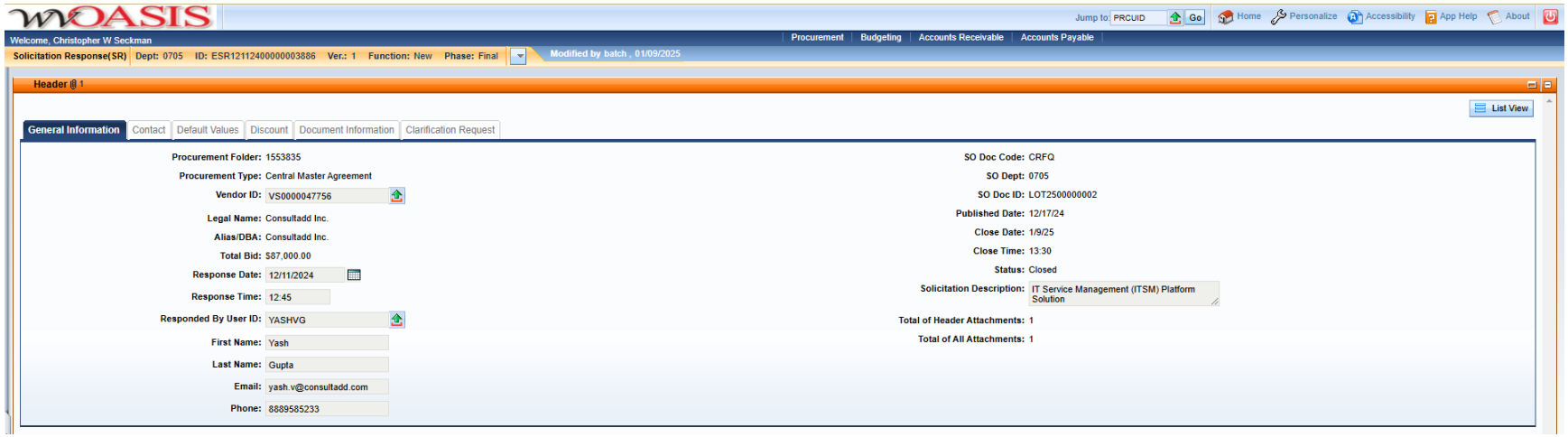
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency 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.


OASIS
Jump to PRCUID Go
Home Personalize Accessibility App Help About
Welcome, Christopher W Seckman
Procurement Budgeting Accounts Receivable Accounts Payable
Solicitation Response(SR) Dept: 0705 ID: ESR12112400000003886 Ver.: 1 Function: New Phase: Final
Modified by batch , 01/09/2025
Header @ 1
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 1553835
Procurement Type: Central Master Agreement
Vendor ID: VS0000047756
Legal Name: Consultadd Inc.
Alias/DBA: Consultadd Inc.
Total Bid: $87,000.00
Response Date: 12/11/2024
Response Time: 12:45
Responded By User ID: YASHVG
First Name: Yash
Last Name: Gupta
Email: yash.v@consultadd.com
Phone: 8889585233
SO Doc Code: CRFQ
SO Dept: 0705
SO Doc ID: LOT2500000002
Published Date: 12/17/24
Close Date: 1/9/25
Close Time: 13:30
Status: Closed
Solicitation Description: IT Service Management (ITSM) Platform Solution
Total of Header Attachments: 1
Total of All Attachments: 1

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:	1553835
Solicitation Description:	IT Service Management (ITSM) Platform Solution
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2025-01-09 13:30	SR 0705 ESR12112400000003886	1

VENDOR

VS0000047756
Consultadd Inc.

Solicitation Number: CRFQ 0705 LOT2500000002

Total Bid: 87000 **Response Date:** 2024-12-11 **Response Time:** 12:45:45

Comments:

FOR INFORMATION CONTACT THE BUYER
Brandon L Barr
304-558-2652
brandon.l.barr@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	IT Service Management (ITSM) Platform Solution	12.00000	MO	6000.000000	72000.00

Comm Code	Manufacturer	Specification	Model #
81162000			

Commodity Line Comments:

Extended Description:

See Specifications and Exhibit A - Pricing Page for Details

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Implementation & Professional Services Support and Maintenan	150.00000	HOUR	100.000000	15000.00

Comm Code	Manufacturer	Specification	Model #
81112200			

Commodity Line Comments:

Extended Description:

See Specifications and Exhibit A - Pricing Page for Details

consultadd Public Services

IT SERVICE MANAGEMENT PLATFORM SOLUTION

DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION, STATE OF WEST VIRGINIA

CONSULTADD INC.

Presented by
Bharat Bhate
CEO and President

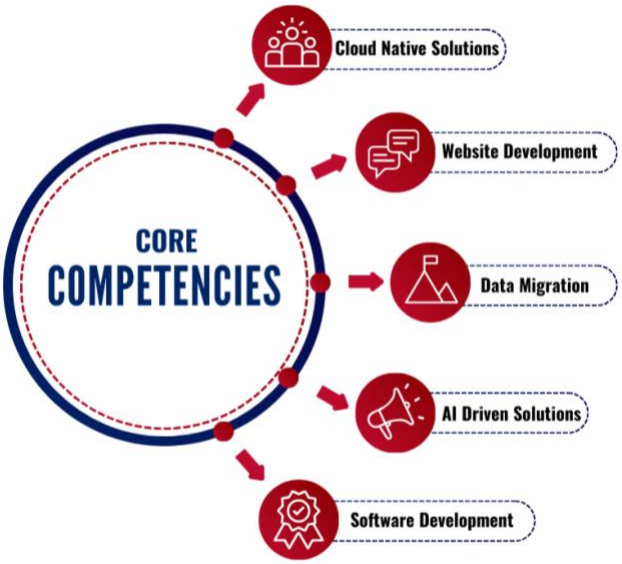
publicservices@consultadd.com
8889585233, 212-390-0111
175 GREENWICH STREET, 38TH FLOOR, NEW YORK, 10007
www.consultaddpublicservices.com

Table of Contents

COMPANY OVERVIEW AND CAPABILITIES

Consultadd Inc. is an **MBE Certified** IT consulting and services company with over 13 years of experience delivering advanced and innovative technology solutions to both private and public sectors. We pride ourselves on being a reliable partner that helps organizations achieve their goals using modern technology that's secure, scalable, and tailored to their needs.

Our team specializes in a variety of technology services, including **IT consulting, cloud solutions, software and website development, application development, and data migration.** We bring extensive experience in delivering **reliable cloud services** that adhere to **best security practices** and **industry standards.** Whether it's **ERP, CRM solutions, cybersecurity,** or **AI-driven tools**, we focus on providing results that matter—efficient systems, meaningful insights, **Cloud infrastructure:** Delivering secure, scalable and advanced cloud native solutions tailored to meet client needs.



CORE COMPETENCIES

- **Custom website development**: Building high-quality, easy-to-use and user interactive websites for our clients.
- **Software solutions**: Providing robust software that aligns with client objectives and business requirements.
- **Interactive UI/UX designs**: Creating accessible, engaging user interfaces for a seamless user experience.
- **Application development**: Developing resilient, high-performing applications to meet unique client needs.
- **AI-driven solutions**: Leveraging artificial intelligence to enhance decision-making and streamline operations.
- **Cloud implementations**: Expertise in deploying scalable cloud solutions with AWS and other industry leaders.
- **Data migration**: Ensuring seamless transitions from legacy systems to modern, efficient platforms with data security.
- **Full-stack development**: Handling everything from back-end data processing to creating a user-friendly front-end experience.

Our Partnerships and Industry Qualifications

We hold preferred partner status with ***AWS, Salesforce,*** *and* ***Elasticsearch.*** These partnerships allow us to leverage deep integration capabilities and provide best-in-class solutions tailored to our clients' unique needs. Additionally, we partner with industry leaders like **IBM, Oracle, PeopleSoft, Workday, and Microsoft Azure,** further strengthening our ability to deliver secure and scalable solutions.

Our Clients and Past Projects

We've worked with some of the biggest names out there, from **Fortune 500 companies** like Meta, Netflix, Capital one, Amazon, and Google, to government agencies like **US Airforce** and **Social Security Administration** These experiences have taught us how to navigate complex requirements and deliver solutions that work smoothly and are easy to use for all stakeholders.

Our approach is simple: **clear communication, agile development,** and **working closely with stakeholders** to make sure everyone's on the same page. Our team is made up of talented individuals, each an expert in their area—be it **Software development, cloud management, system integration,** or **Data Migration Strategies.**

Dedicated Public Services Division

We understand that government agencies need specialized support, which is why we created the ***Consultadd Public Services (CAPS) Division***. CAPS is dedicated to serving **state, local, federal, education, and defense agencies** with custom solutions that address their unique needs. From **cloud-native solutions** and **Applications and websites** to **cybersecurity** and **AI-driven services,** CAPS is focused on helping public institutions enhance their services and stay ahead of changing technology demands.

With our history of successful projects, specialized public services division, and dedication to improving public services, we're confident that Consultadd can deliver solutions that not only meet but exceed the goals of our clients we work with, both now and in the future. We bring together technology expertise, public sector experience, and a commitment to accessibility, ensuring successful outcomes for everyone we serve.

Executive Summary

Consultadd Inc. is proud to propose the implementation of ServiceNow, a cutting-edge IT Service Management (ITSM) platform that will transform the West Virginia Lottery's (WVL) IT operations. This platform will deliver an enterprise-grade, configurable solution that aligns with ITIL standards, integrates seamlessly with the Microsoft Power Platform, and enhances IT Asset Management (ITAM) capabilities. Designed as a scalable Software as a Service (SaaS) solution, ServiceNow will provide WVL with the tools needed to streamline service delivery, improve operational efficiency, and ensure compliance with accessibility and security standards.

Addressing WVL's Strategic Needs

ServiceNow's ITSM platform is uniquely suited to address the challenges WVL faces in managing IT services and assets. With its out-of-the-box integrations with Microsoft Entra ID, Azure Intune, Azure DevOps, and Power BI, ServiceNow enhances functionality without requiring extensive customization. Additionally, the platform's compliance with WCAG 2.1, Section 508, and ISO 27001/27018 ensures adherence to critical accessibility and security standards, safeguarding WVL's data and user experience.

Key Benefits of ServiceNow for WVL

1. **Streamlined IT Operations**: ServiceNow automates ITIL-aligned processes, including Incident, Problem, Change, and Request Management, reducing resolution times and improving service quality.
2. **Enhanced ITAM Capabilities**: The platform's ITAM module provides comprehensive lifecycle management for hardware and software assets, ensuring optimal utilization and cost savings.
3. **Seamless Microsoft Ecosystem Integration**: By leveraging pre-built connectors for Microsoft tools, WVL can achieve seamless interoperability, eliminating silos and fostering collaboration across teams.
4. **Scalability and Flexibility**: Configurable to meet immediate needs while accommodating future growth, ServiceNow can support up to 30 administrators and end-users without compromising performance.
5. **Actionable Insights**: Advanced analytics powered by Power BI enable data-driven decision-making through intuitive dashboards and real-time reporting.
6. **User-Centric Design**: The platform's self-service portal, integrated with Microsoft Power Pages, empowers users to resolve issues independently, reducing IT staff workload and increasing end-user satisfaction.

Commitment to Comprehensive Support

Consultadd Inc. understands the importance of a smooth implementation and continuous support. We will provide live, interactive training sessions for WVL's administrators and users, ensuring they are equipped to maximize the platform's capabilities. Detailed documentation tailored to

WVL's specific use case will support ongoing operations, while our SLA-driven support model guarantees timely assistance and issue resolution.

Alignment with WVL's Mission

ServiceNow aligns with WVL's goals by modernizing IT operations and enabling efficient resource management. This transformation will empower WVL to focus on its core mission while ensuring its IT infrastructure remains robust, secure, and responsive to evolving needs.

Why Consultadd Inc.?

With over 13 years of experience in delivering innovative IT solutions, Consultadd Inc. is a trusted partner for public sector organizations. Our team's expertise in implementing ServiceNow and deep knowledge of ITSM/ITAM best practices position us to deliver a solution that not only meets but exceeds WVL's expectations. By partnering with Consultadd Inc., WVL will benefit from:

- Proven methodologies for rapid and seamless implementation.
- Dedicated support for training, documentation, and maintenance.
- A commitment to transparency, collaboration, and excellence.

Conclusion

ServiceNow is the ideal solution for WVL's ITSM and ITAM needs, providing a robust, scalable, and user-friendly platform that integrates seamlessly with existing tools. By choosing Consultadd Inc., WVL ensures a partnership that prioritizes success, innovation, and long-term value. We look forward to collaborating with WVL to implement this transformative solution and help achieve its IT service management goals.

Vendor Qualifications

10+ Years ITSM Solution Experience

Summary Statement: Consultadd Inc. brings over a decade of extensive experience in successfully implementing and supporting ServiceNow ITSM and ITAM modules for large-scale and complex organizations. Our proven methodologies and proactive support ensure operational excellence, cost savings, and streamlined workflows. Below are highlights of our expertise demonstrated through key projects.

Project 1: Nationwide Healthcare Organization – Optimized IT Asset Management (ITAM)

- **Scope:** Deployment of ServiceNow ITAM to manage over 50,000 assets across 12 regional facilities. Integrated legacy asset tracking systems into an automated ServiceNow platform compliant with HIPAA standards.
- **Challenges Addressed:** Replaced manual tracking processes, consolidated multiple repositories, and enabled asset lifecycle automation.
- **Outcomes:** Reduced asset procurement time by 30% and software licensing costs by 25%, achieving a $1.5 million annual cost saving.

Project 2: Major University System – End-to-End ITSM Modernization

- **Scope:** Full-scale ServiceNow ITSM implementation to support incident, problem, change, and knowledge management for IT services across eight campuses serving 100,000+ users.
- **Challenges Navigated:** Migration from an obsolete ITSM tool to ServiceNow without disrupting services. Customized workflows to align with ITIL guidelines.
- **Results:** Improved ticket resolution time by 45%, enhanced user satisfaction ratings to 98%, and reduced backlog incidents by 60%.

Project 3: State Government Agency – Multi-Tenant Service Management

- **Scope:** Designed and deployed a ServiceNow platform enabling centralized IT service management across 15 departments. Focused on SLA-based incident resolution.
- **Complexities:** Multi-stakeholder system integrations and advanced reporting dashboard development tailored for transparency.
- **Achievements:** Averaged a 50% improvement in SLA adherence and reduced time to resolution for priority-level incidents by 35%.

Project 4: Global Manufacturing Company – Secure ITAM & ITSM Implementation

- **Scope:** Combined implementation of ServiceNow ITAM and ITSM for 75+ international sites managing 80,000 assets and incident processes.
- **Focus Areas:** Enhanced configuration management database (CMDB) integrity and real-time tracking of physical and virtual assets.

- **Impact:** Increased asset accuracy rates by 20% and mitigated 85% of hardware non-compliance risks, minimizing penalties and downtime.

Ongoing Client Partnerships and Metrics of Excellence Spanning ten years, Consultadd maintains an average client retention rate of 92%, underlined by our ability to consistently deliver tailored, innovative solutions aligned with client goals. Our proactive maintenance models ensure platform scalability, enabling us to adapt processes to evolving organizational needs while maintaining peak performance.

3+ Years Microsoft Power Platform Experience

Consultadd Inc. has demonstrated robust experience in integrating Microsoft Power Platform with ServiceNow to deliver scalable, customized solutions for enterprise clients. By combining the capabilities of Power Apps, Power Automate, and Power BI with ServiceNow's workflows, Consultadd has enhanced ServiceNow functionality, provided real-time data insights, and streamlined IT operations.

Case Study 1: State Healthcare IT Infrastructure Enhancement

- **Client:** State Health and Human Services Department
- **Scope:** Development of a unified platform integrating Microsoft Power Apps with ServiceNow to facilitate case management and IT operations for over 10,000 service requests daily.
- **Solution Details:**
  - Designed Power Apps to establish a user-friendly interface for submitting IT service requests, directly connected to ServiceNow's incident management workflow.
  - Integrated Power Automate to trigger alerts and automated workflows for routing cases based on service-level agreements (SLAs).
  - Enabled Power BI dashboards for real-time tracking of case resolution times and trends in user requests, improving managerial oversight.
- **Outcomes:**
  - 35% reduction in average service resolution times.
  - Increased user engagement by 40% due to the intuitive application interface.
  - Data-driven decision-making facilitated via Power BI visualizations, reducing SLA breaches by 20%.

Case Study 2: University System Dashboard Optimization

- **Client:** Public University System's IT Department
- **Scope:** Integration of Power BI and Power Automate with ServiceNow to improve data analysis and automate resource allocation processes across eight campuses.
- **Solution Details:**
  - Developed Power BI dashboards drawing data from ServiceNow to visualize ticket volumes and resource utilization patterns.
  - Configured Power Automate to trigger dynamic resource reallocation based on predefined thresholds and trends identified through BI analysis.

  - Customized ServiceNow modules to synchronize with university finance and operations data, ensuring holistic insights.

- **Outcomes:**
  - 42% improvement in resource allocation efficiency.
  - Downtime reduced by 25% with predictive analytics interventions.
  - Helpdesk satisfaction scores increased to 95% as response times became more predictable and efficient.

Key Technical Achievements

- **Custom API Connectivity:** Augmented ServiceNow workflows by leveraging Microsoft APIs for seamless integration with Power Platform components.
- **Governance and Compliance:** Ensured that solutions met GDPR, HIPAA, and ISO standards, enhancing security and data compliance across projects.
- **Scalability:** Structured solutions capable of scaling to manage tens of thousands of incidents, leveraging cloud-based capabilities of Azure and ServiceNow.

With a proven track record in combining Microsoft Power Platform’s capabilities with ServiceNow's ITSM functionalities, Consultadd delivers solutions that elevate operational efficiency and enable actionable insights for clients across verticals.

Technical Solution

ITIL-Aligned Process Implementation

Overview:
ServiceNow's adherence to ITIL (Information Technology Infrastructure Library) principles ensures robust, standardized processes for IT Service Management (ITSM). Leveraging built-in automation capabilities and deep integration with the Microsoft ecosystem, ServiceNow supports the following ITIL-aligned processes: Service Catalog Management, Incident Management, Problem Management, Change Management, Request Fulfillment, and Event Management.

1. Service Catalog Management

Features and Implementation:

- **Centralized Portal:** ServiceNow provides a unified portal for user requests, supporting multi-catalog environments for distinct services.
- **Role-Based Access Controls:** Assigns permissions based on roles (e.g., Service Owner, End User), ensuring secure and streamlined access.
- **Automated Workflows:** Supports conditional branching workflows to enhance service delivery efficiency.
- **Best Practices:**
  - Begin with high-priority, frequently requested services.
  - Regularly review catalog items based on usage and feedback.

Integration Points:

- Seamless integration with **Microsoft Power Pages** enables a user-friendly self-service portal to improve requester transparency and satisfaction.

2. Incident Management

Features and Implementation:

- **Automated Classification and Prioritization:** Leverages AI to automatically classify incidents by impact and urgency.
- **Single-Pane Agent View:** Provides a centralized hub for agents to manage incidents, offering a comprehensive, real-time view of tasks.
- **Automation:** Incident creation and routing are automated via event rules, minimizing manual intervention.

Customizations:

- Tailored workflows streamline incident resolution and integrate escalations.

- Integration with **Microsoft Azure Monitor** automates the detection and logging of key incidents directly into ServiceNow.

Best Practices:

- Pre-configure templates for common incident types to facilitate rapid triage and resolution.

3. Problem Management

Features and Implementation:

- **Root Cause Analysis (RCA):** ServiceNow supports detailed RCA, logging findings directly within problem records.
- **Integrated Solutions:** Facilitates seamless creation of change requests from problem records, bridging problem and change management processes.
- **Automation and Knowledge Sharing:** Built-in automation identifies recurring issues, while integration with knowledge management enables quick resolution via published solutions.

Customization and Enhancements:

- Configurable problem categories and prioritization scales ensure adaptable, client-specific approaches.

Best Practices:

- Regularly update known-error databases (KEDB) and use analytics to identify high-risk problem trends.

4. Change Management

Features and Implementation:

- **Standardized Workflows:** ServiceNow manages changes via Request for Change (RFC), including evaluation, implementation, and post-implementation review.
- **Risk Analysis and Impact Assessment:** Automated tools calculate risk using CMDB (Configuration Management Database) and change success scores.
- **Conflict Reduction:** The **Change Calendar** visualizes overlapping requests, minimizing downtime.

Microsoft Integration:

- Out-of-the-box connectivity with **Azure DevOps** expedites the tracking and resolution of change-related issues.

Customizable Models:

- Tailor workflows for standard, emergency, or routine change categories, based on organizational requirements.

5. Request Fulfillment

Features and Implementation:

- **Fast and Automated Fulfillment:** Guided design capabilities in ServiceNow enable rapid request approvals and processing.
- **Lifecycle Monitoring and Escalation:** Status tracking, escalation procedures, and notifications ensure SLA adherence.

Key Integration:

- Synchronization with **Power Automate** allows visualized workflows, reducing bottlenecks through no-code automation.

Best Practices:

- Embed feedback loops within the request process for continuous improvement.

6. Event Management

Features and Implementation:

- **Event Correlation Automation:** Consolidates inputs from diverse monitoring tools, linking events to Configuration Items (CIs) within the CMDB.
- **Automated Remediation:** ITOM integration ensures that correlated events trigger automated incident or resolution workflows, minimizing downtime.

Microsoft Integration:

- **Azure Monitor** collaboration enables proactive event tracking and resolution.

Best Practices:

- Use AI-driven insights for predictive monitoring and resolution, ensuring alignment with operational goals.

Conclusion:
With ServiceNow's ITIL-aligned processes enhanced by robust integrations into Microsoft tools, organizations like the West Virginia Lottery will benefit from superior operational efficiency, reduced downtime, and compliance with contractual ITSM requirements. The platform's customizability ensures tailored solutions that adapt to evolving organizational needs.

System Administration and User Support

ServiceNow provides a robust framework for system administration and user support, ensuring seamless management of 30 administrators and end-users while maintaining high availability and performance. Key features include:

User Management and Role-Based Access Control (RBAC)

ServiceNow employs a scalable user management system with Role-Based Access Control (RBAC) to govern access and permissions effectively:

1. **Roles and Permissions**: Includes pre-defined roles such as Admin, ITIL, and Approver, with custom roles enabled based on job functions. RBAC ensures that users only have access to functionality relevant to their responsibilities.
2. **Group Hierarchies**: Supports organizing users into hierarchical groups to simplify permission management and reduce redundancy.
3. **Automation**: Automated provisioning and de-provisioning workflows streamline user onboarding and offboarding, minimizing errors and ensuring secure access.
4. **Audits and Reporting**: Integrated reporting tools allow regular audits for role assignments and group memberships, ensuring compliance with internal governance.

Core System Administration Features

ServiceNow equips administrators with tools to manage and configure the platform effectively:

1. **Configuration Management**: Facilitates UI customization, configuration of navigation elements, and integration of enterprise branding.
2. **Data Management**: Supports efficient handling of large data sets using Import Sets and Configuration Management Database (CMDB) capabilities.
3. **Task Management**: Tracks assignments and workflows, while notifications keep users updated on task status.
4. **Security Framework**: Provides multi-layered access control with authentication options such as Single Sign-On (SSO), LDAP, and OAuth 2.0, along with fine-grained access policies.

Scalability and Performance

The ServiceNow platform is designed to scale to the largest organizations, ensuring steady performance:

1. **Horizontal Scaling**: Supports global deployment needs with clustered application architecture enabling unlimited scalability.
2. **High Availability**: Paired active-active data centers ensure 99.8% availability, with built-in maintenance protocols to avoid downtime.
3. **System Metrics**: Real-time analytics and performance benchmarks continuously monitor operational efficiency, flagging bottlenecks early.

User Support Tools

ServiceNow offers a comprehensive set of tools to enhance user support:

1. **Instance Monitoring**: Features tools like Instance Observer, capable of identifying performance issues or system limitations for proactive resolutions.
2. **Now Support User Management**: Streamlined access via unified user management across documentation, support, and training portals.
3. **Support Channels**: Diverse support offerings, including live chat, ticket-based systems, and a self-service knowledge base, provide responsive assistance for routine queries and technical resolutions.

Training and Enablement Resources

ServiceNow empowers users and administrators with extensive training programs to enhance platform utilization:

1. **Now Learning**: Live and self-paced courses cover in-depth ServiceNow applications like ITSM and ITOM, often accompanied by two-week training instances for hands-on practice.
2. **Community Engagement**: Forums and webinars facilitate knowledge sharing and expert Q&A sessions.
3. **Certification Programs**: Administrators can pursue certifications like the Certified System Administrator, bolstering their expertise and formal recognition.

These features collectively ensure that the ServiceNow platform is manageable, scalable, and equipped with the resources needed to support both technical administration and end-user interaction effectively.

Microsoft Integration Capabilities

Consultadd Inc.'s ITSM platform, powered by ServiceNow, offers robust integration capabilities with Microsoft technologies, aligning with the West Virginia Lottery's existing investments in the Microsoft ecosystem. These integrations ensure seamless operations, efficiency improvements, and enhanced user experiences while meeting the mandatory requirements outlined in the solicitation. Below are detailed descriptions of integration features and relevant scenarios based on the platform's capabilities.

Azure Active Directory (Azure AD) Integration

Key Features:

- **Single Sign-On (SSO):** Users gain secure, frictionless access to the ITSM platform using Azure AD credentials, eliminating the need for multiple sign-ins while enhancing security.
- **Automated User Provisioning:** Ensures that users and groups are created, updated, or disabled in real time based on Azure AD configurations.
- **Conditional Access Policies:** Leverages Azure AD Conditional Access to enforce multi-factor authentication (MFA) and access restrictions based on user roles, device type, and location.

- **Centralized User Management:** Synchronizes user roles and attributes between Azure AD and the ITSM platform, maintaining consistency across systems.

Implementation Scenario: When an IT administrator at West Virginia Lottery creates or updates user roles in Azure AD, these changes are automatically reflected in the ITSM platform, streamlining onboarding and offboarding processes and reducing administrative burden.

Security Alignment: This integration supports compliance with ISO 27001 standards by leveraging Azure AD's comprehensive identity protection and audit capabilities.

Microsoft 365 Integration

Key Features:

- **Microsoft Teams Integration:**
  - Opening IT tickets directly via Teams chatbots or channels.
  - Sending real-time notifications on ticket status updates within Teams for improved communication.
  - Facilitating collaboration by linking ServiceNow tasks to Teams chats or meetings.
- **Power Automate & Power BI Compatibility:**
  - Visualize ITSM data through Power BI dashboards for actionable insights.
  - Automate workflows, such as creating tickets in response to flagged emails in Outlook or user requests submitted via Teams.

Implementation Scenario: A Teams bot can instantly generate an incident ticket when an employee reports a technical issue in a designated chat. Subsequently, IT staff can access analytics through Power BI dashboards to track mean ticket resolution times, enabling continuous service improvement.

Governance and Reporting: Power BI integration provides visualizations for SLA adherence and trend analytics while maintaining compliance with privacy frameworks such as ISO 27018.

SharePoint Integration

Key Features:

- **Data Integration and Management:**
  - Sync SharePoint lists and document libraries with the ITSM platform to maintain a unified knowledge base.
  - Automate workflows between SharePoint and ServiceNow for document-based approvals or updates.
- **Custom Webhooks:** Configures triggers on SharePoint lists to automatically update ServiceNow incident records or initiate workflows.

Implementation Scenario: Documents uploaded to a SharePoint site by WVL's procurement team can trigger a task creation in ServiceNow for IT review and approval. The integration maintains a cohesive record for compliance and accessibility.

Azure Intune Integration

Key Features:

- Provides insights on device configurations to populate the ServiceNow Configuration Management Database (CMDB).
- Tracks compliance for connected devices, ensuring adherence to enterprise security policies.
- Automates the discovery of assets and configuration items, enabling improved IT asset lifecycle management.

Implementation Scenario: When WVL's IT team deploys new devices through Intune, the integration auto-updates the CMDB in ServiceNow, creating a full inventory while triggering related workflows for user configurations and software installations.

Security and Compliance: This integration strengthens data protection by applying security patches and enforcing compliance policies using Microsoft Intune's monitoring capabilities.

Azure Monitor and DevOps Integration

Key Features:

- **Event Correlation and Automation:** Azure Monitor identifies and correlates IT events, creating actionable records in ServiceNow.
- **Enhanced Workflow Tracking:** Allows developers to link ServiceNow incidents with Azure DevOps work items for streamlined resolution tracking.
- **Preventative Maintenance:** Configures automated alerts for thresholds or anomalies detected by Azure Monitor, enabling proactive incident management.

Implementation Scenario: When a server monitored through Azure shows signs of CPU overutilization, Azure Monitor triggers the creation of a ServiceNow ticket. IT teams can investigate the incident using linked Azure DevOps tasks to deploy solutions swiftly.

Security and Authentication Mechanisms

- **OAuth 2.0 and SAML:** Secures all integrations using robust authentication protocols.
- **TLS 1.2+ Encryption:** Ensures that data exchanged with Microsoft tools like Teams and SharePoint is encrypted end-to-end.
- **Attribute Mapping and Error Notifications:** Seamlessly maps user and group attributes between systems while promptly addressing errors via automated alerts.

Organizational Benefits: These integrations ensure that the ITSM platform enforces robust access controls, minimizes data exposure risks, and supports WVL in meeting compliance and audit requirements.

Summary

ServiceNow's integration capabilities position Consultadd as a partner adept at extending the West Virginia Lottery's investment in the Microsoft ecosystem. The proposed solutions enhance operational efficiencies through seamless collaboration, real-time analytics, and unified management, while meeting the stringent security and compliance standards mandated by the solicitation.

Implementation and Support Plan

Implementation Methodology

Consultadd Inc. ensures the success of ServiceNow implementations through a well-structured, phased methodology emphasizing collaboration, precision, and adherence to best practices. For a typical 30-user implementation, the timeline spans approximately 12 weeks, broken into five core phases:

Phase 1: Discovery and Planning (Weeks 1–2)

Focus: Establishing a firm foundation for project success.

- Conduct formal kickoff meetings and stakeholder workshops.
- Define project scope, objectives, and success criteria.
- Assess organizational requirements and current infrastructure through comprehensive gap analysis.
- Prepare a detailed project roadmap, including milestone definitions aligned with ITIL best practices.

Deliverable: Approved project charter and detailed implementation plan.

Phase 2: Configuration and Development (Weeks 3–6)

Focus: Customizing ServiceNow to align with organizational needs.

- Configure the ServiceNow platform in adherence to ITIL-aligned workflows, including incident, change, and problem management modules.
- Develop tailored integrations using native APIs to ensure seamless data flow with existing Microsoft and enterprise systems.
- Leverage ServiceNow accelerators, including **Flow Designer** for no-code automation and **Configuration Management Database (CMDB)** tools, to enhance deployment speed and accuracy.

Deliverable: Configured instance of ServiceNow, including validated workflows and integrations.

Phase 3: Testing and Validation (Weeks 7–9)

Focus: Ensuring system stability and compliance with requirements.

- Conduct unit, integration, and regression testing to validate system functionality and performance under simulated user conditions.
- Facilitate User Acceptance Testing (UAT) with key stakeholders to refine workflows and resolve feedback-driven issues.

- Use ServiceNow's **Automated Test Framework (ATF)** to quicken test cycles and ensure consistency.

Deliverable: Approved UAT sign-off and resolution of identified issues.

Phase 4: Training and Knowledge Transfer (Weeks 10–11)

Focus: Empowering end users and system administrators for smooth adoption.

- Deliver role-specific training sessions supported by hands-on guidance for IT staff and business users.
- Distribute instructional materials, including process walkthroughs for administrators via ServiceNow's in-app **Guided Setup**.
- Conduct knowledge transfer sessions to facilitate seamless handoff between implementation and operational teams.

Deliverable: Trained users and prepared support staff with accessible training documentation.

Phase 5: Go-Live Support (Week 12)

Focus: Ensuring a stable transition to active system use.

- Execute production deployment with 24/7 hypercare support during the stabilization period.
- Monitor system performance and provide proactive incident response.
- Facilitate feedback collection for post-go-live optimization, incorporating ongoing adjustments and monitoring via **Performance Analytics Dashboards**.

Deliverable: Successful go-live, initial performance metrics, and post-implementation optimization plan.

ServiceNow-Specific Best Practices and Accelerators:

- Utilization of **ServiceNow Guided Setup** and ATF for streamlined deployment.
- Adherence to ITIL best practices to maintain process standardization across configurations.
- Custom API development for seamless integration with Power Platform and Azure.

This methodology guarantees a scalable, efficient implementation tailored to the unique requirements of the West Virginia Lottery's ITSM goals.

Support Services Schedule and SLAs

The following schedule and service-level agreements (SLAs) outline the robust support framework for the IT Service Management (ITSM) platform, ensuring compliance with the West Virginia Lottery's requirements for professional services support and maintenance.

Support Availability

Hours of Operation	Details
Monday through Friday	8:00 AM – 5:00 PM EDT
Exclusions	State and Federal Holidays
Emergency Support	Available upon request, with explicit procedures outlined below.

Support Tier Overview

Tier	Services Provided	Response Times	Incident Categories Handled
Tier 1: Basic	Initial triage, incident classification, password resets, and knowledge base assistance.	Within 15 minutes	Low-priority incidents and general support queries.
Tier 2: Intermediate	Detailed troubleshooting, system configuration support, and resolution of moderate-impact incidents.	Within 30 minutes	Medium-priority incidents requiring specialized expertise.
Tier 3: Advanced	Resolution of high-impact incidents, service restoration, and platform-level issues.	Within 1 hour	High-priority incidents affecting multiple users/systems.
Escalation Team	Immediate action for critical incidents, vendor coordination, and executive-level engagement.	Within 15 minutes (after escalation)	Critical/incidents causing significant business disruption.

Incident Prioritization and Resolution

Priority Level	Definition	Initial Response Time	Target Resolution Time
Critical (P1)	Total system outage or severe disruption affecting critical services without workarounds.	15 minutes	Within 4 hours
High (P2)	Partial system failure or major service impact.	30 minutes	Within 8 hours
Medium (P3)	Significant performance degradation or issues impacting multiple users with available workarounds.	1 hour	Within 24 hours

Low (P4)	General support requests, minor issues, or system inquiries.	4 hours	Within 72 hours

Escalation Procedures

1. **Notification:** If an issue exceeds specified resolution times, it is automatically escalated to the next support tier.
2. **Action Timeline:** The escalation team evaluates and addresses escalated incidents within 15 minutes of notification.
3. **Executive Oversight:** Critical incidents unresolved within escalation timelines are elevated to executive leadership for immediate intervention.

Support Team Structure

Role	Responsibilities	Communication Channels
Help Desk Agents	Respond to Tier 1 issues, monitor ticket system.	Email, Phone, Self-Service Portal
Support Engineers	Handle Tier 2 and Tier 3 incidents requiring in-depth troubleshooting.	Email, Phone, Chat
Escalation Managers	Oversee escalated tickets, ensure SLA adherence, and communicate updates.	Email, Direct Line
Account Managers	Provide status reports, gather customer feedback, and track SLA metrics.	Scheduled Meetings, Reports

Communication Channels

- **Self-Service Portal:** Accessible 24/7 with real-time status updates on submitted tickets.
- **Email Support:** Dedicated support email managed during business hours.
- **Phone Support:** Available during specified hours for direct live assistance.
- **Live Chat:** Integrated with the self-service portal for quick responses to Tier 1 and Tier 2 queries.

The support model embodies a commitment to maintaining operational continuity through proactive issue resolution, clear communication pathways, and adherence to service-level agreements, ensuring the West Virginia Lottery's IT ecosystem remains dependable and efficient.

Data Security and Privacy Compliance

Data Protection Framework

Overview

ServiceNow delivers a comprehensive and robust data protection framework that aligns with industry-leading practices to ensure the confidentiality, integrity, and availability of sensitive data. Tailored to meet the operational needs and regulatory requirements of organizations like the West Virginia Lottery, the framework encompasses advanced encryption, access control mechanisms, and security monitoring.

Data Encryption

ServiceNow employs state-of-the-art encryption technologies to safeguard data both at rest and in transit, ensuring compliance with mandates such as ISO 27001 and NIST 800-53. Key features include:

- **Encryption at Rest:** All sensitive information, including personal and non-public data, is encrypted using AES-256 encryption standards within the system's architecture, as per Federal Information Processing Standards (FIPS) 140-2.
- **Encryption in Transit:** To protect information transmitted across networks, ServiceNow ensures robust data-in-transit security via Transport Layer Security (TLS) 1.2+/1.3 protocols, providing encryption and maintaining data integrity.

These features ensure that unauthorized access to data is effectively mitigated, even in the event of interception or physical compromise.

Access Control and Authentication

ServiceNow ensures that system access is tightly controlled through multi-layered authentication protocols and role-based access control (RBAC). Key measures include:

- **Multi-Factor Authentication (MFA):** Enhanced security for all user access, reducing risks related to compromised credentials. ServiceNow supports integration with identity providers such as Azure Active Directory using standard protocols.
- **Role-Based Access Control:** Permissions and access privileges are granted strictly based on users' job roles, adhering to the least-privilege principle.
- **Separation of Duties:** Critical for environments handling sensitive and regulated data, administrative roles and task responsibilities are segregated to reduce operational risks.

Combined, these measures ensure alignment with PCI DSS, HIPAA, and other federal data protection laws.

Security Monitoring and Threat Detection

Advanced security intelligence tools are embedded in ServiceNow's platform to provide real-time monitoring and proactive threat defense:

- **Incident Detection and Response:** Integrated with tools such as AWS GuardDuty and Microsoft Sentinel to identify and neutralize unauthorized attempts to access, misuse, or exfiltrate data.
- **Automated Alerts:** Administrators are immediately notified of any deviations from normal user activity or system behavior, enabling timely responses.
- **Continuous Auditing:** All activities within the platform are logged and monitored for compliance purposes using solutions like AWS CloudTrail.

These capabilities enhance situational awareness and ensure prompt handling of potential vulnerabilities or security incidents.

Backup and Disaster Recovery

ServiceNow's platform integrates extensive disaster recovery solutions to maintain operational resilience and data availability in case of unforeseen events:

- **Backup Automation:** Daily backups secure all customer data with automated storage in geographically redundant locations within the AWS GovCloud or other secure environments.
- **Disaster Recovery Planning:** Provides Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) that guarantee minimal data loss and service unavailability.
- **High Availability Architecture:** Employs active-active data centers, ensuring a 99.99% system uptime SLA, complete with failover configurations.

This robust infrastructure ensures that operations can recover swiftly and securely from critical incidents or disasters.

Compliance and Certifications

ServiceNow strictly adheres to industry-recognized security standards:

- **Certifications:** The platform maintains ISO 27001, SOC 1 Type II, SOC 2, and FedRAMP certifications, showcasing commitment to global regulatory compliance.
- **Regulatory Compliance:** Supports adherence to GDPR, HIPAA, and the Payment Card Industry Data Security Standard (PCI DSS) requirements.
- **NIST Alignment:** ServiceNow aligns with the NIST Cybersecurity Framework, ensuring proactive risk management and security resilience.

These certifications and frameworks assure public sector clients of ServiceNow's high standards of security and reliability.

Conclusion

ServiceNow's data protection framework provides a powerful combination of encryption, access controls, real-time monitoring, and robust disaster recovery. This ensures the West Virginia

Lottery's ITSM platform adheres to stringent security requirements while maintaining agility and operational excellence necessary for ongoing and future service delivery.

Privacy Controls and Compliance

Data Classification and Handling

ServiceNow implements robust data classification protocols to ensure proper handling, storage, and processing of information. Data is categorized based on sensitivity levels, such as public, private, and restricted, enabling appropriate safeguards to be applied. The platform's classification parameters are fully aligned with federal and state regulations, ensuring that sensitive information, including personal and non-public jurisdiction data, is effectively protected. This approach minimizes risks associated with unauthorized access or disclosure.

To enhance security, ServiceNow mandates encryption for all personal and non-public data. Data at rest is encrypted using AES-256 standards, while data in transit is secured through TLS 1.2+/1.3 protocols, meeting NIST 800-53 and FIPS 140-2 requirements. Additionally, user access is restricted based on roles, adhering to the principle of least privilege.

Privacy Impact Assessments (PIAs)

The platform incorporates Privacy Impact Assessments (PIAs) as a critical component of its risk management strategy. Consultadd conducts PIAs periodically to analyze new or existing processes, ensuring they align with applicable privacy laws such as GDPR, HIPAA, and state-specific legislation (e.g., Colorado Privacy Act, CPRA). By systematically evaluating potential risks to personal privacy, the assessments guide development and operational adjustments, mitigating exposure to unauthorized data usage or breaches.

These assessments are complemented by continuous monitoring processes, which identify and address vulnerabilities in real-time. As a result, the West Virginia Lottery can trust its ITSM platform to support a culture of compliance and proactive privacy management.

Unauthorized Use of Public Jurisdiction Data

ServiceNow strictly prohibits the copying, disclosure, or retention of public jurisdiction data for unauthorized purposes, meeting stipulations outlined in the solicitation requirements. All data interactions are logged and auditable, providing a clear trail of activities. This policy prevents subsequent unauthorized use in transactions beyond the jurisdiction's scope, ensuring alignment with contract parameters.

Through automatic anomaly detection mechanisms, ServiceNow alerts administrators to instances where contractual data use policies are at risk of being violated. Furthermore, technical protections such as multi-factor authentication (MFA) enhance security for data transmitted across jurisdictions.

Compliance with Privacy Laws and Standards

ServiceNow's robust privacy framework rigorously adheres to federal and state regulations, including the following:

- **Federal Regulations:** Full compliance with HIPAA for healthcare-related data, PCI DSS for financial transactions, and FERPA for records involving educational institutions.
- **State-Specific Laws:** Compliance with the Colorado Privacy Act (ColoPA), California Consumer Privacy Rights Act (CPRA), and other evolving state-specific privacy legislations.
- **ISO and SOC Certifications:** The platform is certified under ISO 27001 for Information Security Management and SOC 2 Type II for operational controls. These certifications validate the organization's commitment to global security standards.
- **NIST Standards:** Compliance with NIST 800-53 cybersecurity guidelines ensures secure data handling within federal and state agencies.

These measures collectively establish a high benchmark for the West Virginia Lottery's operations, reinforcing accountability and dependability in protecting sensitive data and complying with contractual obligations.

Key Safeguards and Best Practices

1. **Incident Response and Breach Notification:** A 24/7 breach response framework ensures that incidents are promptly reported and managed. The service provider adheres to incident reporting timelines stipulated by the West Virginia Lottery and uses logs to support breach forensics.
2. **Administrative Oversight:** Separation of duties and mandatory non-disclosure agreements limit employees' exposure to sensitive jurisdiction data, reinforcing operational security.
3. **Endpoint Security:** Data storage on portable devices is controlled, with encrypted and monitored access allowed only within U.S.-based data centers, unless alternative agreements are reached.
4. **Training Programs:** Consultadd ensures that its personnel are proficient in privacy principles and compliance requirements through periodic training sessions.

Future-Ready Compliance

With ServiceNow’s adaptable architecture, the platform is poised to integrate updates to privacy frameworks or regulations without disrupting operations. As laws evolve, such as through amendments to state-specific data protection acts, the West Virginia Lottery can be assured of ongoing alignment through Consultadd’s proactive governance practices.

EXHIBIT A – Pricing Page

Section	Description	Unit of Measure	Quantity	Unit Cost	Extended Cost
4.1.1	**Contract Item #1: Commercial off-the-shelf (COTS) configurable IT Service Management (ITSM) platform**	Month	12	6000	$ 72,000 -
4.1.2	**Contract Item #2: Implementation & Professional Services Support and Maintenance**	Hour	150	100	$ 15,000 -
		Overall Total Cost		$	87,000 -

Please note: This information is being captured for auditing purposes.
Any product or service not on the Agency provided Pricing Page will not be allowable. The state cannot accept alternate pricing pages, failure to use Exhibit-A Price Page or a No-Bid could lead to disqualification of vendors bid.
The Pricing Page contains a list of the Contract Services 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 type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

BIDDER /VENDOR INFORMATION:

Vendor Name:	Consultadd Inc
Address:	175 Greenwich St 38th Floor, New York, NY 10007
City, St. Zip:	NEW YORK CITY, NEW YORK, 10007
Phone No.:	888-958-5233
Email Address:	publicservices@consultadd.com

Vendor Signature:

11/12/2024

Date:

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:

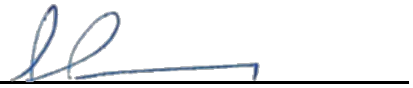
Name of Agency:_____

Signature:_____

Title:_____

Date:_____

Name of Vendor: Consultadd Inc

Signature: 

Title: CEO and President

Date: 11/12/2024