session is focused on a specific area of the application, as well as roles and permissions. The trainings are complimented with a variety of user manuals as well as a knowledge base. Additionally, WV DHHR will be assigned a Customer Success Manager (CSM) upon go-live who will be available to assist with system questions post go-live and these trainings will be at no additional cost.

All system upgrades, enhancements, and error corrections are included in the subscription and will not be charged back to WV DHHR.

4. CONTRACTAWARU:

4.1 Contract Award: The Contract is intended to provide Agencies with a purchase price on all Contract Items. The Contract shall be awarded to the Vendor that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

4.2 Pricing Pages: Vendor should complete the Pricing Pages in WVOasis. Vendor should complete the Pricing Pages in their entirety as failure to do so may result in Vendor's bids being disqualified.

The Pricing Pages contain a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

Vendor should electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document.

5. ORDERING AND PAYMENT:

5.1 Ordering: Vendor shall accept orders through wvOASIS, regular mail, facsimile, e-mail, or any other written form of communication. Vendor may, but is not required to, accept on-line orders through a secure internet ordering portal/website. If Vendor has the ability to accept on-line orders, it should include in its response a brief description of how Agencies may utilize the on-line ordering system. Vendor shall ensure that its on-line ordering system is properly secured prior to processing Agency orders on-line.

5.2 Payment: Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

6. DELIVERY ANI> RETURN:

6.1 Delivery Time: Vendor shall deliver standard orders within thirty (30) working days after orders are received. Vendor shall deliver emergency orders within 10 working day(s) after orders are received. Vendor shall ship all orders in accordance with the above schedule and shall not hold orders until a minimum delivery quantity is met.

6.2 Late Delivery: The Agency placing the order under this Contract must be notified in writing if orders will be delayed for any reason. Any delay in delivery that could cause harm to an Agency will be grounds for cancellation of the delayed order, and/or obtaining the items ordered from a third party.

Any Agency seeking to obtain items from a third party under this provision must first obtain approval of the Purchasing Division.

6.3 Delivery Payment/Risk of Loss: Standard order delivery shall be F.O.B. destination to the Agency's location. Vendor shall include the cost of standard order delivery charges in its bid pricing/discount and is not permitted to charge the Agency separately for such delivery. The Agency will pay delivery charges on all emergency orders provided that Vendor invoices those delivery costs as a separate charge with the original freight bill attached to the invoice.

6.4 Return of Unacceptable Items: If the Agency deems the Contract Items to be unacceptable, the Contract Items shall be returned to Vendor at Vendor's expense and with no restocking charge. Vendor shall either make arrangements for the return within five (5) days of being notified that items are unacceptable or permit the Agency to arrange for the return and reimburse Agency for delivery expenses. If the original packaging cannot be utilized for the return, Vendor will supply the Agency with appropriate return packaging upon request. All returns of unacceptable items shall be F.O.B. the Agency's location. The returned product shall either be replaced, or the Agency shall receive a full credit or refund for the purchase price, at the Agency's discretion.

6.5 Return Due to Agency Error: Items ordered in error by the Agency will be returned for credit within 30 days of receipt, F.O.B. Vendor's location. Vendor shall not charge a restocking fee if returned products are in a resalable condition. Items shall be deemed to be in a resalable condition if they are unused and in the original packaging. Any restocking fee for items not in a resalable condition shall be the lower of the Vendor's customary restocking fee or 5% of the total invoiced value of the returned items.

7. VENDOR DEFAULT:

7.1 The following shall be considered a vendor default under this Contract.

7.1.1 Failure to provide Contract Items in accordance with the requirements contained herein.

7.1.2 Failure to comply with other specifications and requirements contained herein.

7.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

7.1.4 Failure to remedy deficient performance upon request.

7.2 The following remedies shall be available to Agency upon default.

7.2.1 Immediate cancellation of the Contract.

7.2.2 Immediate cancellation of one or more release orders issued under this Contract.

7.2.3 Any other remedies available in law or equity.

8. MISCELLANEOUS:

8.1 **No Substitutions:** Vendor shall supply only Contract Items submitted in response to the Solicitation unless a contract modification is approved in accordance with the provisions contained in this Contract.

8.2 **Vendor Supply:** Vendor must carry sufficient inventory of the Contract Items being offered to fulfill its obligations under this Contract. By signing its bid, Vendor certifies that it can supply the Contract Items contained in its bid response.

8.3 **Reports:** Vendor shall provide quarterly reports and annual summaries to the Agency showing the Agency's items purchased, quantities of items purchased, and total dollar value of the items purchased. Vendor shall also provide reports, upon request, showing the items purchased during the term of this Contract, the quantity purchased for each of those items, and the total value of purchases for each of those items. Failure to supply such reports may be grounds for cancellation of this Contract.

8.4 **Contract Manager:** During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: _______________________
Telephone Number: _________________________

Fax Number: ______________________________
Email Address: ______________________________

Attachment 1

FEDERAL FUNDS ADDENDUM
2 C.F.R. §§ 200.317 -200.327

Purpose: This addendum is intended to modify the solicitation in an attempt to make the contract compliant with the requirements of 2 C.F.R. §§ 200.317 through 200.327 relating to the expenditure of certain federal funds. This solicitation will allow the State to obtain one or more contracts that satisfy standard state procurement, state federal funds procurement, and county/local federal funds procurement requirements.

Instructions: Vendors who are willing to extend their contract to procurements with federal funds and the requirements that go along with doing so, should sign the attached document identified as: "REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317)"

Should the awarded vendor be unwilling to extend the contract to federal funds procurement, the State reserves the right to award additional contracts to vendors that can and are willing to meet federal funds procurement requirements.

Changes to Specifications: Vendors should consider this solicitation as containing two separate solicitations, one for state level procurement and one for county/local procurement.

State Level: In the first solicitation, bid responses will be evaluated with applicable preferences identified in sections 15, 15A, and 16 of the "Instructions to Vendors Submitting Bids" to establish a contract for both standard state procurements and state federal funds procurements.

County Level: In the second solicitation, bid responses will be evaluated with applicable preferences identified in Sections 15, 15A, and 16 of the "Instructions to Vendors Submitting Bids" omitted to establish a contract for County/Local federal funds procurement.

Award: If the two evaluations result in the same vendor being identified as the winning bidder, the two solicitations will be combined into a single contract award. If the evaluations result in a different bidder being identified as the winning bidder, multiple contracts may be awarded. The State reserves the right to award to multiple different entities should it be required to satisfy standard state procurement, state federal funds procurement, and county/local federal funds procurement requirements.

State Government Use Caution: State agencies planning to utilize this contract for procurements subject to the above identified federal regulations should first consult with the federal agency providing the applicable funding to ensure the contract is complaint.

County/Local Government Use Caution: County and Local government entities planning to utilize this contract for procurements subject to the above identified federal regulation should first consult with the federal agency providing the applicable funding to ensure the contract is complaint. For purposes of County/Local government use, the solicitation resulting in this contract was conducted in accordance with the procurement laws, rules, and procedures governing the West Virginia Department of Administration, Purchasing Division, except that vendor preference has been omitted for County/Local use purposes and the contract terms contained in the document entitled "REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317)" have been added.

FEDERAL FUNDS ADDENDUM

REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):

The State of West Virginia Department of Administration, Purchasing Division, and the Vendor awarded this Contract intend that this Contract be compliant with the requirements of the Procurement Standards contained in the Uniform Administrative Requirements, Cost Principles, and Audit Requirements found in 2 C.F.R. § 200.317, et seq. for procurements conducted by a Non-Federal Entity. Accordingly, the Parties agree that the following provisions are included in the Contract.

1. MINORITY BUSINESSES, WOMEN'S BUSINESS ENTERPRISES, AND LABOR SURPLUS AREA FIRMS:
(2 C.F.R. § 200.321)

a. The State confirms that it has taken all necessary affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible. Those affirmative steps include:

(1) Placing qualified small and minority businesses and women's business enterprises on solicitation lists;
(2) Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;
(3) Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;
(4) Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises;
(5) Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce; and
(6) Requiring the prime contractor, if subcontracts are to be let, to take the affirmative steps listed in paragraphs (1) through (5) above.

b. Vendor confirms that if it utilizes subcontractors, it will take the same affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible.

2. DOMESTIC PREFERENCES:
(2 C.F.R. § 200.322)

a. The State confirms that as appropriate and to the extent consistent with law, it has, to the greatest extent practicable under a Federal award, provided a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United

States (including but not limited to iron, aluminum, steel, cement, and other manufactured products).

b. Vendor confirms that will include the requirements of this Section 2. Domestic Preference in all subawards including all contracts and purchase orders for work or products under this award.

c. Definitions: For purposes of this section:

(1) "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.
(2) "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

3. BREACH OF CONTRACT REMEDIES AND PENALTIES:

(2 C.F.R. § 200.327 and Appendix II)

(a) The provisions of West Virginia Code of State Rules§ 148-1-5 provide for breach of contract remedies, and penalties. A copy of that rule is attached hereto as Exhibit A and expressly incorporated herein by reference.

4. TERMINATION FOR CAUSE AND CONVENIENCE:

(2 C.F.R. § 200.327 and Appendix II)

(a) The provisions of West Virginia Code of State Rules§ 148-1-5 govern Contract termination. A copy of that rule is attached hereto as Exhibit A and expressly incorporated herein by reference.

5. EQUAL EMPLOYMENT OPPORTUNITY:

(2 C.F.R. § 200.327 and Appendix II)

Except as otherwise provided under 41 CFR Part 60, and if this contract meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3, this contract includes the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFRpart 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

6. DAVIS-BACON WAGE RATES:

(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that if this Contract includes construction, all construction work in excess of $2,000 will be completed and paid for in compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must:

(a) pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor.
(b) pay wages not less than once a week.

A copy of the current prevailing wage determination issued by the Department of Labor is attached hereto as Exhibit B. The decision to award a contract or subcontract is conditioned upon the acceptance of the wage determination. The State will report all suspected or reported violations to the Federal awarding agency.

7. **ANTI-KICKBACK ACT:**
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that it will comply with the Copeland Anti-KickBack Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Pub1ic Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). Accordingly, Vendor, Subcontractors, and anyone performing under this contract are prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The State must report all suspected or reported violations to the Federal awarding agency.

8. CONTRACT WORK HOURS AND SAFETY STANDARDS ACT
(2 C.F.R. § 200.327 and Appendix II)

Where applicable, and only for contracts awarded by the State in excess of $100,000 that involve the employment of mechanics or laborers, Vendor agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Vendor is required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

9. **RIGHTS TO INVENTIONS MADE UNDER A CONTRACT OR AGREEMENT.**

(2 C.F.R. § 200.327 and Appendix II)

If the Federal award meets the definition of"funding agreement" under 37 CFR § 401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

JO. CLEAN AIR ACT

(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that if this contract exceeds $150,000, Vendor is to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-767lq) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

11. DEBARMENT AND SUSPENSION

(2 C.F.R. § 200.327 and Appendix II)

The State will not award to any vendor that is listed on the governmentwide exclusions in the System for Award Management (SAM), in accordance with the 0MB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

12. BYRD ANTI-LOBBYING AMENDMENT

(2 C.F.R. § 200.327 and Appendix II)

Vendors that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtai ng any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

13. PROCUREMENT OF RECOVERED MATERIALS

(2 C.F.R. § 200.327 and Appendix II; 2 C.F.R. § 200.323)

Vendor agrees that it and the State must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the

Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory]eve] of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,Q00; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

14. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

(2 C.F.R. § 200.327 and Appendix II; 2 CFR § 200.216)

Vendor and State agree that both are prohibited from obligating or expending funds under this Contract to:

(1) Procure or obtain;
(2) Extend or renew a contract to procure or obtain; or
(3) Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(i) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
(ii) Telecommunications or video surveillance services provided by such entities or using such equipment.
(iii) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

In implementing the prohibition under Public Law 115-232, section 889, subsection (f), paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

State of West Virginia	Vendor Name:
By:	By:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:

EXHIBIT A To:
REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY
CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):

W. Va. CSR§ 148-1-5

West Virginia Code of State RuJes
Title 148. Department of Administration
Legislative Rule (Ser. 1)
Series 1. Purchasing

W. Va. Code St. R. § 148-1-5

§ 148-1-5. Remedies.

Cw-rcntncss

5.1. The Director may require that the spending unit attempt to resolve any issues that it may have with the vendor prior to pursuing a remedy contained herein. The spending unit must document any resolution efforts and provide copies of those documents to the Purchasing Division.

5.2. Contract Cancellation.

5.2.1. Cancellation. The Director may cancel a purchase or contract immediately under any one of the following conditions including, but not limited to:

5.2.1.a. The vendor agrees to the cancellation;

5.2.1.b. The vendor has obtained the contract by fraud, collusion, conspiracy, or is in conflict with any statutory or constitutional provision of the State of West Virginia;

5.2.1.c. Failure to honor any contractual tenn or condition or to honor standard commercial practices;

5.2.1.d. The existence of an organizational conflict of interest is identified;

5.2.1.e. Funds are not appropriated or an appropriation is discontinued by the legislature for the acquisition;

5.2.1.f. Violation of any federal, state, or local law, regulation, or ordinance, and

5.2.1.g. The contract was awarded in error.

5.2.2. The Director may cancel a purchase or contract for any reason or no reason, upon providing'the vendor with 30 days' notice of the cancellation.

5.2.3. Opportunity to Cure. In the event that a vendor fails to honor any contractual term or condition, or violates any provision of federal, state, or local law, regulation, or ordinance, the Director may request that the vendor remedy the contract breach or legal violation within a time frame the Director determines to be appropriate. If the vendor fails to remedy the contract breach or legal violation or the Director determines, at his or her sole discretion, that such a request is unlikely to yield a satisfactory result, then he or she may cancel immediately without providing the vendor an opportunity to perform a remedy.

5.2.4. Re-Award. The Director may award the cancelled contract to the next lowest responsible bidder (or next highest scoring bidder if best value procurement) without a subsequent solicitation if the following conditions are met:

5.2.4.a. The next lowest responsible bidder (or next highest scoring bidder if best value procurement) is able to perform at the price contained in its original bid submission, and

5.2.4.b. The contract is an open-end contract, a one-time purchase contract, or a contract for work which has not yet commenced.

Award to the next lowest responsible bidder (or next highest scoring bidder if best value procurement) will not be an option if the vendor's failure has in any way increased or significantly changed the scope of the original contract. The vendor failing to honor contractual and legal obligations is responsible for any increase in cost the state incurs as a result of the re-award.

5.3. Non-Responsible. If the Director believes that a vendor may be non-responsible, the Director may request that a vendor or spending unit provide evidence that the vendor either does or does not have the capability to fully perform the contract requirements, and the integrity and reliability necessary to assure good faith performance. If the Director determines that the vendor is non-responsible, the Director shall reject that vendor's bid and shall not award the contract to that vendor. A determination of non-responsibility must be evaluated on a case-by-case basis and can only be made after the vendor in question has submitted a bid. A determination of non-responsibility will only extend to the contract for which the vendor has submitted a bid and does not operate as a bar against submitting future bids.

5.4. Suspension.

5.4.1. The Director may suspend, for a period not to exceed 1 year, the right of a vendor to bid on procurements issued by the Purchasing Division or any state spending unit under its authority if:

5.4.1.a. The vendor has submitted a bid and then requested that its bid be withdrawn after bids have been publicly opened.

5.4.1.b. The vendor has exhibited poor performance in fulfilling his or her contractual obligations to the State. Poor performance includes, but is not limited to any of the following: violations of law, regulation, or ordinance; failure to deliver timely; failure to deliver quantities ordered; poor performance reports; or failure to deliver commodities, services, or printing at the quality level required by the contract.

5.4. Le. The vendor has breached a contract issued by the Purchasing Division or any state spending unit under its authority and refuses to remedy that breach.

5.4.1.d. The vendor's actions have given rise to one or more of the grounds for debarment listed in W. Va. Code§ 5A-3-33d.

5.4.2. Vendor suspension for the reasons listed in section 5.4 above shall occur as follows:

5.4.2.a. Upon a determination by the Director that a suspension is warranted, the Director will serve a notice of suspension to the vendor.

5.4.2.b. A notice of suspension must inform the vendor:

5.4.2.b.1. Of the grounds for the suspension;

5.4.2.b.2. Of the duration of the suspension;

5.4.2.b.3. Of the right to request a hearing contesting the suspension;

5.4.2.b.4. That a request for a hearing must be served on the Director no later than 5 working days of the vendor's receipt of the notice of suspension;

5.4.2.b.5. That the vendor's failure to request a hearing no later than 5 working days of the receipt of the notice of suspension will be deemed a waiver of the right to a hearing and result in the automatic enforcement of the suspension without further notice or an opportunity to respond; and

5.4.2.b.6. That a request for a hearing must include an explanation of why the vendor believes the Director's asserted grounds for suspension do not apply and why the vendor should not be suspended.

5.4.2.c. A vendor's failure to serve a request for hearing on the Director no later than 5 working days of the vendor's receipt of the notice of suspension will be deemed a waiver of the right to a hearing and may result in the automatic enforcement of the suspension without further notice or an opportunity to respond.

5.4.2.d. A vendor who files a timely request for hearing but nevertheless fails to provide an explanation of why the asserted grounds for suspension are inapplicable or should not result in a suspension, may result in a denial of the vendor's hearing request.

5.4.2.e. Within 5 working days of receiving the vendor's request for a hearing, the Director will serve on the vendor a notice of hearing that includes the date, time and place of the hearing.

5.4.2.f. The hearing will be recorded and an official record prepared. Within 10 working days of the conclusion of the hearing, the Director will issue and serve on the vendor, a written decision either confirming or reversing the suspension.

5.4.3. A vendor may appeal a decision of the Director to the Secretary of the Department of Adrp_inistration. The appeal must be in writing and served on the Secretary no later than 5 working days ofreceipt of the Director's decision.

5.4.4. The Secretary, or his or her designee, will schedule an appeal hearing and serve on the vendor, a notice of hearing that includes the date, time and place of the hearing. The appeal hearing will be recorded and an official record prepared. Within 10 working days of the conclusion of the appeal hearing, the Secretary will issue and serve on the vendor a written decision either confirming or reversing the suspension.

5.4.5. Any notice or service related to suspension actions or proceedings must be provided by certified mail, return receipt requested.

5.5. Vendor Debarn1ent. The Director may debar a vendor on the basis of one or more of the grounds for debarment contained in W. Va. Code§ 5A-3-33d or if the vendor has been declared ineligible to participate in procurement related activities under federal laws and regulation.

5.5.1. Debarment proceedings shall be conducted in accordance with W. Va. Code § 5A-3-33e and these rules. A vendor that has received notice of the proposed debarment by certified mail, return receipt requested, must respond to the proposed debarment within 30 working days after receipt of notice or the debarment will be instituted without further notice. A vendor is deemed to have received notice, notwithstanding the vendor's failure to accept the certified mail, if the letter is addressed to the vendor at its last known address. After considering the matter and reaching a decision, the Director shall notify the vendor of his or her decision by certified mail, return receipt requested.

5.5.2. Any vendor, other than a vendor prohibited from participating in federal procurement, undergoing debarment proceedings is pern1itted to continue participating in the state's procurement process until a final debarment decision has been reached. Any contract that a debarred vendor obtains prior to a final debarment decision shall remain in effect for the current term, but may not be extended or renewed. Notwithstanding the foregoing, the Director may cancel a contract held by a debarred vendor if the Director determines, in his or her sole discretion, that doing so is in the best interest of the State. A vendor prohibited from participating in federal procurement will not be permitted to participate in the state's procurement process during debarment proceedings.

5.5.3. If the Director's final debarment decision is that debarment is warranted and notice of the final debannent decision is mailed, the Purchasing Division shall reject any bid submitted by the debarred vendor, including any bid submitted prior to the final debarment decision if that bid has not yet been accepted and a contract consummated.

5.5.4. Pursuant to W.Va. Code § 5A-3-33e(e), the length of the debarment period will be specified in the debarment decision and will be for a period of time that the Director finds necessary and proper to protect the public from an irresponsible vendor.

5.5.5. List of Debarred Vendors. The Director shall maintain and publicly post a list of debarred vendors on the Purchasing Division's website.

5.5.6. Related Party Debarment. The Director may pursue debarment of a related party at the same time that debarment of the original vendor is proceeding or at any time thereafter that the Director determines a related party debarment is warranted. Any entity that fails to provide the Director with full, complete, and accurate information requested by the Director to determine related party status will be presumed to be a related party subject to debarment.

5.6. Damages.

5.6.1. A vendor who fails to perform as required under a contract shall be liable for actual damages and costs incurred by the state.

5.6.2. If any commodities delivered under a contract have been used or consumed by a spending unit and on testing the commodities are found not to comply with specifications, no payment may be approved by the Spending Unit for the merchandise until the amount of actual damages incurred has been determined.

5.6.3. The Spending Unit shall seek to collect damages by following the procedures established by the Office of the Attorney General for the collection of delinquent obligations.

Credits

History: Filed 4-1-19, eff. 4-1-19; Filed 4-16-21, eff. 5-1-21.

Current through register dated May 7, 2021. Some sections may be more current. See credits for details.

W. Va. C.S.R. 148-1-5 WV ADC 148-1-5

End of Document

EXHIBIT B To:
REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):

Prevailing Wage Determination

[ ] - Not Applicable Because Contract Not for Construction

[ ]- Federal Prevailing Wage Determination on Next Page

Legal Notifications and Modifications

It is not clear what each one is (Addendum No.1, No. 2, etc….) so I do not know which boxes should be checked. This may be a question to ask them about quickly unless it is more clearly labeled in whatever they used to send the RFP. That said, I think it is just Addendum No. 1, which has three parts: the FAQ, the NIST, and the SaaS Addendum.

We can acknowledge we received them; however, we cannot agree to the addenda as is. We have to make revisions on them, which is required to be called out (similar to the General Ts&Cs). I attached the document that seems to incorporate the above 3 parts (Legal Comments- WV DHHR Addendum No.1 _06.26.23).

Contractual modifications to be negotiated:

For the NIST: AbsenceSoft does not follow NIST standards. We follow a few, but not the entirety of such standards. I made a comment stating this. This is not negotiable. I double-checked this with Ari

Software as a Service Addendum:

Section 3: "AbsenceSoft applies the same standards for all customers"

Section 3(g): AbsenceSoft utilizes masked (de-identified) data for problem solving on the Platform, as well as internal benchmarking and analyzing.

Section 4(b): AbsenceSoft notifies within 72 hours (not 24)

Section 5(e): AbsenceSoft generally does not provide this; however, is open to discussion.

Section 7(e): AbsenceSoft does not generally follow NIST standards. We can provide how data is permanently deleted.

Section 8: AbsenceSoft performs criminal background checks; however, hiring is our discretion.

Section 11: AbsenceSoft does not perform the Cloud Security Alliance assessment

Section 13: AbsenceSoft provides at least 10 days advanced notice

Section 21: AbsenceSoft provides for the Employee Self-Service module but not the platform as a whole

Section 23: AbsenceSoft does not comply with all NIST standards; however, while we do not wholly comply with this, we do secure information at rest and in transit

Section 24: AbsenceSoft provides the following licenses and restrictions: how they have it written is too broad

AbsenceSoft hereby grants Customer a non-exclusive, non-transferable, non-sublicensable license to access and use the AbsenceSoft Platform and Documentation for the sole purpose of receiving and using the AbsenceSoft Platform for Customer's internal business purposes. Access and use of the AbsenceSoft Platform shall be web-enabled access only, and nothing herein this Agreement shall entitle Customer or Permitted Users to the object code or source code of the AbsenceSoft Platform.

License Restrictions. Customer shall not, nor allow or authorize its Permitted Users nor any third-party to: (a) reproduce, allow use of, or access the AbsenceSoft Platform, or sell, rent, lease, use in a service bureau, sublicense or otherwise transfer or assign its rights to access and use the AbsenceSoft Platform, in whole or in part, to a third-party;

(b) alter, enhance or otherwise modify or create derivative works of or from the AbsenceSoft Platform; (c) disassemble, decompile, reverse engineer or otherwise attempt to derive the source code of the AbsenceSoft Platform; (d) remove or destroy any proprietary markings, confidential legends or any trademarks or trade names of AbsenceSoft or its licensors placed upon or contained within the AbsenceSoft Platform or the Documentation; or (e) upload, post or transmit into or via the AbsenceSoft Platform any viruses or unlawful, threatening, abusive, libelous, defamatory, obscene, pornographic, profane or offensive information of any kind. Use, duplication or disclosure by the U.S. Government or any of its agencies is subject to restrictions set forth in the Commercial Computer Software and Commercial Computer Software Documentation clause at DFARS 227.7202 and/or the Commercial Computer Software Restricted Rights clause at FAR 52.227.19(c).

Contractual Modifications/Negations for General T&C's & Addenda

Section 11 (pg. 8 of 47) states that Vendor must clearly mark any exceptions, clarifications, or other proposed modifications, as the solicitation is the basis of the contract I made these as comments, which you are free to carry over.

General Ts&Cs comments: I focused on the terms that were there, not the all of ones we would want to add, just the major ones (as this is just the "base"). As an internal reminder, we generally do not use a customer's paper unless they are $250k ARR and it is SaaS specific. The exceptions are few and far between (MBTA may be an exception because they are a migration and Jimmy/I already have a relationship with them). This is not a SaaS specific RFP, so there will be necessary redlines to account for SaaS products.

Section 13 (pg. 16 of 47): pricing is subject to increase during renewal periods or if the number of employees grows by more than 10% for 3 consecutive months.

Section 14 (pg. 16 of 47): AbsenceSoft requires at least partial payment to be upfront unless it is time and materials basis only for implementation. Luckily for us, they are good with paying for subscription fees upfront.

Section 19 (pg. 17 of 47): AbsenceSoft requires mutual termination/cancellation right. AbsenceSoft also does not generally accept termination for convenience/without cause

Section 30 (pg. 18 of 47): AbsenceSoft will provide our privacy and security addendum in the event AbsenceSoft wins the bid. There are elements in the documents within the link that are not fully aligned with AbsenceSoft internal procedures. We are open to discussion. Internal note: I don't want to provide specifics at this time, as Ari would need to do an extensive review to point out what we can/cannot agree to. Based on their current ARR but potential for more ARR, the posts may change with this; however, we do try to put in our security/privacy terms and not have a link wherein changes can be made at anytime.

Section 36 (pg. 20 of 47): AbsenceSoft requires some form of mutual indemnification, including indemnification from customers on their employment decisions.

Additional comment: pg 23 of 47, right below section 46. I made this comment which should be included so they are not surprised: AbsenceSoft may request additional inclusions as a Software as a Service (SaaS) product, including but not limited to: for protection of its intellectual property as well as that ownership of customer data belongs to customer, limitation of liability, usage of customer data, and a service level agreement.

Federal Funds addendum, Required Contract provisions: I made a few comments throughout, which we would typically not agree to:

Section 4 (pg. 36 of 47): AbsenceSoft does not generally accept termination for convenience

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.

c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.

d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.

b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.

c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:

   - 10 days after the effective date of termination, if the termination is in accordance with the contract period
   - 30 days after the effective date of termination, if the termination is for convenience
   - 60 days after the effective date of termination, if the termination is for cause

   After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.

e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.

c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

a. Access and use the service for its business purposes;
b. For SaaS, use underlying software as embodied or used in the service; and
c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency:_____________________

Signature:___________________________

Title:______________________________

Date:____________________________

Name of Vendor:___AbsenceSoft________

Signature:___Max Cook___________

Title:___Account Executive___

Date:___________6/28/2023_____________________

AbsenceSoft Response: Subject to negotiation. See legal modifications doc submitted with bid.

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: AbsenceSoft

Name of Agency:____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☒
   No □

2. If yes to #1, does the restricted information include personal data?
   Yes ☒
   No □

3. If yes to #1, does the restricted information include non-public data?
   Yes ☒
   No □

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes □
   No ☒

5. Provide name and email address for the Department privacy officer:

   Name: Chris Snyder

   Email address: chris.s.snyder@wv.gov

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: Max Cook

   Email address: mcook@absencesoft.com

   Phone Number: 385-437-2544

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Info Technology

Proc Folder:	1234820	**Reason for Modification:** ADDENDUM 1 TO PROVIDE ANSWERS TO VENDOR QUESTIONS AND SAAS
Doc Description:	ATTENDANCE CASELOAD MANAGEMENT SOFTWARE	
Proc Type:	Central Master Agreement	

Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2023-06-21	2023-06-28 13:30	CRFQ 0511 MIS2300000005	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name :

Address :

Street :

City :

State : **Country :** **Zip :**

Principal Contact :

Vendor Contact Phone: **Extension:**

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION
THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, WEST VIRGINIA DEPARTMENT OF HEALTH AND HUMAN RESOURCES (DHHR), OFFICE OF MANAGEMENT INFORMATION SERVICES, IS SOLICITING BIDS TO ESTABLISH AN OPEN-END CONTRACT FOR ATTENDANCE CASELOAD MANAGEMENT SOFTWARE (FMLA/FLOA/PLA TRACKING) PER THE ATTACHED DOCUMENTS. ***QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS***

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES		HEALTH AND HUMAN RESOURCES	
OFFICE OF HUMAN RESOURCES MGMT		OFFICE OF HUMAN RESOURCES MGMT	
ONE DAVIS SQUARE, STE 400		ONE DAVIS SQUARE, STE 400	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Attendance Caseload Management Software (FMLA/FLOA/PLA)	9.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
3.1.2 Attendance Caseload Management Software (FMLA/FLOA/PLA)

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES		HEALTH AND HUMAN RESOURCES	
OFFICE OF HUMAN RESOURCES MGMT		OFFICE OF HUMAN RESOURCES MGMT	
ONE DAVIS SQUARE, STE 400		ONE DAVIS SQUARE, STE 400	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Year One Optional Renewal				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Optional Renewal Year One

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES		HEALTH AND HUMAN RESOURCES	
OFFICE OF HUMAN RESOURCES MGMT		OFFICE OF HUMAN RESOURCES MGMT	
ONE DAVIS SQUARE, STE 400		ONE DAVIS SQUARE, STE 400	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Year Two Optional Renewal				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Optional Renewal Year Two

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES		HEALTH AND HUMAN RESOURCES	
OFFICE OF HUMAN RESOURCES MGMT		OFFICE OF HUMAN RESOURCES MGMT	
ONE DAVIS SQUARE, STE 400		ONE DAVIS SQUARE, STE 400	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Year Three Optional Renewal				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Optional Renewal Year Three

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON US	WV	HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	Additional Users/Licenses	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:

3.1.2.21 Additional Users/Licenses- each add on user/license (9 used for bidding scenario only, quantity could increase or decrease during life of contract)

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON US	WV	HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	Online Training for Licenses Holders				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:

3.1.2.22 Must provide online training for license holders at no cost. System upgrades, enhancements, and error corrections must be at no additional cost/charge when such upgrades, enhancements, and error corrections are generally made available to its other clients of similar systems at no additional cost/charge.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2023-06-15

SOLICITATION NUMBER: CRFQ MIS2300000005
Addendum Number:

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[✓] Other

Description of Modification to Solicitation:

1. To provide answers to vendor questions
2. To include Software as a Service Addendum
3. To provide NIST Special Publication 800-210

No other changes

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

CRFQ-0511-MIS23*5

FMLA/Attendance Caseload Management Software

Vendor Questions and Agency Responses

1. Could you please clarify if you are looking for a custom case management solution or if you are interested in an off-the-shelf product? This information will help us tailor our response to meet your specific needs.

   Agency response - The RFQ was written for an off-the-shelf product with customizable options per the specifications provided by the RFQ.

2. In multiple sections, it is referenced that this solution should be accessible for self-service by employees and should track appropriate employee information regarding leave and attendance.
   a. Are there any other user types such as contractors, external unionized workers, etc. that are expected to use this solution?

      Agency response - Contract workers.

   b. Based on those user types including employees that will have this solution made available to them, what is the total number of employees/other user types that will be served by this solution?

      Agency response - Approximately 5,000 would need to have access through a portal to submit information. Could be more as we have vacancies that need to be filled.

   c. Does the population of employees being served by this solution include the entire state of West Virginia employees or is this limited to a specific agency/agencies?

      Agency response - Around 5000-6000 employees in total for the Agencies/Units resulting from the reorganization of the West Virginia Department of Health and Human Resources.

3. In section 3.1.2.4 it is requested that the "Software must offer recommendations based on state and federal employment and attendance regulations." Can you provide more detail here, for example, is the expectation that the software provides a library of state and federal regulations for the case workers to search through and match against cases that are submitted or is there another intent?

   Agency response - It is the expectation that the software provides a library of state and federal regulations for the case workers to search through and *match against cases. With this, the software must be able to update state and federal regulations as they change or are updated. The software should be able to pull information from WVOASIS and UKG/Kronos to determine employee eligibility based on federal and state guidelines.*

4. In multiple sections there are requirements for the software to interact with UKG/Kronos. Can you describe some common actions that are expected to occur? For example, actions like updating a person record, sending time card information between the UKG and the software, and interacting with time off/leave of absence requests?

   Agency response - The software must be able to collect timecard information from KRONOS. This includes but is not limited to total number of worked hours within a 12 month period, accrued leave, how much accrued leave has been used and if the employee is on authorized or unauthorized leave. As well as the system should be able to track leave of absence balances.

   a. What version of UKG/Kronos is the software expected to integrate and interact with?

      Agency response - WVDHHR and the State of WV are using Workforce Central Version 8.1.17.

   b. Would there be any limitations regarding integration technology to be aware of?

      Agency response - None that we are aware of at this time, however, vendor must present any third party vendor terms and/or software terms with their bid for Agency review.

5. In section 3.1.2.18 it is requested that the "Software must be compatible with Google Docs and Microsoft Office Suite." Can you provide more detail here, for example, is the expectation that certain information from within the software is exportable into Microsoft Office and or Google Docs formats? Or are there other intended use cases between these softwares?

   Agency response - The ability to upload template letters from Google Docs and Microsoft Word and like forms to the software system for distribution.

6. In section 3.1.1.2 it is requested that the software "Must be compatible with WVOasis..." Can you expound on what exactly WVOasis is and its functions/integration use cases with this attendance caseload solution?

   Agency response - WVOasis is the State of West Virginia's ERP. There are several facets of WVOasis. With that said, what we are looking for from the software is to collect employee information to create profiles on the software. For example, WVOASIS houses this information under Employee

Profile Manager (EPM), we would like for the software to take that information and create employee profiles to link cases to that specific employee. Important information within WVOASIS is probation dates, dates of service and employee addresses and phone numbers.

7. What is driving the state of West Virginia's interest in an Attendance Caseload Management System?

   Agency response - We do not currently have a case management system. How we manage cases presently is not as functional as we would like. For example, having FMLA or ADA requests fall through the cracks and having to research all eligibility requirements manually.

8. Is there a larger digital transformation that this proposal is a part of and could you share any details relating to that roadmap if one exists?

   Agency response - No, there is not.

9. Is there a desired timeline for implementation and go-live of this software solution for Attendance Caseload management?

   Agency response - Desired implementation by September 2023, sooner if possible as time is of the essence.

10. Is this project dependent upon funding that has any timeline restrictions tied to it?

    Agency response - No. Please refer to contract terms and conditions regarding funding or cancelations.

11. Does the state of West Virginia have any other HR-related case management tools in place today that this software is replacing and/or standing alongside?

    Agency response - No. Should be able to interact with WVOASIS and KRONOS.

12. Are there any other core HR or Attendance related systems with which there could be integration needs either in a first or future phase besides Kronos and WVOasis?

    Agency response - Business Intelligence (BI) Reports which are housed in the WVOASIS system.

13. Are there any encryption needs outside of using HTTPS? For example, encryption at rest and or disk encryption?

Agency response - Please refer to attached Exhibit - NIST SP 800-210.

14. Are there any government cloud (GCC - Government Community Cloud) requirements for cloud software solutions?

    Agency response - Please refer to attached Exhibit - NIST SP 800-210.

15. Is this a Request for Quotation for Software for all employees of West Virginia or a particular agency in West Virginia?

    Agency response - This solicitation is for the Department of Health and Human Resources.

16. How many employees on payroll are in West Virginia or the agency?

    Agency response - DHHR currently has approximately 5,000-6,000 employees. This number could increase or decrease.

17. Can you explain what "must prompt restricted leave approvals" mean? Also, what "must prompt donated leave approvals" mean.

    Agency response - Please see response to question 18 below.

18. Can you explain what "must prompt restricted leave approvals" mean? Also, what "must prompt donated leave approvals" mean (3.1.2.20)

    Agency response - Software must prompt work restriction approvals, track, and notify when length of leave is nearing (90) ninety days, which will automatically send out ADA paperwork. It must also allow users to review and approve final approval letters for donated leave .

19. Is there a response format to use in preparing our response?

    Agency response - Please follow the instructions for submitting bids contained in the solicitation announcement.

20. We want to confirm you are looking for FMLA/State LOA/PLOA management cloud (SaaS) software.

    Agency response - Yes, that along with just case tracking for ADA and eventually investigations. Please note a SaaS addendum is being included in this solicitation.

21. Do you have a target go live date?

    Agency response - Desired implementation is by September 2023, or sooner if possible as time is of the essence.

22. How is the department currently managing FMLA/State Leave & ADA Accommodations?

    Agency response - We use spreadsheets to track cases and file folders to house all case related information. Everything is currently being done manually.

23. Is the department also looking for a software to streamline/automate the ADA accommodations process?

    Agency response - Yes.

24. On average, how many cases do each of them handle at once?

    Agency response - At least 6-15 cases come in a day, but the volume could increase or decrease.

25. How many cases are submitted per year?

    Agency response - Approximately 1,400-1,500. This amount could increase or decrease.

26. How many employees are you looking to manage with the software?

    Agency response - Three employees will be using the software to manage approximately 1,500 cases a year. This number could increase or decrease.

27. Is this outsourced for a vendor to manage, or do you want the leave team to manage the software?

    Agency response - The agency will manage the software and will rely on the software vendor to provide support and or make changes to the structure of the software as needed. Maintenance agreements beyond the scope or terms of this contract will be procured as needed.

NIST Special Publication 800-210

General Access Control Guidance for Cloud Systems

Vincent C. Hu
Michaela Iorga
Wei Bao
Ang Li
Qinghua Li
Antonios Gouglidis

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-210

General Access Control Guidance for Cloud Systems

Vincent C. Hu
Michaela Iorga
Computer Security Division
Information Technology Laboratory

Wei Bao
Ang Li
Qinghua Li
Department of Computer Science and Computer Engineering
University of Arkansas
Fayetteville, AR

Antonios Gouglidis
School of Computing and Communications
Lancaster University
Lancaster, United Kingdom

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

July 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-210
Natl. Inst. Stand. Technol. Spec. Publ. 800-210, 34 pages (July 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sp800-210-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This document presents cloud access control characteristics and a set of general access control guidance for cloud service models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). Different service delivery models require managing different types of access on offered service components. Such service models can be considered hierarchical, thus the access control guidance of functional components in a lower-level service model are also applicable to the same functional components in a higher-level service model. In general, access control guidance for IaaS is also applicable to PaaS and SaaS, and access control guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to access control requirements for its service.

Keywords

access control; access control mechanism; Cloud; cloud systems; policy; authorization ABAC; RBAC.

Acknowledgements

The authors, Vincent C. Hu and Michaela Iorga of the National Institute of Standards and Technology (NIST), Bao Wei, Ang Li, and Qinghua Li of Department of Computer Science and Computer Engineering University of Arkansas, and Antonios Gouglidis of School of Computing and Communications Lancaster University wish to thank Isabel Van Wyk, Jim Foti, and David Ferraiolo (NIST) who reviewed drafts of this document. The authors also gratefully acknowledge and appreciate the comments and contributions made by government agencies, private organizations, and individuals in providing direction and assistance in the development of this document.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Executive Summary

Cloud systems have been developed over time and conceptualized through a combination of software, hardware components, and virtualization technologies. Characteristics of the cloud, such as resource pooling, rapid elasticity, and pay-as-you-go services, accelerated its wide adoption by industry, government, and academia. Specifically, cloud systems offer application services, data storage, data management, networking, and computing resources management to consumers over a network (the internet in general). Despite the great advancements of cloud systems, concerns have been raised about the offered level of security and privacy. The importance of these concerns becomes more evident when considering the increasing number of users who have adopted cloud services.

This document presents cloud access control (AC) characteristics and a set of general access control guidance for cloud service models—IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). The main focus is on technical aspects of access control without considering deployment models (e.g., public, private, hybrid clouds etc.), as well as trust and risk management issues, which require different layers of discussions that depend on the security requirements of the business function or the organization of deployment for which the cloud system is implemented. Different service delivery models need to consider managing different types of access on offered service components. Such considerations can be hierarchical, such as how the access control considerations of functional components in a lower-level service model (e.g., networking and storage layers in the IaaS model) are also applicable to the same functional components in a higher-level service model (e.g., networking and storage in PaaS and SaaS models). In general, access control considerations for IaaS are also applicable to PaaS and SaaS, and access control considerations for IaaS and PaaS are also applicable to SaaS. Therefore, AC guidance for IaaS is applicable to PaaS and SaaS, and AC guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to access control requirements for its service.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 Purpose

Access control (AC) dictates how subjects (i.e., users and processes) can access objects based on defined AC policies to protect sensitive data and critical computing objects in the cloud systems. Considering the heterogeneity and remote nature of the cloud service models, AC and its general concepts should be revisited. In recent years, many works have focused on AC in cloud systems [23, 25, 26, 27]. However, these are primarily ad hoc solutions targeted at specific cloud applications and do not provide comprehensive views of cloud AC.

This document presents a set of general AC guidance for cloud service models independent from its deployment models because it requires another layer of access control that depends on the security requirements of the business function for which the cloud system is used. As shown in Figure 3, different cloud service models require the management of access to different components of the offered service. Since such cloud service models can be considered hierarchical, the AC considerations of functional components in a lower-level (according to Figure 2) service model (e.g., networking and storage layers in the Infrastructure as a Service (IaaS) model) are also applicable to the same functional components in a higher-level service model (e.g., networking and storage in Platform as a Service (PaaS) and Software as a Service (SaaS) models). In general, AC considerations for IaaS are also applicable to PaaS and SaaS, and AC considerations for IaaS and PaaS are also applicable to SaaS. Thus, AC guidance for IaaS is applicable to PaaS and SaaS, and AC guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to AC. For instance, an IaaS provider may put more effort into virtualization control, and in addition to the virtualization control, a SaaS provider needs to consider data security and the privacy of services it provides.

1.2 Scope

This document focuses on providing guidance for access control systems that are applicable to an organization's cloud implementation and security management. It does not prescribe the internal cloud access control standards that an organization may need in their enterprise systems or within a community other than the organization itself.

1.3 Audience

The intended audience for this document is an organizational entity that implements access control solutions for sharing information in cloud systems. This document assumes that readers are familiar with the cloud and access (authorization) control systems and have basic knowledge of operating systems, databases, networking, and security. Given the constantly changing nature of the information technology (IT) industry, readers are strongly encouraged to take advantage of other documents—including those listed in this document—for more current and detailed information.

1.4 Document Structure

The sections and appendix presented in this document are as follows:

- Section 1 states the purpose and scope of access control and cloud systems.
- Section 2 provides an overview of cloud access control characteristics.
- Section 3 discusses guidance for access control systems for IaaS (Infrastructure as a Service).
- Section 4 discusses guidance for access control systems for PaaS (Platform as a Service).
- Section 5 discusses guidance for access control systems for SaaS (Software as a Service).
- Section 6 discusses guidance for access control systems for inter- and intra-cloud operations.
- Section 7 concludes the document with future directions.

2 Cloud Access Control Characteristics

With the support of different service models, cloud systems can provide a wide range of services to its end-users, developers, and system administrators. Cloud systems have been developed over time and conceptualized through a combination of software, hardware components, and virtualization technologies. Characteristics of the cloud, such as resource pooling, rapid elasticity, and pay-as-you-go services, have accelerated its wide adoption by industry, government, and academia. Specifically, cloud systems offer application services, data storage, data management, networking, and computing resources management to consumers[1] over a network (and the internet in general). Examples of popular cloud applications include web-based email services (e.g., Google's Gmail, Microsoft's Office 365 Outlook), data storage (e.g., Google Drive, Microsoft's OneDrive, Dropbox) for end users, and consumer relationship management and business intelligence systems (e.g., Customer Relationship Management (CRM) Cloud, Workday) for business management. Despite the great advancements of cloud systems, concerns have been raised about offered levels of security and privacy. The importance of these concerns becomes more evident when considering the increasing number of users that have adopted cloud services [1].

NIST publications defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2,3]. Cloud deployment models (e.g., public cloud, private cloud, community cloud, hybrid cloud, etc.) are configured by the scope of cloud users, services, and resources based on service requirements, they may be deployed privately, hosted on the premises of a cloud consumer or provider's dedicated infrastructure, or hosted publicly by one or more cloud service providers. The system may be configured and used by one consumer or a group of trusted partners or support multi-tenancy and be used publicly by different end users who acquire the service. Depending on the type of cloud deployment model, the cloud may have limited private computing resources or access to large quantities of remotely accessed resources. The different deployment models present a number of trade-offs in how consumers can control their resources as well as the scale, cost, and availability of those resources [4]. As depicted in Figure 1, the architecture of a cloud system is composed, in general, by layers of functions:

- VM (Virtual Machine), including:
  - Applications
  - Application Programming Interface (API)
  - Operating System (OS)
- Hypervisor
- Storage
- Networking
- Hardware

[1] Cloud service **consumers** play various roles in the consumption of the cloud services, e.g. system planners, program managers, technologists. **End-users** are individuals using cloud services as direct clients of a cloud provider, of a cloud consumer leveraging a cloud service, or individuals employed by a cloud consumer. A **user** is in a generic term associated with any entity using the cloud service. Depending on scenario, the user can be referred as either cloud service consumer or end-user where applicable.

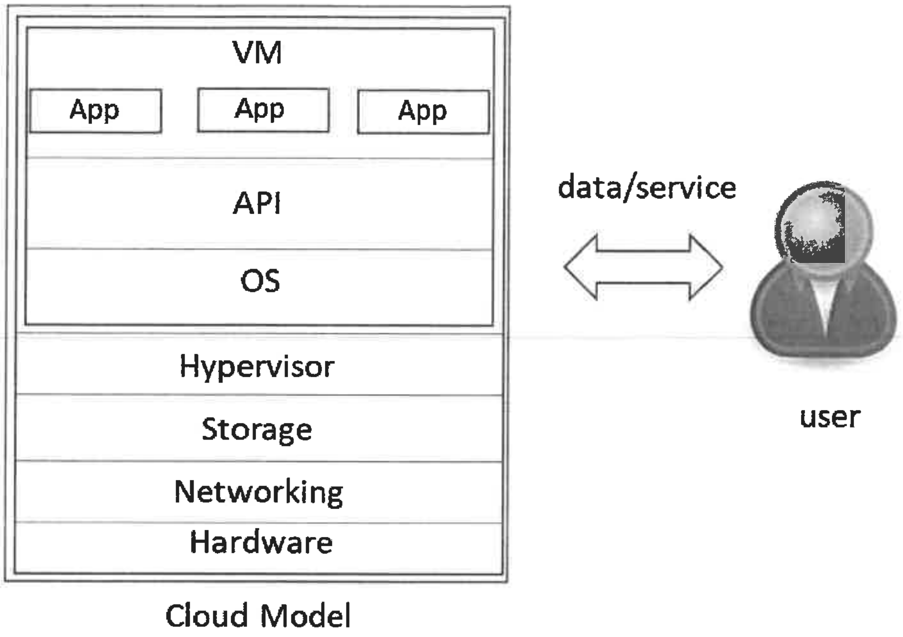


Figure 1: The general architecture of a cloud system

A cloud service can provide access to software applications, such as email or office productivity tools (i.e., the Software as a Service, or SaaS, service model); an environment for consumers to build and operate their own software (i.e., the Platform as a Service, or PaaS, service model), or network access to virtualized computing resources such as processing power and storage (i.e., the Infrastructure as a Service, or IaaS, service model). The different service models have different strengths and are suitable for different consumers and business objectives [4], as illustrated in Figure 2, the arrows show the support relations between models.

A cloud system that deploys the SaaS model can be accessible over a network by an end user utilizing various client devices (e.g., a thin client interface, such as a web browser, for accessing a web-based email application) or via a program with the correct set of interfaces whose execution would enable communication with a cloud application. In the SaaS model, an application user is limited to user-specific application configuration settings and does not manage or control the underlying cloud infrastructure, which typically includes the network, servers, operating systems, storage, or individual applications.

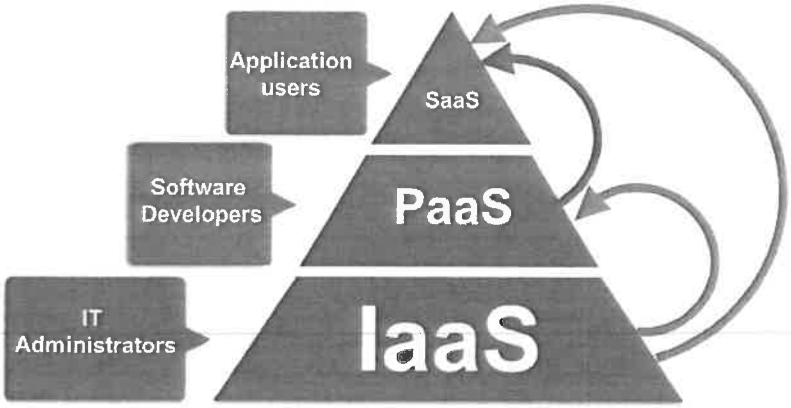


Figure 2: The service models of a cloud system

The PaaS model in a cloud system allows developers to create and deploy applications onto the cloud infrastructure using programming languages, libraries, services, and tools. A software developer does not manage or control the underlying cloud infrastructure but has control over the deployed applications (software) and, possibly, configuration settings for the application-hosting environment.

When analyzing the responsibilities between consumer and cloud service providers for protecting cloud data, it is not always clear-cut, if an IaaS system provides only the computation resources, or offers also the virtualized storage, and network resources to consumers for deploying and running arbitrary software, including operating systems and applications. The consumer may in turn have control over virtual storage, virtualized network components, and the ability to deploy their own VMs and applications given access provisioned by the cloud service provider.

The shared responsibility of access control needs to be considered in the PaaS and SaaS model [42]; For example software developers might need to access data in systems provided by PaaS for their developmental needs, and internal application users (i.e., users that need to access the application system data) might need to access application system data that is managed by the applications. In general, for PaaS, consumer software developers might share access control responsibilities with cloud service providers; for SaaS, internal application users might share such responsibilities with cloud service providers.

Note that unless there is express prior approval from the consumer, a PaaS or SaaS provider must manage access control with the IaaS provider and the consumer (if it is not also the IaaS provider). If the consumer approves, the provider should inform the consumer of its intention to store the specified data in the IaaS provider, where it will be accessed as well as the extent to which the data can be accessed by the IaaS provider, foreign entities, or authorities. A public consultation and hearing process must then be conducted before a decision is made.

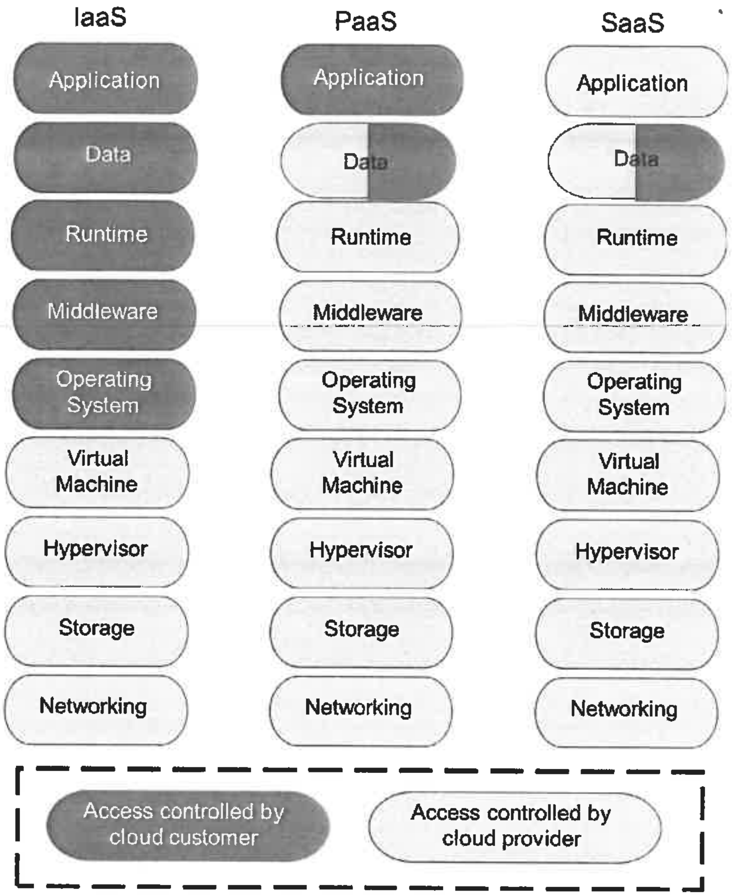


Figure 3: Accesses controlled by the cloud service provider and the consumer

The five essential characteristics that challenge AC system design are summarized as follows [2]:

1. *Broad network access*: Cloud services are available over the network and accessible through standard mechanisms that promote use by heterogeneous thick and thin client platforms (e.g., mobile phones, tablets, laptops, workstations). This raises security concerns with regard to network access. For example, denial of service (DoS) attacks can be launched against a cloud system, rendering its resources unavailable to legitimate users. Thus, AC for network access should be managed.

2. *Resource pooling*: The computing resources of a cloud system (e.g., storage, memory, processing, network bandwidth) are pooled to serve multiple consumers using a multi-tenant model (i.e., a single instance of the software and its supporting infrastructure serves multiple consumers) through different physical and virtual resources, each dynamically assigned and reassigned according to consumer demands. Information may be leaked if the resource allocated to a consumer can be accessed by another co-located consumer or if the allocated resource, such as memory, is not wiped before being reallocated to another consumer. There is also a sense of location independence in that the consumer generally has no control over or knowledge of the exact location of the provided resources. Location may be specified at a higher level of abstraction (e.g., country, state, data center) that brings

security concerns. Therefore, methods for implementing resource pooling while ensuring the isolation of shared resources should be considered in the AC design.

3. *Rapid elasticity*: Cloud services can be elastically provisioned and released—automatically, in some cases—to rapidly scale outward and inward commensurate with demands. To the consumer, services available for provisioning often appear to be unlimited and appropriated in any quantity at any time and are supported by adding new *virtual machines* (VMs) with specified computing resources. A challenge for AC design involves the capability to rapidly verify the security of new VMs and determine whether the newly added VMs are qualified to execute a specific task.

4. *Measured service*: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active end user accounts). Resource usage is monitored, controlled, and reported to provide transparency to both the provider and consumer of the utilized service. To maintain resource usage, cloud consumers should be authorized to review but not to modify their own metering data since this could lead to the falsification of payments required for cloud services. Thus, it is reasonable for AC to consider the protection of metering data.

5. *Data sharing*: Sharing information among different organizations is not a trivial task since a cloud system needs to meet the same security requirements of organizations to achieve that. To facilitate data sharing, concepts such as trust of federated identities and AC attributes need to be considered, and building that trust is paramount. In this document, it is assumed that trust and federated identities/attributes are already established, and further discussion on that topic will be considered in another document. Regardless of the service model, consumers are entitled to be responsible for the security of their cloud-based data and, implicitly, of who has access to it [5]. For this reason, data is never controlled by cloud service providers but rather always stays with the cloud consumers. (The exception to this is log data, but consideration should still be given to how privacy and security is affected by such data.) Although a cloud service provider might become the custodian of consumers' data, it should not have access to that data. If a consumer's data is not encrypted, then cloud administrators might be able to read it. In such a case, the consumer's data should be identified (by the provider's access privileges to the data) and red-flagged as accessible by the service provider, and the consumer should be informed immediately.

Guidance for AC system for each cloud service model, as described in Sections 3, 4, and 6 of this document, can be further extended to system requirements by referring to the AC control elements listed in NIST SP 800-53, Revision 4, *Security and Privacy Control for Federal Information Systems and Organizations* [6] based on the operation requirements of the cloud service. Appendix A maps the guidance to the AC control elements listed in the NIST SP 800-53, Revision 4.

3 Access Control Guidance for IaaS

IaaS is the cornerstone of all cloud services that offer computing and storage through a network such as the internet. Through virtualization technology, IaaS enables end users to dynamically allocate computing resources by instantiating new *virtual machines* (VMs) or releasing them based on their requirements. A VM is a software container that behaves like a physical machine with its own operating system (OS) and virtual resources (e.g., CPU, memory, hard disk, etc.). Leasing VMs is more cost-effective than purchasing new physical machines. The virtualization technology is composed of VMs and a *hypervisor,* as shown in Figure 1. VMs are managed by the hypervisor, which controls the flow of data and instructions between the VMs and the physical hardware. On the consumer side, system administrators are usually the major users of IaaS services since IaaS services are flexible to configure resources (e.g., network, data storage).

Cloud virtualization adds additional security management burdens by introducing security controls that arise from combining multiple VMs onto a single physical computer, which can have potential negative impacts if a security compromise occurs. Some cloud systems make it easy to share information among VMs by, for instance, allowing users to create multiple VMs on top of the same hypervisor if multiple VMs are available. However, this convenience can also become an attack vector since data leakage could occur among VMs. Additionally, virtualized environments are transient since they are created and vanish frequently, thereby making the creation and maintenance of necessary security boundaries more complex.

As shown in Figure 3, data in the middleware, data, applications, and OS layers is owned and controlled by the consumer. The IaaS system and the consumer need to ensure that access to the data is not granted to IaaS system administrators or any other IaaS consumers in these layers unless any of them are permitted. IaaS administrators are responsible for access control on the virtual machine, hypervisor, storage, and networking layers and should consider Sections 3.1 to 3.5 below.

3.1 Guidance for Network

The network is shared among IaaS consumers, and it is important to secure the network traffic and the cloud's environment from being exploited by unauthorized consumers. Thus, access control for network boundaries and allowlists for network communications are required and may be applied through, for example, dedicated virtual local area networks (VLANs) leveraging automated access control lists (ACLs). Using the Institute of Electrical and Electronics Engineers (IEEE) 802.1Q VLAN tagging for network traffic with a cloud data center will result in routing only traffic tagged with the server's unique VLAN identifier to or from that server [7].

3.2 Guidance for Hypervisor

A hypervisor plays an important role in the security of the entire virtualized architecture since it manages consumer loads and guest operating systems (OSs),[2] creates new guest OS images, and controls hardware resources. The security implications of actions like managing guest OS and hardware resources means that access to the hypervisor should be restricted to authorized cloud administrators only. Otherwise, a cloud end user could potentially obtain a VM from the cloud

[2] An OS that is secondary to the originally installed OS.

service provider and install a malicious guest OS that compromises the hypervisor by gaining unauthorized access to and altering the memory of other VMs [8]. Moreover, an attacker in a VM with lower access rights may be able to escalate their access privilege to a higher level by compromising the hardware resources allocation within the hypervisor [9]. Protecting the hypervisor from unauthorized access is therefore critical to the security of IaaS services.

3.3 Guidance for Virtual Machines

VMs that are created by different end users allow resources to be shared among multiple end users. In such cases, it must be ensured that no application from one VM can directly access other VMs since covert channels [10, 11] may leak information between VMs by accessing shared physical resources (e.g., memory). Similarly, although the ability to copy and paste information between VMs via the clipboard is a convenient feature, such a capability could be made available on other VMs running on the same hypervisor and thus introduce an attack vector (i.e., information can be leaked to other VMs through the clipboard). Organizations should have policies regarding the use of shared clipboards.

Isolation between VMs is necessary to keep VMs running independently of each other, and quotas on VM resource usage should be regulated so that a malicious VM can be prohibited from exhausting computation resources. If a malicious application consumes the majority of computation resources, legitimate applications may not be able to obtain sufficient resources to perform their operations. Moreover, end users might terminate the execution of their tasks before they are finished. The state and data of the current VM would then be saved as a guest OS image, and when the task is resumed, the VM might be migrated from a different hypervisor. In such scenarios, guest OS images must be protected from unauthorized access, tampering, or storage. Furthermore, VMs that are not active may also store sensitive data. Monitoring access to the sensitive data in inactive VMs should be considered.

3.4 Guidance for APIs

There are several popular open-source platforms for deploying an IaaS system [12, 13, 14]. These solution platforms enable APIs to manage access control of VMs, hypervisors, and networks (note that a consumer cannot control hypervisors and networks in a multi-tenant environment unless it is a private cloud). For example, [14] consists of control components, including API, communication, lifecycle, storage, volume, scheduler, network, *API server* for managing AC policies for hypervisors, and *network controller* for constructing network bridges and firewall AC rules. The lack of monitoring AC within these APIs might result in unenforced or wrongly enforced AC policies by the hypervisors, VMs, and networks. Thus, a service for monitoring the AC APIs in cloud platforms should also be taken into consideration.

3.5 Recommendations for IaaS Access Control

As shown in previous sections, the security of an IaaS cloud system is heavily dependent on the virtualization (hypervisor). One of the most widely adopted solutions for protecting them is a *virtualization management system* [15], which lies between the underlying hardware and the hypervisor. The virtualization management system enforces AC on both hypervisors and VMs in different ways. Virtualization management systems enforce different levels of access on different

users. Some users are given read-only access to the administrative interface of a guest OS; some are allowed to control particular guest OSs; and some are given complete administrative control. There are existing solutions for providing AC for hypervisors and VMs. For example, the approach in [16] secures the hypervisor against control hijacking attacks by protecting its code from unauthorized access and offering isolation of VMs with the flexible security of mandatory access control (MAC). To enforce AC on interoperations, a service level agreement should be designed to include appropriate control to secure external interoperations. Other isolation mechanisms [17, 18] are helpful in ensuring the security of internal interoperations.

Guideline rules for IaaS AC policy that consider the main elements in AC (i.e., subject, object, and operation) are listed in Table 1. While each row indicates a possible AC rule, the AC policy designer should ultimately decide whether the decision in each rule is permitted or denied based on system requirements. For example, if an authorized IaaS end user requires the use of cloud services, a login operation in the hypervisor for the end user should be granted; otherwise, it should be denied.

Table 1: Potential policy rules expressed by Subject, Operation, Object for IaaS AC policy

Subjects	Operations	Objects	Environment Conditions
IaaS end user	Login, Read, Write, Create	Hypervisor	Time, Location, Security impact level etc.
IaaS end user	Read, Write, Create	VMs	Time, Location, Security impact level etc.
VM	Write	Hypervisor	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs within the same host	Time, Location, Security impact level etc.
VM	Read, Write, Create	Guest OS images	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs from different hosts but within the same IaaS provider	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs from different IaaS providers	Time, Location, Security impact level etc.
Hypervisor	Read, Write, Create	Guest OS images	Time, Location, Security impact level etc.
Hypervisor	Read, Write	Hardware resources	Time, Location, Security impact level etc.
Hypervisor	Read, Write, Create	VMs	Time, Location, Security impact level etc.

4 Access Control Guidance for PaaS

PaaS is a platform that provides a framework for developers to create and deploy customized applications. As shown in Figure 3, security assurance considerations include some and all below the data level, and during the application development process lifecycle should be offered by the PaaS provider. The primary focus of AC in the PaaS model is to protect data during runtime, which is managed by middleware and OS. PaaS systems are primarily concerned with developing, deploying and operating customer applications. The security and privacy offered by the PaaS provider protect the applications and data from potential leaks through a covert channel introduced by unsecure shared memory. Therefore, enforcing AC over data during runtime in the PaaS is critical for the security of PaaS services.

The PaaS system administrator is responsible for the access control of runtime, middleware, OS, virtual machine, hypervisor, storage, and networking layers, as described by the guidance in Sections 4.1 to 4.3 below.

4.1 Guidance for Memory Data

The PaaS system permits users to deploy tasks in a provider-controlled middleware and host OS, which may be shared with other PaaS applications. As such, PaaS typically leverages OS-based techniques (e.g., Linux Containers and Docker for isolating applications) [19]. However, numerous existing memory-related attacks can compromise sensitive application-related data by hacking through the shared OS memory in PaaS [20]. Thus, AC for OS memory, such as AC of different processes on top of processor caches [21], should be considered.

4.2 Guidance for APIs

As the PaaS system allows cloud developers to build applications on top of the platform, APIs should control the scope of each user's application such that user data remains inaccessible between different applications. In addition, packaged APIs can be serviced as microservices in a PaaS cloud. A centralized architecture for provisioning and enforcement of access policies governing access to all microservices is required due to the sheer number of services needed for service composition to support real-world business transactions (e.g., consumer order processing and shipping). Since each of the microservices may be implemented in a different language, policy provisioning and computation of access decisions may require the use of an authorization server [22].

4.3 Recommendations for PaaS Access Control

An efficient method should be established for protecting memory data by flushing processor caches during context switches. However, in order to avoid significant performance degradation, only highly sensitive memory data should be flushed.

To handle access control for multiple replicas of data, a method to manage the central AC policy system should be introduced. Thus, once the data within a PaaS provider is duplicated across PaaS providers, any change in the policy should result in an appropriate update to the central AC policy

system. Moreover, the AC policy related to the replicated data in other PaaS providers should be synchronized accordingly based on an AC policy in the central system.

Guideline rules for PaaS AC policy are listed in Table 2 with respect to the three basic elements of AC (i.e., subject, object, and operation). Each row indicates a possible AC rule, but the AC designer should decide whether access should be granted or denied based on the system requirements. For example, if a user of an application needs to access memory data related to their application, permission to read memory data will be granted. However, access to that memory data will be denied to other users.

Table 2: Potential policy rules expressed by Subject, Operation, Object for PaaS AC policy

Subjects	Operations	Objects	Environment Conditions
Application user	Read	Memory data	Time, Location, Security impact level etc.
VM of a hosted application	Read, Write	Other applications' data within the same host	Time, Location, Security impact level etc.
Application developer	Create, Read, Write	Middleware data, memory data	Time, Location, Security impact level etc.
Cloud service provider	Replicate	Application-related data	Time, Location, Security impact level etc.

5 Access Control Guidance for SaaS

In SaaS, a cloud service provider delivers an application as a service to end users through a network such as the internet. Thus, there is no need for users to install and execute applications locally on their own computers. As shown in Figure 4, multiple applications and users can be supported simultaneously by the cloud system to share common resources, including applications and underlying databases.

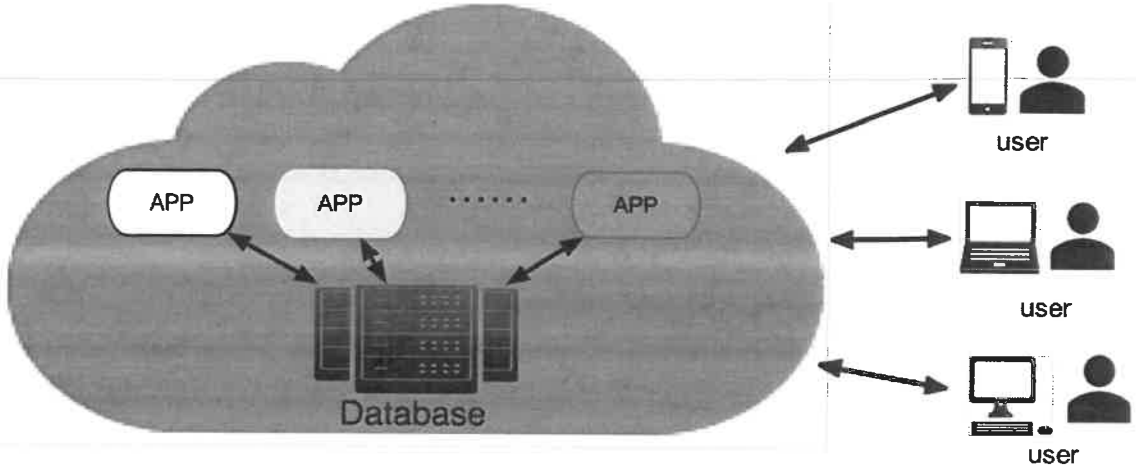


Figure 4: Multiple applications and users of an SaaS provider

If a developer deploys a third-party application, data in that application and other unrelated applications might be stored in the cloud system. End users have to rely on the security and privacy offered by the cloud service provider to protect their data from unauthorized access introduced by those unrelated applications. Note that data managed by the application layer is owned and controlled by the consumer. The SaaS system and consumer need to ensure that access to application data in these layers is not granted to the SaaS system administrator, consumers, or other users unless they are trusted. SaaS administrators are responsible for the access control of all operation layers except for the consumer's application data as shown in Figure 3 and should consider the guidance in Sections 3, 4, and 5.1 to 5.4.

5.1 Guidance for Data Owner's Control

A data provider is the creator or source of application data owned by consumer organizations. Application data is typically stored in the SaaS service provider's database. How a data provider manages access to its data is a challenge. Example questions to be addressed are related to data retention by the provider (e.g., where data is kept and for how long) and whether the provider has any permission to determine access rights to the data it hosts. If a data provider has the capability to determine access rights on data it holds, consideration should be given to ensure that an up-to-date AC policy is always enforced within the SaaS system.

5.2 Guidance for Confidentiality

In the application deployment model, the integrity of sensitive data residing within the data owner's domain must be protected. Protection mechanisms for application data include data

encryption schemes by which data can be encrypted through certain cryptographic primitives, and decryption keys will only be disclosed to authorized users [23]. For such enforcement, attribute-based access control (ABAC) [24] and attribute-based encryption (ABE) schemes can be used to control access to SaaS data [23, 25, 26, 27, 28] since these schemes can use the identity of users through attributes to manage, encrypt, and decrypt application data. However, considering the high volume of data in the SaaS model, the involved encryption and decryption significantly reduce performance. Hence, when encryption is used, consideration should be given to ensure the confidentiality of data while offering good performance.

5.3 Guidance for Privilege Management

In addition to AC enforcement, privilege management involves adding, removing, and changing the privileges of a subject. It is crucial to design a flexible or real-time mechanism for assigning and revoking privileges to maintain the usability of the SaaS service [29].

5.4 Guidance for Multiple Replicas of Data

To maintain high availability, the cloud service provider may replicate data at multiple locations, even across countries. Thus, it is important to make sure that all data replicas are protected under the same AC policy. In other words, the same AC policy for the replicated data object should be populated to all hosts that process the same data. The technology for policy synchronization upon changes must also be considered for inclusion.

5.5 Guidance for Multi-tenancy

The SaaS system introduces additional considerations with regard to the management of access to applications. An immediate necessity is to focus on users' access to applications. The access rights are granted to end users through AC policies based on predefined attributes or roles. This can be specified by attribute-based access control (ABAC) policy models [30, 31], role-based access control [32] (RBAC), and context-based access control [33] (CBAC).

The SaaS model is a typical, multi-tenancy platform that supports multiple end users simultaneously accessing an application with the data of different users' applications residing at the same location. Exploiting vulnerabilities in the application or injecting code into the SaaS system might expose data to other users [34]. Therefore, strategic planning should be given to implementing multi-tenancy while segregating data from different users' applications during the design of an AC system.

5.6 Guidance for Attribute and Role Management

In the SaaS system, attribute and role-based AC management employs policies and predefined roles to manage access rights to applications and underlying databases. The primary challenge of deploying attribute or role-based AC management is reaching an agreement on what types of attributes or roles should be used and what should be considered when designing the AC systems [35]. If the set of considered attributes or roles is too small, flexibility will be reduced. However, if the number of attributes or roles is too large, the complexity of policies will increase.

5.7 Guidance for Policies

SaaS applications provide application-specific access control configurations for different user applications, and in this case, user policies for each application are enforced by the SaaS provider. This configuration does not support collaboration between the SaaS provider and the consumer's access control infrastructure. For example, while large organizations often employ on-premises access control systems for managing their users centrally and efficiently, SaaS applications typically provide organizations with an AC configuration interface for managing AC policies, which forces the AC policies to be stored and evaluated on the SaaS provider's side. This approach might result in disclosing sensitive data required for evaluating the AC policies to the SaaS provider. Therefore, methods for enforcing authorization in the SaaS provider while not disclosing sensitive access control data to the SaaS provider should be considered. Federated authorization [36] is an efficient technique that utilizes a middleware layer to transfer the management of access control policies from the SaaS provider to the consumer side and enforce policies on the SaaS applications without disclosing sensitive data required for evaluating the policies.

5.8 Guidance for APIs

An API in the SaaS model serves as an interface between the cloud server and its users. The API should be designed to protect against both accidental and malicious attempts to circumvent any AC policy. Applications for organizations and third parties often build upon the APIs, which introduce the AC complexity of the new layered API. For example, if the APIs do not require memory access for their tasks, then the AC policy for the APIs should enforce the non-memory access. Additionally, AC policies should be specified to manage the authorization process for web APIs. For example, when APIs connect through SOAP and REST protocols, the AC should control whether to allow end users to interface between Microsoft or non-Microsoft tools and technologies. For authorized API connections through Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) protocols, the AC should grant all related access requested by the protocols. For unauthorized API connections through these protocols, no access or partial access should be granted by the AC.

5.9 Recommendations for SaaS Access Control

With regard to multi-tenancy, authorization may be enforced using a *centralized*, *decentralized*, or *hybrid* authorization system. In a centralized authorization system, the SaaS provider manages a central authorization database for every end user and their accounts [37]. In a decentralized or hybrid authorization system, individual tenants are responsible for all or part of the authorization process. Note that different tenants may require different systems. Considering the attributes or roles of tenants is crucial when selecting the most suitable system. There are many ways to specify attributes or roles, such as in ABAC and RBAC models [31,32]. Attributes or roles must be well-designed and take into account hierarchy relationships when implementing AC policies for different tenants.

Authorization federation [36] is an efficient way to enforce AC policies in the SaaS provider. A generic middleware architecture that incorporates access control requirements from consumers and handles local and remote attributes or roles can be used to extend and shift AC policy management from the SaaS provider to the consumer side. This approach centralizes consumer AC policy

management and lowers the required trust in the SaaS provider. In addition, the AC for VM-supporting federation operations should also be specified (e.g., an end user may create a VM to run different applications). Within the VM of the same host, one application may need to access the application code of other applications to fulfill its task. Unlike the PaaS architecture, where consumers can fully manage the design, testing, and development of the software, SaaS consumers have limited control of the applications hosted in the cloud server.

To achieve the application data owner's control, a security class agreement (SCA) [28] may be of use. SCA is mutually agreed upon by both the data provider of PaaS subscribers and the PaaS service provider and is used for defining the security class of data providers. Multiple replicas of the same data share the same security level as its data provider. This means that given data from a particular data provider, the security class for multiple replicas of the data should be identical. As a result, the host within the PaaS service that is qualified for executing the access request can be determined by referring to the SCA. The data provider can manage access to its data by specifying security classes for the SCA to keep the data provider and the cloud host synchronized in determining the access right of data. For example, in a Bell-LaPadula model [38], assuming a patient's report is written by a doctor with confidential clearance, the report can only be read by a host with the same or higher security clearance. Additionally, when multiple data sources that are not intended to be accessed in the same cloud system are accessed, the privacy of data should not be leaked due to different security classes of these data sources and their data in the SCA. However, due to the high computation complexity of encryption and decryption, cryptographic schemes should be carefully designed to maintain the performance of cloud systems while protecting data confidentiality.

A privilege management infrastructure (PMI) [39] can be employed to dynamically manage assigning and revoking privileges through the use of attributes or role specification certificates in the PaaS model. PMI specifies the privileges for different users and links the privileges with different attribute or role specification certificates, which contain different attribute or role assignments to enforce privilege management.

To handle access control of multiple replicas of data, a method to manage the central AC policy system should be introduced. Thus, once the data within an SaaS provider is duplicated across SaaS providers, any change in the policy should result in an appropriate update to the central AC policy system. Moreover, the AC policy related to the replicated data in other SaaS providers should be synchronized accordingly based on an AC policy in the central system.

Guideline rules for SaaS AC policy are listed in Table 3. The AC designer should decide whether access in each rule is permitted or denied based on the system requirements. For example, during federation operation, VM read/write to other application code within the same host is permitted; otherwise, it is denied.

Table 3: Potential policy rules expressed by Subject, Operation, Object for SaaS AC policy

Subjects	Operations	Objects	Environment Conditions
Application user	Read, Write	Application-related data	Time, Location, Security impact level etc.
Application user	Read	Memory	Time, Location, Security impact level etc.
Application user	Execute	Application	Time, Location, Security impact level etc.
Application user	Read, Write	Application data	Time, Location, Security impact level etc.
Application user	Execute	Application code	Time, Location, Security impact level etc.
VM of a hosted application	Execute	Other application code within the same host	Time, Location, Security impact level etc.

6 Access Control Guidance for Inter- and Intra- Operation

In general, collaboration (i.e., two or more systems that work together as a combined system) in the context of the cloud may lead to a seamless exchange of data and services among various cloud infrastructures. There are two types of collaborations: *inter-operation* and *intra-operation*. Inter-operation refers to the capability of using multiple cloud infrastructures. For example, as shown in Figure 5, a consumer may purchase IaaS services from two different cloud service providers, *Cloud A* and *Cloud B*, and the collaboration between them should be allowed due to data processing requirements.

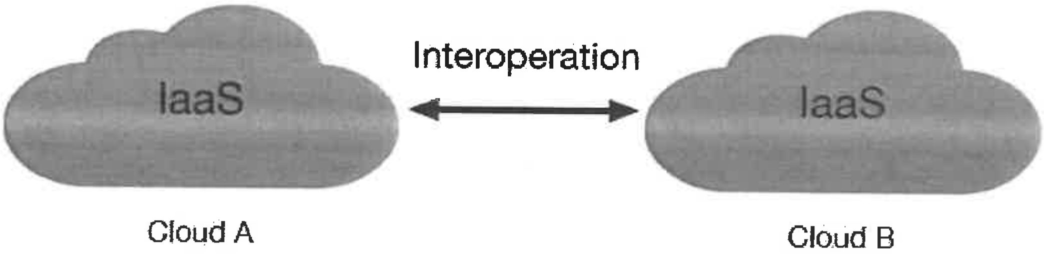


Figure 5: The external collaboration (inter-operation) between different Clouds

Intra-Operation

With regard to intra-operation, two scenarios on intra-operation can be presented as derived from Figure 6. First, a consumer may own multiple VMs in a single cloud host (e.g., *VM A* and *VM B*), and communication among those VMs may be required. Second, a consumer may rent multiple hosts within the same IaaS service, and collaboration among VMs from these different hosts may be required (e.g., an inter-operation between *VM B* and *VM C*).

For intra-operation, the AC policy should enable the operations of VMs for the same consumer to access each as needed during the collaboration period and disable access when the collaboration period ends. There are two primary cases in intra-operation: inter-host case (i.e., VMs from different cloud hosts are operating collaboratively) and intra-host case (i.e., VMs are from the same cloud host and must exchange data and services). Additionally, for some applications, VMs might be distributed in multiple host computers, so the AC policy should cover both intra-host and inter-host cases.

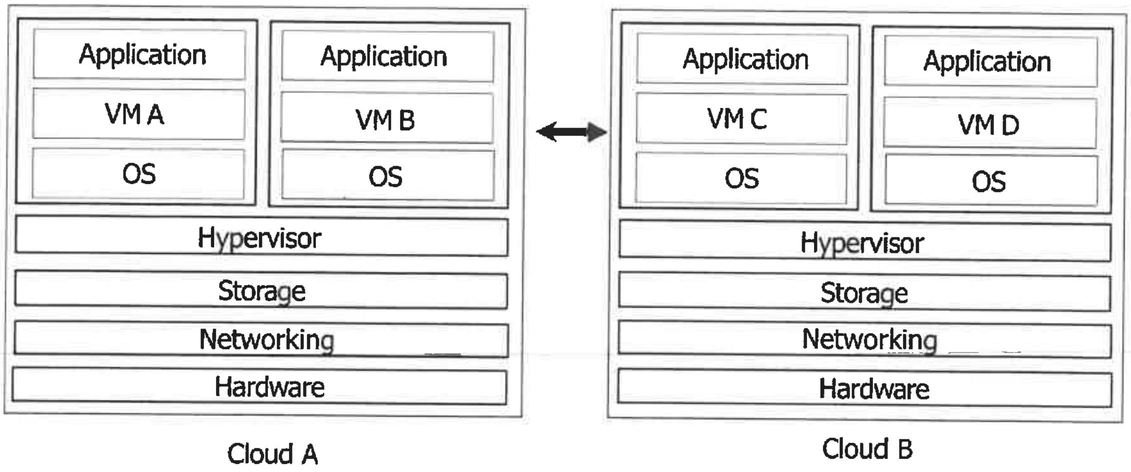


Figure 6: The internal collaboration (intra-operation) within the same cloud

Inter-Operation

There is the possibility that inconsistent management of access elements leads to incorrect access control policy integration for inter-operation. For instance, different cloud service providers using different sets of subject attributes for AC may cause potential conflicts or leak access permissions [40]. Attributes with the same name may result in different privileges when switching providers. Enforcing AC among different cloud service providers without incurring conflicts or blocks of privilege for individual users/VMs is a challenge. This would require examining how to achieve secure inter-operation among the cloud service providers [1], such as in cross hybrid environments. Some cloud AC systems adopt centralized mechanisms to create global AC policies that manage policy integration among different cloud service providers [41]. However, the cloud inter-operation is transient and, thus, inefficient to manage global AC policies as frequent updates for individual cloud AC policies.

7 Conclusions

This document presents an initial step toward understanding access control (AC) challenges in cloud systems by analyzing the AC considerations in all three cloud service delivery models—IaaS, PaaS, and SaaS. Essential characteristics that would affect the cloud's AC design are also summarized, such as broad network access, resource pooling, rapid elasticity, measured service, and data sharing. Various guidance for AC design of IaaS, PaaS, and SaaS are proposed according to their different characteristics. Recommendations for AC design in different cloud systems are also included to facilitate future implementations. Additionally, potential policy rules are summarized for each cloud system. However, many issues remain open, such as AC management across different devices and platforms, as well as new challenges that have yet to emerge with the wide adoption of the cloud.

References

[1] Gouglidis A, Mavridis I, Hu VC (2014) Security policy verification for multi-domains in Cloud systems. *International Journal of Information Security* 13(2):97-111. https://doi.org/10.1007/s10207-013-0205-x

[2] Mell PM, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-145. https://doi.org/10.6028/NIST.SP.800-145

[3] Liu F, Tong J, Mao J, Bohn R, Messina J, Badger ML, Leaf D (2011), NIST Cloud Computing Reference Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-292. https://doi.org/10.6028/NIST.SP.500-292

[4] Badger ML, Grance T, Patt-Corner R, Voas JM (2012) Cloud Computing Synopsis and Recommendations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-146. https://doi.org/10.6028/NIST.SP.800-146.

[5] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

[6] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[7] Bartock MJ, Souppaya MP, Scarfone KA, Carroll D, Masten R, Scinta G, Massis P, Prafullchandra H, Malnar J, Singh H, Yeluri R, Shea T, Dalton M, Dukes A, Phoenix C Swarts B (2018) Trust Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments. (National Institute of Standards and Technology, Gaithersburg, MD), Preliminary Draft NIST Special Publication (SP) 1800-19B. Available at https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud

[8] Szefer J, Lee RB (2011) A case for hardware protection of guest VMs from compromised hypervisors in cloud computing. *2011 31st International Conference on Distributed Computing Systems Workshops (ICDCSW)* (IEEE, Minneapolis, MN), pp 248–252. https://doi.org/10.1109/ICDCSW.2011.51

[9] Krutz RL, Vines RD (2010) *Cloud security: A comprehensive guide to secure cloud computing* (Wiley Publishing, Indianapolis, IN).

[10] Wu J, Ding L, Wu Y, Min-Allah N, Khan SU, Wang Y (2014) C2detector: a covert channel detection framework in cloud computing. *Security and Communication Networks* 7(3):544–557. https://doi.org/10.1002/sec.754

[11] Rushby J (1992) Noninterference, transitivity, and channel-control security policies. (SRI International, Menlo Park, CA), Technical Report CSL-92-02. Available at http://www.csl.sri.com/papers/csl-92-2/

[12] Change ATC, Foster JL, Hall DK (1987) Nimbus-7 SMMR derived global snow cover parameters. *Annals of Glaciology* 9:39-44. https://doi.org/10.3189/S0260305500200736

[13] Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, Zagorodnov D (2009) The Eucalyptus open-source cloud-computing system. *9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'09)* (IEEE, Shanghai, China), pp 124-131. https://doi.org/10.1109/CCGRID.2009.93

[14] Sefraoui O, Aissaoui M, Eleuldj M (2012) OpenStack: toward an open-source solution for cloud computing. *International Journal of Computer Applications* 55(3):38-42. https://doi.org/10.5120/8738-2991

[15] Scarfone KA, Souppaya MP, Hoffman P (2011) Guide to Security for Full Virtualization Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125. https://doi.org/10.6028/NIST.SP.800-125

[16] Wang Z, Jiang X (2010) Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. *2010 IEEE Symposium on Security and Privacy (SP)* (IEEE, Berkeley/Oakland, CA), pp 380–395. https://doi.org/10.1109/SP.2010.30

[17] Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D (2008) TVDc: managing security in the trusted virtual datacenter. *ACM SIGOPS Operating Systems Review* 42(1):40–47. https://doi.org/10.1145/1341312.1341321

[18] Sailer R, Valdez E, Jaeger T, Perez R, Doorn LV, Griffin JL, Berger S (2005) sHype: Secure hypervisor approach to trusted virtualized systems. (IBM Research Division, Yorktown Heights, NY) IBM Research Report RC23511. Available at https://domino.research.ibm.com/library/cyberdig.nsf/papers/265C8E3A6F95CA8D85256FA1005CBF0F/$File/rc23511.pdf

[19] Zhang Y, Juels A, Reiter MK, Ristenpart T (2014) Cross-tenant Side-channel Attacks in PaaS Clouds. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (ACM, Scottsdale, AZ), pp 990–1003. https://doi.org/10.1145/2660267.2660356

[20] Osvik DA, Shamir A, Tromer E (2006) Cache attacks and countermeasures: the case of AES. Pointcheval D. (eds) Topics in Cryptology – CT-RSA 2006. CT-RSA 2006. Lecture Notes in Computer Science 3860 (Springer, Berlin), pp 1–20. https://doi.org/10.1007/11605805_1

[21] Tromer E, Osvik DA, Shamir A (2010) Efficient cache attacks on AES, and countermeasures. *Journal of Cryptology* 23(1):37–71. https://doi.org/10.1007/s00145-009-9049-y

[22] Chandramouli R (2019) Security Strategies for Microservices-based Application Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-204. https://doi.org/10.6028/NIST.SP.800-204

[23] Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. *INFOCOM, 2010 Proceedings* (IEEE, San Diego, CA), pp 1-9. https://doi.org/10.1109/INFCOM.2010.5462174

[24] Hu VC, Ferraiolo DF, Kuhn DR, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 02, 2019. https://doi.org/10.6028/NIST.SP.800-162

[25] Sahai A, Waters B (2005) Fuzzy identity-based encryption. *Advances in Cryptology – EUROCRYPT 2005*. Lecture Notes in Computer Science 3494 (Springer, Berlin), pp 457–473. https://doi.org/10.1007/11426639_27

[26] Nali D, Adams CM, Miri A (2005) Using threshold attribute-based encryption for practical biometric-based access control. *International Journal of Network Security* 1(3):173–182. Available at http://ijns.jalaxy.com.tw/download_paper.jsp?PaperID=IJNS-2005-06-30-2&PaperName=ijns-v1-n3/ijns-2005-v1-n3-p173-182.pdf

[27] Zhu Y, Hu H, Ahn G-J, Huang D, Wang S (2012) Towards temporal access control in cloud computing. *INFOCOM, 2012 Proceedings* (IEEE, Orlando, FL), pp 2576–2580. https://doi.org/10.1109/INFCOM.2012.6195656

[28] Hu VC, Grance T, Ferraiolo DF, Kuhn DR (2014) An access control scheme for big data processing. *2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (IEEE, Miami, FL), pp 1–7. https://doi.org/10.4108/icst.collaboratecom.2014.257649

[29] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874. https://doi.org/10.6028/NIST.IR.7874

[30] Vipul G, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)* (ACM, Alexandria, VA), pp 89-98. https://doi.org/10.1145/1180405.1180418

[31] Hu VC, Kuhn DR, Ferraiolo DF, Voas J (2015) Attribute-based access control. *Computer* 48(2):85-88. http://doi.org/10.1109/MC.2015.33

[32] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE (1996) Role-based access control models. *Computer* 29(2):38-47. https://doi.org/10.1109/2.485845

[33] Rubart J (2005) Context-based access control. *Proceedings of the 2005 Symposia on Metainformatics (MIS '05).* (ACM, New York, NY), pp 13-18. https://doi.org/10.1145/1234324.1234337

[34] Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(1), pp 1–11. https://doi.org/10.1016/j.jnca.2010.07.006

[35] Jin X, Krishnan R, Sandhu R (2012) A unified attribute-based access control model covering DAC, MAC, and RBAC. *Data and Applications Security and Privacy XXVI, DBSec 2012.* Lecture Notes in Computer Science 7371 (Springer, Berlin), pp 41-55. https://doi.org/10.1007/978-3-642-31540-4_4

[36] Decat M, Lagaisse B, Van Landuyt D, Crispo B, Joosen W (2013) Federated authorization for software-as-a-service applications. *On the Move to Meaningful Internet Systems: OTM 2013 Conferences.* Lecture Notes in Computer Science 8185 (Springer, Berlin), pp 342–359. https://doi.org/10.1007/978-3-642-41030-7_25

[37] Dimitrios Z, Lekkas D (2012) Addressing cloud computing security issues. *Future Generation Computer Systems* 28(3):583-592. https://doi.org/10.1016/j.future.2010.12.006

[38] McLean J (1985) A comment on the 'basic security theorem' of Bell and LaPadula. *Information Processing Letters* 20(2):67-70. https://doi.org/10.1016/0020-0190(85)90065-1

[39] Blobel B, Nordberg R, Davis JM, Pharow P (2006) Modelling privilege management and access control. *International Journal of Medical Informatics* 75(8), pp 597–623. https://doi.org/10.1016/j.ijmedinf.2005.08.010

[40] Bertino E, Federica P, Rodolfo F, Shang N (2009) Privacy-preserving digital identity management for cloud computing. *IEEE Data Engineering Bulletin* 32(1):21-27. Available at http://sites.computer.org/debull/A09mar/bertino.pdf

[41] Catteddu D (2010) Cloud Computing: Benefits, risks and recommendations for information security. *Web Application Security.* Communications in Computer and Information Science 72 (Springer, Berlin), pp 17-17. https://doi.org/10.1007/978-3-642-16120-9_9

[42] Simorjay F, Tierling E (2019) Shared Responsibility for Cloud Computing. (Microsoft, Redmond, WA), Version 2.0. Available at https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91/file/225366/1/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf

Appendix A—Guidance and SP 800-53 Revision 4 Access Control (AC) Family Mapping

The following table maps the cloud access control guidance to the AC controls listed in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Table 4 Mapping the cloud access control guidance to the AC controls listed in NIST SP 800-53, Revision 4

Guidance	AC Control in 800-53
3.1 Guidance for Network	AC-1, AC-3, AC-4, AC-5, AC-10, AC-17, AC-21, AC-22
3.2 Guidance for Hypervisor	AC-1, AC-3, AC-5, AC-17, AC-21
3.3 Guidance for Virtual Machine	AC-1, AC-3, AC-4, AC-5, AC-11
3.4 Guidance for API	AC-1, AC-3, AC-4, AC-5, AC-11, AC-17, AC-21, AC-22
4.1 Guidance for Memory Data	AC-1, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
4.2 Guidance for APIs	AC-1, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
5.1 Guidance for Data Owner's Control	AC-1, AC-3, AC-5
5.2 Guidance for Confidentiality	AC-3, AC-6, AC-21
5.3 Guidance for Privilege Management	AC-2, AC-11, AC-14, AC-22
5.4 Guidance for Multiple Replicas of Data	AC-1, AC-3, AC-4, AC-5, AC-17, AC-21
5.5 Guidance for Multi-tenancy	AC-1, AC-2, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
5.6 Guidance for Attribute and Role Management	AC-6, AC-1, AC-3
5.7 Guidance for Policies	AC-1, AC-3
5.8 Guidance for APIs	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-11, AC-14, AC-17, AC-21

AC-1: Access Control Policy and Procedures

AC-2: Account Management

AC-3: Access Enforcement

AC-4: Information Flow Enforcement

AC-5: Separation of Duties

AC-6: Least Privilege

AC-10: Concurrent Session Control

AC-11: Session Lock

AC-14: Permitted Actions without Identification or Authentication

AC-17: Remote Access

AC-21: Collaboration and Information Sharing

AC-22: Publicly Accessible Content

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.

c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.

d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.

b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.

c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.

e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.

c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

a. Access and use the service for its business purposes;
b. For SaaS, use underlying software as embodied or used in the service; and
c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency:______________________	Name of Vendor: AbsenceSoft
Signature:____________________________	Signature: Max Cook
Title:_________________________________	Title: Account Executive
Date:_______________________________	Date: 6/28/2023

AbsenceSoft Response: This will need to be further negotiated. See legal modifications document attached with bid.

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: AbsenceSoft

Name of Agency: ____________________

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☒
   No ☐

2. If yes to #1, does the restricted information include personal data?
   Yes ☒
   No ☐

3. If yes to #1, does the restricted information include non-public data?
   Yes ☒
   No ☐

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes ☐
   No ☒

5. Provide name and email address for the Department privacy officer:

   Name: Chris Snyder

   Email address: chris.s.snyder@wv.gov

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: Max Cook

   Email address: mcook@absencesoft.com

   Phone Number: 358-437-2544

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: MIS2300000005

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[x] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

AbsenceSoft Response: This will need to be further negotiated. See legal modifications document attached with bid.

AbsenceSoft
Company

Max Cook
Authorized Signature

6/28/2023
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Info Technology

Proc Folder:	1234820		**Reason for Modification:**
Doc Description:	ATTENDANCE CASELOAD MANAGEMENT SOFTWARE		ADDENDUM 1 TO PROVIDE ANSWERS TO VENDOR QUESTIONS AND SAAS
Proc Type:	Central Master Agreement		
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2023-06-21	2023-06-28 13:30	CRFQ 0511 MIS2300000005	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name :

Address :

Street :

City :

State : **Country :** **Zip :**

Principal Contact :

Vendor Contact Phone: **Extension:**

FOR INFORMATION CONTACT THE BUYER
Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Vendor Signature X Max Cook **FEIN#** **DATE** 6/28/2023

All offers subject to all terms and conditions contained in this solicitation

AbsenceSoft Response: This will need to be further negotiated. See legal modifications document attached with bid

ADDITIONAL INFORMATION
THE STATE OF WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, WEST VIRGINIA DEPARTMENT OF HEALTH AND HUMAN RESOURCES (DHHR), OFFICE OF MANAGEMENT INFORMATION SERVICES, IS SOLICITING BIDS TO ESTABLISH AN OPEN-END CONTRACT FOR ATTENDANCE CASELOAD MANAGEMENT SOFTWARE (FMLA/FLOA/PLA TRACKING) PER THE ATTACHED DOCUMENTS. ***QUESTIONS REGARDING THE SOLICITATION MUST BE SUBMITTED IN WRITING TO CRYSTAL.G.HUSTEAD@WV.GOV PRIOR TO THE QUESTION PERIOD DEADLINE CONTAINED IN THE INSTRUCTIONS TO VENDORS SUBMITTING BIDS***

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES		HEALTH AND HUMAN RESOURCES	
OFFICE OF HUMAN RESOURCES MGMT		OFFICE OF HUMAN RESOURCES MGMT	
ONE DAVIS SQUARE, STE 400		ONE DAVIS SQUARE, STE 400	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Attendance Caseload Management Software (FMLA/FLOA/PLA)	9.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
3.1.2 Attendance Caseload Management Software (FMLA/FLOA/PLA)

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES		HEALTH AND HUMAN RESOURCES	
OFFICE OF HUMAN RESOURCES MGMT		OFFICE OF HUMAN RESOURCES MGMT	
ONE DAVIS SQUARE, STE 400		ONE DAVIS SQUARE, STE 400	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Year One Optional Renewal				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Optional Renewal Year One

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON US	WV	HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Year Two Optional Renewal				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Optional Renewal Year Two

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON US	WV	HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Year Three Optional Renewal				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Optional Renewal Year Three

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON	WV	HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	Additional Users/Licenses	1.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:

3.1.2.21 Additional Users/Licenses- each add on user/license (9 used for bidding scenario only, quantity could increase or decrease during life of contract)

INVOICE TO		SHIP TO	
HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON	WV	HEALTH AND HUMAN RESOURCES OFFICE OF HUMAN RESOURCES MGMT ONE DAVIS SQUARE, STE 400 CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
6	Online Training for Licenses Holders				

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:

3.1.2.22 Must provide online training for license holders at no cost. System upgrades, enhancements, and error corrections must be at no additional cost/charge when such upgrades, enhancements, and error corrections are generally made available to its other clients of similar systems at no additional cost/charge.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	VENDOR QUESTION DEADLINE	2023-06-15

SOLICITATION NUMBER: CRFQ MIS2300000005
Addendum Number:

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[✓] Other

Description of Modification to Solicitation:

1. To provide answers to vendor questions
2. To include Software as a Service Addendum
3. To provide NIST Special Publication 800-210

No other changes

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

CRFQ-0511-MIS23*5

FMLA/Attendance Caseload Management Software

Vendor Questions and Agency Responses

1. Could you please clarify if you are looking for a custom case management solution or if you are interested in an off-the-shelf product? This information will help us tailor our response to meet your specific needs.

   Agency response - The RFQ was written for an off-the-shelf product with customizable options per the specifications provided by the RFQ.

2. In multiple sections, it is referenced that this solution should be accessible for self-service by employees and should track appropriate employee information regarding leave and attendance.
   a. Are there any other user types such as contractors, external unionized workers, etc. that are expected to use this solution?

      Agency response - Contract workers.

   b. Based on those user types including employees that will have this solution made available to them, what is the total number of employees/other user types that will be served by this solution?

      Agency response - Approximately 5,000 would need to have access through a portal to submit information. Could be more as we have vacancies that need to be filled.

   c. Does the population of employees being served by this solution include the entire state of West Virginia employees or is this limited to a specific agency/agencies?

      Agency response - Around 5000-6000 employees in total for the Agencies/Units resulting from the reorganization of the West Virginia Department of Health and Human Resources.

3. In section 3.1.2.4 it is requested that the "Software must offer recommendations based on state and federal employment and attendance regulations." Can you provide more detail here, for example, is the expectation that the software provides a library of state and federal regulations for the case workers to search through and match against cases that are submitted or is there another intent?

   Agency response - It is the expectation that the software provides a library of state and federal regulations for the case workers to search through and *match against cases. With this, the software must be able to update state and federal regulations as they change or are updated. The software should be able to pull information from WVOASIS and UKG/Kronos to determine employee eligibility based on federal and state guidelines.*

4. In multiple sections there are requirements for the software to interact with UKG/Kronos. Can you describe some common actions that are expected to occur? For example, actions like updating a person record, sending time card information between the UKG and the software, and interacting with time off/leave of absence requests?

   Agency response - The software must be able to collect timecard information from KRONOS. This includes but is not limited to total number of worked hours within a 12 month period, accrued leave, how much accrued leave has been used and if the employee is on authorized or unauthorized leave. As well as the system should be able to track leave of absence balances.

   a. What version of UKG/Kronos is the software expected to integrate and interact with?

      Agency response - WVDHHR and the State of WV are using Workforce Central Version 8.1.17.

   b. Would there be any limitations regarding integration technology to be aware of?

      Agency response - None that we are aware of at this time, however, vendor must present any third party vendor terms and/or software terms with their bid for Agency review.

5. In section 3.1.2.18 it is requested that the "Software must be compatible with Google Docs and Microsoft Office Suite." Can you provide more detail here, for example, is the expectation that certain information from within the software is exportable into Microsoft Office and or Google Docs formats? Or are there other intended use cases between these softwares?

   Agency response - The ability to upload template letters from Google Docs and Microsoft Word and like forms to the software system for distribution.

6. In section 3.1.1.2 it is requested that the software "Must be compatible with WVOasis..." Can you expound on what exactly WVOasis is and its functions/integration use cases with this attendance caseload solution?

   Agency response - WVOasis is the State of West Virginia's ERP. There are several facets of WVOasis. With that said, what we are looking for from the software is to collect employee information to create profiles on the software. For example, WVOASIS houses this information under Employee

Profile Manager (EPM), we would like for the software to take that information and create employee profiles to link cases to that specific employee. Important information within WVOASIS is probation dates, dates of service and employee addresses and phone numbers.

7. What is driving the state of West Virginia's interest in an Attendance Caseload Management System?

   Agency response - We do not currently have a case management system. How we manage cases presently is not as functional as we would like. For example, having FMLA or ADA requests fall through the cracks and having to research all eligibility requirements manually.

8. Is there a larger digital transformation that this proposal is a part of and could you share any details relating to that roadmap if one exists?

   Agency response - No, there is not.

9. Is there a desired timeline for implementation and go-live of this software solution for Attendance Caseload management?

   Agency response - Desired implementation by September 2023, sooner if possible as time is of the essence.

10. Is this project dependent upon funding that has any timeline restrictions tied to it?

    Agency response - No. Please refer to contract terms and conditions regarding funding or cancelations.

11. Does the state of West Virginia have any other HR-related case management tools in place today that this software is replacing and/or standing alongside?

    Agency response - No. Should be able to interact with WVOASIS and KRONOS.

12. Are there any other core HR or Attendance related systems with which there could be integration needs either in a first or future phase besides Kronos and WVOasis?

    Agency response - Business Intelligence (BI) Reports which are housed in the WVOASIS system.

13. Are there any encryption needs outside of using HTTPS? For example, encryption at rest and or disk encryption?

Agency response - Please refer to attached Exhibit - NIST SP 800-210.

14. Are there any government cloud (GCC - Government Community Cloud) requirements for cloud software solutions?

    Agency response - Please refer to attached Exhibit - NIST SP 800-210.

15. Is this a Request for Quotation for Software for all employees of West Virginia or a particular agency in West Virginia?

    Agency response - This solicitation is for the Department of Health and Human Resources.

16. How many employees on payroll are in West Virginia or the agency?

    Agency response - DHHR currently has approximately 5,000-6,000 employees. This number could increase or decrease.

17. Can you explain what "must prompt restricted leave approvals" mean? Also, what "must prompt donated leave approvals" mean.

    Agency response - Please see response to question 18 below.

18. Can you explain what "must prompt restricted leave approvals" mean? Also, what "must prompt donated leave approvals" mean (3.1.2.20)

    Agency response - Software must prompt work restriction approvals, track, and notify when length of leave is nearing (90) ninety days, which will automatically send out ADA paperwork. It must also allow users to review and approve final approval letters for donated leave .

19. Is there a response format to use in preparing our response?

    Agency response - Please follow the instructions for submitting bids contained in the solicitation announcement.

20. We want to confirm you are looking for FMLA/State LOA/PLOA management cloud (SaaS) software.

    Agency response - Yes, that along with just case tracking for ADA and eventually investigations. Please note a SaaS addendum is being included in this solicitation.

21. Do you have a target go live date?

    Agency response - Desired implementation is by September 2023, or sooner if possible as time is of the essence.

22. How is the department currently managing FMLA/State Leave & ADA Accommodations?

    Agency response - We use spreadsheets to track cases and file folders to house all case related information. Everything is currently being done manually.

23. Is the department also looking for a software to streamline/automate the ADA accommodations process?

    Agency response - Yes.

24. On average, how many cases do each of them handle at once?

    Agency response - At least 6-15 cases come in a day, but the volume could increase or decrease.

25. How many cases are submitted per year?

    Agency response - Approximately 1,400-1,500. This amount could increase or decrease.

26. How many employees are you looking to manage with the software?

    Agency response - Three employees will be using the software to manage approximately 1,500 cases a year. This number could increase or decrease.

27. Is this outsourced for a vendor to manage, or do you want the leave team to manage the software?

    Agency response - The agency will manage the software and will rely on the software vendor to provide support and or make changes to the structure of the software as needed. Maintenance agreements beyond the scope or terms of this contract will be procured as needed.

NIST Special Publication 800-210

General Access Control Guidance for Cloud Systems

Vincent C. Hu
Michaela Iorga
Wei Bao
Ang Li
Qinghua Li
Antonios Gouglidis

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-210

General Access Control Guidance for Cloud Systems

Vincent C. Hu
Michaela Iorga
Computer Security Division
Information Technology Laboratory

Wei Bao
Ang Li
Qinghua Li
Department of Computer Science and Computer Engineering
University of Arkansas
Fayetteville, AR

Antonios Gouglidis
School of Computing and Communications
Lancaster University
Lancaster, United Kingdom

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

July 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-210
Natl. Inst. Stand. Technol. Spec. Publ. 800-210, 34 pages (July 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sp800-210-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This document presents cloud access control characteristics and a set of general access control guidance for cloud service models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). Different service delivery models require managing different types of access on offered service components. Such service models can be considered hierarchical, thus the access control guidance of functional components in a lower-level service model are also applicable to the same functional components in a higher-level service model. In general, access control guidance for IaaS is also applicable to PaaS and SaaS, and access control guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to access control requirements for its service.

Keywords

access control; access control mechanism; Cloud; cloud systems; policy; authorization ABAC; RBAC.

Acknowledgements

The authors, Vincent C. Hu and Michaela Iorga of the National Institute of Standards and Technology (NIST), Bao Wei, Ang Li, and Qinghua Li of Department of Computer Science and Computer Engineering University of Arkansas, and Antonios Gouglidis of School of Computing and Communications Lancaster University wish to thank Isabel Van Wyk, Jim Foti, and David Ferraiolo (NIST) who reviewed drafts of this document. The authors also gratefully acknowledge and appreciate the comments and contributions made by government agencies, private organizations, and individuals in providing direction and assistance in the development of this document.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Executive Summary

Cloud systems have been developed over time and conceptualized through a combination of software, hardware components, and virtualization technologies. Characteristics of the cloud, such as resource pooling, rapid elasticity, and pay-as-you-go services, accelerated its wide adoption by industry, government, and academia. Specifically, cloud systems offer application services, data storage, data management, networking, and computing resources management to consumers over a network (the internet in general). Despite the great advancements of cloud systems, concerns have been raised about the offered level of security and privacy. The importance of these concerns becomes more evident when considering the increasing number of users who have adopted cloud services.

This document presents cloud access control (AC) characteristics and a set of general access control guidance for cloud service models—IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). The main focus is on technical aspects of access control without considering deployment models (e.g., public, private, hybrid clouds etc.), as well as trust and risk management issues, which require different layers of discussions that depend on the security requirements of the business function or the organization of deployment for which the cloud system is implemented. Different service delivery models need to consider managing different types of access on offered service components. Such considerations can be hierarchical, such as how the access control considerations of functional components in a lower-level service model (e.g., networking and storage layers in the IaaS model) are also applicable to the same functional components in a higher-level service model (e.g., networking and storage in PaaS and SaaS models). In general, access control considerations for IaaS are also applicable to PaaS and SaaS, and access control considerations for IaaS and PaaS are also applicable to SaaS. Therefore, AC guidance for IaaS is applicable to PaaS and SaaS, and AC guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to access control requirements for its service.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 Purpose

Access control (AC) dictates how subjects (i.e., users and processes) can access objects based on defined AC policies to protect sensitive data and critical computing objects in the cloud systems. Considering the heterogeneity and remote nature of the cloud service models, AC and its general concepts should be revisited. In recent years, many works have focused on AC in cloud systems [23, 25, 26, 27]. However, these are primarily ad hoc solutions targeted at specific cloud applications and do not provide comprehensive views of cloud AC.

This document presents a set of general AC guidance for cloud service models independent from its deployment models because it requires another layer of access control that depends on the security requirements of the business function for which the cloud system is used. As shown in Figure 3, different cloud service models require the management of access to different components of the offered service. Since such cloud service models can be considered hierarchical, the AC considerations of functional components in a lower-level (according to Figure 2) service model (e.g., networking and storage layers in the Infrastructure as a Service (IaaS) model) are also applicable to the same functional components in a higher-level service model (e.g., networking and storage in Platform as a Service (PaaS) and Software as a Service (SaaS) models). In general, AC considerations for IaaS are also applicable to PaaS and SaaS, and AC considerations for IaaS and PaaS are also applicable to SaaS. Thus, AC guidance for IaaS is applicable to PaaS and SaaS, and AC guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to AC. For instance, an IaaS provider may put more effort into virtualization control, and in addition to the virtualization control, a SaaS provider needs to consider data security and the privacy of services it provides.

1.2 Scope

This document focuses on providing guidance for access control systems that are applicable to an organization's cloud implementation and security management. It does not prescribe the internal cloud access control standards that an organization may need in their enterprise systems or within a community other than the organization itself.

1.3 Audience

The intended audience for this document is an organizational entity that implements access control solutions for sharing information in cloud systems. This document assumes that readers are familiar with the cloud and access (authorization) control systems and have basic knowledge of operating systems, databases, networking, and security. Given the constantly changing nature of the information technology (IT) industry, readers are strongly encouraged to take advantage of other documents—including those listed in this document—for more current and detailed information.

1.4 Document Structure

The sections and appendix presented in this document are as follows:

- Section 1 states the purpose and scope of access control and cloud systems.
- Section 2 provides an overview of cloud access control characteristics.
- Section 3 discusses guidance for access control systems for IaaS (Infrastructure as a Service).
- Section 4 discusses guidance for access control systems for PaaS (Platform as a Service).
- Section 5 discusses guidance for access control systems for SaaS (Software as a Service).
- Section 6 discusses guidance for access control systems for inter- and intra-cloud operations.
- Section 7 concludes the document with future directions.

2 Cloud Access Control Characteristics

With the support of different service models, cloud systems can provide a wide range of services to its end-users, developers, and system administrators. Cloud systems have been developed over time and conceptualized through a combination of software, hardware components, and virtualization technologies. Characteristics of the cloud, such as resource pooling, rapid elasticity, and pay-as-you-go services, have accelerated its wide adoption by industry, government, and academia. Specifically, cloud systems offer application services, data storage, data management, networking, and computing resources management to consumers[1] over a network (and the internet in general). Examples of popular cloud applications include web-based email services (e.g., Google's Gmail, Microsoft's Office 365 Outlook), data storage (e.g., Google Drive, Microsoft's OneDrive, Dropbox) for end users, and consumer relationship management and business intelligence systems (e.g., Customer Relationship Management (CRM) Cloud, Workday) for business management. Despite the great advancements of cloud systems, concerns have been raised about offered levels of security and privacy. The importance of these concerns becomes more evident when considering the increasing number of users that have adopted cloud services [1].

NIST publications defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2,3]. Cloud deployment models (e.g., public cloud, private cloud, community cloud, hybrid cloud, etc.) are configured by the scope of cloud users, services, and resources based on service requirements, they may be deployed privately, hosted on the premises of a cloud consumer or provider's dedicated infrastructure, or hosted publicly by one or more cloud service providers. The system may be configured and used by one consumer or a group of trusted partners or support multi-tenancy and be used publicly by different end users who acquire the service. Depending on the type of cloud deployment model, the cloud may have limited private computing resources or access to large quantities of remotely accessed resources. The different deployment models present a number of trade-offs in how consumers can control their resources as well as the scale, cost, and availability of those resources [4]. As depicted in Figure 1, the architecture of a cloud system is composed, in general, by layers of functions:

- VM (Virtual Machine), including:
  - Applications
  - Application Programming Interface (API)
  - Operating System (OS)
- Hypervisor
- Storage
- Networking
- Hardware

[1] Cloud service **consumers** play various roles in the consumption of the cloud services, e.g. system planners, program managers, technologists. **End-users** are individuals using cloud services as direct clients of a cloud provider, of a cloud consumer leveraging a cloud service, or individuals employed by a cloud consumer. A **user** is in a generic term associated with any entity using the cloud service. Depending on scenario, the user can be referred as either cloud service consumer or end-user where applicable.

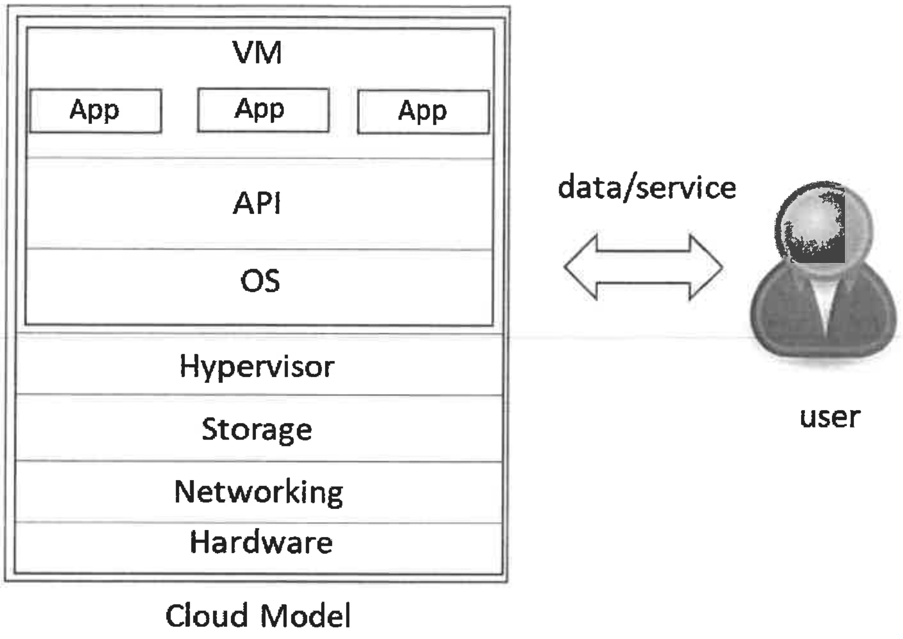


Figure 1: The general architecture of a cloud system

A cloud service can provide access to software applications, such as email or office productivity tools (i.e., the Software as a Service, or SaaS, service model); an environment for consumers to build and operate their own software (i.e., the Platform as a Service, or PaaS, service model), or network access to virtualized computing resources such as processing power and storage (i.e., the Infrastructure as a Service, or IaaS, service model). The different service models have different strengths and are suitable for different consumers and business objectives [4], as illustrated in Figure 2, the arrows show the support relations between models.

A cloud system that deploys the SaaS model can be accessible over a network by an end user utilizing various client devices (e.g., a thin client interface, such as a web browser, for accessing a web-based email application) or via a program with the correct set of interfaces whose execution would enable communication with a cloud application. In the SaaS model, an application user is limited to user-specific application configuration settings and does not manage or control the underlying cloud infrastructure, which typically includes the network, servers, operating systems, storage, or individual applications.

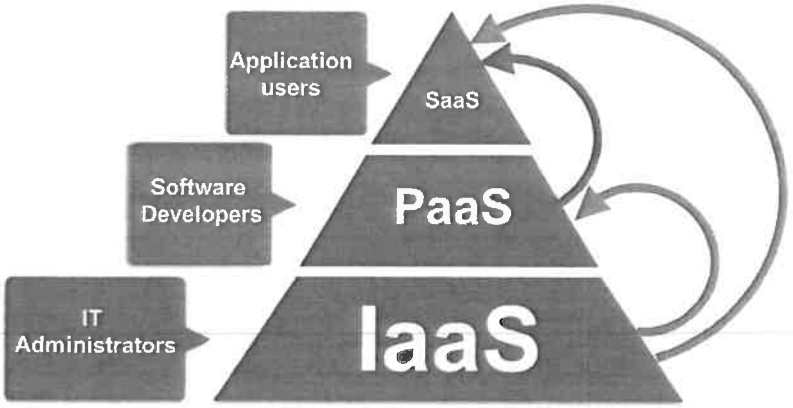


Figure 2: The service models of a cloud system

The PaaS model in a cloud system allows developers to create and deploy applications onto the cloud infrastructure using programming languages, libraries, services, and tools. A software developer does not manage or control the underlying cloud infrastructure but has control over the deployed applications (software) and, possibly, configuration settings for the application-hosting environment.

When analyzing the responsibilities between consumer and cloud service providers for protecting cloud data, it is not always clear-cut, if an IaaS system provides only the computation resources, or offers also the virtualized storage, and network resources to consumers for deploying and running arbitrary software, including operating systems and applications. The consumer may in turn have control over virtual storage, virtualized network components, and the ability to deploy their own VMs and applications given access provisioned by the cloud service provider.

The shared responsibility of access control needs to be considered in the PaaS and SaaS model [42]; For example software developers might need to access data in systems provided by PaaS for their developmental needs, and internal application users (i.e., users that need to access the application system data) might need to access application system data that is managed by the applications. In general, for PaaS, consumer software developers might share access control responsibilities with cloud service providers; for SaaS, internal application users might share such responsibilities with cloud service providers.

Note that unless there is express prior approval from the consumer, a PaaS or SaaS provider must manage access control with the IaaS provider and the consumer (if it is not also the IaaS provider). If the consumer approves, the provider should inform the consumer of its intention to store the specified data in the IaaS provider, where it will be accessed as well as the extent to which the data can be accessed by the IaaS provider, foreign entities, or authorities. A public consultation and hearing process must then be conducted before a decision is made.

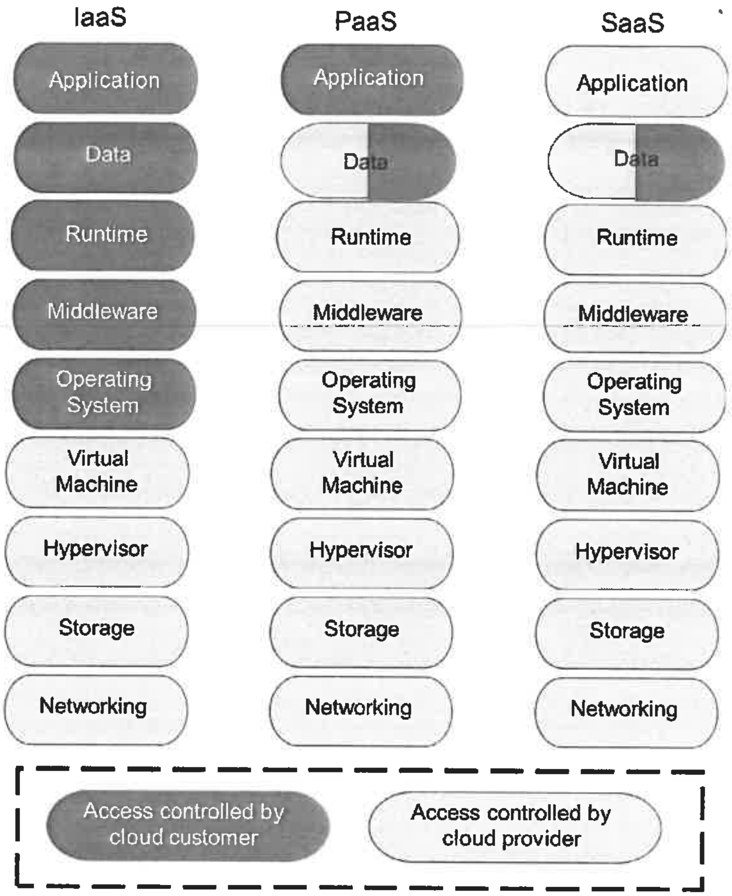


Figure 3: Accesses controlled by the cloud service provider and the consumer

The five essential characteristics that challenge AC system design are summarized as follows [2]:

1. *Broad network access*: Cloud services are available over the network and accessible through standard mechanisms that promote use by heterogeneous thick and thin client platforms (e.g., mobile phones, tablets, laptops, workstations). This raises security concerns with regard to network access. For example, denial of service (DoS) attacks can be launched against a cloud system, rendering its resources unavailable to legitimate users. Thus, AC for network access should be managed.

2. *Resource pooling*: The computing resources of a cloud system (e.g., storage, memory, processing, network bandwidth) are pooled to serve multiple consumers using a multi-tenant model (i.e., a single instance of the software and its supporting infrastructure serves multiple consumers) through different physical and virtual resources, each dynamically assigned and reassigned according to consumer demands. Information may be leaked if the resource allocated to a consumer can be accessed by another co-located consumer or if the allocated resource, such as memory, is not wiped before being reallocated to another consumer. There is also a sense of location independence in that the consumer generally has no control over or knowledge of the exact location of the provided resources. Location may be specified at a higher level of abstraction (e.g., country, state, data center) that brings

security concerns. Therefore, methods for implementing resource pooling while ensuring the isolation of shared resources should be considered in the AC design.

3. *Rapid elasticity*: Cloud services can be elastically provisioned and released—automatically, in some cases—to rapidly scale outward and inward commensurate with demands. To the consumer, services available for provisioning often appear to be unlimited and appropriated in any quantity at any time and are supported by adding new *virtual machines* (VMs) with specified computing resources. A challenge for AC design involves the capability to rapidly verify the security of new VMs and determine whether the newly added VMs are qualified to execute a specific task.

4. *Measured service*: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active end user accounts). Resource usage is monitored, controlled, and reported to provide transparency to both the provider and consumer of the utilized service. To maintain resource usage, cloud consumers should be authorized to review but not to modify their own metering data since this could lead to the falsification of payments required for cloud services. Thus, it is reasonable for AC to consider the protection of metering data.

5. *Data sharing*: Sharing information among different organizations is not a trivial task since a cloud system needs to meet the same security requirements of organizations to achieve that. To facilitate data sharing, concepts such as trust of federated identities and AC attributes need to be considered, and building that trust is paramount. In this document, it is assumed that trust and federated identities/attributes are already established, and further discussion on that topic will be considered in another document. Regardless of the service model, consumers are entitled to be responsible for the security of their cloud-based data and, implicitly, of who has access to it [5]. For this reason, data is never controlled by cloud service providers but rather always stays with the cloud consumers. (The exception to this is log data, but consideration should still be given to how privacy and security is affected by such data.) Although a cloud service provider might become the custodian of consumers' data, it should not have access to that data. If a consumer's data is not encrypted, then cloud administrators might be able to read it. In such a case, the consumer's data should be identified (by the provider's access privileges to the data) and red-flagged as accessible by the service provider, and the consumer should be informed immediately.

Guidance for AC system for each cloud service model, as described in Sections 3, 4, and 6 of this document, can be further extended to system requirements by referring to the AC control elements listed in NIST SP 800-53, Revision 4, *Security and Privacy Control for Federal Information Systems and Organizations* [6] based on the operation requirements of the cloud service. Appendix A maps the guidance to the AC control elements listed in the NIST SP 800-53, Revision 4.

3 Access Control Guidance for IaaS

IaaS is the cornerstone of all cloud services that offer computing and storage through a network such as the internet. Through virtualization technology, IaaS enables end users to dynamically allocate computing resources by instantiating new *virtual machines* (VMs) or releasing them based on their requirements. A VM is a software container that behaves like a physical machine with its own operating system (OS) and virtual resources (e.g., CPU, memory, hard disk, etc.). Leasing VMs is more cost-effective than purchasing new physical machines. The virtualization technology is composed of VMs and a *hypervisor,* as shown in Figure 1. VMs are managed by the hypervisor, which controls the flow of data and instructions between the VMs and the physical hardware. On the consumer side, system administrators are usually the major users of IaaS services since IaaS services are flexible to configure resources (e.g., network, data storage).

Cloud virtualization adds additional security management burdens by introducing security controls that arise from combining multiple VMs onto a single physical computer, which can have potential negative impacts if a security compromise occurs. Some cloud systems make it easy to share information among VMs by, for instance, allowing users to create multiple VMs on top of the same hypervisor if multiple VMs are available. However, this convenience can also become an attack vector since data leakage could occur among VMs. Additionally, virtualized environments are transient since they are created and vanish frequently, thereby making the creation and maintenance of necessary security boundaries more complex.

As shown in Figure 3, data in the middleware, data, applications, and OS layers is owned and controlled by the consumer. The IaaS system and the consumer need to ensure that access to the data is not granted to IaaS system administrators or any other IaaS consumers in these layers unless any of them are permitted. IaaS administrators are responsible for access control on the virtual machine, hypervisor, storage, and networking layers and should consider Sections 3.1 to 3.5 below.

3.1 Guidance for Network

The network is shared among IaaS consumers, and it is important to secure the network traffic and the cloud's environment from being exploited by unauthorized consumers. Thus, access control for network boundaries and allowlists for network communications are required and may be applied through, for example, dedicated virtual local area networks (VLANs) leveraging automated access control lists (ACLs). Using the Institute of Electrical and Electronics Engineers (IEEE) 802.1Q VLAN tagging for network traffic with a cloud data center will result in routing only traffic tagged with the server's unique VLAN identifier to or from that server [7].

3.2 Guidance for Hypervisor

A hypervisor plays an important role in the security of the entire virtualized architecture since it manages consumer loads and guest operating systems (OSs),[2] creates new guest OS images, and controls hardware resources. The security implications of actions like managing guest OS and hardware resources means that access to the hypervisor should be restricted to authorized cloud administrators only. Otherwise, a cloud end user could potentially obtain a VM from the cloud

[2] An OS that is secondary to the originally installed OS.

service provider and install a malicious guest OS that compromises the hypervisor by gaining unauthorized access to and altering the memory of other VMs [8]. Moreover, an attacker in a VM with lower access rights may be able to escalate their access privilege to a higher level by compromising the hardware resources allocation within the hypervisor [9]. Protecting the hypervisor from unauthorized access is therefore critical to the security of IaaS services.

3.3 Guidance for Virtual Machines

VMs that are created by different end users allow resources to be shared among multiple end users. In such cases, it must be ensured that no application from one VM can directly access other VMs since covert channels [10, 11] may leak information between VMs by accessing shared physical resources (e.g., memory). Similarly, although the ability to copy and paste information between VMs via the clipboard is a convenient feature, such a capability could be made available on other VMs running on the same hypervisor and thus introduce an attack vector (i.e., information can be leaked to other VMs through the clipboard). Organizations should have policies regarding the use of shared clipboards.

Isolation between VMs is necessary to keep VMs running independently of each other, and quotas on VM resource usage should be regulated so that a malicious VM can be prohibited from exhausting computation resources. If a malicious application consumes the majority of computation resources, legitimate applications may not be able to obtain sufficient resources to perform their operations. Moreover, end users might terminate the execution of their tasks before they are finished. The state and data of the current VM would then be saved as a guest OS image, and when the task is resumed, the VM might be migrated from a different hypervisor. In such scenarios, guest OS images must be protected from unauthorized access, tampering, or storage. Furthermore, VMs that are not active may also store sensitive data. Monitoring access to the sensitive data in inactive VMs should be considered.

3.4 Guidance for APIs

There are several popular open-source platforms for deploying an IaaS system [12, 13, 14]. These solution platforms enable APIs to manage access control of VMs, hypervisors, and networks (note that a consumer cannot control hypervisors and networks in a multi-tenant environment unless it is a private cloud). For example, [14] consists of control components, including API, communication, lifecycle, storage, volume, scheduler, network, *API server* for managing AC policies for hypervisors, and *network controller* for constructing network bridges and firewall AC rules. The lack of monitoring AC within these APIs might result in unenforced or wrongly enforced AC policies by the hypervisors, VMs, and networks. Thus, a service for monitoring the AC APIs in cloud platforms should also be taken into consideration.

3.5 Recommendations for IaaS Access Control

As shown in previous sections, the security of an IaaS cloud system is heavily dependent on the virtualization (hypervisor). One of the most widely adopted solutions for protecting them is a *virtualization management system* [15], which lies between the underlying hardware and the hypervisor. The virtualization management system enforces AC on both hypervisors and VMs in different ways. Virtualization management systems enforce different levels of access on different

users. Some users are given read-only access to the administrative interface of a guest OS; some are allowed to control particular guest OSs; and some are given complete administrative control. There are existing solutions for providing AC for hypervisors and VMs. For example, the approach in [16] secures the hypervisor against control hijacking attacks by protecting its code from unauthorized access and offering isolation of VMs with the flexible security of mandatory access control (MAC). To enforce AC on interoperations, a service level agreement should be designed to include appropriate control to secure external interoperations. Other isolation mechanisms [17, 18] are helpful in ensuring the security of internal interoperations.

Guideline rules for IaaS AC policy that consider the main elements in AC (i.e., subject, object, and operation) are listed in Table 1. While each row indicates a possible AC rule, the AC policy designer should ultimately decide whether the decision in each rule is permitted or denied based on system requirements. For example, if an authorized IaaS end user requires the use of cloud services, a login operation in the hypervisor for the end user should be granted; otherwise, it should be denied.

Table 1: Potential policy rules expressed by Subject, Operation, Object for IaaS AC policy

Subjects	Operations	Objects	Environment Conditions
IaaS end user	Login, Read, Write, Create	Hypervisor	Time, Location, Security impact level etc.
IaaS end user	Read, Write, Create	VMs	Time, Location, Security impact level etc.
VM	Write	Hypervisor	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs within the same host	Time, Location, Security impact level etc.
VM	Read, Write, Create	Guest OS images	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs from different hosts but within the same IaaS provider	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs from different IaaS providers	Time, Location, Security impact level etc.
Hypervisor	Read, Write, Create	Guest OS images	Time, Location, Security impact level etc.
Hypervisor	Read, Write	Hardware resources	Time, Location, Security impact level etc.
Hypervisor	Read, Write, Create	VMs	Time, Location, Security impact level etc.

4 Access Control Guidance for PaaS

PaaS is a platform that provides a framework for developers to create and deploy customized applications. As shown in Figure 3, security assurance considerations include some and all below the data level, and during the application development process lifecycle should be offered by the PaaS provider. The primary focus of AC in the PaaS model is to protect data during runtime, which is managed by middleware and OS. PaaS systems are primarily concerned with developing, deploying and operating customer applications. The security and privacy offered by the PaaS provider protect the applications and data from potential leaks through a covert channel introduced by unsecure shared memory. Therefore, enforcing AC over data during runtime in the PaaS is critical for the security of PaaS services.

The PaaS system administrator is responsible for the access control of runtime, middleware, OS, virtual machine, hypervisor, storage, and networking layers, as described by the guidance in Sections 4.1 to 4.3 below.

4.1 Guidance for Memory Data

The PaaS system permits users to deploy tasks in a provider-controlled middleware and host OS, which may be shared with other PaaS applications. As such, PaaS typically leverages OS-based techniques (e.g., Linux Containers and Docker for isolating applications) [19]. However, numerous existing memory-related attacks can compromise sensitive application-related data by hacking through the shared OS memory in PaaS [20]. Thus, AC for OS memory, such as AC of different processes on top of processor caches [21], should be considered.

4.2 Guidance for APIs

As the PaaS system allows cloud developers to build applications on top of the platform, APIs should control the scope of each user's application such that user data remains inaccessible between different applications. In addition, packaged APIs can be serviced as microservices in a PaaS cloud. A centralized architecture for provisioning and enforcement of access policies governing access to all microservices is required due to the sheer number of services needed for service composition to support real-world business transactions (e.g., consumer order processing and shipping). Since each of the microservices may be implemented in a different language, policy provisioning and computation of access decisions may require the use of an authorization server [22].

4.3 Recommendations for PaaS Access Control

An efficient method should be established for protecting memory data by flushing processor caches during context switches. However, in order to avoid significant performance degradation, only highly sensitive memory data should be flushed.

To handle access control for multiple replicas of data, a method to manage the central AC policy system should be introduced. Thus, once the data within a PaaS provider is duplicated across PaaS providers, any change in the policy should result in an appropriate update to the central AC policy

system. Moreover, the AC policy related to the replicated data in other PaaS providers should be synchronized accordingly based on an AC policy in the central system.

Guideline rules for PaaS AC policy are listed in Table 2 with respect to the three basic elements of AC (i.e., subject, object, and operation). Each row indicates a possible AC rule, but the AC designer should decide whether access should be granted or denied based on the system requirements. For example, if a user of an application needs to access memory data related to their application, permission to read memory data will be granted. However, access to that memory data will be denied to other users.

Table 2: Potential policy rules expressed by Subject, Operation, Object for PaaS AC policy

Subjects	Operations	Objects	Environment Conditions
Application user	Read	Memory data	Time, Location, Security impact level etc.
VM of a hosted application	Read, Write	Other applications' data within the same host	Time, Location, Security impact level etc.
Application developer	Create, Read, Write	Middleware data, memory data	Time, Location, Security impact level etc.
Cloud service provider	Replicate	Application-related data	Time, Location, Security impact level etc.

5 Access Control Guidance for SaaS

In SaaS, a cloud service provider delivers an application as a service to end users through a network such as the internet. Thus, there is no need for users to install and execute applications locally on their own computers. As shown in Figure 4, multiple applications and users can be supported simultaneously by the cloud system to share common resources, including applications and underlying databases.

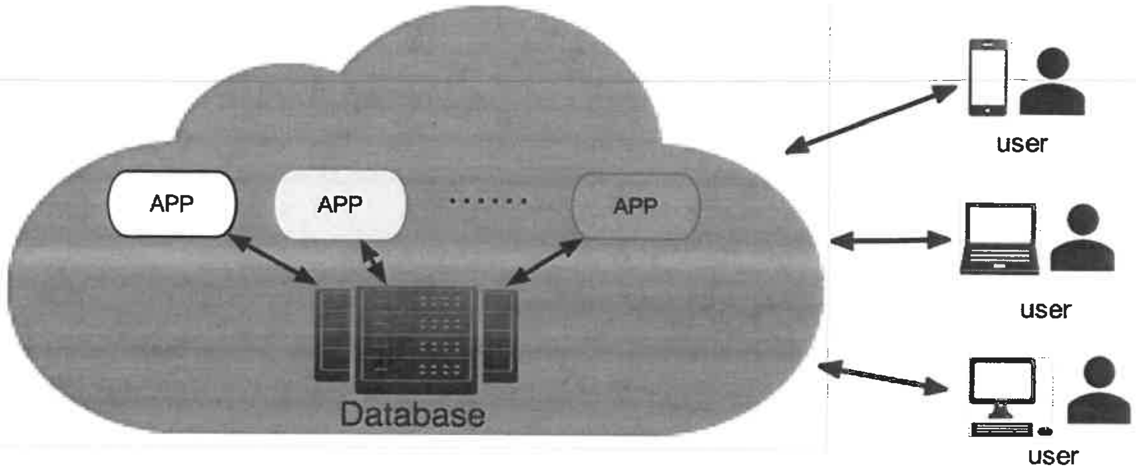


Figure 4: Multiple applications and users of an SaaS provider

If a developer deploys a third-party application, data in that application and other unrelated applications might be stored in the cloud system. End users have to rely on the security and privacy offered by the cloud service provider to protect their data from unauthorized access introduced by those unrelated applications. Note that data managed by the application layer is owned and controlled by the consumer. The SaaS system and consumer need to ensure that access to application data in these layers is not granted to the SaaS system administrator, consumers, or other users unless they are trusted. SaaS administrators are responsible for the access control of all operation layers except for the consumer's application data as shown in Figure 3 and should consider the guidance in Sections 3, 4, and 5.1 to 5.4.

5.1 Guidance for Data Owner's Control

A data provider is the creator or source of application data owned by consumer organizations. Application data is typically stored in the SaaS service provider's database. How a data provider manages access to its data is a challenge. Example questions to be addressed are related to data retention by the provider (e.g., where data is kept and for how long) and whether the provider has any permission to determine access rights to the data it hosts. If a data provider has the capability to determine access rights on data it holds, consideration should be given to ensure that an up-to-date AC policy is always enforced within the SaaS system.

5.2 Guidance for Confidentiality

In the application deployment model, the integrity of sensitive data residing within the data owner's domain must be protected. Protection mechanisms for application data include data

encryption schemes by which data can be encrypted through certain cryptographic primitives, and decryption keys will only be disclosed to authorized users [23]. For such enforcement, attribute-based access control (ABAC) [24] and attribute-based encryption (ABE) schemes can be used to control access to SaaS data [23, 25, 26, 27, 28] since these schemes can use the identity of users through attributes to manage, encrypt, and decrypt application data. However, considering the high volume of data in the SaaS model, the involved encryption and decryption significantly reduce performance. Hence, when encryption is used, consideration should be given to ensure the confidentiality of data while offering good performance.

5.3 Guidance for Privilege Management

In addition to AC enforcement, privilege management involves adding, removing, and changing the privileges of a subject. It is crucial to design a flexible or real-time mechanism for assigning and revoking privileges to maintain the usability of the SaaS service [29].

5.4 Guidance for Multiple Replicas of Data

To maintain high availability, the cloud service provider may replicate data at multiple locations, even across countries. Thus, it is important to make sure that all data replicas are protected under the same AC policy. In other words, the same AC policy for the replicated data object should be populated to all hosts that process the same data. The technology for policy synchronization upon changes must also be considered for inclusion.

5.5 Guidance for Multi-tenancy

The SaaS system introduces additional considerations with regard to the management of access to applications. An immediate necessity is to focus on users' access to applications. The access rights are granted to end users through AC policies based on predefined attributes or roles. This can be specified by attribute-based access control (ABAC) policy models [30, 31], role-based access control [32] (RBAC), and context-based access control [33] (CBAC).

The SaaS model is a typical, multi-tenancy platform that supports multiple end users simultaneously accessing an application with the data of different users' applications residing at the same location. Exploiting vulnerabilities in the application or injecting code into the SaaS system might expose data to other users [34]. Therefore, strategic planning should be given to implementing multi-tenancy while segregating data from different users' applications during the design of an AC system.

5.6 Guidance for Attribute and Role Management

In the SaaS system, attribute and role-based AC management employs policies and predefined roles to manage access rights to applications and underlying databases. The primary challenge of deploying attribute or role-based AC management is reaching an agreement on what types of attributes or roles should be used and what should be considered when designing the AC systems [35]. If the set of considered attributes or roles is too small, flexibility will be reduced. However, if the number of attributes or roles is too large, the complexity of policies will increase.

5.7 Guidance for Policies

SaaS applications provide application-specific access control configurations for different user applications, and in this case, user policies for each application are enforced by the SaaS provider. This configuration does not support collaboration between the SaaS provider and the consumer's access control infrastructure. For example, while large organizations often employ on-premises access control systems for managing their users centrally and efficiently, SaaS applications typically provide organizations with an AC configuration interface for managing AC policies, which forces the AC policies to be stored and evaluated on the SaaS provider's side. This approach might result in disclosing sensitive data required for evaluating the AC policies to the SaaS provider. Therefore, methods for enforcing authorization in the SaaS provider while not disclosing sensitive access control data to the SaaS provider should be considered. Federated authorization [36] is an efficient technique that utilizes a middleware layer to transfer the management of access control policies from the SaaS provider to the consumer side and enforce policies on the SaaS applications without disclosing sensitive data required for evaluating the policies.

5.8 Guidance for APIs

An API in the SaaS model serves as an interface between the cloud server and its users. The API should be designed to protect against both accidental and malicious attempts to circumvent any AC policy. Applications for organizations and third parties often build upon the APIs, which introduce the AC complexity of the new layered API. For example, if the APIs do not require memory access for their tasks, then the AC policy for the APIs should enforce the non-memory access. Additionally, AC policies should be specified to manage the authorization process for web APIs. For example, when APIs connect through SOAP and REST protocols, the AC should control whether to allow end users to interface between Microsoft or non-Microsoft tools and technologies. For authorized API connections through Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) protocols, the AC should grant all related access requested by the protocols. For unauthorized API connections through these protocols, no access or partial access should be granted by the AC.

5.9 Recommendations for SaaS Access Control

With regard to multi-tenancy, authorization may be enforced using a *centralized*, *decentralized*, or *hybrid* authorization system. In a centralized authorization system, the SaaS provider manages a central authorization database for every end user and their accounts [37]. In a decentralized or hybrid authorization system, individual tenants are responsible for all or part of the authorization process. Note that different tenants may require different systems. Considering the attributes or roles of tenants is crucial when selecting the most suitable system. There are many ways to specify attributes or roles, such as in ABAC and RBAC models [31,32]. Attributes or roles must be well-designed and take into account hierarchy relationships when implementing AC policies for different tenants.

Authorization federation [36] is an efficient way to enforce AC policies in the SaaS provider. A generic middleware architecture that incorporates access control requirements from consumers and handles local and remote attributes or roles can be used to extend and shift AC policy management from the SaaS provider to the consumer side. This approach centralizes consumer AC policy

management and lowers the required trust in the SaaS provider. In addition, the AC for VM-supporting federation operations should also be specified (e.g., an end user may create a VM to run different applications). Within the VM of the same host, one application may need to access the application code of other applications to fulfill its task. Unlike the PaaS architecture, where consumers can fully manage the design, testing, and development of the software, SaaS consumers have limited control of the applications hosted in the cloud server.

To achieve the application data owner's control, a security class agreement (SCA) [28] may be of use. SCA is mutually agreed upon by both the data provider of PaaS subscribers and the PaaS service provider and is used for defining the security class of data providers. Multiple replicas of the same data share the same security level as its data provider. This means that given data from a particular data provider, the security class for multiple replicas of the data should be identical. As a result, the host within the PaaS service that is qualified for executing the access request can be determined by referring to the SCA. The data provider can manage access to its data by specifying security classes for the SCA to keep the data provider and the cloud host synchronized in determining the access right of data. For example, in a Bell-LaPadula model [38], assuming a patient's report is written by a doctor with confidential clearance, the report can only be read by a host with the same or higher security clearance. Additionally, when multiple data sources that are not intended to be accessed in the same cloud system are accessed, the privacy of data should not be leaked due to different security classes of these data sources and their data in the SCA. However, due to the high computation complexity of encryption and decryption, cryptographic schemes should be carefully designed to maintain the performance of cloud systems while protecting data confidentiality.

A privilege management infrastructure (PMI) [39] can be employed to dynamically manage assigning and revoking privileges through the use of attributes or role specification certificates in the PaaS model. PMI specifies the privileges for different users and links the privileges with different attribute or role specification certificates, which contain different attribute or role assignments to enforce privilege management.

To handle access control of multiple replicas of data, a method to manage the central AC policy system should be introduced. Thus, once the data within an SaaS provider is duplicated across SaaS providers, any change in the policy should result in an appropriate update to the central AC policy system. Moreover, the AC policy related to the replicated data in other SaaS providers should be synchronized accordingly based on an AC policy in the central system.

Guideline rules for SaaS AC policy are listed in Table 3. The AC designer should decide whether access in each rule is permitted or denied based on the system requirements. For example, during federation operation, VM read/write to other application code within the same host is permitted; otherwise, it is denied.

Table 3: Potential policy rules expressed by Subject, Operation, Object for SaaS AC policy

Subjects	Operations	Objects	Environment Conditions
Application user	Read, Write	Application-related data	Time, Location, Security impact level etc.
Application user	Read	Memory	Time, Location, Security impact level etc.
Application user	Execute	Application	Time, Location, Security impact level etc.
Application user	Read, Write	Application data	Time, Location, Security impact level etc.
Application user	Execute	Application code	Time, Location, Security impact level etc.
VM of a hosted application	Execute	Other application code within the same host	Time, Location, Security impact level etc.

6 Access Control Guidance for Inter- and Intra- Operation

In general, collaboration (i.e., two or more systems that work together as a combined system) in the context of the cloud may lead to a seamless exchange of data and services among various cloud infrastructures. There are two types of collaborations: *inter-operation* and *intra-operation*. Inter-operation refers to the capability of using multiple cloud infrastructures. For example, as shown in Figure 5, a consumer may purchase IaaS services from two different cloud service providers, *Cloud A* and *Cloud B*, and the collaboration between them should be allowed due to data processing requirements.

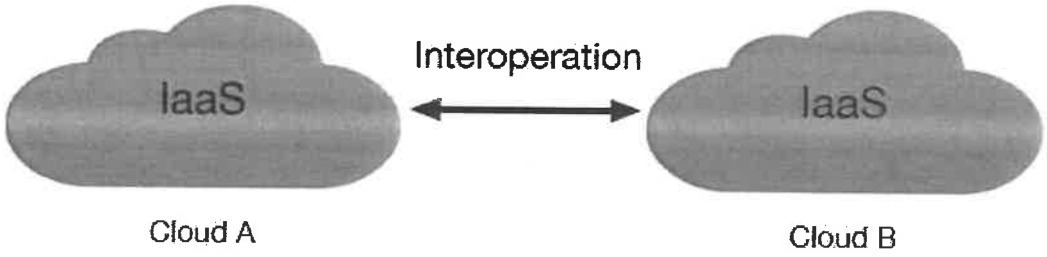


Figure 5: The external collaboration (inter-operation) between different Clouds

Intra-Operation

With regard to intra-operation, two scenarios on intra-operation can be presented as derived from Figure 6. First, a consumer may own multiple VMs in a single cloud host (e.g., *VM A* and *VM B*), and communication among those VMs may be required. Second, a consumer may rent multiple hosts within the same IaaS service, and collaboration among VMs from these different hosts may be required (e.g., an inter-operation between *VM B* and *VM C*).

For intra-operation, the AC policy should enable the operations of VMs for the same consumer to access each as needed during the collaboration period and disable access when the collaboration period ends. There are two primary cases in intra-operation: inter-host case (i.e., VMs from different cloud hosts are operating collaboratively) and intra-host case (i.e., VMs are from the same cloud host and must exchange data and services). Additionally, for some applications, VMs might be distributed in multiple host computers, so the AC policy should cover both intra-host and inter-host cases.

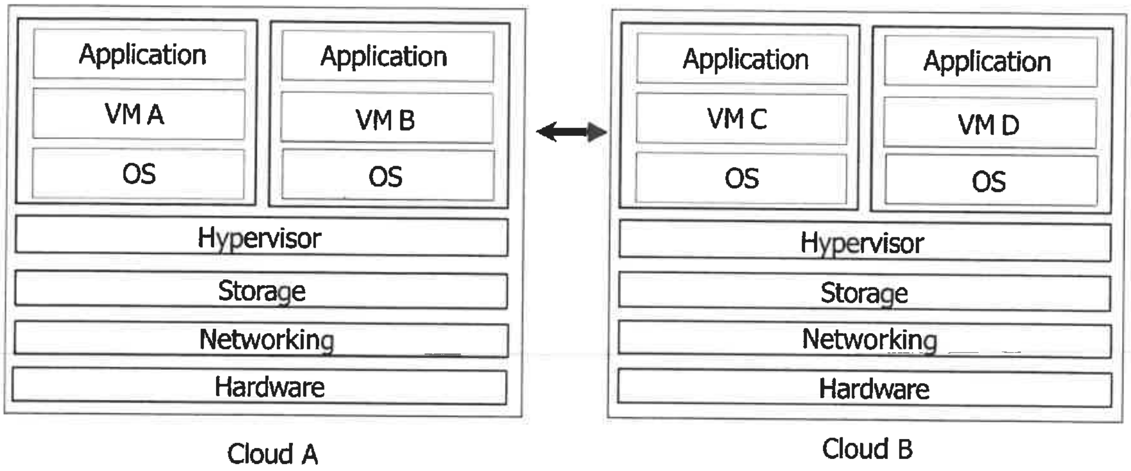


Figure 6: The internal collaboration (intra-operation) within the same cloud

Inter-Operation

There is the possibility that inconsistent management of access elements leads to incorrect access control policy integration for inter-operation. For instance, different cloud service providers using different sets of subject attributes for AC may cause potential conflicts or leak access permissions [40]. Attributes with the same name may result in different privileges when switching providers. Enforcing AC among different cloud service providers without incurring conflicts or blocks of privilege for individual users/VMs is a challenge. This would require examining how to achieve secure inter-operation among the cloud service providers [1], such as in cross hybrid environments. Some cloud AC systems adopt centralized mechanisms to create global AC policies that manage policy integration among different cloud service providers [41]. However, the cloud inter-operation is transient and, thus, inefficient to manage global AC policies as frequent updates for individual cloud AC policies.

7 Conclusions

This document presents an initial step toward understanding access control (AC) challenges in cloud systems by analyzing the AC considerations in all three cloud service delivery models—IaaS, PaaS, and SaaS. Essential characteristics that would affect the cloud's AC design are also summarized, such as broad network access, resource pooling, rapid elasticity, measured service, and data sharing. Various guidance for AC design of IaaS, PaaS, and SaaS are proposed according to their different characteristics. Recommendations for AC design in different cloud systems are also included to facilitate future implementations. Additionally, potential policy rules are summarized for each cloud system. However, many issues remain open, such as AC management across different devices and platforms, as well as new challenges that have yet to emerge with the wide adoption of the cloud.

References

[1] Gouglidis A, Mavridis I, Hu VC (2014) Security policy verification for multi-domains in Cloud systems. *International Journal of Information Security* 13(2):97-111. https://doi.org/10.1007/s10207-013-0205-x

[2] Mell PM, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-145. https://doi.org/10.6028/NIST.SP.800-145

[3] Liu F, Tong J, Mao J, Bohn R, Messina J, Badger ML, Leaf D (2011), NIST Cloud Computing Reference Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-292. https://doi.org/10.6028/NIST.SP.500-292

[4] Badger ML, Grance T, Patt-Corner R, Voas JM (2012) Cloud Computing Synopsis and Recommendations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-146. https://doi.org/10.6028/NIST.SP.800-146.

[5] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

[6] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[7] Bartock MJ, Souppaya MP, Scarfone KA, Carroll D, Masten R, Scinta G, Massis P, Prafullchandra H, Malnar J, Singh H, Yeluri R, Shea T, Dalton M, Dukes A, Phoenix C Swarts B (2018) Trust Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments. (National Institute of Standards and Technology, Gaithersburg, MD), Preliminary Draft NIST Special Publication (SP) 1800-19B. Available at https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud

[8] Szefer J, Lee RB (2011) A case for hardware protection of guest VMs from compromised hypervisors in cloud computing. *2011 31st International Conference on Distributed Computing Systems Workshops (ICDCSW)* (IEEE, Minneapolis, MN), pp 248–252. https://doi.org/10.1109/ICDCSW.2011.51

[9] Krutz RL, Vines RD (2010) *Cloud security: A comprehensive guide to secure cloud computing* (Wiley Publishing, Indianapolis, IN).

[10] Wu J, Ding L, Wu Y, Min-Allah N, Khan SU, Wang Y (2014) C2detector: a covert channel detection framework in cloud computing. *Security and Communication Networks* 7(3):544–557. https://doi.org/10.1002/sec.754

[11] Rushby J (1992) Noninterference, transitivity, and channel-control security policies. (SRI International, Menlo Park, CA), Technical Report CSL-92-02. Available at http://www.csl.sri.com/papers/csl-92-2/

[12] Change ATC, Foster JL, Hall DK (1987) Nimbus-7 SMMR derived global snow cover parameters. *Annals of Glaciology* 9:39-44. https://doi.org/10.3189/S0260305500200736

[13] Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, Zagorodnov D (2009) The Eucalyptus open-source cloud-computing system. *9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'09)* (IEEE, Shanghai, China), pp 124-131. https://doi.org/10.1109/CCGRID.2009.93

[14] Sefraoui O, Aissaoui M, Eleuldj M (2012) OpenStack: toward an open-source solution for cloud computing. *International Journal of Computer Applications* 55(3):38-42. https://doi.org/10.5120/8738-2991

[15] Scarfone KA, Souppaya MP, Hoffman P (2011) Guide to Security for Full Virtualization Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125. https://doi.org/10.6028/NIST.SP.800-125

[16] Wang Z, Jiang X (2010) Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. *2010 IEEE Symposium on Security and Privacy (SP)* (IEEE, Berkeley/Oakland, CA), pp 380–395. https://doi.org/10.1109/SP.2010.30

[17] Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D (2008) TVDc: managing security in the trusted virtual datacenter. *ACM SIGOPS Operating Systems Review* 42(1):40–47. https://doi.org/10.1145/1341312.1341321

[18] Sailer R, Valdez E, Jaeger T, Perez R, Doorn LV, Griffin JL, Berger S (2005) sHype: Secure hypervisor approach to trusted virtualized systems. (IBM Research Division, Yorktown Heights, NY) IBM Research Report RC23511. Available at https://domino.research.ibm.com/library/cyberdig.nsf/papers/265C8E3A6F95CA8D85256FA1005CBF0F/$File/rc23511.pdf

[19] Zhang Y, Juels A, Reiter MK, Ristenpart T (2014) Cross-tenant Side-channel Attacks in PaaS Clouds. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (ACM, Scottsdale, AZ), pp 990–1003. https://doi.org/10.1145/2660267.2660356

[20] Osvik DA, Shamir A, Tromer E (2006) Cache attacks and countermeasures: the case of AES. Pointcheval D. (eds) Topics in Cryptology – CT-RSA 2006. CT-RSA 2006. Lecture Notes in Computer Science 3860 (Springer, Berlin), pp 1–20. https://doi.org/10.1007/11605805_1

[21] Tromer E, Osvik DA, Shamir A (2010) Efficient cache attacks on AES, and countermeasures. *Journal of Cryptology* 23(1):37–71. https://doi.org/10.1007/s00145-009-9049-y

[22] Chandramouli R (2019) Security Strategies for Microservices-based Application Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-204. https://doi.org/10.6028/NIST.SP.800-204

[23] Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. *INFOCOM, 2010 Proceedings* (IEEE, San Diego, CA), pp 1-9. https://doi.org/10.1109/INFCOM.2010.5462174

[24] Hu VC, Ferraiolo DF, Kuhn DR, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 02, 2019. https://doi.org/10.6028/NIST.SP.800-162

[25] Sahai A, Waters B (2005) Fuzzy identity-based encryption. *Advances in Cryptology – EUROCRYPT 2005*. Lecture Notes in Computer Science 3494 (Springer, Berlin), pp 457–473. https://doi.org/10.1007/11426639_27

[26] Nali D, Adams CM, Miri A (2005) Using threshold attribute-based encryption for practical biometric-based access control. *International Journal of Network Security* 1(3):173–182. Available at http://ijns.jalaxy.com.tw/download_paper.jsp?PaperID=IJNS-2005-06-30-2&PaperName=ijns-v1-n3/ijns-2005-v1-n3-p173-182.pdf

[27] Zhu Y, Hu H, Ahn G-J, Huang D, Wang S (2012) Towards temporal access control in cloud computing. *INFOCOM, 2012 Proceedings* (IEEE, Orlando, FL), pp 2576–2580. https://doi.org/10.1109/INFCOM.2012.6195656

[28] Hu VC, Grance T, Ferraiolo DF, Kuhn DR (2014) An access control scheme for big data processing. *2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (IEEE, Miami, FL), pp 1–7. https://doi.org/10.4108/icst.collaboratecom.2014.257649

[29] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874. https://doi.org/10.6028/NIST.IR.7874

[30] Vipul G, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)* (ACM, Alexandria, VA), pp 89-98. https://doi.org/10.1145/1180405.1180418

[31] Hu VC, Kuhn DR, Ferraiolo DF, Voas J (2015) Attribute-based access control. *Computer* 48(2):85-88. http://doi.org/10.1109/MC.2015.33

[32] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE (1996) Role-based access control models. *Computer* 29(2):38-47. https://doi.org/10.1109/2.485845

[33] Rubart J (2005) Context-based access control. *Proceedings of the 2005 Symposia on Metainformatics (MIS '05).* (ACM, New York, NY), pp 13-18. https://doi.org/10.1145/1234324.1234337

[34] Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(1), pp 1–11. https://doi.org/10.1016/j.jnca.2010.07.006

[35] Jin X, Krishnan R, Sandhu R (2012) A unified attribute-based access control model covering DAC, MAC, and RBAC. *Data and Applications Security and Privacy XXVI, DBSec 2012.* Lecture Notes in Computer Science 7371 (Springer, Berlin), pp 41-55. https://doi.org/10.1007/978-3-642-31540-4_4

[36] Decat M, Lagaisse B, Van Landuyt D, Crispo B, Joosen W (2013) Federated authorization for software-as-a-service applications. *On the Move to Meaningful Internet Systems: OTM 2013 Conferences.* Lecture Notes in Computer Science 8185 (Springer, Berlin), pp 342–359. https://doi.org/10.1007/978-3-642-41030-7_25

[37] Dimitrios Z, Lekkas D (2012) Addressing cloud computing security issues. *Future Generation Computer Systems* 28(3):583-592. https://doi.org/10.1016/j.future.2010.12.006

[38] McLean J (1985) A comment on the 'basic security theorem' of Bell and LaPadula. *Information Processing Letters* 20(2):67-70. https://doi.org/10.1016/0020-0190(85)90065-1

[39] Blobel B, Nordberg R, Davis JM, Pharow P (2006) Modelling privilege management and access control. *International Journal of Medical Informatics* 75(8), pp 597–623. https://doi.org/10.1016/j.ijmedinf.2005.08.010

[40] Bertino E, Federica P, Rodolfo F, Shang N (2009) Privacy-preserving digital identity management for cloud computing. *IEEE Data Engineering Bulletin* 32(1):21-27. Available at http://sites.computer.org/debull/A09mar/bertino.pdf

[41] Catteddu D (2010) Cloud Computing: Benefits, risks and recommendations for information security. *Web Application Security.* Communications in Computer and Information Science 72 (Springer, Berlin), pp 17-17. https://doi.org/10.1007/978-3-642-16120-9_9

[42] Simorjay F, Tierling E (2019) Shared Responsibility for Cloud Computing. (Microsoft, Redmond, WA), Version 2.0. Available at https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91/file/225366/1/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf

Appendix A—Guidance and SP 800-53 Revision 4 Access Control (AC) Family Mapping

The following table maps the cloud access control guidance to the AC controls listed in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

Table 4 Mapping the cloud access control guidance to the AC controls listed in NIST SP 800-53, Revision 4

Guidance	AC Control in 800-53
3.1 Guidance for Network	AC-1, AC-3, AC-4, AC-5, AC-10, AC-17, AC-21, AC-22
3.2 Guidance for Hypervisor	AC-1, AC-3, AC-5, AC-17, AC-21
3.3 Guidance for Virtual Machine	AC-1, AC-3, AC-4, AC-5, AC-11
3.4 Guidance for API	AC-1, AC-3, AC-4, AC-5, AC-11, AC-17, AC-21, AC-22
4.1 Guidance for Memory Data	AC-1, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
4.2 Guidance for APIs	AC-1, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
5.1 Guidance for Data Owner's Control	AC-1, AC-3, AC-5
5.2 Guidance for Confidentiality	AC-3, AC-6, AC-21
5.3 Guidance for Privilege Management	AC-2, AC-11, AC-14, AC-22
5.4 Guidance for Multiple Replicas of Data	AC-1, AC-3, AC-4, AC-5, AC-17, AC-21
5.5 Guidance for Multi-tenancy	AC-1, AC-2, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
5.6 Guidance for Attribute and Role Management	AC-6, AC-1, AC-3
5.7 Guidance for Policies	AC-1, AC-3
5.8 Guidance for APIs	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-11, AC-14, AC-17, AC-21

AC-1: Access Control Policy and Procedures

AC-2: Account Management

AC-3: Access Enforcement

AC-4: Information Flow Enforcement

AC-5: Separation of Duties

AC-6: Least Privilege

AC-10: Concurrent Session Control

AC-11: Session Lock

AC-14: Permitted Actions without Identification or Authentication

AC-17: Remote Access

AC-21: Collaboration and Information Sharing

AC-22: Publicly Accessible Content

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.

c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.

d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.

b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.

c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.

e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.

c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

a. Access and use the service for its business purposes;
b. For SaaS, use underlying software as embodied or used in the service; and
c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency:________________________

Signature:________________________

Title:________________________

Date:________________________

Name of Vendor: AbsenceSoft

Signature: Max Cook

Title: Account Executive

Date: 6/28/2023

AbsenceSoft Response: This will need to be further negotiated. See legal modifications document attached with bid.

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: AbsenceSoft

~~Name of Agency:~~ ______

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☒
   No □

2. If yes to #1, does the restricted information include personal data?
   Yes ☒
   No □

3. If yes to #1, does the restricted information include non-public data?
   Yes ☒
   No □

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes □
   No ☒

5. Provide name and email address for the Department privacy officer:

   Name: Chris Snyder

   Email address: chris.s.snyder@wv.gov

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: Max Cook

   Email address: mcook@absencesoft.com

   Phone Number: 358-437-2544

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: MIS2300000005

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

[x] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

AbsenceSoft
Company

Max Cook
Authorized Signature

6/28/2023
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

NIST Special Publication 800-210

General Access Control Guidance for Cloud Systems

Vincent C. Hu
Michaela Iorga
Wei Bao
Ang Li
Qinghua Li
Antonios Gouglidis

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

COMPUTER SECURITY

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-210

General Access Control Guidance for Cloud Systems

Vincent C. Hu
Michaela Iorga
Computer Security Division
Information Technology Laboratory

Wei Bao
Ang Li
Qinghua Li
Department of Computer Science and Computer Engineering
University of Arkansas
Fayetteville, AR

Antonios Gouglidis
School of Computing and Communications
Lancaster University
Lancaster, United Kingdom

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

July 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-210
Natl. Inst. Stand. Technol. Spec. Publ. 800-210, 34 pages (July 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-210

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sp800-210-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This document presents cloud access control characteristics and a set of general access control guidance for cloud service models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). Different service delivery models require managing different types of access on offered service components. Such service models can be considered hierarchical, thus the access control guidance of functional components in a lower-level service model are also applicable to the same functional components in a higher-level service model. In general, access control guidance for IaaS is also applicable to PaaS and SaaS, and access control guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to access control requirements for its service.

Keywords

access control; access control mechanism; Cloud; cloud systems; policy; authorization ABAC; RBAC.

Acknowledgements

The authors, Vincent C. Hu and Michaela Iorga of the National Institute of Standards and Technology (NIST), Bao Wei, Ang Li, and Qinghua Li of Department of Computer Science and Computer Engineering University of Arkansas, and Antonios Gouglidis of School of Computing and Communications Lancaster University wish to thank Isabel Van Wyk, Jim Foti, and David Ferraiolo (NIST) who reviewed drafts of this document. The authors also gratefully acknowledge and appreciate the comments and contributions made by government agencies, private organizations, and individuals in providing direction and assistance in the development of this document.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Executive Summary

Cloud systems have been developed over time and conceptualized through a combination of software, hardware components, and virtualization technologies. Characteristics of the cloud, such as resource pooling, rapid elasticity, and pay-as-you-go services, accelerated its wide adoption by industry, government, and academia. Specifically, cloud systems offer application services, data storage, data management, networking, and computing resources management to consumers over a network (the internet in general). Despite the great advancements of cloud systems, concerns have been raised about the offered level of security and privacy. The importance of these concerns becomes more evident when considering the increasing number of users who have adopted cloud services.

This document presents cloud access control (AC) characteristics and a set of general access control guidance for cloud service models—IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). The main focus is on technical aspects of access control without considering deployment models (e.g., public, private, hybrid clouds etc.), as well as trust and risk management issues, which require different layers of discussions that depend on the security requirements of the business function or the organization of deployment for which the cloud system is implemented. Different service delivery models need to consider managing different types of access on offered service components. Such considerations can be hierarchical, such as how the access control considerations of functional components in a lower-level service model (e.g., networking and storage layers in the IaaS model) are also applicable to the same functional components in a higher-level service model (e.g., networking and storage in PaaS and SaaS models). In general, access control considerations for IaaS are also applicable to PaaS and SaaS, and access control considerations for IaaS and PaaS are also applicable to SaaS. Therefore, AC guidance for IaaS is applicable to PaaS and SaaS, and AC guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to access control requirements for its service.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 Purpose

Access control (AC) dictates how subjects (i.e., users and processes) can access objects based on defined AC policies to protect sensitive data and critical computing objects in the cloud systems. Considering the heterogeneity and remote nature of the cloud service models, AC and its general concepts should be revisited. In recent years, many works have focused on AC in cloud systems [23, 25, 26, 27]. However, these are primarily ad hoc solutions targeted at specific cloud applications and do not provide comprehensive views of cloud AC.

This document presents a set of general AC guidance for cloud service models independent from its deployment models because it requires another layer of access control that depends on the security requirements of the business function for which the cloud system is used. As shown in Figure 3, different cloud service models require the management of access to different components of the offered service. Since such cloud service models can be considered hierarchical, the AC considerations of functional components in a lower-level (according to Figure 2) service model (e.g., networking and storage layers in the Infrastructure as a Service (IaaS) model) are also applicable to the same functional components in a higher-level service model (e.g., networking and storage in Platform as a Service (PaaS) and Software as a Service (SaaS) models). In general, AC considerations for IaaS are also applicable to PaaS and SaaS, and AC considerations for IaaS and PaaS are also applicable to SaaS. Thus, AC guidance for IaaS is applicable to PaaS and SaaS, and AC guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to AC. For instance, an IaaS provider may put more effort into virtualization control, and in addition to the virtualization control, a SaaS provider needs to consider data security and the privacy of services it provides.

1.2 Scope

This document focuses on providing guidance for access control systems that are applicable to an organization's cloud implementation and security management. It does not prescribe the internal cloud access control standards that an organization may need in their enterprise systems or within a community other than the organization itself.

1.3 Audience

The intended audience for this document is an organizational entity that implements access control solutions for sharing information in cloud systems. This document assumes that readers are familiar with the cloud and access (authorization) control systems and have basic knowledge of operating systems, databases, networking, and security. Given the constantly changing nature of the information technology (IT) industry, readers are strongly encouraged to take advantage of other documents—including those listed in this document—for more current and detailed information.

1.4 Document Structure

The sections and appendix presented in this document are as follows:

- Section 1 states the purpose and scope of access control and cloud systems.
- Section 2 provides an overview of cloud access control characteristics.
- Section 3 discusses guidance for access control systems for IaaS (Infrastructure as a Service).
- Section 4 discusses guidance for access control systems for PaaS (Platform as a Service).
- Section 5 discusses guidance for access control systems for SaaS (Software as a Service).
- Section 6 discusses guidance for access control systems for inter- and intra-cloud operations.
- Section 7 concludes the document with future directions.

2 Cloud Access Control Characteristics

With the support of different service models, cloud systems can provide a wide range of services to its end-users, developers, and system administrators. Cloud systems have been developed over time and conceptualized through a combination of software, hardware components, and virtualization technologies. Characteristics of the cloud, such as resource pooling, rapid elasticity, and pay-as-you-go services, have accelerated its wide adoption by industry, government, and academia. Specifically, cloud systems offer application services, data storage, data management, networking, and computing resources management to consumers[1] over a network (and the internet in general). Examples of popular cloud applications include web-based email services (e.g., Google's Gmail, Microsoft's Office 365 Outlook), data storage (e.g., Google Drive, Microsoft's OneDrive, Dropbox) for end users, and consumer relationship management and business intelligence systems (e.g., Customer Relationship Management (CRM) Cloud, Workday) for business management. Despite the great advancements of cloud systems, concerns have been raised about offered levels of security and privacy. The importance of these concerns becomes more evident when considering the increasing number of users that have adopted cloud services [1].

NIST publications defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2,3]. Cloud deployment models (e.g., public cloud, private cloud, community cloud, hybrid cloud, etc.) are configured by the scope of cloud users, services, and resources based on service requirements, they may be deployed privately, hosted on the premises of a cloud consumer or provider's dedicated infrastructure, or hosted publicly by one or more cloud service providers. The system may be configured and used by one consumer or a group of trusted partners or support multi-tenancy and be used publicly by different end users who acquire the service. Depending on the type of cloud deployment model, the cloud may have limited private computing resources or access to large quantities of remotely accessed resources. The different deployment models present a number of trade-offs in how consumers can control their resources as well as the scale, cost, and availability of those resources [4]. As depicted in Figure 1, the architecture of a cloud system is composed, in general, by layers of functions:

- VM (Virtual Machine), including:
  - Applications
  - Application Programming Interface (API)
  - Operating System (OS)
- Hypervisor
- Storage
- Networking
- Hardware

[1] Cloud service **consumers** play various roles in the consumption of the cloud services, e.g. system planners, program managers, technologists. **End-users** are individuals using cloud services as direct clients of a cloud provider, of a cloud consumer leveraging a cloud service, or individuals employed by a cloud consumer. A **user** is in a generic term associated with any entity using the cloud service. Depending on scenario, the user can be referred as either cloud service consumer or end-user where applicable.

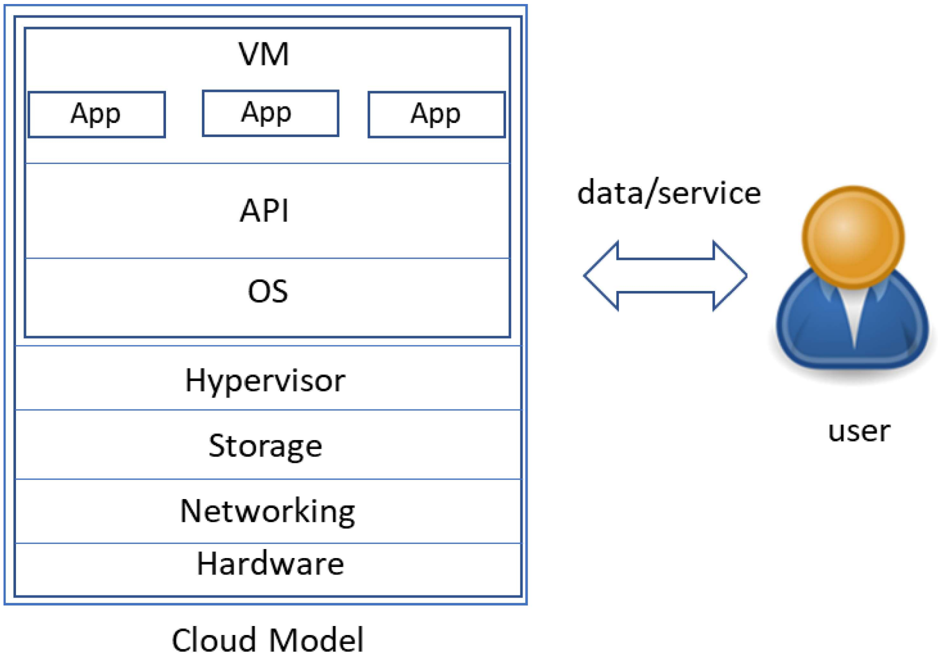


Figure 1: The general architecture of a cloud system

A cloud service can provide access to software applications, such as email or office productivity tools (i.e., the Software as a Service, or SaaS, service model); an environment for consumers to build and operate their own software (i.e., the Platform as a Service, or PaaS, service model), or network access to virtualized computing resources such as processing power and storage (i.e., the Infrastructure as a Service, or IaaS, service model). The different service models have different strengths and are suitable for different consumers and business objectives [4], as illustrated in Figure 2, the arrows show the support relations between models.

A cloud system that deploys the SaaS model can be accessible over a network by an end user utilizing various client devices (e.g., a thin client interface, such as a web browser, for accessing a web-based email application) or via a program with the correct set of interfaces whose execution would enable communication with a cloud application. In the SaaS model, an application user is limited to user-specific application configuration settings and does not manage or control the underlying cloud infrastructure, which typically includes the network, servers, operating systems, storage, or individual applications.

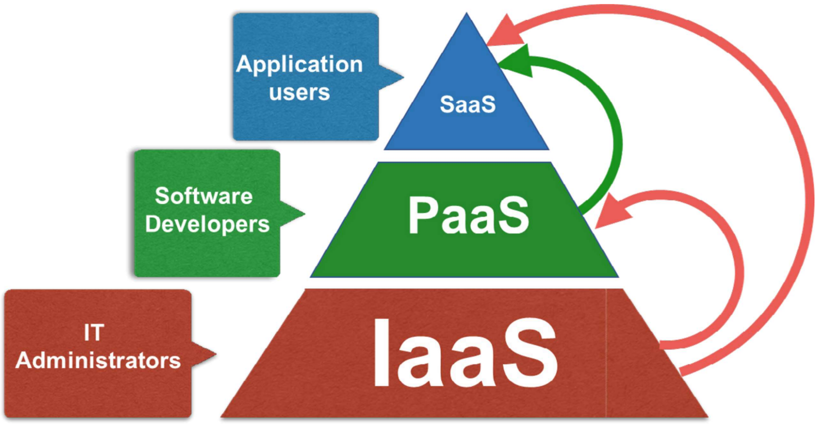


Figure 2: The service models of a cloud system

The PaaS model in a cloud system allows developers to create and deploy applications onto the cloud infrastructure using programming languages, libraries, services, and tools. A software developer does not manage or control the underlying cloud infrastructure but has control over the deployed applications (software) and, possibly, configuration settings for the application-hosting environment.

When analyzing the responsibilities between consumer and cloud service providers for protecting cloud data, it is not always clear-cut, if an IaaS system provides only the computation resources, or offers also the virtualized storage, and network resources to consumers for deploying and running arbitrary software, including operating systems and applications. The consumer may in turn have control over virtual storage, virtualized network components, and the ability to deploy their own VMs and applications given access provisioned by the cloud service provider.

The shared responsibility of access control needs to be considered in the PaaS and SaaS model [42]; For example software developers might need to access data in systems provided by PaaS for their developmental needs, and internal application users (i.e., users that need to access the application system data) might need to access application system data that is managed by the applications. In general, for PaaS, consumer software developers might share access control responsibilities with cloud service providers; for SaaS, internal application users might share such responsibilities with cloud service providers.

Note that unless there is express prior approval from the consumer, a PaaS or SaaS provider must manage access control with the IaaS provider and the consumer (if it is not also the IaaS provider). If the consumer approves, the provider should inform the consumer of its intention to store the specified data in the IaaS provider, where it will be accessed as well as the extent to which the data can be accessed by the IaaS provider, foreign entities, or authorities. A public consultation and hearing process must then be conducted before a decision is made.

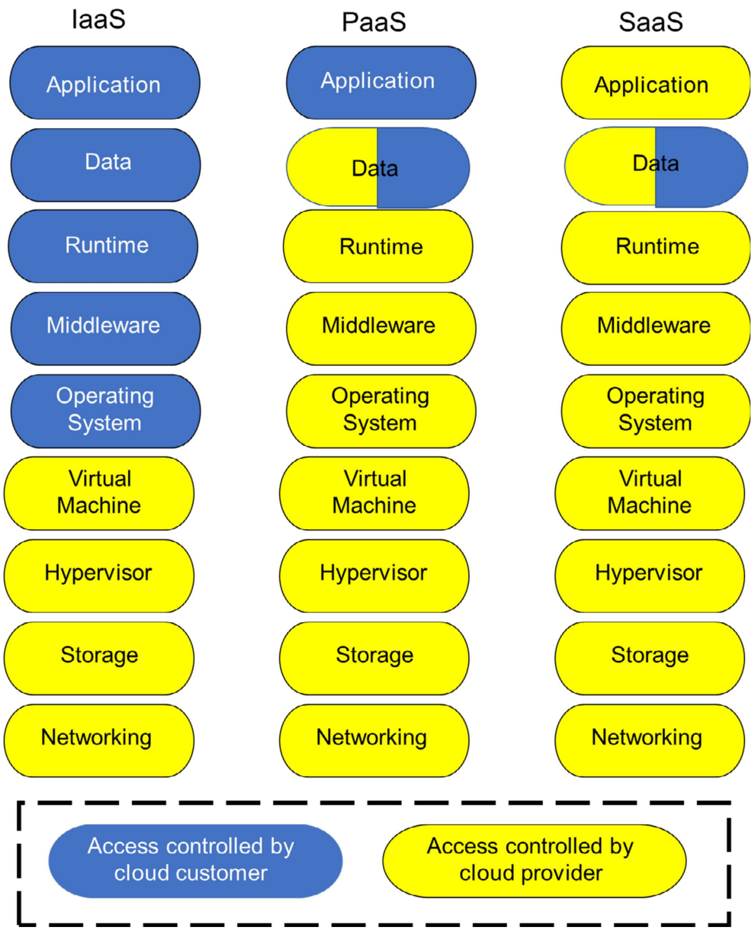


Figure 3: Accesses controlled by the cloud service provider and the consumer

The five essential characteristics that challenge AC system design are summarized as follows [2]:

1. *Broad network access*: Cloud services are available over the network and accessible through standard mechanisms that promote use by heterogeneous thick and thin client platforms (e.g., mobile phones, tablets, laptops, workstations). This raises security concerns with regard to network access. For example, denial of service (DoS) attacks can be launched against a cloud system, rendering its resources unavailable to legitimate users. Thus, AC for network access should be managed.

2. *Resource pooling*: The computing resources of a cloud system (e.g., storage, memory, processing, network bandwidth) are pooled to serve multiple consumers using a multi-tenant model (i.e., a single instance of the software and its supporting infrastructure serves multiple consumers) through different physical and virtual resources, each dynamically assigned and reassigned according to consumer demands. Information may be leaked if the resource allocated to a consumer can be accessed by another co-located consumer or if the allocated resource, such as memory, is not wiped before being reallocated to another consumer. There is also a sense of location independence in that the consumer generally has no control over or knowledge of the exact location of the provided resources. Location may be specified at a higher level of abstraction (e.g., country, state, data center) that brings

security concerns. Therefore, methods for implementing resource pooling while ensuring the isolation of shared resources should be considered in the AC design.

3. *Rapid elasticity*: Cloud services can be elastically provisioned and released—automatically, in some cases—to rapidly scale outward and inward commensurate with demands. To the consumer, services available for provisioning often appear to be unlimited and appropriated in any quantity at any time and are supported by adding new *virtual machines* (VMs) with specified computing resources. A challenge for AC design involves the capability to rapidly verify the security of new VMs and determine whether the newly added VMs are qualified to execute a specific task.

4. *Measured service*: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active end user accounts). Resource usage is monitored, controlled, and reported to provide transparency to both the provider and consumer of the utilized service. To maintain resource usage, cloud consumers should be authorized to review but not to modify their own metering data since this could lead to the falsification of payments required for cloud services. Thus, it is reasonable for AC to consider the protection of metering data.

5. *Data sharing*: Sharing information among different organizations is not a trivial task since a cloud system needs to meet the same security requirements of organizations to achieve that. To facilitate data sharing, concepts such as trust of federated identities and AC attributes need to be considered, and building that trust is paramount. In this document, it is assumed that trust and federated identities/attributes are already established, and further discussion on that topic will be considered in another document. Regardless of the service model, consumers are entitled to be responsible for the security of their cloud-based data and, implicitly, of who has access to it [5]. For this reason, data is never controlled by cloud service providers but rather always stays with the cloud consumers. (The exception to this is log data, but consideration should still be given to how privacy and security is affected by such data.) Although a cloud service provider might become the custodian of consumers' data, it should not have access to that data. If a consumer's data is not encrypted, then cloud administrators might be able to read it. In such a case, the consumer's data should be identified (by the provider's access privileges to the data) and red-flagged as accessible by the service provider, and the consumer should be informed immediately.

Guidance for AC system for each cloud service model, as described in Sections 3, 4, and 6 of this document, can be further extended to system requirements by referring to the AC control elements listed in NIST SP 800-53, Revision 4, *Security and Privacy Control for Federal Information Systems and Organizations* [6] based on the operation requirements of the cloud service. Appendix A maps the guidance to the AC control elements listed in the NIST SP 800-53, Revision 4.

3 Access Control Guidance for IaaS

IaaS is the cornerstone of all cloud services that offer computing and storage through a network such as the internet. Through virtualization technology, IaaS enables end users to dynamically allocate computing resources by instantiating new *virtual machines* (VMs) or releasing them based on their requirements. A VM is a software container that behaves like a physical machine with its own operating system (OS) and virtual resources (e.g., CPU, memory, hard disk, etc.). Leasing VMs is more cost-effective than purchasing new physical machines. The virtualization technology is composed of VMs and a *hypervisor,* as shown in Figure 1. VMs are managed by the hypervisor, which controls the flow of data and instructions between the VMs and the physical hardware. On the consumer side, system administrators are usually the major users of IaaS services since IaaS services are flexible to configure resources (e.g., network, data storage).

Cloud virtualization adds additional security management burdens by introducing security controls that arise from combining multiple VMs onto a single physical computer, which can have potential negative impacts if a security compromise occurs. Some cloud systems make it easy to share information among VMs by, for instance, allowing users to create multiple VMs on top of the same hypervisor if multiple VMs are available. However, this convenience can also become an attack vector since data leakage could occur among VMs. Additionally, virtualized environments are transient since they are created and vanish frequently, thereby making the creation and maintenance of necessary security boundaries more complex.

As shown in Figure 3, data in the middleware, data, applications, and OS layers is owned and controlled by the consumer. The IaaS system and the consumer need to ensure that access to the data is not granted to IaaS system administrators or any other IaaS consumers in these layers unless any of them are permitted. IaaS administrators are responsible for access control on the virtual machine, hypervisor, storage, and networking layers and should consider Sections 3.1 to 3.5 below.

3.1 Guidance for Network

The network is shared among IaaS consumers, and it is important to secure the network traffic and the cloud's environment from being exploited by unauthorized consumers. Thus, access control for network boundaries and allowlists for network communications are required and may be applied through, for example, dedicated virtual local area networks (VLANs) leveraging automated access control lists (ACLs). Using the Institute of Electrical and Electronics Engineers (IEEE) 802.1Q VLAN tagging for network traffic with a cloud data center will result in routing only traffic tagged with the server's unique VLAN identifier to or from that server [7].

3.2 Guidance for Hypervisor

A hypervisor plays an important role in the security of the entire virtualized architecture since it manages consumer loads and guest operating systems (OSs),[2] creates new guest OS images, and controls hardware resources. The security implications of actions like managing guest OS and hardware resources means that access to the hypervisor should be restricted to authorized cloud administrators only. Otherwise, a cloud end user could potentially obtain a VM from the cloud

[2] An OS that is secondary to the originally installed OS.

service provider and install a malicious guest OS that compromises the hypervisor by gaining unauthorized access to and altering the memory of other VMs [8]. Moreover, an attacker in a VM with lower access rights may be able to escalate their access privilege to a higher level by compromising the hardware resources allocation within the hypervisor [9]. Protecting the hypervisor from unauthorized access is therefore critical to the security of IaaS services.

3.3 Guidance for Virtual Machines

VMs that are created by different end users allow resources to be shared among multiple end users. In such cases, it must be ensured that no application from one VM can directly access other VMs since covert channels [10, 11] may leak information between VMs by accessing shared physical resources (e.g., memory). Similarly, although the ability to copy and paste information between VMs via the clipboard is a convenient feature, such a capability could be made available on other VMs running on the same hypervisor and thus introduce an attack vector (i.e., information can be leaked to other VMs through the clipboard). Organizations should have policies regarding the use of shared clipboards.

Isolation between VMs is necessary to keep VMs running independently of each other, and quotas on VM resource usage should be regulated so that a malicious VM can be prohibited from exhausting computation resources. If a malicious application consumes the majority of computation resources, legitimate applications may not be able to obtain sufficient resources to perform their operations. Moreover, end users might terminate the execution of their tasks before they are finished. The state and data of the current VM would then be saved as a guest OS image, and when the task is resumed, the VM might be migrated from a different hypervisor. In such scenarios, guest OS images must be protected from unauthorized access, tampering, or storage. Furthermore, VMs that are not active may also store sensitive data. Monitoring access to the sensitive data in inactive VMs should be considered.

3.4 Guidance for APIs

There are several popular open-source platforms for deploying an IaaS system [12, 13, 14]. These solution platforms enable APIs to manage access control of VMs, hypervisors, and networks (note that a consumer cannot control hypervisors and networks in a multi-tenant environment unless it is a private cloud). For example, [14] consists of control components, including API, communication, lifecycle, storage, volume, scheduler, network, *API server* for managing AC policies for hypervisors, and *network controller* for constructing network bridges and firewall AC rules. The lack of monitoring AC within these APIs might result in unenforced or wrongly enforced AC policies by the hypervisors, VMs, and networks. Thus, a service for monitoring the AC APIs in cloud platforms should also be taken into consideration.

3.5 Recommendations for IaaS Access Control

As shown in previous sections, the security of an IaaS cloud system is heavily dependent on the virtualization (hypervisor). One of the most widely adopted solutions for protecting them is a *virtualization management system* [15], which lies between the underlying hardware and the hypervisor. The virtualization management system enforces AC on both hypervisors and VMs in different ways. Virtualization management systems enforce different levels of access on different

users. Some users are given read-only access to the administrative interface of a guest OS; some are allowed to control particular guest OSs; and some are given complete administrative control. There are existing solutions for providing AC for hypervisors and VMs. For example, the approach in [16] secures the hypervisor against control hijacking attacks by protecting its code from unauthorized access and offering isolation of VMs with the flexible security of mandatory access control (MAC). To enforce AC on interoperations, a service level agreement should be designed to include appropriate control to secure external interoperations. Other isolation mechanisms [17, 18] are helpful in ensuring the security of internal interoperations.

Guideline rules for IaaS AC policy that consider the main elements in AC (i.e., subject, object, and operation) are listed in Table 1. While each row indicates a possible AC rule, the AC policy designer should ultimately decide whether the decision in each rule is permitted or denied based on system requirements. For example, if an authorized IaaS end user requires the use of cloud services, a login operation in the hypervisor for the end user should be granted; otherwise, it should be denied.

Table 1: Potential policy rules expressed by Subject, Operation, Object for IaaS AC policy

Subjects	Operations	Objects	Environment Conditions
IaaS end user	Login, Read, Write, Create	Hypervisor	Time, Location, Security impact level etc.
IaaS end user	Read, Write, Create	VMs	Time, Location, Security impact level etc.
VM	Write	Hypervisor	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs within the same host	Time, Location, Security impact level etc.
VM	Read, Write, Create	Guest OS images	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs from different hosts but within the same IaaS provider	Time, Location, Security impact level etc.
VM	Read, Write	Other VMs from different IaaS providers	Time, Location, Security impact level etc.
Hypervisor	Read, Write, Create	Guest OS images	Time, Location, Security impact level etc.
Hypervisor	Read, Write	Hardware resources	Time, Location, Security impact level etc.
Hypervisor	Read, Write, Create	VMs	Time, Location, Security impact level etc.

4 Access Control Guidance for PaaS

PaaS is a platform that provides a framework for developers to create and deploy customized applications. As shown in Figure 3, security assurance considerations include some and all below the data level, and during the application development process lifecycle should be offered by the PaaS provider. The primary focus of AC in the PaaS model is to protect data during runtime, which is managed by middleware and OS. PaaS systems are primarily concerned with developing, deploying and operating customer applications. The security and privacy offered by the PaaS provider protect the applications and data from potential leaks through a covert channel introduced by unsecure shared memory. Therefore, enforcing AC over data during runtime in the PaaS is critical for the security of PaaS services.

The PaaS system administrator is responsible for the access control of runtime, middleware, OS, virtual machine, hypervisor, storage, and networking layers, as described by the guidance in Sections 4.1 to 4.3 below.

4.1 Guidance for Memory Data

The PaaS system permits users to deploy tasks in a provider-controlled middleware and host OS, which may be shared with other PaaS applications. As such, PaaS typically leverages OS-based techniques (e.g., Linux Containers and Docker for isolating applications) [19]. However, numerous existing memory-related attacks can compromise sensitive application-related data by hacking through the shared OS memory in PaaS [20]. Thus, AC for OS memory, such as AC of different processes on top of processor caches [21], should be considered.

4.2 Guidance for APIs

As the PaaS system allows cloud developers to build applications on top of the platform, APIs should control the scope of each user's application such that user data remains inaccessible between different applications. In addition, packaged APIs can be serviced as microservices in a PaaS cloud. A centralized architecture for provisioning and enforcement of access policies governing access to all microservices is required due to the sheer number of services needed for service composition to support real-world business transactions (e.g., consumer order processing and shipping). Since each of the microservices may be implemented in a different language, policy provisioning and computation of access decisions may require the use of an authorization server [22].

4.3 Recommendations for PaaS Access Control

An efficient method should be established for protecting memory data by flushing processor caches during context switches. However, in order to avoid significant performance degradation, only highly sensitive memory data should be flushed.

To handle access control for multiple replicas of data, a method to manage the central AC policy system should be introduced. Thus, once the data within a PaaS provider is duplicated across PaaS providers, any change in the policy should result in an appropriate update to the central AC policy

system. Moreover, the AC policy related to the replicated data in other PaaS providers should be synchronized accordingly based on an AC policy in the central system.

Guideline rules for PaaS AC policy are listed in Table 2 with respect to the three basic elements of AC (i.e., subject, object, and operation). Each row indicates a possible AC rule, but the AC designer should decide whether access should be granted or denied based on the system requirements. For example, if a user of an application needs to access memory data related to their application, permission to read memory data will be granted. However, access to that memory data will be denied to other users.

Table 2: Potential policy rules expressed by Subject, Operation, Object for PaaS AC policy

Subjects	Operations	Objects	Environment Conditions
Application user	Read	Memory data	Time, Location, Security impact level etc.
VM of a hosted application	Read, Write	Other applications' data within the same host	Time, Location, Security impact level etc.
Application developer	Create, Read, Write	Middleware data, memory data	Time, Location, Security impact level etc.
Cloud service provider	Replicate	Application-related data	Time, Location, Security impact level etc.

5 Access Control Guidance for SaaS

In SaaS, a cloud service provider delivers an application as a service to end users through a network such as the internet. Thus, there is no need for users to install and execute applications locally on their own computers. As shown in Figure 4, multiple applications and users can be supported simultaneously by the cloud system to share common resources, including applications and underlying databases.

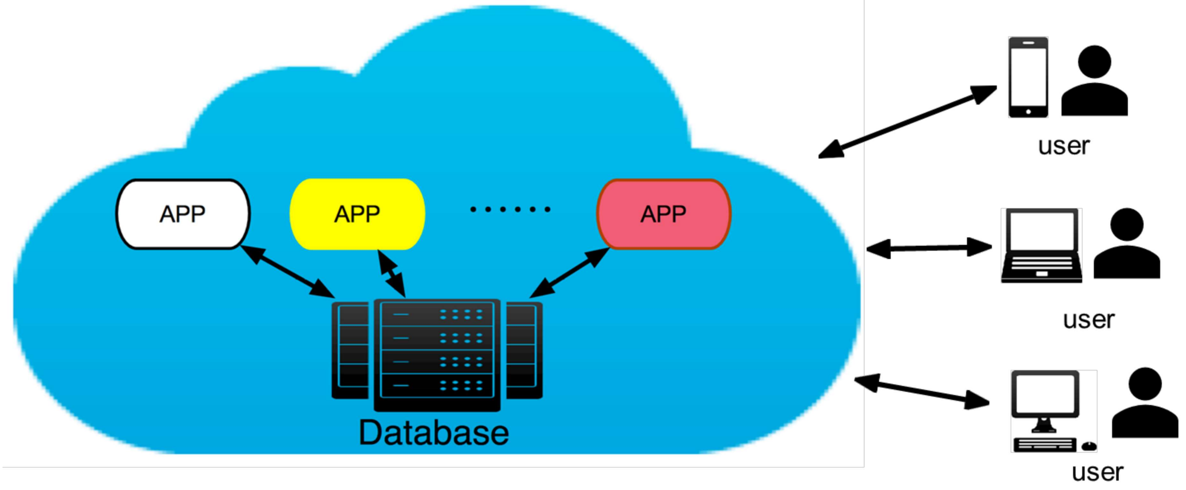


Figure 4: Multiple applications and users of an SaaS provider

If a developer deploys a third-party application, data in that application and other unrelated applications might be stored in the cloud system. End users have to rely on the security and privacy offered by the cloud service provider to protect their data from unauthorized access introduced by those unrelated applications. Note that data managed by the application layer is owned and controlled by the consumer. The SaaS system and consumer need to ensure that access to application data in these layers is not granted to the SaaS system administrator, consumers, or other users unless they are trusted. SaaS administrators are responsible for the access control of all operation layers except for the consumer's application data as shown in Figure 3 and should consider the guidance in Sections 3, 4, and 5.1 to 5.4.

5.1 Guidance for Data Owner's Control

A data provider is the creator or source of application data owned by consumer organizations. Application data is typically stored in the SaaS service provider's database. How a data provider manages access to its data is a challenge. Example questions to be addressed are related to data retention by the provider (e.g., where data is kept and for how long) and whether the provider has any permission to determine access rights to the data it hosts. If a data provider has the capability to determine access rights on data it holds, consideration should be given to ensure that an up-to-date AC policy is always enforced within the SaaS system.

5.2 Guidance for Confidentiality

In the application deployment model, the integrity of sensitive data residing within the data owner's domain must be protected. Protection mechanisms for application data include data

encryption schemes by which data can be encrypted through certain cryptographic primitives, and decryption keys will only be disclosed to authorized users [23]. For such enforcement, attribute-based access control (ABAC) [24] and attribute-based encryption (ABE) schemes can be used to control access to SaaS data [23, 25, 26, 27, 28] since these schemes can use the identity of users through attributes to manage, encrypt, and decrypt application data. However, considering the high volume of data in the SaaS model, the involved encryption and decryption significantly reduce performance. Hence, when encryption is used, consideration should be given to ensure the confidentiality of data while offering good performance.

5.3 Guidance for Privilege Management

In addition to AC enforcement, privilege management involves adding, removing, and changing the privileges of a subject. It is crucial to design a flexible or real-time mechanism for assigning and revoking privileges to maintain the usability of the SaaS service [29].

5.4 Guidance for Multiple Replicas of Data

To maintain high availability, the cloud service provider may replicate data at multiple locations, even across countries. Thus, it is important to make sure that all data replicas are protected under the same AC policy. In other words, the same AC policy for the replicated data object should be populated to all hosts that process the same data. The technology for policy synchronization upon changes must also be considered for inclusion.

5.5 Guidance for Multi-tenancy

The SaaS system introduces additional considerations with regard to the management of access to applications. An immediate necessity is to focus on users' access to applications. The access rights are granted to end users through AC policies based on predefined attributes or roles. This can be specified by attribute-based access control (ABAC) policy models [30, 31], role-based access control [32] (RBAC), and context-based access control [33] (CBAC).

The SaaS model is a typical, multi-tenancy platform that supports multiple end users simultaneously accessing an application with the data of different users' applications residing at the same location. Exploiting vulnerabilities in the application or injecting code into the SaaS system might expose data to other users [34]. Therefore, strategic planning should be given to implementing multi-tenancy while segregating data from different users' applications during the design of an AC system.

5.6 Guidance for Attribute and Role Management

In the SaaS system, attribute and role-based AC management employs policies and predefined roles to manage access rights to applications and underlying databases. The primary challenge of deploying attribute or role-based AC management is reaching an agreement on what types of attributes or roles should be used and what should be considered when designing the AC systems [35]. If the set of considered attributes or roles is too small, flexibility will be reduced. However, if the number of attributes or roles is too large, the complexity of policies will increase.

5.7 Guidance for Policies

SaaS applications provide application-specific access control configurations for different user applications, and in this case, user policies for each application are enforced by the SaaS provider. This configuration does not support collaboration between the SaaS provider and the consumer's access control infrastructure. For example, while large organizations often employ on-premises access control systems for managing their users centrally and efficiently, SaaS applications typically provide organizations with an AC configuration interface for managing AC policies, which forces the AC policies to be stored and evaluated on the SaaS provider's side. This approach might result in disclosing sensitive data required for evaluating the AC policies to the SaaS provider. Therefore, methods for enforcing authorization in the SaaS provider while not disclosing sensitive access control data to the SaaS provider should be considered. Federated authorization [36] is an efficient technique that utilizes a middleware layer to transfer the management of access control policies from the SaaS provider to the consumer side and enforce policies on the SaaS applications without disclosing sensitive data required for evaluating the policies.

5.8 Guidance for APIs

An API in the SaaS model serves as an interface between the cloud server and its users. The API should be designed to protect against both accidental and malicious attempts to circumvent any AC policy. Applications for organizations and third parties often build upon the APIs, which introduce the AC complexity of the new layered API. For example, if the APIs do not require memory access for their tasks, then the AC policy for the APIs should enforce the non-memory access. Additionally, AC policies should be specified to manage the authorization process for web APIs. For example, when APIs connect through SOAP and REST protocols, the AC should control whether to allow end users to interface between Microsoft or non-Microsoft tools and technologies. For authorized API connections through Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) protocols, the AC should grant all related access requested by the protocols. For unauthorized API connections through these protocols, no access or partial access should be granted by the AC.

5.9 Recommendations for SaaS Access Control

With regard to multi-tenancy, authorization may be enforced using a *centralized*, *decentralized*, or *hybrid* authorization system. In a centralized authorization system, the SaaS provider manages a central authorization database for every end user and their accounts [37]. In a decentralized or hybrid authorization system, individual tenants are responsible for all or part of the authorization process. Note that different tenants may require different systems. Considering the attributes or roles of tenants is crucial when selecting the most suitable system. There are many ways to specify attributes or roles, such as in ABAC and RBAC models [31,32]. Attributes or roles must be well-designed and take into account hierarchy relationships when implementing AC policies for different tenants.

Authorization federation [36] is an efficient way to enforce AC policies in the SaaS provider. A generic middleware architecture that incorporates access control requirements from consumers and handles local and remote attributes or roles can be used to extend and shift AC policy management from the SaaS provider to the consumer side. This approach centralizes consumer AC policy

management and lowers the required trust in the SaaS provider. In addition, the AC for VM-supporting federation operations should also be specified (e.g., an end user may create a VM to run different applications). Within the VM of the same host, one application may need to access the application code of other applications to fulfill its task. Unlike the PaaS architecture, where consumers can fully manage the design, testing, and development of the software, SaaS consumers have limited control of the applications hosted in the cloud server.

To achieve the application data owner's control, a security class agreement (SCA) [28] may be of use. SCA is mutually agreed upon by both the data provider of PaaS subscribers and the PaaS service provider and is used for defining the security class of data providers. Multiple replicas of the same data share the same security level as its data provider. This means that given data from a particular data provider, the security class for multiple replicas of the data should be identical. As a result, the host within the PaaS service that is qualified for executing the access request can be determined by referring to the SCA. The data provider can manage access to its data by specifying security classes for the SCA to keep the data provider and the cloud host synchronized in determining the access right of data. For example, in a Bell-LaPadula model [38], assuming a patient's report is written by a doctor with confidential clearance, the report can only be read by a host with the same or higher security clearance. Additionally, when multiple data sources that are not intended to be accessed in the same cloud system are accessed, the privacy of data should not be leaked due to different security classes of these data sources and their data in the SCA. However, due to the high computation complexity of encryption and decryption, cryptographic schemes should be carefully designed to maintain the performance of cloud systems while protecting data confidentiality.

A privilege management infrastructure (PMI) [39] can be employed to dynamically manage assigning and revoking privileges through the use of attributes or role specification certificates in the PaaS model. PMI specifies the privileges for different users and links the privileges with different attribute or role specification certificates, which contain different attribute or role assignments to enforce privilege management.

To handle access control of multiple replicas of data, a method to manage the central AC policy system should be introduced. Thus, once the data within an SaaS provider is duplicated across SaaS providers, any change in the policy should result in an appropriate update to the central AC policy system. Moreover, the AC policy related to the replicated data in other SaaS providers should be synchronized accordingly based on an AC policy in the central system.

Guideline rules for SaaS AC policy are listed in Table 3. The AC designer should decide whether access in each rule is permitted or denied based on the system requirements. For example, during federation operation, VM read/write to other application code within the same host is permitted; otherwise, it is denied.

Table 3: Potential policy rules expressed by Subject, Operation, Object for SaaS AC policy

Subjects	Operations	Objects	Environment Conditions
Application user	Read, Write	Application-related data	Time, Location, Security impact level etc.
Application user	Read	Memory	Time, Location, Security impact level etc.
Application user	Execute	Application	Time, Location, Security impact level etc.
Application user	Read, Write	Application data	Time, Location, Security impact level etc.
Application user	Execute	Application code	Time, Location, Security impact level etc.
VM of a hosted application	Execute	Other application code within the same host	Time, Location, Security impact level etc.

6 Access Control Guidance for Inter- and Intra- Operation

In general, collaboration (i.e., two or more systems that work together as a combined system) in the context of the cloud may lead to a seamless exchange of data and services among various cloud infrastructures. There are two types of collaborations: *inter-operation* and *intra-operation*. Inter-operation refers to the capability of using multiple cloud infrastructures. For example, as shown in Figure 5, a consumer may purchase IaaS services from two different cloud service providers, *Cloud A* and *Cloud B*, and the collaboration between them should be allowed due to data processing requirements.

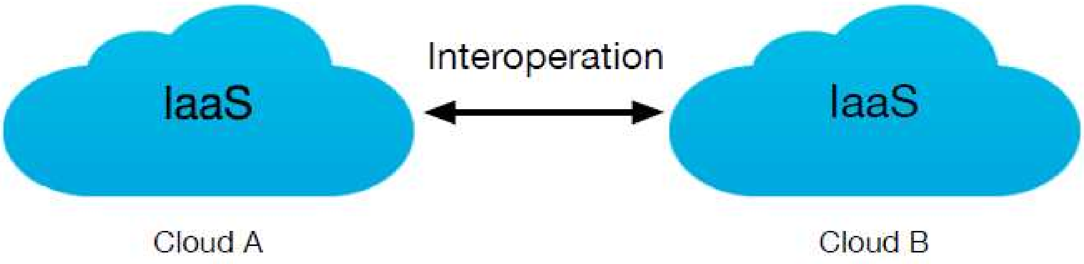


Figure 5: The external collaboration (inter-operation) between different Clouds

Intra-Operation

With regard to intra-operation, two scenarios on intra-operation can be presented as derived from Figure 6. First, a consumer may own multiple VMs in a single cloud host (e.g., *VM A* and *VM B*), and communication among those VMs may be required. Second, a consumer may rent multiple hosts within the same IaaS service, and collaboration among VMs from these different hosts may be required (e.g., an inter-operation between *VM B* and *VM C*).

For intra-operation, the AC policy should enable the operations of VMs for the same consumer to access each as needed during the collaboration period and disable access when the collaboration period ends. There are two primary cases in intra-operation: inter-host case (i.e., VMs from different cloud hosts are operating collaboratively) and intra-host case (i.e., VMs are from the same cloud host and must exchange data and services). Additionally, for some applications, VMs might be distributed in multiple host computers, so the AC policy should cover both intra-host and inter-host cases.

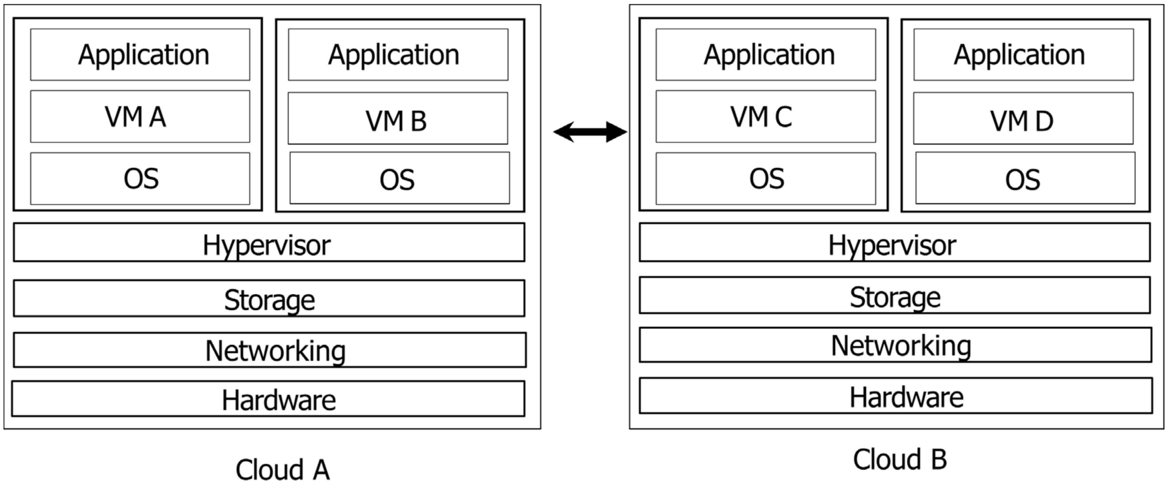


Figure 6: The internal collaboration (intra-operation) within the same cloud

Inter-Operation

There is the possibility that inconsistent management of access elements lead~~s~~ to incorrect access control policy integration for inter-operation. For instance, different cloud service providers using different sets of subject attributes for AC may cause potential conflicts or leak access permissions [40]. Attributes with the same name may result in different privileges when switching providers. Enforcing AC among different cloud service providers without incurring conflicts or blocks of privilege for individual users/VMs is a challenge. This would require examining how to achieve secure inter-operation among the cloud service providers [1], such as in cross hybrid environments. Some cloud AC systems adopt centralized mechanisms to create global AC policies that manage policy integration among different cloud service providers [41]. However, the cloud inter-operation is transient and, thus, inefficient to manage global AC policies as frequent updates for individual cloud AC policies.

7 Conclusions

This document presents an initial step toward understanding access control (AC) challenges in cloud systems by analyzing the AC considerations in all three cloud service delivery models—IaaS, PaaS, and SaaS. Essential characteristics that would affect the cloud's AC design are also summarized, such as broad network access, resource pooling, rapid elasticity, measured service, and data sharing. Various guidance for AC design of IaaS, PaaS, and SaaS are proposed according to their different characteristics. Recommendations for AC design in different cloud systems are also included to facilitate future implementations. Additionally, potential policy rules are summarized for each cloud system. However, many issues remain open, such as AC management across different devices and platforms, as well as new challenges that have yet to emerge with the wide adoption of the cloud.

References

[1] Gouglidis A, Mavridis I, Hu VC (2014) Security policy verification for multi-domains in Cloud systems. *International Journal of Information Security* 13(2):97-111. https://doi.org/10.1007/s10207-013-0205-x

[2] Mell PM, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-145. https://doi.org/10.6028/NIST.SP.800-145

[3] Liu F, Tong J, Mao J, Bohn R, Messina J, Badger ML, Leaf D (2011), NIST Cloud Computing Reference Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-292. https://doi.org/10.6028/NIST.SP.500-292

[4] Badger ML, Grance T, Patt-Corner R, Voas JM (2012) Cloud Computing Synopsis and Recommendations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-146. https://doi.org/10.6028/NIST.SP.800-146.

[5] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

[6] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[7] Bartock MJ, Souppaya MP, Scarfone KA, Carroll D, Masten R, Scinta G, Massis P, Prafullchandra H, Malnar J, Singh H, Yeluri R, Shea T, Dalton M, Dukes A, Phoenix C Swarts B (2018) Trust Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments. (National Institute of Standards and Technology, Gaithersburg, MD), Preliminary Draft NIST Special Publication (SP) 1800-19B. Available at https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud

[8] Szefer J, Lee RB (2011) A case for hardware protection of guest VMs from compromised hypervisors in cloud computing. *2011 31st International Conference on Distributed Computing Systems Workshops (ICDCSW)* (IEEE, Minneapolis, MN), pp 248–252. https://doi.org/10.1109/ICDCSW.2011.51

[9] Krutz RL, Vines RD (2010) *Cloud security: A comprehensive guide to secure cloud computing* (Wiley Publishing, Indianapolis, IN).

[10] Wu J, Ding L, Wu Y, Min-Allah N, Khan SU, Wang Y (2014) C2detector: a covert channel detection framework in cloud computing. *Security and Communication Networks* 7(3):544–557. https://doi.org/10.1002/sec.754

[11] Rushby J (1992) Noninterference, transitivity, and channel-control security policies. (SRI International, Menlo Park, CA), Technical Report CSL-92-02. Available at http://www.csl.sri.com/papers/csl-92-2/

[12] Change ATC, Foster JL, Hall DK (1987) Nimbus-7 SMMR derived global snow cover parameters. *Annals of Glaciology* 9:39-44. https://doi.org/10.3189/S0260305500200736

[13] Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, Zagorodnov D (2009) The Eucalyptus open-source cloud-computing system. *9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'09)* (IEEE, Shanghai, China), pp 124-131. https://doi.org/10.1109/CCGRID.2009.93

[14] Sefraoui O, Aissaoui M, Eleuldj M (2012) OpenStack: toward an open-source solution for cloud computing. *International Journal of Computer Applications* 55(3):38-42. https://doi.org/10.5120/8738-2991

[15] Scarfone KA, Souppaya MP, Hoffman P (2011) Guide to Security for Full Virtualization Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125. https://doi.org/10.6028/NIST.SP.800-125

[16] Wang Z, Jiang X (2010) Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. *2010 IEEE Symposium on Security and Privacy (SP)* (IEEE, Berkeley/Oakland, CA), pp 380–395. https://doi.org/10.1109/SP.2010.30

[17] Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D (2008) TVDc: managing security in the trusted virtual datacenter. *ACM SIGOPS Operating Systems Review* 42(1):40–47. https://doi.org/10.1145/1341312.1341321

[18] Sailer R, Valdez E, Jaeger T, Perez R, Doorn LV, Griffin JL, Berger S (2005) sHype: Secure hypervisor approach to trusted virtualized systems. (IBM Research Division, Yorktown Heights, NY) IBM Research Report RC23511. Available at https://domino.research.ibm.com/library/cyberdig.nsf/papers/265C8E3A6F95CA8D85256FA1005CBF0F/$File/rc23511.pdf

[19] Zhang Y, Juels A, Reiter MK, Ristenpart T (2014) Cross-tenant Side-channel Attacks in PaaS Clouds. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (ACM, Scottsdale, AZ), pp 990–1003. https://doi.org/10.1145/2660267.2660356

[20] Osvik DA, Shamir A, Tromer E (2006) Cache attacks and countermeasures: the case of AES. Pointcheval D. (eds) Topics in Cryptology – CT-RSA 2006. CT-RSA 2006. Lecture Notes in Computer Science 3860 (Springer, Berlin), pp 1–20. https://doi.org/10.1007/11605805_1

[21] Tromer E, Osvik DA, Shamir A (2010) Efficient cache attacks on AES, and countermeasures. *Journal of Cryptology* 23(1):37–71. https://doi.org/10.1007/s00145-009-9049-y

[22] Chandramouli R (2019) Security Strategies for Microservices-based Application Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-204. https://doi.org/10.6028/NIST.SP.800-204

[23] Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. *INFOCOM, 2010 Proceedings* (IEEE, San Diego, CA), pp 1-9. https://doi.org/10.1109/INFCOM.2010.5462174

[24] Hu VC, Ferraiolo DF, Kuhn DR, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 02, 2019. https://doi.org/10.6028/NIST.SP.800-162

[25] Sahai A, Waters B (2005) Fuzzy identity-based encryption. *Advances in Cryptology – EUROCRYPT 2005*. Lecture Notes in Computer Science 3494 (Springer, Berlin), pp 457–473. https://doi.org/10.1007/11426639_27

[26] Nali D, Adams CM, Miri A (2005) Using threshold attribute-based encryption for practical biometric-based access control. *International Journal of Network Security* 1(3):173–182. Available at http://ijns.jalaxy.com.tw/download_paper.jsp?PaperID=IJNS-2005-06-30-2&PaperName=ijns-v1-n3/ijns-2005-v1-n3-p173-182.pdf

[27] Zhu Y, Hu H, Ahn G-J, Huang D, Wang S (2012) Towards temporal access control in cloud computing. *INFOCOM, 2012 Proceedings* (IEEE, Orlando, FL), pp 2576–2580. https://doi.org/10.1109/INFCOM.2012.6195656

[28] Hu VC, Grance T, Ferraiolo DF, Kuhn DR (2014) An access control scheme for big data processing. *2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (IEEE, Miami, FL), pp 1–7. https://doi.org/10.4108/icst.collaboratecom.2014.257649

[29] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874. https://doi.org/10.6028/NIST.IR.7874

[30] Vipul G, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)* (ACM, Alexandria, VA), pp 89-98. https://doi.org/10.1145/1180405.1180418

[31] Hu VC, Kuhn DR, Ferraiolo DF, Voas J (2015) Attribute-based access control. *Computer* 48(2):85-88. http://doi.org/10.1109/MC.2015.33

[32] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE (1996) Role-based access control models. *Computer* 29(2):38-47. https://doi.org/10.1109/2.485845

[33] Rubart J (2005) Context-based access control. *Proceedings of the 2005 Symposia on Metainformatics (MIS '05).* (ACM, New York, NY), pp 13-18. https://doi.org/10.1145/1234324.1234337

[34] Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(1), pp 1–11. https://doi.org/10.1016/j.jnca.2010.07.006

[35] Jin X, Krishnan R, Sandhu R (2012) A unified attribute-based access control model covering DAC, MAC, and RBAC. *Data and Applications Security and Privacy XXVI, DBSec 2012*. Lecture Notes in Computer Science 7371 (Springer, Berlin), pp 41-55. https://doi.org/10.1007/978-3-642-31540-4_4

[36] Decat M, Lagaisse B, Van Landuyt D, Crispo B, Joosen W (2013) Federated authorization for software-as-a-service applications. *On the Move to Meaningful Internet Systems: OTM 2013 Conferences*. Lecture Notes in Computer Science 8185 (Springer, Berlin), pp 342–359. https://doi.org/10.1007/978-3-642-41030-7_25

[37] Dimitrios Z, Lekkas D (2012) Addressing cloud computing security issues. *Future Generation Computer Systems* 28(3):583-592. https://doi.org/10.1016/j.future.2010.12.006

[38] McLean J (1985) A comment on the 'basic security theorem' of Bell and LaPadula. *Information Processing Letters* 20(2):67-70. https://doi.org/10.1016/0020-0190(85)90065-1

[39] Blobel B, Nordberg R, Davis JM, Pharow P (2006) Modelling privilege management and access control. *International Journal of Medical Informatics* 75(8), pp 597–623. https://doi.org/10.1016/j.ijmedinf.2005.08.010

[40] Bertino E, Federica P, Rodolfo F, Shang N (2009) Privacy-preserving digital identity management for cloud computing. *IEEE Data Engineering Bulletin* 32(1):21-27. Available at http://sites.computer.org/debull/A09mar/bertino.pdf

[41] Catteddu D (2010) Cloud Computing: Benefits, risks and recommendations for information security. *Web Application Security*. Communications in Computer and Information Science 72 (Springer, Berlin), pp 17-17. https://doi.org/10.1007/978-3-642-16120-9_9

[42] Simorjay F, Tierling E (2019) Shared Responsibility for Cloud Computing. (Microsoft, Redmond, WA), Version 2.0. Available at https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91/file/225366/1/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf

Appendix A—Guidance and SP 800-53 Revision 4 Access Control (AC) Family Mapping

The following table maps the cloud access control guidance to the AC controls listed in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

Table 4 Mapping the cloud access control guidance to the AC controls listed in NIST SP 800-53, Revision 4

Guidance	AC Control in 800-53
3.1 Guidance for Network	AC-1, AC-3, AC-4, AC-5, AC-10, AC-17, AC-21, AC-22
3.2 Guidance for Hypervisor	AC-1, AC-3, AC-5, AC-17, AC-21
3.3 Guidance for Virtual Machine	AC-1, AC-3, AC-4, AC-5, AC-11
3.4 Guidance for API	AC-1, AC-3, AC-4, AC-5, AC-11, AC-17, AC-21, AC-22
4.1 Guidance for Memory Data	AC-1, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
4.2 Guidance for APIs	AC-1, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
5.1 Guidance for Data Owner’s Control	AC-1, AC-3, AC-5
5.2 Guidance for Confidentiality	AC-3, AC-6, AC-21
5.3 Guidance for Privilege Management	AC-2, AC-11, AC-14, AC-22
5.4 Guidance for Multiple Replicas of Data	AC-1, AC-3, AC-4, AC-5, AC-17, AC-21
5.5 Guidance for Multi-tenancy	AC-1, AC-2, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
5.6 Guidance for Attribute and Role Management	AC-6, AC-1, AC-3
5.7 Guidance for Policies	AC-1, AC-3
5.8 Guidance for APIs	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-11, AC-14, AC-17, AC-21

AC-1: Access Control Policy and Procedures

AC-2: Account Management

AC-3: Access Enforcement

AC-4: Information Flow Enforcement

AC-5: Separation of Duties

AC-6: Least Privilege

AC-10: Concurrent Session Control

AC-11: Session Lock

AC-14: Permitted Actions without Identification or Authentication

AC-17: Remote Access

AC-21: Collaboration and Information Sharing

AC-22: Publicly Accessible Content