



Proposal for the State of West Virginia Department of  
Administration Purchasing Division

CRFP#: 0947 ERP2400000002

Identity Management Single Sign-On Solution

Technical Response

Proposal Due: April 4, 2024

RECEIVED

2024 APR -4 AM 8:17

WV PURCHASING  
DIVISION



April 4, 2024

Larry D McDonnell  
State of West Virginia Department of Administration Purchasing Division  
2019 Washington Street, East  
Charleston, WV 25305

Dear Mr. McDonnell,

Thank you for this opportunity to submit a proposal for State of West Virginia Department of Administration Purchasing Division's forthcoming technology project. We have studied the information provided to us about your business requirements and carefully analyzed your technology needs. The solution recommended for State of West Virginia Department of Administration Purchasing Division has been designed to meet your needs in the most cost-effective way without compromising on quality, service or ongoing support.

Dell is helping our customers to bring down the Total Cost of Ownership by simplifying IT. We are committed to providing solutions that will allow State of West Virginia Department of Administration Purchasing Division to reclaim time and cost and increase the productivity of your IT. In addition, we have built environmental consideration into every stage of the Dell product lifecycle including power consumption, helping our customers demonstrate environmentally responsible procurement.

Along with award winning products and services, Dell also offers you a dedicated program account team that is committed to working with you and your procurement needs. This team includes:

- An Account Manager to ensure overall account satisfaction.
- System Consultants to provide a seamless deployment experience.
- Technical Sales Representatives to facilitate order management.
- Customer Service Representatives to provide post-sale support.

Dell looks forward to working with you on this project. Should you have any questions regarding this response, please contact your dedicated Account Executive, Brian Tatum at (440) 334-9419 or online at [Brian.Tatum@Dell.com](mailto:Brian.Tatum@Dell.com).

Sincerely,

*Kiara Daniels*  
Kiara Daniels  
Proposal Manager

## Table of Contents

---

Dell Technologies Profile.....	4
Executive Summary .....	5
Qualifications and Experience.....	6
Dell Response to CRFQ.....	53
Legal Clarifications and Exceptions .....	54
One Identity LLC NDA.....	55
Memorandum of Insurance .....	56
Proposal Legal Notes.....	57

## Dell Technologies Profile

---

At Dell Technologies, our purpose is to drive human progress on a global scale, through greater access to better technology, to create new markets, reshape industries, and improve the lives of every person on the planet. Our unique combination and unprecedented capabilities power true transformation for people and organizations everywhere.

Digital transformation has become essential to all businesses, and we have expanded our portfolio to include holistic solutions that enable our customers to drive their ongoing digital transformation initiatives. Dell Technologies' integrated solutions help customers modernize their IT infrastructure, manage and operate in a multi-cloud world, address workforce transformation, and provide critical security solutions to protect against the ever increasing and evolving security threats.

With our extensive portfolio and our commitment to innovation, we have the ability to offer secure, integrated solutions that extend from the edge to the core to the cloud, and we are at the forefront of the software-defined and cloud native infrastructure era.

## Executive Summary

---

In responding to State of West Virginia Department of Administration Purchasing Division's requirement, Dell has derived a solution that addresses your expressed business challenges and offers tangible financial, operational and business benefits.

Dell offers superior quality and value of solutions through operational excellence based on:

### Expertise

- Dell uses a Business Process Improvement (BPI) methodology, based upon the internationally recognized 6-Sigma, for continuous innovation and process quality improvement.
- Dell offers validated, best of breed solutions based on thousands of successful deployments.
- Intellectual property and solution project management are maintained by Dell.

### Efficiency

- Dell's solution framework (based upon industry best practice) can be customized to meet your business needs and allows for rapid design and deployment of solutions.
- Our expertise in delivering core infrastructure services ensures the efficiency of solution planning, implementation and on-going maintenance.

### Dependability

- Dell's unique business model provides State of West Virginia Department of Administration Purchasing Division with a single point of accountability for everything we do
- Dell is passionate about its customer relationships. That passion means that you can be assured of high-quality delivery – and also that doing business with Dell will be easy.

### Choosing Dell as your Supplier

In summary, we believe that Dell can deliver real value to State of West Virginia Department of Administration Purchasing Division's business.

You can be assured that Dell is committed to deliver the solutions and services described in this proposal in a manner that will meet both your short- and long-term requirements.

## Qualifications and Experience

---

**Provide a state-wide solution for the ERP solution and supporting applications to provide a single sign on solution.**

**Dell Response:** Onelogin is a versatile cloud-based Identity as a Service provider. By leveraging its services, the State of West Virginia can centralize identity management, improve user experience, enhance security and meet compliance requirements. In addition, Onelogin is scalable, easy to implement and provide cost savings.

- Centralize Identity Management - The Onelogin platform provide a centralized location for managing user identities, access rights, and permissions. This centralized approach simplifies identity management tasks, such as user provisioning, de-provisioning, and access control policies.
- Improve User Experience - The Onelogin platform includes features such as single sign-on (SSO), which allows users to access multiple applications with a single set of credentials. This improves the user experience by reducing the need for multiple logins and passwords. SAML, OIDC and OAuth are all supported through a catalog of over 7K out of the box application connectors. Additionally, Generic SAML, OIDC, and OAuth connectors are available for applications that are not in the catalog.
- Enhance Security - The Onelogin platform offers robust security features, such as multi-factor authentication (MFA), adaptive access controls (SmartFactor), and threat detection capabilities (SmartFactor). These security measures will help the State of West Virginia protect against unauthorized access and data breaches.
- Compliance Requirements - The Onelogin platform can help the State of West Virginia achieve compliance with regulatory requirements and industry standards by enforcing access policies, auditing user activity, and providing reporting capabilities. This ensures that the State of West Virginia maintains control over access to sensitive data and resources.
- Scalability - The Onelogin platform can scale to accommodate the changing needs of the State of West Virginia, whether you are experiencing growth or fluctuations in user populations. This scalability allows the State of West Virginia to adapt their IAM capabilities without the need for significant infrastructure investments.
- Easy to Implement - The Onelogin platform is cloud-based, which means it can be implemented quickly and without the need for extensive on-premises infrastructure. This ease of implementation reduces deployment time and minimizes the burden on IT resources. Additionally, the Administration UI of Onelogin is very straight forward, easy to use and well documented here - > <https://support.onelogin.com/>
- Cost Savings - The Onelogin platform is subscription-based, which means the State of West Virginia can avoid upfront capital expenditures and instead pay for the services used on a per-user or per-month basis. This subscription model can result in cost savings compared to traditional on-premises IAM solutions.



**Obtain a complete single sign solution that is cloud based and will provide robust security solutions to include encryption, logging, and provide common industry standard options for a single sign on solution.**

**Dell Response:** OneLogin is a cloud-based Identity as a Service provider that is built on AWS cloud infrastructure.

Encryption - Summary of Encryption Standards applied to Customer Data within the OneLogin product and service offering are as follows:

- Secure entry of Customer Data: Client-side encryption, TLS min version enforced 1.2 with AES-256 cyphers
- Secure processing of Customer Data: S3 Buckets, PGP Asymmetric Encryption
- Secure storage of Customer Data: FIPS-compliant AES 256 soft-HSM
- How we protect our tenant application layer with encryption ensuring separation from infrastructure services is as follows:
- Communication within OneLogin's VPC is encrypted. We use HTTPS between micro-services and layers within our private VPC. This prevents network-level Man-in-the-middle attacks.
- Data at rest is encrypted in two ways:
- programmatically we encrypt data before being stored using a KMS and HSM.
- Volumes are encrypted, including DB and host volumes
- We managed data security as a customer of AWS using the shared security model. Data and content belongs to OneLogin, and we secure data at our account and deployment layer.

Logging - OneLogin provides the capability to configure an Event Broadcaster to send your OneLogin event data to your SIEM solution. The OneLogin event data is compatible with any SIEM solution that accepts data in JSON format, including Sumo Logic, ELK, Splunk, and many others. The Event Broadcaster will send real-time event data in JSON format to a listener via an HTTP/S POST to the endpoint, streaming the event data every 10 seconds or in 10 event bundles, as necessary. This information has more debugged logging levels and information. Logged events can also be retrieved via REST API. See our developer documentation on how to use the Events API, and our our support article about SIEM Webhook integrations for more details.

Single-Sign On - OneLogin primarily acts as an Identity Provider (IdP) with regard to SSO, supporting numerous SSO standards such as SAML, OIDC, WS-Fed, RADIUS, RDP, Forms-Based Authentication, Header-based Authentication and more.

While OneLogin is an SSO provider itself, OneLogin can also create a trust between itself and other identity providers (TIdP or Trusted IdP), to allow users or partners within 3rd party IdPs to access applications within OneLogin. In this extended hub and spoke model, TIdP users can also be created and managed in the source IdP, and allow just-in-time provisioning to the right applications. As long as your applications support open standards, they will be able to consume tokens issued by OneLogin.

Synchronize users with any number of directories, such as Active Directory, LDAP, Workday, or Google Apps. Leverage identity and access management (IAM) technology to import custom user attributes and

pass them on to downstream apps via SAML or API-based provisioning. The integration with Active Directory synchronizes users in real-time and supports multiple forests and domains via a single connector.

Aside from the thousands of applications listed in the docs below, OneLogin provides the ability to create custom app integrations via our connector templates for all supported authentication protocols.

List of Supported SAML-based Apps

List of Supported Provisioning Apps

List of Supported Form-Based Apps

The OneLogin platform is extremely extensible and can integrate with 3rd party systems via:

- Webhooks for SIEM integration
- API
- CSV export/import
- Agent installation
- LDAP
- RADIUS

OneLogin also provides free, open-source SAML toolkits for Java, .NET, Ruby and PHP which both vendors and enterprises can use to add enterprise-strength SSO to their applications.

**The solution must be able integrate with our existing identity sources including Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Ultimate Kronos Group (UKG)**

**Dell Response:** Onelogin seamlessly integrates with established identity sources such as Ultimate Kronos Group (UKG), Active Directory (AD), and Lightweight Directory Access Protocol (LDAP). Onelogin connects with Ultimate Kronos Group (UKG) via a pre-configured connector accessible within the Onelogin administrator portal. Setting up this connector is a straightforward process, providing a powerful capability to transfer data efficiently between Onelogin and UKG.

Integration with AD and LDAP involves the deployment of a lightweight agent on a system within your environment. This agent ensures secure data transfer between the directory and Onelogin via HTTPS, minimizing the need for extensive firewall modifications. To enhance redundancy, it is advisable to install this agent on a minimum of two systems.

**The solution must provide a seamless migration path for users from our existing identity infrastructure.**

**Dell Response:** There are several ways to migrate users from existing platforms. OneLogin supports importing users using custom database connections as well as API driven migrations, bulk import and syncing users from a directory.



For database migrations, if the user passwords are hashed in a format that OneLogin supports, a simple import of the users into OneLogin is possible. If the passwords are not stored in a format that OneLogin supports, then OneLogin's User Migration SmartHook would be the best option.

Upon first login of a user to OneLogin, there will not be a user record in the OneLogin user directory. At this point, a SmartHook connection can retrieve the user's record from your existing database. Once the authentication request is completed, OneLogin adds the newly acquired user record to the OneLogin user directory. Over the course weeks or months, most of the users will have been automatically migrated over without seeing any user experience changes. For the remaining users, bulk import can be used, but they will require password resets. Once the process is complete, the existing external database can be retired.

Additionally, data can be migrated via Rest API, CSV upload, or Directory synchronization (e.g. AD, LDAP). Users can also be migrated 'Just In Time' (JIT) at point of authentication by leveraging the OneLogin User Migration Hook. There is more information regarding this subject in our Introduction to User Management Knowledge Base article.

**Authentication methods must include SAML2.0, SP(Service Provider) and IDP (Identity Provider) methods of authentication.**

**Dell Response:** OneLogin supports both SP and IDP authentication methods using SAML 2.0.

**The solution presented must be cloud-based.**

**Dell Response:** OneLogin is a cloud-based Identity as a Service (IDaaS) provider. The system is constructed in AWS, employing a microservices architecture to enhance flexibility and efficiency. Its scalability is ensured through AWS technologies like elastic load balancing, allowing the platform to efficiently handle varying workloads. The implementation incorporates shards, specifically in EU and US regions. To ensure failover and redundancy, the system spans multiple operating regions and availability zones, enhancing overall reliability. Additionally, the design incorporates shared tenants, with the assurance that no customer data or keys are shared, emphasizing security and privacy.

### Qualifications and Experience:

- 1. Can apps integrate directly with the solution's Application Programming Interface (API) to perform restful Application Programming Interface calls such as reading user information, or making changes to user objects, group membership.**

**Dell Response:** OneLogin offers a full suite of REST APIs, including Users APIs, that can be leveraged to sync application changes, provide authentication and access management for external parties, and otherwise extend the platform's functionality through customization.

- 2. Indicate if the proposed solution provides the ability to create custom Application Programming Interface access policies and/or authorized servers. Provide details.**

**Dell Response:** OneLogin offers a full suite of REST APIs, including Users APIs, that can be leveraged to sync application changes, provide authentication and access management for external

parties, and otherwise extend the platform's functionality through customization. OneLogin has built API authorization capabilities into our OIDC framework, meaning that OneLogin is able to generate custom access tokens with configurable claims/scopes/audiences to be used for internal APIs. This authorization server capability can be easily combined with OIDC flows so that client apps can receive both id tokens as well as access tokens from a single request.

A sample of such APIs include:

- Credential validation
- AML assertion generation
- Vigilance AI
- Roles management
- Configuration management of features such as apps, mappings, API authorization, etc

Alternatively, some scenarios (in particular relating to federation), rely upon the user interacting to some extent with the OneLogin (authentication) UI. In these situations, OneLogin can be configured to make the wrapper service the target for subsequent redirects (e.g. to deliver SAML assertions or OIDC tokens) rather than the end-applications themselves.

There are different permissions that can be granted for API access. Please reference scoped API privileges here for what would be most appropriate for your use case.

3. **Indicate if your service/solution offers Application Programming Interface token management and creation. If the solution offers this capability, provide details on API token management and creation capabilities.**

**Dell Response:** Generation of Access and Refresh Tokens for the OneLogin API follows The OAuth 2.0 Authorization Framework specified in RFC Specification 6749

Tokens can be generated via the Generate Tokens endpoint: <https://developers.onelogin.com/api-docs/2/oauth20-tokens/generate-tokens-2>

Once generated, an Access Token is valid for 10 hours. Assuming that you are using the same Client ID & Client Secret, the request to generate a token will always return the same token set until the token expires, or is revoked.

Access Tokens can be revoked via the Revoke Token endpoint: <https://developers.onelogin.com/api-docs/2/oauth20-tokens/revoke-tokens>

4. **Describe the Application Programming Interface capabilities your solution offers for integration with custom applications and workflows.**

**Dell Response:** Aside from the thousands of applications listed in the docs below, OneLogin provides the ability to create custom app integrations via our connector templates for all supported authentication protocols.

List of Supported SAML-based Apps

List of Supported Provisioning Apps

List of Supported Form-Based Apps

The OneLogin platform is extremely extensible and can integrate with 3rd party systems via:

- Webhooks for SIEM integration
- API
- OneLogin provides a comprehensive RESTful API that can be used for administering the OneLogin platform. The APIs available include but are not limited to tasks such as user CRUD operations, granting/revoking application access, password resets, force logouts, security policy assignment, app configuration and more. As a part of our developer resources we provide SDKs in many popular programming languages and also support Swagger/OpenAPI Specification to enable developers to create SDKs in other languages.
- Our API is fully documented within our developer portal.
- CSV export/import
- Agent installation
- LDAP
- RADIUS

OneLogin also provides free, open-source SAML toolkits for Java, .NET, Ruby and PHP which both vendors and enterprises can use to add enterprise-strength SSO to their applications.

##### 5. How do you ensure the security and privacy of data transmitted through your Application Programming Interfaces?

**Dell Response:** Access to the OneLogin API is authorized via unique API Credential Pairs, which you may configure and permission appropriately. You can read all about this in the "API Credentials" section of the API Documentation here: <https://developers.onelogin.com/api-docs/1/getting-started/working-with-api-credentials>

Currently, the following permission sets are available for any API Credential Pair that you create:

- Authentication Only

Gives the credential pair the ability to generate an access token that can perform POST calls only to authentication endpoints, providing least privileged access to authentication code. These endpoints include: Verify Factor (SAML Assertion), Generate SAML Assertion, Verify Factor (Login), Create Session Login Token, Log User Out

- Read Users (Read user fields, roles, and groups)

Gives the credential pair the ability to generate an access token that can perform GET calls available for the User, Role, and Group API resources.

- Manage Users (Read/write user fields, roles, and groups)

Gives the credential pair the ability to generate an access token that can perform GET, POST, PUT, and DELETE calls available for the User, Role, and Group API resources, with the exception of setting passwords and assigning and removing roles.

- Read All (Read all objects)

Gives the credential pair the ability to generate an access token that can perform GET calls available for all API resources.

- Manage All (Read/Write all objects. Equivalent of Super User)

Gives the credential pair the ability to generate an access token that can perform GET, POST, PUT, and DELETE calls for all available API resources, including the ability to set passwords and assign and remove roles.

**6. Can your solution support standards like Open Authorization (OAuth) 2.0 and OpenID Connect for secure Application Programming Interface access?**

**Dell Response:** OneLogin supports the standard OAuth/OIDC flows, including the code+PKCE flow which is best practice for modern native mobile applications and SPAs.

**7. Detail the scalability of your Application Programming Interface infrastructure to support high volumes of authentication and authorization requests.**

**Dell Response:** The SSO tier is primarily responsible for handling login requests and serving end users with the web interface they use to log into 3rd-party applications. The tier is front ended by an Elastic Load Balancer (ELB) and distributed between three availability zones (AZ) within each AWS region, with each tenant operating in two AWS regions. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ.

The Admin tier is primarily responsible for handling administrative functions within an instance and serving admin users with the web interface to manage their OneLogin instance. The tier is front ended by an Elastic Load Balancer (ELB) and distributed between three availability zones (AZ) within one AWS region. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ, and the Admin tier can fail over to the secondary AWS region if required.

As additional services are created and come online, they are deployed following a common pattern with minor deviations based on the specific needs of the service. The front end tier is front ended by an Elastic Load Balancer (ELB) and distributed between three availability zones (AZ) within one AWS region. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ. Additional services can fail over to the secondary AWS region if required.

**8. Does your solution provide Remote Authentication Dial-In User Service (RADIUS) support that does not require on-premise components?**

**Dell Response:** Yes, the Onelogin RADIUS solution is 100% cloud based and does not require the use of on-premises components such as agents installed on a device the State of West Virginia manages. There is detailed information on how this is configured here - > [https://onelogin.servicenow.com/support?id=kb\\_article&sys\\_id=041a52f887e17150695f0f66cebb357b](https://onelogin.servicenow.com/support?id=kb_article&sys_id=041a52f887e17150695f0f66cebb357b)

**9. Indicate if the solution provides supported push notification. If so, what controls can be used to lower the risk of push fatigue attacks.**

**Dell Response:** Yes, Onelogin provides a TOTP authenticator called Onelogin Protect. This mobile application is available on iOS and Android devices and is provided free of charge to Onelogin customers. Onelogin Protect supports push notifications, biometric verification, prevention of jailbroken devices, screen lock enforcement and backup/restore functionality. To defend against push fatigue attacks, Onelogin Protect offers number matching and the ability to disable push notifications, such that the user must enter their code.

**10. List the Multi-factor methods supported.**

**Dell Response:** OneLogin provides support for a variety of different authenticators and methods for performing MFA. The most popular of these is OneLogin Protect, our proprietary OTP mobile application, which is easy for users to install on their devices and supports multiple accounts on the same device.

Other factors include WebAuthN (for biometric & NFC devices), OneLogin Voice, SMS text, email, and security questions, and integrations with all major third-party MFA vendors such as Yubikey, Google Authenticator, DUO, and more.

These factors can be enabled or required for different sets of users or different applications based on the security policies your administrators can configure and assign.

OneLoginPartnersOneLogin ProtectTrusted IdPOneLogin SMSRADIUSOneLogin Security QuestionsYubicoWebAuthNSymantecOneLogin VoiceAuthenticatorEmail MFADUO SecurityOneSpan

**11. Does your service offer out of the box login flows that protect against brute force attacks?**

**Dell Response:** Yes, OneLogin offers out of the box login flows that protect against brute-force attacks. OneLogin Smart Factor Authentication uses machine learning to determine the risk level for every login event. It uses a broad set of inputs, including networks, devices, geography, geo-velocity, time of day, and other threat factors to build a risk score of each login attempt. Admins can set risk tolerance thresholds that determine what the user experience is based on risk score. For example, logins with a low risk don't get challenged for MFA, logins with moderate risk must perform an MFA challenge, and logins with high risk are blocked from access. Admins can fine-tune the risk engine using custom rules to do things such as blacklist/whitelist specific IPs or geographies. Using roles-based access controls, security restrictions can be applied to users on an individual or group basis.

SmartFactor Authentication includes the ability to perform a compromised credential check and customize the login flow. Using SmartFactor's compromised credential check feature, OneLogin is able to check a user's password when they update it or set it for the first time against databases of compromised credentials that have been stolen in large-scale attacks to prevent the use of stolen passwords. Any previously compromised credentials can be blocked from usage.

Upon using a previously compromised credential, the end-user will receive a visual alert that the password submission contains insecure elements and prevented from using that password. Admins can view attempted compromised credential usage within the events log and this of course can also be streamed to a SIEM or CASB. Additionally, custom notifications can be built for admins to be notified when such a password change failure occurs.

SmartFactor Authentication also detects anomalies, and mitigates known malicious threats.

#### Brute Force Attack Mitigation

SmartFactor enabled security policies provide a "brute force protection" login flow. MFA is integrated into a brute-force defense login flow that is designed to protect accounts from common brute force, brute spray and dictionary style attacks. The brute-force authentication flow follows a UserID/MFA/Password login flow.

#### Anomaly Detection

SmartFactor Authentication uses machine learning from a broad set of inputs to establish a baseline of user login behavior. Each login attempt is evaluated for anomalies or exceptions to the established user baseline generating a risk score. The risk score can be used to take mitigation actions including challenge for MFA or denial of access.

#### Known Malicious Threat Mitigation

SmartFactor Authentication evaluates each login session against real time threat intelligence services to mitigate malicious activity from known malicious threats.

**12. Indicate if the proposed service offers out of the box login flows that protect against brute-force attacks and describe the protection against these attacks.**

**Dell Response:** This is a duplicate of the previous question. Please see the answer to 4.3.1.11.

**13. Detail the authentication methods supported by your platform (e.g., Email Multi-Factor Authentication (MFA), Short Message/Messaging Service (SMS) MFA, Biometric/Web Authentication API (WebAuthN), and define any other capabilities that the vendor offers.**

**Dell Response:** OneLogin provides support for a variety of different authenticators and methods for performing MFA. The most popular of these is OneLogin Protect, our proprietary OTP mobile application, which is easy for users to install on their devices and supports multiple accounts on the same device.



Other factors include WebAuthN (for biometric & NFC devices), OneLogin Voice, SMS text, email, and security questions, and integrations with all major third-party MFA vendors such as Yubikey, Google Authenticator, DUO, and more.

These factors can be enabled or required for different sets of users or different applications based on the security policies your administrators can configure and assign. Security policies can be highly customizable, allowing you to create the best authentication processes to meet your org's needs, or even to support multiple users with different needs. Users in the office might prefer a hardware factor like YubiKey because of its ease of use, for example, while users who travel could instead use OneLogin Protect because it's conveniently on their phone. You can configure user settings individually or with a mapping, but the best way to maximize security and ease of access is to set up MFA with user groups and policies. You can apply any desired exceptions for your MFA policies. For example, you can allow users to bypass MFA if they're signing in from a trusted device or specific IP address.

#### 14. How does your solution provide adaptive authentication based on risk assessment?

**Dell Response:** OneLogin's SmartFactor Authentication uses machine learning to determine the risk level for every login event. It uses a broad set of inputs, including networks, devices, geography, time of day, and many other threat factors to build a risk score of each login attempt. Admins can set risk tolerance thresholds that determine what the user experience is based on risk score.

SmartFactor is powered by OneLogin's proprietary UEBA engine known as Vigilance AI.

Vigilance AI has a series of predefined and customer-generated rules that are run alongside behavioral and machine learning models which are collectively known as Analyzers. Each Analyzer is assigned a dynamic weight that is influenced by the quantity of data, peer insights, and user behavior. The weights drive the overall risk score produced by the service and can be further influenced by the customer through the creation of black/whitelist rules.

For example, Vigilance AI may determine that a user's device usage, location, and threat intelligence are all normal, but the fact that they are accessing a resource at an unusual time of day based on their previous behavior could trigger a higher risk score.

The resulting risk score can be used to modify the amount of authentication friction that is required. For example, logins with low risk don't get challenged for MFA, logins with moderate risk must perform an MFA challenge, and logins with high risk are blocked from access. Admins can fine-tune the risk engine using custom rules to do things such as blocklist/allowlist specific IPs or Geographies.

SmartFactor Authentication also includes the ability to perform a compromised credential check and customize the login flows.

#### 15. Can your solution integrate with third-party identity providers for federated authentication?

**Dell Response:** Yes, OneLogin can integrate with third-party identity providers for federated authentication. The Trusted IdP (identity provider) feature in OneLogin enables you to configure multiple identity providers to securely sign users into OneLogin and OneLogin-protected



applications. Trusted IdP supports 3 protocols: SAML, OIDC and OAuth. This feature allows users to log in to OneLogin with credentials from a different identity provider.

#### IdP-Initiated Flow

Using SAML assertion or OIDC/OAuth flow from one or more 3rd-party identity providers, users can authenticate into the OneLogin Portal.

#### OneLogin-Initiated Flow

Or users can access and gain SSO to any application integrated with OneLogin (SAML, OIDC, WS-Federation, Forms-based, or via OneLogin Access).

#### Just-In-Time (JIT) Provisioning

Create new users in the OneLogin directory with just-in-time provisioning (JIT), with the information specified by trusted identity providers.

- 16. Indicate which authentication protocols the proposed solution supports (e.g., Security Assertion Markup Language (SAML) 2.0, OpenID Connect (OIDC) , Remote Authentication Dial-In User Service (RADIUS). Identify any other authentication protocols the proposed solution offers.**

**Dell Response:** OneLogin supports the open authentication standards of SAML 2.0, WS-Fed, OpenID Connect (OIDC), Remote Authentication Dial-In User Service(RADIUS), LDAP, API-based, and Header-based authentication as primary protocols. With these open-source standards, organizations can tie endpoints to their OneLogin account for streamlined and securely controlled user access.

- 17. Explain how your solution adapts authentication methods based on contextual factors like location and device.**

**Dell Response:** OneLogin has a feature called "Smart Factor Authentication" this uses machine learning to determine the risk level for every login event. It uses a broad set of inputs, including networks, devices, geography, geo-velocity, time of day, and other threat factors to build a risk score of each login attempt. Admins can set risk tolerance thresholds that determine what the user experience is based on risk score. For example, logins with a low risk don't get challenged for MFA, logins with moderate risk must perform an MFA challenge, and logins with high risk are blocked from access. Admins can fine-tune the risk engine using custom rules to do things such as blacklist/whitelist specific IPs or geographies. Using roles-based access controls, security restrictions can be applied to users on an individual or group basis.

- 18. How does your solution handle scenarios where a user has lost their primary authentication device?**

**Dell Response:** OneLogin administrators can issue a temporary OTP code to allow a user to sign in without their second factor. Alternatively, additional factors can be enabled so that a user can still authenticate without their primary second factor (ex. security questions).

**19. Can the solution block access based on blacklisted Internet Protocol (IP) addresses or Geogrphah (GEO) location?**

**Dell Response:** OneLogin security policies can be used to set allowable IP addresses or ranges, this can be applied to users for overall access to the portal or to just specific applications. Through OneLogin SmartFactor you have the ability to specify country based blocklisting to deny access from selected countries.

**20. Does the service identify, detect, and block suspicious authentication activity?**

**Dell Response:** OneLogin's Smart Factor Authentication uses machine learning to determine the risk level for every login event. It uses a broad set of inputs, including networks, devices, geography, time of day, and many other threat factors to build a risk score of each login attempt. Admins can set risk tolerance thresholds that determine what the user experience is based on risk score.

Smart Factor is powered by OneLogin's proprietary UEBA engine known as Vigilance AI.

Vigilance AI has a series of predefined and customer-generated rules that are run alongside behavioural and machine learning models which are collectively known as Analysers. Each Analyser is assigned a dynamic weight that is influenced by the quantity of data, peer insights, and user behaviour. The weights drive the overall risk score produced by the service and can be further influenced by the customer through the creation of black/whitelist rules.

For example, Vigilance AI may determine that a user's device usage, location, and threat intelligence are all normal, but the fact that they are accessing a resource at an unusual time of day based on their previous behaviour could trigger a higher risk score.

The resulting risk score can be used to modify the amount of authentication friction that is required.

For example, logins with low risk don't get challenged for MFA, logins with moderate risk must perform an MFA challenge, and logins with high risk are blocked from access. Admins can fine-tune the risk engine using custom rules to do things such as blacklist/whitelist specific IPs or Geographies.

SmartFactor Authentication also includes the ability to perform a compromised credential check and customize the login flows.

**21. Does the solution perform behavior detection during authentication? (Example: Impossible Travel, Device context, Network Context,)**

**Dell Response:** OneLogin Smart Factor Authentication uses machine learning to determine the risk level for every login event. It uses a broad set of inputs, including networks, devices, geography, geo-velocity, time of day, and other threat factors to build a risk score of each login attempt. Admins can set risk tolerance thresholds that determine what the user experience is based on risk score. For example, logins with a low risk don't get challenged for MFA, logins with moderate risk must perform an MFA challenge, and logins with high risk are blocked from access. Admins can fine-tune the risk engine using custom rules to do things such as blacklist/whitelist specific IPs or

geographies. Using roles-based access controls, security restrictions can be applied to users on an individual or group basis.

SmartFactor Authentication includes the ability to perform a compromised credential check and customize the login flow. Using SmartFactor's compromised credential check feature, OneLogin is able to check a user's password when they update it or set it for the first time against databases of compromised credentials that have been stolen in large-scale attacks to prevent the use of stolen passwords. Any previously compromised credentials can be blocked from usage.

Upon using a previously compromised credential, the end-user will receive a visual alert that the password submission contains insecure elements and prevented from using that password. Admins can view attempted compromised credential usage within the events log and this of course can also be streamed to a SIEM or CASB. Additionally, custom notifications can be built for admins to be notified when such a password change failure occurs.

SmartFactor Authentication also offers protection against brute force attacks, anomaly detection, and mitigates known malicious threats.

#### Brute Force Attack Mitigation

SmartFactor enabled security policies provide a "brute force protection" login flow. MFA is integrated into a brute-force defense login flow that is designed to protect accounts from common brute force, brute spray and dictionary style attacks. The brute-force authentication flow follows a UserID/MFA/Password login flow.

#### Anomaly Detection

SmartFactor Authentication uses machine learning from a broad set of inputs to establish a baseline of user login behavior. Each login attempt is evaluated for anomalies or exceptions to the established user baseline generating a risk score. The risk score can be used to take mitigation actions including challenge for MFA or denial of access.

#### Known Malicious Threat Mitigation

SmartFactor Authentication evaluates each login session against real time threat intelligence services to mitigate malicious activity from known malicious threats.

For more information, check out some of our Knowledge Base articles:

- Smart Passwords
- Roles
- Groups
- User Policies
- App Policies
- SmartFactor Authentication

## **22. How does your platform detect and prevent unauthorized access?**

---

**Dell Response:** OneLogin's Smart Factor Authentication uses machine learning to determine the risk level for every login event. It uses a broad set of inputs, including networks, devices, geography, time of day, and many other threat factors to build a risk score of each login attempt. Admins can set risk tolerance thresholds that determine what the user experience is based on risk score.

Smart Factor is powered by OneLogin's proprietary UEBA engine known as Vigilance AI.

Vigilance AI has a series of predefined and customer-generated rules that are run alongside behavioural and machine learning models which are collectively known as Analysers. Each Analyser is assigned a dynamic weight that is influenced by the quantity of data, peer insights, and user behaviour. The weights drive the overall risk score produced by the service and can be further influenced by the customer through the creation of black/whitelist rules.

For example, Vigilance AI may determine that a user's device usage, location, and threat intelligence are all normal, but the fact that they are accessing a resource at an unusual time of day based on their previous behaviour could trigger a higher risk score.

The resulting risk score can be used to modify the amount of authentication friction that is required. For example, logins with low risk don't get challenged for MFA, logins with moderate risk must perform an MFA challenge, and logins with high risk are blocked from access. Admins can fine-tune the risk engine using custom rules to do things such as blacklist/whitelist specific IPs or Geographies.

SmartFactor Authentication also includes the ability to perform a compromised credential check and customize the login flows.

**23. Can your platform support attribute-based access control (ABAC) to dynamically adjust access based on user attributes?**

**Dell Response:** Attributes assigned to a user can be used to automatically assign security policies inside of OneLogin. The Security Policies define the access/ access requirements of the user. If the user's attributes change the security policies can dynamically be reassigned, changing the user's access/ access requirements.

**24. Can your solution integrate with external identity providers to extend authorization capabilities?**

**Dell Response:** The Trusted IdP (identity provider) feature in OneLogin enables you to configure multiple identity providers to securely sign users into OneLogin and OneLogin-protected applications. Trusted IdP supports 3 protocols: SAML, OIDC and OAuth. This feature allows users to log in to OneLogin with credentials from a different identity provider.

IdP-Initiated Flow

Using SAML assertion or OIDC/OAuth flow from one or more 3rd-party identity providers, users can authenticate into the OneLogin Portal.

### OneLogin-Initiated Flow

Or users can access and gain SSO to any application integrated with OneLogin (SAML, OIDC, WS-Federation, Forms-based, or via OneLogin Access).

### Just-In-Time (JIT) Provisioning

Create new users in the OneLogin directory with just-in-time provisioning (JIT), with the information specified by trusted identity providers.

## **25. Can your platform enforce access policies based on contextual factors such as, but not limited to time of day, location, and user behavior?**

**Dell Response:** OneLogin Smart Factor Authentication uses machine learning to determine the risk level for every login event. It uses a broad set of inputs, including networks, devices, geography, geo-velocity, time of day, and other threat factors to build a risk score of each login attempt. Admins can set risk tolerance thresholds that determine what the user experience is based on risk score. For example, logins with a low risk don't get challenged for MFA, logins with moderate risk must perform an MFA challenge, and logins with high risk are blocked from access. Admins can fine-tune the risk engine using custom rules to do things such as blacklist/whitelist specific IPs or geographies. Using roles-based access controls, security restrictions can be applied to users on an individual or group basis.

SmartFactor Authentication includes the ability to perform a compromised credential check and customize the login flow. Using SmartFactor's compromised credential check feature, OneLogin is able to check a user's password when they update it or set it for the first time against databases of compromised credentials that have been stolen in large-scale attacks to prevent the use of stolen passwords. Any previously compromised credentials can be blocked from usage.

Upon using a previously compromised credential, the end-user will receive a visual alert that the password submission contains insecure elements and prevented from using that password. Admins can view attempted compromised credential usage within the events log and this of course can also be streamed to a SIEM or CASB. Additionally, custom notifications can be built for admins to be notified when such a password change failure occurs.

SmartFactor Authentication also offers protection against brute force attacks, anomaly detection, and mitigates known malicious threats.

### Brute Force Attack Mitigation

SmartFactor enabled security policies provide a "brute force protection" login flow. MFA is integrated into a brute-force defense login flow that is designed to protect accounts from common brute force, brute spray and dictionary style attacks. The brute-force authentication flow follows a UserID/MFA/Password login flow.

### Anomaly Detection

SmartFactor Authentication uses machine learning from a broad set of inputs to establish a baseline of user login behavior. Each login attempt is evaluated for anomalies or exceptions to the

established user baseline generating a risk score. The risk score can be used to take mitigation actions including challenge for MFA or denial of access.

#### Known Malicious Threat Mitigation

SmartFactor Authentication evaluates each login session against real time threat intelligence services to mitigate malicious activity from known malicious threats.

For more information, check out some of our Knowledge Base articles:

- Smart Passwords
- Roles
- Groups
- User Policies
- App Policies
- SmartFactor Authentication

#### **26. Describe your solution's approach to enforcing the principle of least privilege for user access.**

**Dell Response:** OneLogin has a flexible Role-Based Access Control engine that can be used to grant access to specific applications or assign users to security policies.

Users are only assigned access based on what is relevant to their position, this allows for granular assignment compared to broad access.

Roles are the most efficient way to control your users' access to apps. Create a role, assign apps to it, and when you assign users to the role, you grant them access to all of the apps included in the role. This gives you the ability to give or take away a user's access to multiple apps at once, or to grant or remove an app's access to multiple users at once. You can also use roles to filter and search for users when performing a variety of other OneLogin functions, such as sending invitations, creating mappings, or configuring reports and notifications.

#### **27. How does your platform support session termination and re-authentication based on inactivity or specific triggers?**

**Dell Response:** OneLogin has the option to allow sessions to the OneLogin platform to persist when the browser is closed. This persistent session allows users to remain authenticated after they exit so they can then return to their browser and have access to a resource. Session duration can be based upon a fixed amount of time or a period of time since the user performed any activity. For example, a user must re-authenticate with OneLogin after 2 hours regardless if the user is active or not or if after a set period of Inactivity the user must re-authenticate with OneLogin.

Session expiration is controlled by set user policies within OneLogin and combined with a cookie in the users' browser. Session duration can be configured to be as short as one minute or as long as



never expiring. Because this is configured on a user policy it can be different for different groups of users or scenarios (including shared kiosks). The user's policies, then, influences session management and these include scenarios where detected anomalies and feedback from step-up authentication can trigger session/user expiration.

Session duration for applications hosted through OneLogin is managed by the applications.

**28. Does the solution have the ability to have isolated lower environments for the purposes of testing / development?**

**Dell Response:** OneLogin can make available for configuration a sandbox environment if applicable environment has been purchased. There are two different Sandbox environments OneLogin provides, as detailed below.

**Developer Sandbox:** The OneLogin Developer Sandbox allows organizations to test and unlock the full functionality of the OneLogin platform, without the production data involved.

Details:

- Provides an additional non-production OneLogin account
- Intended for development and small scale testing
- Blank slate - does not include production configuration and data

**Enterprise Sandbox:** Unlike others, the OneLogin Enterprise Sandbox empowers you to test new capabilities and configurations in a safe staging environment at scale, using near-production data, before confidently deploying to production. Other vendors in the space offer a standard sandbox, where you will be required to build and reconfigure each time you would like to test. OneLogin's Enterprise Sandbox is different - with the click of a button, we will clone all configurations in your production account (unconnected from SAML and Provisioning for safety sake) and replicate it in a sandbox so you can begin testing right away.

Details:

- Provides an additional non-production OneLogin account
- Intended for full-scale testing
- Includes near-complete data replication from production
- Limited to the same number of seats as the production account

**29. Does your solution provide multiple environments for testing purposes?**

**Dell Response:** More than one Sandbox environment could be made available. OneLogin can make available for configuration a sandbox environment if applicable environment has been purchased. There are two different Sandbox environments OneLogin provides, as detailed below.



**Developer Sandbox:** The OneLogin Developer Sandbox allows organizations to test and unlock the full functionality of the OneLogin platform, without the production data involved.

Details:

- Provides an additional non-production OneLogin account
- Intended for development and small scale testing
- Blank slate - does not include production configuration and data

**Enterprise Sandbox:** Unlike others, the OneLogin Enterprise Sandbox empowers you to test new capabilities and configurations in a safe staging environment at scale, using near-production data, before confidently deploying to production. Other vendors in the space offer a standard sandbox, where you will be required to build and reconfigure each time you would like to test. OneLogin's Enterprise Sandbox is different - with the click of a button, we will clone all configurations in your production account (unconnected from SAML and Provisioning for safety sake) and replicate it in a sandbox so you can begin testing right away.

Details:

- Provides an additional non-production OneLogin account
- Intended for full-scale testing
- Includes near-complete data replication from production
- Limited to the same number of seats as the production account

**30. Does the solution allow automation of tasks through scripting or Application Programming Interface calls?**

**Dell Response:** OneLogin allows for automation of tasks through both plug and play options found within the Administration console as well as through API calls.

**31. Do you offer flexible application integrations such as general Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and Open Authorization (Oauth) connectors?**

**Dell Response:** OneLogin supports SSO connections to integrated applications over OIDC, SAML, WsFed, OpenID and forms based authentication. OneLogin also supports integration to other external iDPs via our Trusted iDP capability which supports federation via the OIDC/Oauth2/SAML2 standards.

**32. Do you offer deployment assistance, documentation, or training to ensure a smooth transition to your platform?**

**Dell Response:** OneLogin offers deployment assistance through professional services, which is a paid service that would be scoped to your requirements. We have a public facing Knowledge Base that has documentation around configuration and feature sets. OneLogin also offers a paid multi-

day instructor led virtual course around administration essentials. All of these options are designed to ensure a smooth transition for our customers.

**33. Can the solution leverage Active Directory as the Identity Provider? If so, do agents need to be installed on our systems to facilitate that communication? Additionally, is your solution capable of syncing that information in real time?**

**Dell Response:** OneLogin Active Directory Connectors provide real-time synchronization of users between Active Directory (AD) and OneLogin.

The OneLogin Active Directory Connector (ADC) is an MSI which is deployed on any member server and runs as a Windows Service. Several ADCs can be deployed on different servers to provide high availability, load balancing, and automatic failover.

There are two optional configuration settings:

- Enable directory fallback password cache. Enabled by default, this setting caches a hash of the user AD passwords that enables OneLogin to authenticate a user with the last successful password, in the event of lost communication between OneLogin and AD.
- Enable password mapping. This setting caches encrypted AD passwords in OneLogin to provide access to apps that use SSO password for app authentication.

**34. If an agent is required to facilitate a connection between Active Directory and your service, please describe how that information is exchanged securely. Additionally, please describe how redundancy and failover can be configured to ensure there is a constant flow of information.**

**Dell Response:** For Active Directory, the OneLogin Active Directory Connector is an MSI which is deployed on any member server and runs as a Windows Service, the agent communicates to OneLogin via port 443. Several Active Directory Connectors can be deployed on different servers to provide high availability, load balancing, and automatic failover. The LDAP connector is very similar, but runs in a Java Runtime Environment (JRE), and also supports high availability and failover.

**35. Does the solution support the ability to import password hashes from other Identity Providers (IDPs)? If so, describe what hashing algorithms are supported and how that process works.**

**Dell Response:** Yes. Data import from databases can be done through API connections or manually with CSV file imports. If you have access to salts and know the hashing algorithm, OneLogin can even import pre-existing user passwords.

**36. Do you have an administrator dashboard User Interface (UI) to manage users? Can you enforce a specific multi-factor type for administrative access?**

**Dell Response:** OneLogin offers an Administrator dashboard UI to manage users, specific MFA requirements can be made to ensure Administrators perform a specific MFA type compared to an end user.

**37. Does the solution support external federation? If so, how, and what Identity Providers (IdPs) are supported?**

**Dell Response:** The Trusted IdP (identity provider) feature in OneLogin enables you to configure multiple identity providers to securely sign users into OneLogin and OneLogin-protected applications. Trusted IdP supports 3 protocols: SAML, OIDC and OAuth. This feature allows users to log in to OneLogin with credentials from a different identity provider.

IdP-Initiated Flow

Using SAML assertion or OIDC/OAuth flow from one or more 3rd-party identity providers, users can authenticate into the OneLogin Portal.

OneLogin-Initiated Flow

Or users can access and gain SSO to any application integrated with OneLogin (SAML, OIDC, WS-Federation, Forms-based, or via OneLogin Access).

Just-In-Time (JIT) Provisioning

Create new users in the OneLogin directory with just-in-time provisioning (JIT), with the information specified by trusted identity providers.

**38. How does your solution streamline user onboarding and offboarding processes?**

**Dell Response:** OneLogin can help to automate many of the processes of user lifecycle management!

- Automatic user synchronization from external directories such as AD, LDAP, and HRIS
- Automatic user provisioning into both cloud-based and on-premises applications
- User de-provisioning/deletion
- Assigning user entitlements within downstream applications using flexible conditions-based rules.

OneLogin has existing, out of the box integrations for user provisioning with SaaS applications, and we offer toolkits and SDKs to enable custom developed applications to support this functionality. Our app connector catalog has thousands of pre-built connectors, and OneLogin provides a general SCIM connector that can be used to configure provisioning to any app that support SCIM provisioning. OneLogin also offers an embedded extensible provisioning platform which is GUI-based and can be used to create custom provisioning integrations using a variety of different protocols and methods including SCIM, Generic HTTP (REST/SOAP), CSV via SFTP, Databases (MySQL, SQL Server, PostgreSQL), AD/LDAP, and on-premises command line scripts.

OneLogin fully supports rules-based workflow automation, allowing you to control and automate the process of granting users permissions based on OneLogin attributes like roles and groups, or custom attributes to match your needs. Custom workflows can be triggered via the OneLogin Event Broadcaster or via a SCIM integration. OneLogin workflows can also help integrate OneLogin with external systems and provide more complex ways of manipulating user data during provisioning and de-provisioning processes.

Since rules-based mappings are enforced, OneLogin immediately recognizes changes and appropriates the user into the correct role. For example, if a teacher has the title attribute for 5th grade but the next year becomes a 6th-grade teacher, then once that AD attribute reflects that update, the teacher will have all 6th-grade teaching applications immediately applied to their account.

When a user logs into the platform for the first time, they will be sent an invitation email or given a subdomain and initial username/password for the OneLogin tenant. Once the user authenticates, they will be forced to change their password in compliance with password policies.

When a user leaves the system, their account can be immediately de-provisioned. Once the user account is disabled in AD or OneLogin, access is immediately revoked. Access for any SAML app is automatically restricted, and accounts linked through provisioning are automatically suspended or deleted in the associated apps.

For more in-depth information about provisioning, check out our Knowledge Base articles:

[Introduction to User Provisioning](#)

[Introduction to App Management](#)

### 39. How does your platform handle role-based access control and user provisioning?

**Dell Response:** OneLogin has a flexible Role-Based Access Control engine that can be used to grant access to specific applications or assign users to security policies. This flexible RBAC engine allows admins to configure condition based rules using any user attribute as a condition. (Ex. AD Security groups, DistinguishedName, Title, Department, etc.)

Using our RBAC, OneLogin can assign applications and security policies associated with these applications automatically based on the user's role with the organization which provide levels of access to each application if they support provisioning.

OneLogin supports directory services over LDAP for search and bind functions from LDAP clients using the VLDAP feature. VLDAP frees you from having to run LDAP servers. It adds an LDAP interface to OneLogin's cloud directory, giving you a high availability, scalable LDAP service.

OneLogin VLDAP integrates with your VPN, network-attached storage (NAS), older web servers, and office WiFi, allowing them to use identities from cloud directories such as Workday, Google Apps, UltiPro, BambooHR, etc. for authentication and authorization.

**40. What customization options are available for the user interface and branding?**

**Dell Response:** Our powerful Branding tools allow you to customize OneLogin's user interface so that it mirrors your organization's brand identity, visually integrates with your help desk, and provides your users with a consistent look and feel. Almost every aspect of the user portal can be customized, including the banner, logo, and UI element colors, login screen prompts and imagery, notifications and user invitations, and error messages and help and support text.

With a OneLogin plan that includes Advanced Branding, you can additionally create and manage multiple different brand identities to provide unique branding options for your different applications.

**41. Are all Multi-Factor Authentication (MFA) factors available for use in authenticating a user prior to performing self-service password maintenance?(E.g., Forgot Password, Change Password, Account Unlock)**

**Dell Response:** OneLogin provides support for a variety of different authenticators and methods for performing MFA. The most popular of these is OneLogin Protect, our proprietary OTP mobile application, which is easy for users to install on their devices and supports multiple accounts on the same device.

Other factors include WebAuthN (for biometric & NFC devices), OneLogin Voice, SMS text, email, and security questions, and integrations with all major third-party MFA vendors such as Yubikey, Google Authenticator, DUO, and more.

These factors can be enabled or required for password resets (i.e., when the user clicks "forgot password" and enters their username). These factors can also be enabled or required for different sets of users or different applications based on the security policies your administrators can configure and assign.

**42. During a password reset, does the solution compare the supplied new password against a public database of known-compromised credentials and blocked the use of compromised credentials?**

**Dell Response:** Using SmartFactor Authentication's compromised credential check feature, OneLogin is able to check a user's password when they update it or set it for the first time against databases of compromised credentials that have been stolen in large-scale attacks to prevent the use of stolen passwords. Any previously compromised credentials can be blocked from usage.

Upon using a previously compromised credential, the end-user will receive a visual alert that the password submission contains insecure elements and be prevented from using that password. Admins can view attempted compromised credential usage within the events log and this of course can also be streamed to a SIEM or CASB. Additionally, custom notifications can be built for admins to be notified when such a password change failure occurs.

**43. Describe the self-service features available to end-users for password resets and profile updates.**

**Dell Response:** Please reference the following Knowledge Base articles:

- Sign In and Change Your Password
- Changing Password
- Password Reset
- Set Up Your User Profile

**44. How does your platform handle de-provisioning of user access when an employee leaves the organization?**

**Dell Response:** OneLogin can help to automate many of the processes of user lifecycle management, including user de-provisioning/deletion.

When a user leaves the system, their account can be immediately de-provisioned. Once the user account is disabled in AD or OneLogin, access is immediately revoked. Access for any SAML app is automatically restricted, and accounts linked through provisioning are automatically suspended or deleted in the associated apps.

For more in-depth information about provisioning and de-provisioning, please reference the following Knowledge Base articles:

Introduction to User Provisioning

Introduction to App Management

**45. What mechanisms are in place to ensure that user access is granted or revoked promptly?**

**Dell Response:** OneLogin's Active Directory Connector provides real-time synchronization of users between Active Directory (AD) and OneLogin.

Additionally, Mappings in OneLogin enable you to automate changes to user attributes, roles, and groups, based on conditions that you define. Mappings are typically used to grant application access based on user attributes stored in third-party directories. For example, you can use mappings to assign a OneLogin role (and access to all of the apps defined by that role) to users whose memberOf attribute from Active Directory contains a specified security group. This article provides an overview of creating and using mappings in OneLogin.

**46. Does your service integrate with third-party logging solutions? If so, what logging formats are supported (i.e. JavaScript Object Notation (JSON), Comma separated Variable (CSV), and define any other capabilities that the vendor offers. And are they sent in real-time?**

**Dell Response:** OneLogin provides the capability to configure an Event Broadcaster to send your OneLogin event data to your SIEM solution. The OneLogin event data is compatible with any SIEM solution that accepts data in JSON format, including Sumo Logic, ELK, Splunk, and many others.

The Event Broadcaster will send real-time event data in JSON format to a listener via an HTTP/S POST to the endpoint, streaming the event data every 10 seconds or in 10 event bundles, as



necessary. This information has more debugged logging levels and information. Logged events can also be retrieved via REST API.

See our developer documentation on how to use the Events API, and our our support article about SIEM Webhook integrations for more details.

**47. Does the solution provide reporting on authentication statistics (Single Sign On (SSO) attempts, Multi-Factor Authentication (MFA) enrollment, new user creation, lockouts, permission changes, password resets), and define any other capabilities that the vendor offers.**

**Dell Response:** Logging is managed through the event & reporting logs which is built into the OneLogin platform. The events log monitors all the actions that occur within your organization's OneLogin account. From individual user actions to administrative operations, provisioning, and MFA device registration, everything that happens within an organization's OneLogin account is tracked here.

We log all requests going through our system as well as provide additional information for authentication, the elevation of privileges attempts, session lifecycle, application errors, and high-risk functionality areas. Every request has a logical correlation id which helps us to trace the request in the system between multiple layers.

For advanced logging levels, you can set up an Event Broadcaster to send your OneLogin event data to your SIEM (Security Information and Event Management) solution to gather, analyze, and display events generated by OneLogin. The OneLogin event data is compatible with any SIEM solution that accepts data in JSON format, including Sumo Logic, ELK, Splunk, and many others.

The Event Broadcaster will send real-time event data in JSON format to a listener via an HTTP/S POST to the endpoint. It will make a POST whenever there are 10 events or every 10 seconds, whichever comes first. This information has more debugged logging levels and information.

### Reports

OneLogin accounts include a standard set of reports located in Activity > Reports. If your subscription supports it, you can also create your own reports based on a wide variety of attributes and details.

Of the 200 most popular reports that review application authentication and access events, most commonly run reports include:

- Who's accessed which applications — e.g., a person accessing a Treasury app
- Who's unsuccessfully logged in — indicating a potential attack in progress
- Who's recently changed their password — another potential indicator of an attack
- Which users have been suspended — to confirm that a compromised account is inactive
- User provision and deprovision activity - to track that users are removed from systems after leaving a department



- Which applications are the most popular and which might be underutilized, indicating potential areas of budget waste

#### 48. How long are the logs maintained?

**Dell Response:** OneLogin event logs are maintained for a minimum of one year.

#### 49. Do you provide any ability to create or pull reports? Do you have any templates for executive type reports?

**Dell Response:** Reports

OneLogin accounts include a standard set of reports located in Activity > Reports. If your subscription supports it, you can also create your own reports based on a wide variety of attributes and details.

Of the 200 most popular reports that review application authentication and access events, most commonly run reports include:

- Who's accessed which applications — e.g., a person accessing a Treasury app
- Who's unsuccessfully logged in — indicating a potential attack in progress
- Who's recently changed their password — another potential indicator of an attack
- Which users have been suspended — to confirm that a compromised account is inactive
- User provision and deprovision activity - to track that users are removed from systems after leaving a department
- Which applications are the most popular and which might be underutilized, indicating potential areas of budget waste

#### 50. Please provide the full list of security events and descriptions captured by your service.

**Dell Response:** List of Events

These are all event types that are currently tracked in the OneLogin admin portal:

##### Apps

Actor\_user manually added user to app  
 Actor\_user manually removed user from app  
 Api - app rules apply for app failed  
 Api - app rules apply for app success  
 Api - app rules create for app failed  
 Api - app rules create for app success  
 Api - app rules delete for app failed  
 Api - app rules delete for app success  
 Api - app rules dryrun for app failed  
 Api - app rules dryrun for app success  
 Api - app rules get for app failed  
 Api - app rules get for app success  
 Api - app rules list action values for app failed  
 Api - app rules list action values for app success  
 Api - app rules list actions for app failed  
 Api - app rules list actions for app success  
 Api - app rules list condition operators for app failed  
 Api - app rules list condition operators for app success  
 Api - app rules list conditions for app failed  
 Api - app rules list conditions for app success  
 Api - app rules list for app failed  
 Api - app rules list for app success  
 Api - app rules refresh entitlements for app failed  
 Api - app rules refresh entitlements for app success

- app rules sort for app failed  
 Api - app rules sort for app success  
 Api - app rules update for app failed  
 Api - app rules update for app success  
 App app removed from role  
 App was added by user  
 App was removed by user  
 App was updated by user  
 Users

Account granted permission to privilege\_name  
 Account revoked permission to privilege\_name  
 Actor\_user assumed user  
 Actor\_user changed password for user  
 Actor\_user deleted secure note id: note\_id  
 Actor\_user disabled task\_name  
 Actor\_user disabled terms and conditions for policy  
 Actor\_user edited secure note id: note\_id  
 Actor\_user enabled task\_name  
 Actor\_user enabled terms and conditions for policy  
 Actor\_user failed to change password for user  
 Actor\_user failed to import csv  
 Actor\_user generated temporary otp token for user  
 Actor\_user initiated offboarding for user  
 Actor\_user initiated onboarding for user  
 Actor\_user marked task\_name complete for user  
 Actor\_user marked task\_name complete for user  
 Actor\_user redirected to an external site for password reset  
 Actor\_user removed profile picture for user  
 Actor\_user revealed password to app for user  
 Actor\_user revoked device certificate  
 Actor\_user revoked temporary otp token for user  
 Actor\_user revoked user certificate  
 Actor\_user unlocked user  
 Actor\_user unlocked user in directory  
 Actor\_user updated credit card  
 Actor\_user updated terms and conditions for policy  
 Actor\_user uploaded profile picture for user  
 Actor\_user viewed secure note id: note\_id  
 Admin actor\_user changed password for user  
 App configuration error  
 App throttled  
 Credit card update failed  
 Directory sync directory\_sync\_run\_id  
 Downloaded browser cert  
 Entitlement action  
 Failed to import user from directory  
 Nameid was successfully proxied to app via idp trusted\_idp.  
 No users to import  
 One of directory's connectors was disabled  
 One of directory's connectors was enabled  
 Otp\_device deregistered for user  
 Otp\_device registered for user  
 Ous were updated for directory  
 Password request approved from user  
 Provisioning deprovisioning mode do nothing  
 warning  
 Refresh schema action failed  
 Self registration approved for user  
 Self registration denied for user  
 Self registration request for user  
 Smart password could not be updated for user  
 Smart password updated for user  
 Task\_name for user was completed by actor\_user  
 Task\_name for user was completed by actor\_user  
 Task\_name for user was marked incomplete by actor\_user  
 Unmatched users  
 User added phone number  
 User added to role  
 User added to role failed  
 User agreed to terms and conditions  
 User authenticated by radius\_config  
 User authenticated via api  
 User authentication policy does not allow sign-in via social network: notes  
 User automatically added to role  
 User automatically removed from role  
 User could not be created  
 User could not be determined by radius\_config  
 User could not be updated  
 User deactivated by actor\_user  
 User deleted device for onelogin desktop  
 User denied access to app  
 User did not agree to terms and conditions  
 User disabled offboarding  
 User disabled onboarding  
 User enabled offboarding  
 User enabled onboarding  
 User failed authentication  
 User failed authentication via api  
 User failed authentication with vldap, notes  
 User failed to authenticate via onelogin desktop  
 User failed to log in on a trusted device  
 User failed to log into app  
 User failed to login via onelogin desktop  
 User granted access to app  
 User granted permission to manage role  
 User granted permission to manage role failed  
 User granted permission to privilege\_name  
 User is not authorized to access app  
 app  
 User limit reached  
 User locked  
 User logged into app  
 User logged into onelogin  
 User logged out of onelogin  
 User not updated in app  
 User permission to manage role revoked  
 User permission to manage role revoked failed  
 User permission to privilege\_name revoked  
 User reactivated  
 User rejected by radius\_config  
 User removed from role  
 User removed from role failed  
 User requested access to app  
 User requested new password  
 User signed in into onelogin via social network: notes  
 User successfully authenticated with vldap  
 User successfully logged in on a trusted device  
 User successfully logged in via onelogin desktop  
 User successfully verified authenticator otp\_device  
 User

suspended by actor\_userUser unbind user from device for onelogin desktopUser updated by actor\_userUser updated phone numberUser was activated by actor\_userUser was created by actor\_userUser was created by tidp trusted\_idpUser was deleted by actor\_userUser was force logged outUser was importedOneLogin

A mapping was skipped for user; notesAccount approaching seat limitAccount at seat limitActor\_user added license to userActor\_user added mapping\_name mappingActor\_user added user\_field\_name custom user fieldActor\_user attempted to update login informationActor\_user bulk licensed usersActor\_user created broadcasterActor\_user created group groupActor\_user created privilege privilege\_nameActor\_user created secure note id: note\_idActor\_user created self registrationActor\_user deleted broadcasterActor\_user deleted mapping\_name mappingActor\_user deleted privilege privilege\_nameActor\_user deleted self registrationActor\_user deleted user\_field\_name custom user fieldsActor\_user destroyed group groupActor\_user disabled mapping\_name mappingActor\_user enabled mapping\_name mappingActor\_user failed to license userActor\_user failed to reapply mappings for userActor\_user is not authorized to perform privilege\_actionon\_appActor\_user is not authorized to perform privilege\_actionon\_userActor\_user manually updated user login for appActor\_user reapplied mappings for userActor\_user removed license from userActor\_user retried provisioningActor\_user tried to manually add user to app.Actor\_user unlocked user via apiActor\_user updated broadcasterActor\_user updated group groupActor\_user updated mapping\_name mappingActor\_user updated privilege privilege\_nameActor\_user updated self registrationActor\_user updated user login informationAdmin actor\_user changed account settings for objectAdmin actor\_user created payment record for objectAdmin actor\_user deleted payment record for objectAdmin actor\_user updated payment record for objectApi - authorization app createdApi - authorization app creation failedApi - authorization app destroy failedApi - authorization app destroyedApi - authorization app update failedApi - authorization app updatedApi - authorization claim createdApi - authorization claim destroy failedApi - authorization claim destroyedApi - authorization claim failedApi - authorization claim update failedApi - authorization client createdApi - authorization client creation failedApi - authorization client destroy failedApi - authorization client destroyedApi - authorization client update failedApi - authorization client updatedApi - authorization scope createdApi - authorization scope creation failedApi - authorization scope destroy failedApi - authorization scope destroyedApi - authorization scope update failedApi - authorization scope updatedApi - authorization token call failed using client\_nameApi - authorization token called using client\_nameApi - bad request using client\_nameApi - confirm otp for user using client\_name failedApi - confirm otp for user using client\_name succeededApi - custom attributes set for user using client\_nameApi - failed to set custom attributeApi - get otps for user using client\_nameApi - get resource / attributes on resource using client\_nameApi - invite link not obtained using client\_nameApi - invite link not sent using client\_nameApi - invite link sent using client\_nameApi - invite link using client\_nameApi - one record returned on resource using client\_nameApi - otp created for user using client\_nameApi - page of results returned on resource using client\_nameApi - password not updated for user using client\_nameApi - password not updated for user using client\_nameApi - password updated for user using client\_nameApi - password updated for user using client\_nameApi - privilege privilege\_name assigned to role using api\_credential\_nameApi - privilege privilege\_name removed from role using api\_credential\_nameApi - privilege privilege\_name removed from user user using api\_credential\_nameApi - privilege privilege\_name was assigned to user user using api\_credential\_nameApi - privilege privilege\_name was created

using api\_credential\_nameApi - privilege privilege\_name was deleted using api\_credential\_nameApi - privilege privilege\_name was updated using api\_credential\_nameApi - roles added to user using client\_nameApi - roles get for failedApi - roles get for successApi - roles list administrators for failedApi - roles list administrators for successApi - roles list apps for failedApi - roles list apps for successApi - roles list failedApi - roles list successApi - roles list users for failedApi - roles list users for successApi - roles not added to user using client\_nameApi - roles not removed for user using client\_nameApi - roles removed for user using client\_nameApi - roles update for failedApi - roles update for successApi - trigger factor for user using client\_name succeededApi - unauthorized using client\_nameApi - user created using client\_nameApi - user deleted using client\_nameApi - user failed to log out using client\_nameApi - user locked using client\_nameApi - user logged out using client\_nameApi - user not created using client\_nameApi - user not deleted using client\_nameApi - user not locked using client\_nameApi - user not updated using client\_nameApi - user updated using client\_nameApi - verify factor called using client\_nameApi - verify factor failed using client\_nameApp app added to roleApp app added to role failedApp app failed to create via apiApp app failed to destroy via apiApp app failed to update via apiApp app removed from role failedApp app was created via apiApp app was destroyed via apiApp app was updated via apiApp has reached user limitAssigned to user userBrand created via apiBrand destroyed via apiBrand failed to create via apiBrand failed to destroy via apiBrand failed to update via apiBrand updated via apiBulk operation failed for user userBulk operation triggeredCertificate\_name is about to expireConnector object could not be createdConnector object could not be deletedConnector object could not be updatedConnector object was created by userConnector object was deleted by userConnector object was updated by userConnector stats updatedDelete user failedDirectory attributes import failed for directoryDirectory attributes import from directory finishedDirectory attributes import from directory startedDirectory caught an exceptionDirectory caught an exceptionDirectory connector provisioning error in directoryDirectory external id was deleted for userDirectory external id was updated for userDirectory failed overDirectory failed overDirectory field(s) is not uniqueDirectory import limit reachedDirectory in useDirectory reloaded configurationDirectory reloaded configurationDirectory startedDirectory startedDirectory stoppedDirectory stoppedEntitlements cache actionExport from directory finishedExport from directory startedExternal assume userExternal groups import from directory finishedExternal groups import from directory startedFailed to create sandbox by userFailed to create sandbox using api\_credential\_nameFailed to delete sandbox by userFailed to delete sandbox using api\_credential\_nameFailed to provision user to directoryFailed to reapply entitlement mappings for user in app appFailed to reapply mappings for userFailed to remove user user from app appFailed to sync sandbox by userFailed to update sandbox by userFailed to update sandbox using api\_credential\_nameImport from directory finishedImport from directory startedImport user failedJob already scheduledJob failed to startJob terminatedLdap directory directory caught an exceptionNameid failed to login to app via idp trusted\_idp.Notification from directoryNotification from directoryNt hash requested for userObject - notification was sent to userOidc authorization code for app failedOidc authorization code for app successOidc client credentials for app failedOidc client credentials for app successOidc general failOidc get code for app failedOidc get code for app successOidc implicit flow for app failedOidc implicit flow for app successOidc password for app failedOidc password for app successOidc refresh token for app failedOidc refresh token for app successOidc revoke token for app failedOidc revoke token for app successOidc user info for app failedOidc user info for app successOidc validate token for app

failedOidc validate token for app successOtp\_device unlocked for userParameter object could not be createdParameter object could not be deletedParameter object could not be updatedParameter object was created by userParameter object was deleted by userParameter object was updated by userProvisioning eventReapplied entitlement mappings for user in app appReport report\_name cloned by actor\_userReport report\_name created by actor\_userReport report\_name destroyed by actor\_userReport report\_name failed generation in backgroundReport report\_name terminated during generation in backgroundReport report\_name updated by actor\_userReport report\_name was generated in backgroundRole (role\_id) created by user (user\_id)Role (role\_id) deleted by user (user\_id)Role created failedRole deleted failedSaml assertion warning for actor\_user noteSandbox created using api\_credential\_nameSandbox deleted by userSandbox deleted using api\_credential\_nameSandbox sync initiated by userSandbox updated by userSandbox updated using api\_credential\_nameScriptlet error: nameidSelf registration request submitted for userSelf registration request verified for userSending email with custom smtp settings failedSmart hook createdSmart hook creation failedSmart hook deletedSmart hook deletion failedSmart hook environment variable createdSmart hook environment variable creation failedSmart hook environment variable deletedSmart hook environment variable deletion failedSmart hook environment variable retrievedSmart hook environment variable update failedSmart hook environment variable updatedSmart hook environment variables retrievedSmart hook execution failedSmart hook execution was successfulSmart hook fetchedSmart hook logs retrievedSmart hook update failedSmart hook updatedSmart hooks retrievedSms failureSmtp configuration updatedSuccessfully reapplied mappings for userSync sandbox by user completedUser actor\_user assigned the privilege privilege\_name to roleUser actor\_user assigned the privilege privilege\_name to user userUser actor\_user is not authorized to perform privilege\_action on policyUser actor\_user is not authorized to perform privilege\_actionon\_groupUser actor\_user is not authorized to perform privilege\_actionon\_reportUser actor\_user is not authorized to perform privilege\_actionon\_roleUser actor\_user is not authorized to perform privilege\_actionon\_trusted\_idpUser actor\_user removed the privilege privilege\_name from roleUser actor\_user removed the privilege privilege\_name from user userUser added connector instance to directory directoryUser added directory directoryUser associated to directoryUser challenged for otpUser changed default portal/profile languageUser changed new login detection settingUser changed password through profileUser changed phone numberUser changed portal default tab through profileUser changed tabs settingUser created a sandbox linked to objectUser created api\_credential\_name api credentialUser created authentication factor authentication\_factorUser created certificate\_name certificateUser created policy policyUser created proxy agent proxy\_agentUser created radius attribute in radius\_configUser created radius configuration radius\_configUser deleted api\_credential\_name api credentialUser deleted authentication factor authentication\_factorUser deleted certificate\_name certificateUser deleted connector instance from directory directoryUser deleted directory directoryUser deleted in directoryUser deleted policy policyUser deleted proxy agent proxy\_agentUser deleted radius attribute in radius\_configUser deleted radius configuration radius\_configUser deleted security factorUser denied auth via otp push requestUser disabled adaptive login for accountUser disabled api\_credential\_name api credentialUser disabled brandingUser disabled desktop ssoUser disabled embeddingUser disabled virtual ldapUser disabled vpnUser disassociated from directoryUser enabled adaptive login for accountUser enabled api\_credential\_name api credentialUser enabled brandingUser enabled desktop ssoUser enabled embeddingUser enabled virtual ldapUser enabled vpnUser failed authentication with vldap

(onelogin desktop mac), notesUser failed otp challengeUser failed remote authenticationUser failed to provision in directoryUser has added trusted\_idp to trusted idpsUser has been provisioned to directory successfullyUser has changed the default trusted idp to trusted\_idpUser has modified the trusted idp trusted\_idpUser has removed trusted\_idp as default trusted idpUser has removed trusted\_idp from trusted idpsUser imported from directoryUser invited by actor\_userUser locked via apiUser logged out of appUser provisioned in directoryUser reactivated in directoryUser reactivated via apiUser reauthenticated into appUser recently removedUser rejectedUser renamed security factorUser set new default factorUser successfully authenticated with vldap (onelogin desktop mac), notesUser suspended by actor\_user via apiUser suspended in directoryUser unset default factorUser updated account settingsUser updated authentication factor authentication\_factorUser updated brandingUser updated by directoryUser updated company infoUser updated desktop sso settingsUser updated directory directoryUser updated embedding settingsUser updated policy policyUser updated profile photoUser updated radius attribute in radius\_configUser updated radius configuration radius\_configUser updated security questionsUser updated virtual ldap settingsUser updated vpn settingsUser-synch active directory connector not respondingUsers in unlicensed stateWorkday real-time notificationProvisioning

Could not authenticate to appProvisioning exceptionUser could not be deleted in appUser could not be provisioned in appUser could not be reactivated in appUser could not be suspended in appUser could not be updated in appUser deleted in appUser linked in appUser provisioned in appUser reactivated in appUser suspended in appUser updated in app

**51. Explain the logging mechanisms in place to capture identity-related events and activities.**

**Dell Response:** Logging is managed through the event & reporting logs which is built into the OneLogin platform. The events log monitors all the actions that occur within your organization's OneLogin account. From individual user actions to administrative operations, provisioning, and MFA device registration, everything that happens within an organization's OneLogin account is tracked here.

We log all requests going through our system as well as provide additional information for authentication, the elevation of privileges attempts, session lifecycle, application errors, and high-risk functionality areas. Every request has a logical correlation id which helps us to trace the request in the system between multiple layers.

For advanced logging levels, you can set up an Event Broadcaster to send your OneLogin event data to your SIEM (Security Information and Event Management) solution to gather, analyze, and display events generated by OneLogin. The OneLogin event data is compatible with any SIEM solution that accepts data in JSON format, including Sumo Logic, ELK, Splunk, and many others.

The Event Broadcaster will send real-time event data in JSON format to a listener via an HTTP/S POST to the endpoint. It will make a POST whenever there are 10 events or every 10 seconds, whichever comes first. This information has more debugged logging levels and information.

**52. How does your solution provide real-time alerts for security incidents and policy violations?**

**Dell Response:** OneLogin's Notifications feature can be configured to automatically send notification emails to administrators or specific end users when a trigger condition occurs. These notifications can be triggered by any event or change that happens in OneLogin and can be customized to meet your organization's needs, including recipients, trigger conditions, and even using your own text with markdown formatting and a large selection of macros that can be used as value placeholders to tailor the email content for your individual users.

**53. Can your solution meet compliance requirements by generating audit trails and activity reports?**

**Dell Response:** OneLogin provides the capability to configure an Event Broadcaster to send your OneLogin event data to your SIEM solution. The OneLogin event data is compatible with any SIEM solution that accepts data in JSON format, including Sumo Logic, ELK, Splunk, and many others.

The Event Broadcaster will send real-time event data in JSON format to a listener via an HTTP/POST to the endpoint, streaming the event data every 10 seconds or in 10 event bundles, as necessary. This information has more debugged logging levels and information. Logged events can also be retrieved via REST API.

See our developer documentation on how to use the Events API, and our support article about SIEM Webhook integrations for more details.

The below are the identified business processes to integrate OneLogin Trusted Experience platform for governance and audit assurance.

- Financial Procurement Process: Integration compatibility with OneLogin Trusted Experience platform should be a consideration in this process and enforced if certain criteria are met: An example of compulsory criteria would be all systems classified as 'critical' must integrate with OneLogin Trusted Experience platform.
- Third Party Risk Management Process: Third party vendors and suppliers classified as contractors must access required systems and/or data via OneLogin Trusted Experience platform via a set defined third party policy within OneLogin Trusted Experience platform. If the third party vendors/suppliers providing software, applications and systems must provide these services via OneLogin Trusted Experience platform.
- End-User Management Process: Joiners, movers and leavers processes can be streamlined with key actions automated.
- Compliance Assessment Processes: Incorporating OneLogin Trusted Experience platform into your compliance assessment processes will support the compliance team and ensure your organization continues to deliver to their industry regulated access control requirements. SOX Compliance is an example of segregation of duties within financial systems with separation of duties forming the basis of SOX Compliance requirement and our Trusted Experience Platform supports access control policies formation both for applications and/or user-group level. Two-factor authentication is a mandated requirement for PCI-DSS Compliance.
- Privacy Impact Assessments: The OneLogin Trusted Experience Platform allows for policies to be applied at an individual end-user level and end-user group level supporting



the business needs in regards to privacy requirements. Policies can be aligned to applications within the Smart Factor configuration features. OneLogin can set up policies to explicitly allow access only from certain geographical locations. This allows the business to continue to meet privacy adequacy requirements and/or binding corporate rules requirements into account.

- Cyber Security Risk Assessments: OneLogin SmartFactor features within the Trusted Experience Platform support organizations' cyber security team by reducing threats and risks to an acceptable business level as the team can make the Smart Factor features a compulsory policy.
- Business Continuity Assessments Process: The OneLogin Trusted Experience Platform and access control policies for user management and applications support organizations to continue to deliver business services from any place, any location and any device. Therefore, it should be a key component for business continuity assessments as one of the core business continuity solutions. Access control policies can be set up per business continuity requirements, tested during business continuity testing and activated if and/when required.
- Audit and Assurance Process: The OneLogin Trusted Experience Platform can be used to provide independent assurances for end-user management, application management providing a centralized access management system with audit reporting functionality.
- Merger and Acquisition Process: The OneLogin Trusted Experience Platform is a vital platform to integrate in this process to transfer ownership of critical information assets - systems and data.

**54. What options are available for exporting logs and reports to external systems or Security information and event management (SIEM) solutions?**

**Dell Response:** Please see the above answer.

**55. Indicate and identify any countries where you provide services to clients outside of the United States (and US territories).**

**Dell Response:** Our AWS data center locations for our USA shard are Oregon and Virginia. Our data center locations for EU shard are AWS Frankfurt, Germany and Dublin, Ireland.

OneLogin translates our end-user experience into 20+ languages!

By default, OneLogin sets the language to match the user's browser's default language setting. If they prefer, users can select their language preference from their profile and their portal is rendered accordingly.

Additionally, OneLogin leverages AWS Global Accelerator to direct end users to the closest AWS Network ingress point. Once on the AWS network, the user will have millisecond latency to the relevant OneLogin instance. This ensures that users around the globe experience minimal latency.

- 56. Have there been any significant security breaches in the past 24 months? If so please provide documentation of how this breach occurred, how many accounts were involved, and the remedy/solution for the breach.**

**Dell Response:** No

With the ever changing threat landscape we have put in place a dedicated monitoring, incident response and investigation team. The team has a global operations remit to continue to build a best in class incident response. A fundamental component to this is working with you our Customers and Partners via our dedicated 'Responsible Disclosure' program.

This program alerts us to vulnerabilities that we need to investigate and address to continue to protect our OneLogin environment and collaborate with you our Customers/Partners to protect the global ecosystem from malicious attackers. Please see Security section of our website for more details on Security and our 'Responsible Disclosure program: <https://www.onelogin.com/security>

All reported threats, and their associated vulnerabilities are now investigated by OneLogins Incident Response and Investigations team. The investigation process categorizes each treat, and assigns it a risk category rating based on the technology service, data it processes, associated information assets and most importantly assessing the vulnerability factors. From this the incident is prioritised and remediation actions are implemented.

With our "Security First " culture, dedication to security by design principle. Coupled with how we operate both from a program management of security control implementation and security operations monitoring perspective, OneLogin is equipped with for a defence in depth incident response. An incident response that supports reducing business impacts for not only OneLogin, our Customers and Partners avoiding all the consequences of a data breach.

- 57. Provide information on how clients are informed of maintenance and patch releases.**

**Dell Response:** OneLogin product releases are conducted on a monthly basis and the release notes can be found here.

OneLogin notifies all customers 2 weeks in advance prior to performing upgrades. Upgrades are performed approximately 10 times per year, with patches / hot fixes as needed. The upgrade process is performed by our cloud operations team within the standard maintenance windows for scheduled downtime. Normal backup and recovery processes will apply. Backups will be taken before upgrade / patches are run.

OneLogin will provide advanced notice of ad-hoc maintenance windows. There will not be down-time for the platform in any maintenance case.

- 58. Where does the solution reside?**

**Dell Response:** OneLogin is a cloud-based, SaaS-delivered solution. OneLogin is hosted entirely in AWS. We have two distinct Shards, US and EU. Each Shard has redundancy in multiple operating regions and multiple availability zones in each operating region.

Our AWS data center locations for our USA shard are Oregon and Virginia. Our data center locations for EU shard are AWS Frankfurt, Germany and Dublin, Ireland.

**59. Describe how your service is compliant with Americans with Disabilities Act (ADA) standards and how you support screen readers and descriptive technology.**

**Dell Response:** For a detailed breakdown of our conformance with each individual section of the WCAG, see this link: <https://www.oneidentity.com/docs/identity-manager-as-a-service-legal-147767.pdf>

**60. Describe how your service provides failover and redundancy.**

**Dell Response:** OneLogin has gone to great lengths to develop a platform that's both reliable and scalable while maintaining a high level of performance 24/7/365. To support this, we use regional login clusters in our AWS footprint and our architecture incorporates an intelligent and resilient DNS infrastructure to direct users to the nearest available login cluster.

The platform uses a combination of multiple operating regions with multiple availability zones within each of these regions, as well as Content Delivery Networks (CDNs) to deliver assets via hundreds of edge locations around the globe. Our microservices architecture allows us to auto-scale services independently based on different factors for each service, which in turn allows us to make scaling decisions faster than any other standard solution by inspecting requests in near real-time and evaluating the load impact that the requests cause.

The OneLogin HydraBoost platform has been extensively tested to ensure reliability and scale, with key performance metrics demonstrating the ability to handle a sustained load of 17,000 requests per second, or 1 million requests per minute, with an average response time under 200ms.

OneLogin's architecture is born in the cloud and built to scale with millions of users accessing resources at the same time. We've built a fully cloud-based multitenancy model designed for speed, efficiency and low cost while solving hard engineering problems such as securing controls, risks of downtime, and data corruption.

- **APIs & SDKs:** OneLogin provides a comprehensive RESTful API that can be used for administering the OneLogin platform, including APIs for tasks such as user CRUD operations, granting/revoking application access, password resets, force logouts, security policy assignment, app configuration, and more. As a part of our developer resources, we also provide SDKs in many popular programming languages and support Swagger/OpenAPI Specification to enable developers to create SDKs in other languages as well.
- **Provisioning:** The provisioning system handles the scheduling and fulfillment of provisioning requests into 3rd-party applications. This is fully cloud based with no on-prem installation requirements.
- **Authentication:** When an unauthenticated user attempts to access a resource whose access is controlled by the OneLogin platform, the user is redirected to the login page. Based on your custom security policies, as well as any trusted IdPs or other integrations

you may have configured, OneLogin identifies and authenticates the user and proceeds to the requested resource.

- Events: The OneLogin platform generates close to 300 different types of events, pushed to a central queue, where they are stored and processed for various purposes and available for retrieval by customers.

#### Physical Architecture

- The SSO tier is primarily responsible for handling login requests and serving end users with the web interface they use to log into 3rd-party applications. The tier is front ended by an Elastic Load Balancer (ELB) and distributed between three availability zones (AZ) within each AWS region, with each tenant operating in two AWS regions. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ.
- The Admin tier is primarily responsible for handling administrative functions within an instance and serving admin users with the web interface to manage their OneLogin instance. The tier is front ended by an Elastic Load Balancer (ELB) and distributed between three availability zones (AZ) within one AWS region. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ, and the Admin tier can fail over to the secondary AWS region if required.
- As additional services are created and come online, they are deployed following a common pattern with minor deviations based on the specific needs of the service. The front end tier is front ended by an Elastic Load Balancer (ELB) and distributed between three availability zones (AZ) within one AWS region. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ. Additional services can fail over to the secondary AWS region if required.

For more information, see:

- OneLogin Trust: Status, Uptime, Availability
- OneLogin Service Subscription Agreement (US)
- OneLogin Service Subscription Agreement (EU)

#### 61. What controls does your service have in place to prevent automated attacks?

**Dell Response:** OneLogin Smart Factor Authentication uses machine learning to determine the risk level for every login event. It uses a broad set of inputs, including networks, devices, geography, geo-velocity, time of day, and other threat factors to build a risk score of each login attempt. Admins can set risk tolerance thresholds that determine what the user experience is based on risk score. For example, logins with a low risk don't get challenged for MFA, logins with moderate risk must perform an MFA challenge, and logins with high risk are blocked from access. Admins can fine-tune the risk engine using custom rules to do things such as blacklist/whitelist specific IPs or

geographies. Using roles-based access controls, security restrictions can be applied to users on an individual or group basis.

SmartFactor Authentication includes the ability to perform a compromised credential check and customize the login flow. Using SmartFactor's compromised credential check feature, OneLogin is able to check a user's password when they update it or set it for the first time against databases of compromised credentials that have been stolen in large-scale attacks to prevent the use of stolen passwords. Any previously compromised credentials can be blocked from usage.

Upon using a previously compromised credential, the end-user will receive a visual alert that the password submission contains insecure elements and prevented from using that password. Admins can view attempted compromised credential usage within the events log and this of course can also be streamed to a SIEM or CASB. Additionally, custom notifications can be built for admins to be notified when such a password change failure occurs.

SmartFactor Authentication also offers protection against brute force attacks, anomaly detection, and mitigates known malicious threats.

#### Brute Force Attack Mitigation

SmartFactor enabled security policies provide a "brute force protection" login flow. MFA is integrated into a brute-force defense login flow that is designed to protect accounts from common brute force, brute spray and dictionary style attacks. The brute-force authentication flow follows a UserID/MFA/Password login flow.

#### Anomaly Detection

SmartFactor Authentication uses machine learning from a broad set of inputs to establish a baseline of user login behavior. Each login attempt is evaluated for anomalies or exceptions to the established user baseline generating a risk score. The risk score can be used to take mitigation actions including challenge for MFA or denial of access.

#### Known Malicious Threat Mitigation

SmartFactor Authentication evaluates each login session against real time threat intelligence services to mitigate malicious activity from known malicious threats.

For more information, check out some of our Knowledge Base articles:

- Smart Passwords
- Roles
- Groups
- User Policies
- App Policies
- SmartFactor Authentication

**62. How does your solution ensure high availability and resilience in the face of unexpected outages or disasters?**

**Dell Response:** OneLogin has gone to great lengths to develop a platform that's both reliable and scalable while maintaining a high level of performance 24/7/365. To support this, we use regional login clusters in our AWS footprint and our architecture incorporates an intelligent and resilient DNS infrastructure to direct users to the nearest available login cluster.

The platform uses a combination of multiple operating regions with multiple availability zones within each of these regions, as well as Content Delivery Networks (CDNs) to deliver assets via hundreds of edge locations around the globe. Our microservices architecture allows us to auto-scale services independently based on different factors for each service, which in turn allows us to make scaling decisions faster than any other standard solution by inspecting requests in near real-time and evaluating the load impact that the requests cause.

The OneLogin HydraBoost platform has been extensively tested to ensure reliability and scale, with key performance metrics demonstrating the ability to handle a sustained load of 17,000 requests per second, or 1 million requests per minute, with an average response time under 200ms.

OneLogin's architecture is born in the cloud and built to scale with millions of users accessing resources at the same time. We've built a fully cloud-based multitenancy model designed for speed, efficiency and low cost while solving hard engineering problems such as securing controls, risks of downtime, and data corruption.

- APIs & SDKs: OneLogin provides a comprehensive RESTful API that can be used for administering the OneLogin platform, including APIs for tasks such as user CRUD operations, granting/revoking application access, password resets, force logouts, security policy assignment, app configuration, and more. As a part of our developer resources, we also provide SDKs in many popular programming languages and support Swagger/OpenAPI Specification to enable developers to create SDKs in other languages as well.
- Provisioning: The provisioning system handles the scheduling and fulfillment of provisioning requests into 3rd-party applications. This is fully cloud based with no on-prem installation requirements.
- Authentication: When an unauthenticated user attempts to access a resource whose access is controlled by the OneLogin platform, the user is redirected to the login page. Based on your custom security policies, as well as any trusted IdPs or other integrations you may have configured, OneLogin identifies and authenticates the user and proceeds to the requested resource.
- Events: The OneLogin platform generates close to 300 different types of events, pushed to a central queue, where they are stored and processed for various purposes and available for retrieval by customers.

**Physical Architecture**

- The SSO tier is primarily responsible for handling login requests and serving end users with the web interface they use to log into 3rd-party applications. The tier is front ended by an Elastic Load



Balancer (ELB) and distributed between three availability zones (AZ) within each AWS region, with each tenant operating in two AWS regions. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ.

- The Admin tier is primarily responsible for handling administrative functions within an instance and serving admin users with the web interface to manage their OneLogin instance. The tier is front ended by an Elastic Load Balancer (ELB) and distributed between three availability zones (AZ) within one AWS region. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ, and the Admin tier can fail over to the secondary AWS region if required.
- As additional services are created and come online, they are deployed following a common pattern with minor deviations based on the specific needs of the service. The front end tier is front ended by an Elastic Load Balancer (ELB) and distributed between three availability zones (AZ) within one AWS region. The multiple AZs allow for platform resiliency in case of AWS issues within a specific AZ. Additional services can fail over to the secondary AWS region if required.

For more information, see:

- OneLogin Trust: Status, Uptime, Availability
- OneLogin Service Subscription Agreement (US)
- OneLogin Service Subscription Agreement (EU)

### 63. Provide your data backup and recovery strategies to safeguard against data loss?

**Dell Response:** OneLogin will replicate the State of West Virginia's tenant to multiple data centers across two AWS regions. Additionally, we do logical (on the DB level) and physical (on the underlying storage volume level) backups twice a day with 30-day retention. Backups are stored in multiple geographically separated regions. Backups are encrypted and require multiple keys to decrypt and database decryption/recovery is tested periodically.

### 64. Describe your approach to continuous monitoring and threat detection within your identity infrastructure.

**Dell Response:** "Security First" is today how we operate at OneLogin.

Our Global Enterprise Trust and Security program scope covers our technologies, business processes and security culture across our global operating environments of our production and our corporate facilities. Our Trust and Security function have dedicated teams carrying out focused risk assessments throughout our technology and data management lifecycle. The scope of these risk assessments include our service partners suppliers and vendors. Our Security Engineers design the Security controls in our product and corporate service offerings. Our Application Security team has an independent mandate to test our technologies to provide Trust Assurance that threat vectors and their associated vulnerabilities have appropriate controls applied to reduce the confidentiality, integrity, availability, and privacy risks reduced to acceptable business operating level.

Our policies, standards and business operating procedures are reviewed at least annually and/or amended to ensure we continue to align against OneLogin, our product offerings and entire operating environments against the latest threat and threat vectors.

#### Data Trust & Security Framework

Data Management is at the core of the OneLogin Trust and Security framework. The framework is built from a full range of factors that inform the security approach, from the broadest government laws and regulations to the details of specific contractual agreements. OneLogin then takes all these externally focused factors to translate them into our internal policies, standards and procedures that make up how we at OneLogin operate. This includes how we provide you with Trust Assurance for the management of our Customer Data.

OneLogin works at international and global level to stay abreast of security and privacy requirements as set forth under international, federal, and state laws. By continually monitoring the security and privacy landscape, OneLogin can modify its data governance approach to remain in step and comply with the latest requirements.

Regardless of industry, the need for data governance has driven the creation of best practices and standards to guide companies in their security and privacy strategy and capabilities. OneLogin provides its customers with Trust Assurance on how their data is protected and managed via our certifications and attestations to industry best practice standards. OneLogin Trust Assurance earned, includes:

ISO 27001:2013 – The highest level of certification available today for assuring global information security. OneLogin has earned this certification for all aspects of the enterprise, including the OneLogin Product and Service Offering along with our company operations. ISO 27001 is core to OneLogin's Security Standard model, and OneLogin's ISO 27001 results can be made available to customers so that they can map them into their own vendor management programs.

ISO 27017:2015 – This standard provides guidance to both cloud service providers and consumers of these services in the form of objectives, controls, and guidelines. OneLogin aligned its existing security controls to be compliant to this standard in order to augment its security program. These controls are tested as part of the periodic SOC 2 Type 2 report and an independent body has audited our compliance with this standard as part of our ISO 27001:2013 certificate annual audits.

SOC 1 Type 2, SOC 2 Type 2 – Provides confirmation of OneLogin's financial and information security controls. A SOC 1 Type 2 report describes the internal controls in place over financial reporting at an organization and requires a third-party service auditor to review and examine the organization's operations over a set period of time. The SOC 2 Type 2 report specifically indicates that OneLogin's technology meets the criteria for security, availability, confidentiality, and processing integrity and is protected against unauthorized physical and logical access. The report also confirms the platform is available for operation and use as an information system designated as confidential and protected, and is complete, accurate, timely, and authorized.

PCI DSS – The Payment Card Industry Data Security Standard outlines the security requirements for organizations that process, manage and store cardholder data. As a data processor OneLogin is in alignment supporting organizations meet their PCI-DSS Compliance requirements.

**65. Can your solution provide insights into user behavior anomalies that might indicate compromised accounts?**

**Dell Response:** OneLogin does provide such insights. Our platform utilizes advanced machine learning algorithms and behavioral analytics to monitor user activity continuously.

Key features include:

- Behavioral Analytics: OneLogin establishes a baseline of normal user activity and flags deviations that may indicate suspicious behavior.
- Anomaly Detection: We monitor user logins, access patterns, application usage, and data transfers in real-time, identifying any unusual activity.
- Insightful Reporting: Our reporting tools offer insights into user behavior anomalies and potential security risks, aiding in swift investigation and remediation.
- Automated Response: OneLogin allows for automated responses such as suspending compromised accounts or enforcing multi-factor authentication based on predefined security policies.
- Continuous Improvement: We are dedicated to enhancing our platform with the latest security features to ensure effective threat detection and mitigation.

In summary, OneLogin provides robust capabilities for detecting user behavior anomalies indicative of compromised accounts, helping organizations safeguard their assets effectively.

**66. How does your platform ensure data integrity and protection against unauthorized modifications of user attributes?**

**Dell Response:** OneLogin ensures data integrity and protection against unauthorized modifications of user attributes through several measures:

- Encryption: OneLogin employs encryption techniques to protect user data in transit and at rest. This encryption helps prevent unauthorized access to sensitive user attributes and ensures data integrity.
- Access Controls: OneLogin implements robust access controls to restrict access to user attributes only to authorized personnel. Role-based access control (RBAC) and granular permission settings help ensure that only users with the appropriate permissions can view or modify user attributes.
- Audit Trails: OneLogin maintains detailed audit trails of all user attribute modifications. This allows administrators to track changes made to user attributes, including who made the changes and when they were made. By maintaining these audit trails, OneLogin enables organizations to detect and investigate unauthorized modifications promptly.
- Two-Factor Authentication (2FA): Implementing 2FA adds an additional layer of security to user accounts, making it more difficult for unauthorized individuals to access and modify user attributes. OneLogin supports various 2FA methods, including SMS, authenticator apps, and hardware tokens, providing organizations with flexible options to enhance authentication security.

- Integration with Identity Providers: OneLogin integrates seamlessly with identity providers (IdPs) and directory services, such as Active Directory (AD) or LDAP. By leveraging existing authentication mechanisms and user attribute repositories, OneLogin helps ensure data integrity by centralizing user attribute management and enforcing consistent access policies across the organization.

Overall, OneLogin employs a combination of encryption, access controls, audit trails, two-factor authentication, and integration with identity providers to ensure data integrity and protect against unauthorized modifications of user attributes effectively. These measures help organizations maintain user data's confidentiality, integrity, and availability within their identity and access management systems.

#### 67. Can sessions be configured to timeout? If so, what are the configurable parameters?

**Dell Response:** OneLogin can be configured to timeout, and there are several configurable parameters available to adjust session behavior according to organizational requirements:

- Session timeout by fixed time value: This setting allows administrators to specify the number of minutes or hours that a user session remains valid after sign-in. A value of 0 disables fixed-time expirations.
- Session timeout by fixed time unit: Administrators can select either "Minutes" or "Hours" to specify the unit of time used in the previous setting.
- Session timeout by inactivity value: This setting enables administrators to define the number of minutes or hours that a session remains valid since the user was last active in OneLogin. A value of 0 disables inactivity-based expirations.
- Session timeout by inactivity unit: Similar to the fixed time unit setting, administrators can choose between "Minutes" or "Hours" to specify the unit of time for inactivity-based expirations.
- "Keep me signed in" option: Enabling this setting allows users to choose to persist their OneLogin sessions even after closing their browser. This option appears on the login page, giving users control over the longevity of their sessions.

It's important to note that enabling the "Keep me signed in" option allows sessions to persist beyond the configured timeout settings, providing flexibility for users who require continuous access to OneLogin services.

By configuring these parameters, organizations can tailor session timeout settings to meet their specific security and operational needs, balancing user convenience with the need for session management for security purposes.

#### 68. Are sessions cleared upon logging off?

**Dell Response:** Yes. With OneLogin, when a user logs off or signs out of their account, their session is terminated, and any associated session data, such as authentication tokens or session

identifiers, are invalidated and removed from the system. This ensures that the user is effectively logged out and helps enhance security by preventing unauthorized access to the user's account and sensitive information after logging off.

OneLogin follows standard security practices to clear sessions upon logging off to ensure the integrity of user accounts and data. This behavior helps maintain a secure user environment and aligns with best practices for session management in identity and access management systems.

**69. Can active user sessions be forcibly terminated by administrators?**

**Dell Response:** OneLogin has the option to allow sessions to the OneLogin platform to persist when the browser is closed. This persistent session allows users to remain authenticated after they exit so they can then return to their browser and have access to a resource. Session duration can be based upon a fixed amount of time or a period of time since the user performed any activity. For example, a user must re-authenticate with OneLogin after 2 hours regardless of if the user is active or not or if after a set period of inactivity, the user must re-authenticate with OneLogin.

Session expiration is controlled by set user policies within OneLogin and combined with a cookie in the users' browser. Session duration can be configured to be as short as one minute or as long as never expiring. Because this is configured on a user policy it can be different for different groups of users or scenarios (including shared kiosks). The user's policies, then, influences session management and these include scenarios where detected anomalies and feedback from step-up authentication can trigger session/user expiration.

Session duration for applications hosted through OneLogin is managed by the applications.

**70. Describe your approach to managing long-running sessions.**

**Dell Response:** When it comes to managing long-running sessions in OneLogin, administrators have a range of options at their disposal to customize the approach according to their organization's specific security requirements and user experience preferences:

- **Session Timeout Configuration:** OneLogin allows administrators to set session timeout durations based on their organization's security policies. Admins can define the period of inactivity after which a user's session will automatically expire.
- **Token-Based Authentication:** OneLogin utilizes tokens for authentication and authorization, which have finite lifespans. Admins can configure token expiration times, ensuring that sessions are periodically refreshed for active users to maintain security.
- **Granular Session Management Policies:** Administrators can establish detailed policies governing session behavior. This includes defining rules for session duration, idle timeout thresholds, and requirements for reauthentication. These policies can be tailored to align with security best practices and compliance standards.
- **User Interface and API:** OneLogin provides an intuitive administrative interface where admins can monitor and manage active user sessions. Additionally, APIs are available for programmatic interaction, enabling customization and automation of session-related tasks.

- Single Sign-On (SSO) Control: OneLogin's SSO capabilities streamline access to multiple applications. Administrators can configure SSO behavior to manage session continuity across various integrated services while maintaining security standards.
- Event Logging and Monitoring: OneLogin logs crucial user authentication and session management events. Admins can leverage these logs for real-time monitoring, anomaly detection, and enforcement of security policies.

By leveraging these customizable options, organizations can design a tailored approach to managing long-running sessions in OneLogin that optimizes both security and user experience according to your organization's unique needs.

**71. How does your platform manage user sessions in scenarios where users access applications from various locations?**

**Dell Response:** OneLogin manages user sessions across various locations through a combination of security measures and session management policies. Here's how the OneLogin platform typically handles sessions in scenarios involving users accessing applications from different locations:

- Single Sign-On (SSO) and Centralized Authentication: OneLogin offers SSO functionality, allowing users to access multiple applications with a single set of credentials. When users authenticate through OneLogin, a session is established, and they gain access to all integrated applications they have been provisioned access to. This centralized authentication approach ensures consistency and security across different locations.
- Session Context and Device Recognition: OneLogin maintains session context and device recognition capabilities to identify and validate user access from different locations and devices. By analyzing factors such as IP address, user agent, and geolocation data, OneLogin can detect suspicious or unauthorized access attempts and take appropriate action.
- Multi-Factor Authentication (MFA): OneLogin supports multi-factor authentication (MFA), adding an extra layer of security to user sessions, especially in scenarios involving access from various locations. Administrators can configure MFA policies to require additional authentication factors such as SMS codes, push notifications, or biometric verification, further verifying the user's identity before granting access.
- Session Policies and Controls: Administrators can define session policies and controls to manage user sessions effectively. This includes setting session timeout durations, specifying trusted networks or locations where access is permitted without additional authentication, and enforcing reauthentication requirements for sensitive operations or after certain events.
- Event Logging and Monitoring: OneLogin logs user authentication events and session activities, giving administrators visibility into user access patterns and potential security threats across different locations. Real-time monitoring and alerting capabilities enable prompt responses to suspicious activities or policy violations.



- Geofencing and IP Allow-Listing/Block-Listing: OneLogin offers geofencing capabilities, allowing administrators to define geographical boundaries where users can access applications. Additionally, administrators can configure IP allow listing or block listing rules to control access based on specific IP addresses or ranges, further enhancing security in multi-location scenarios.

Combining these features and controls, the OneLogin platform effectively manages user sessions in scenarios where users access applications from various locations. This ensures a balance between accessibility and security, providing a seamless experience for users while protecting against unauthorized access and potential security threats.

**72. Explain how your solution assists administrators in remotely terminating active sessions when necessary.**

**Dell Response:** OneLogin equips administrators with various options for remotely terminating active user sessions. However, the efficacy of these capabilities hinges on the specific protocols in use and how applications are implementing them. Here's how OneLogin empowers administrators to terminate active sessions remotely:

- Sign-Out Options from Administration Interface: Administrators can manually sign out users from active sessions via the administration interface. This feature allows admins to revoke access for specific users. However, it's important to note that the effectiveness of this function relies on the native abilities of the protocols and applications being used. While OneLogin provides the interface to trigger sign-out, the actual termination of the session depends on the capabilities of the underlying protocol applications.
- Session Management Policies: OneLogin lets administrators define session management policies, including timeout durations and reauthentication requirements for sessions. By configuring these policies appropriately, administrators can automatically enforce session terminations after a specified period of inactivity or trigger reauthentication prompts to verify user identities periodically. This ensures active sessions are managed according to security best practices and organizational policies.
- API Access for Session Control: OneLogin provides APIs that allow administrators to interact with active user sessions programmatically. Administrators can retrieve information about active sessions through these APIs, revoke specific sessions, or perform other session-related actions as needed.
- Event Logging and Monitoring: OneLogin logs user authentication events and session activities, giving administrators visibility into active sessions and user access patterns. Administrators can monitor these logs in real-time and identify suspicious or unauthorized sessions. Administrators can take appropriate action to terminate active sessions and mitigate risks in case of a security incident or policy violation. This proactive monitoring helps in promptly identify and address potential security threats.

While OneLogin provides several features and tools to assist administrators in remotely terminating active sessions, it's essential to understand the dependencies on the capabilities of the underlying protocols and applications. Administrators should review and configure session management

settings carefully and leverage available tools to maintain security and compliance standards effectively.

### 73. Does your solution integrate with Active Roles Server?

**Dell Response:** Yes, there are 2 primary integrations available.

- OneLogin can be utilized to provide Single Sign-On with Multifactor Authentication to the Active Roles Web Interface
- OneLogin can synchronize with Active Directory via its real-time Active Directory Connector. You can utilize Active Roles features like Administration Policies, Dynamic Groups, and Workflows to accurately and strictly define your user accounts and their attributes and group memberships. Then, OneLogin can utilize Mappings to automatically assign Security Policies, Applications, Permissions, and more based on that data.

### 74. Explain how your platform complies with industry standards and regulations related to data security and privacy.

**Dell Response:** "Security First" is today how we operate at OneLogin.

Our Global Enterprise Trust and Security program scope covers our technologies, business processes and security culture across our global operating environments of our production and our corporate facilities. Our Trust and Security function have dedicated teams carrying out focused risk assessments throughout our technology and data management lifecycle. The scope of these risk assessments include our service partners suppliers and vendors. Our Security Engineers design the Security controls in our product and corporate service offerings. Our Application Security team has an independent mandate to test our technologies to provide Trust Assurance that threat vectors and their associated vulnerabilities have appropriate controls applied to reduce the confidentiality, integrity, availability, and privacy risks reduced to acceptable business operating level.

Our polices, standards and business operating procedures are reviewed at least annually and/or amended to ensure we continue to against OneLogin, our product offerings and entire operating environments against the latest threat and threat vectors.

#### Data Trust & Security Framework

Data Management is at the core of the OneLogin Trust and Security framework. The framework is built from a full range of factors that inform the security approach, from the broadest government laws and regulations to the details of specific contractual agreements. OneLogin then take all these externally focused factors to translate them into our internal policies, standards and procedure that make up how we at Onelogin operate. This includes how we provide you with Trust Assurance for the management of our Customer Data.

OneLogin works at international and global level to stay abreast of security and privacy requirements as set forth under international, federal, and state laws. By continually monitoring the security and privacy landscape, OneLogin can modify its data governance approach to remain in step and comply with the latest requirements.

Regardless of industry, the need for data governance has driven the creation of best practices and standards to guide companies in their security and privacy strategy and capabilities. OneLogin provides its customers with Trust Assurance on how their data is protected and managed via our certifications and attestations to industry best practice standards. OneLogin Trust Assurance earned, includes:

ISO 27001:2013 – The highest level of certification available today for assuring global information security. OneLogin has earned this certification for all aspects of the enterprise, including the OneLogin Product and Service Offering along with our company operations. ISO 27001 is core to OneLogin’s Security Standard model, and OneLogin’s ISO 27001 results can be made available to customers so that they can map them into their own vendor management programs.

ISO 27017:2015 – This standard provides guidance to both cloud service providers and consumers of these services in the form of objectives, controls, and guidelines. OneLogin aligned its existing security controls to be compliant to this standard in order to augment its security program. These controls are tested as part of the periodic SOC 2 Type 2 report and an independent body has audited our compliance with this standard as part of our ISO 27001:2013 certificate annual audits.

SOC 1 Type 2, SOC 2 Type 2 – Provides confirmation of OneLogin’s financial and information security controls. A SOC 1 Type 2 report describes the internal controls in place over financial reporting at an organization and requires a third-party service auditor to review and examine the organization’s operations over a set period of time. The SOC 2 Type 2 report specifically indicates that OneLogin’s technology meets the criteria for security, availability, confidentiality, and processing integrity and is protected against unauthorized physical and logical access. The report also confirms the platform is available for operation and use as an information system designated as confidential and protected, and is complete, accurate, timely, and authorized.

PCI DSS – The Payment Card Industry Data Security Standard outlines the security requirements for organizations that process, manage and store cardholder data. As a data processor OneLogin is in alignment supporting organizations meet their PCI-DSS Compliance requirements.

- 75. Vendor must provide three references of clients with similar requirements and user base. Vendor must provide contact information for each reference and current user count range. The estimated range should be greater than 30,000 users.**

**Dell Response:**

Cracker Barrel	OneLogin	30K users
Airbus	OneLogin	475K users
Salvation Army - Canada	OneLogin	45K users
Pandora	OneLogin	25K users

One Identity is a privately held company and does not share reference information other than company name and deployed solution. This information is considered confidential, internal information. However, upon down select, and confirmation of a NDA in place, your One Identity Account Executive will coordinate conversations with referenceable customers.

Additionally, you can read case studies on our website: [Customer Success \(oneidentity.com\)](#)

**Mandatory Qualification/Experience Requirements** – The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

- Vendor must provide SSAE No. 18 SOC 1 Type 2 report results yearly to satisfy overall State of WV SOC1 requirements.

**Dell Response:** Will be provided annually upon request and receipt of an executed NDA with One Identity. Please see the One Identity NDA for execution for more information.

## Dell Response to CRFQ

---

Please see the following page for Dell's Response.



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

State of West Virginia  
 Centralized Request for Proposals  
 Info Technology

<b>Proc Folder:</b> 1376334			<b>Reason for Modification:</b> To post addendum 02.
<b>Doc Description:</b> Identity Management Single Sign-On Solution			
<b>Proc Type:</b> Central Master Agreement			
<b>Date Issued</b>	<b>Solicitation Closes</b>	<b>Solicitation No</b>	<b>Version</b>
2024-03-20	2024-04-04 13:30	CRFP 0947 ERP2400000002	3

**BID RECEIVING LOCATION**

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

**VENDOR**

**Vendor Customer Code:**

**Vendor Name :** Dell Marketing, L.P.

**Address :** One Dell Way

**Street :**

**City :** Round Rock

**State :** TX **Country :** USA **Zip :** 78682

**Principal Contact :** Brian Tatum

**Vendor Contact Phone:** (440) 334-9419 **Extension:**

**FOR INFORMATION CONTACT THE BUYER**  
 Larry D McDonnell  
 304-558-2063  
 larry.d.mcdonnell@wv.gov

**Signature X** *Kiara Daniels* **FEIN#** 74-2616805 **DATE** 4/2/2024

All offers subject to all terms and conditions contained in this solicitation and Dell's clarifications and exceptions to certain terms and conditions as stated herein. Dell is committed to enter into a good faith negotiation of mutually agreeable terms and conditions.



**ADDITIONAL INFORMATION**

1. Post answers to vendor questions.
2. Do not attach Exhibit B - State of WV Unique Login History.
3. Do not attach WV Software As a Service Addendum
4. To extend the bid opening from March 26, 2024 to April 04, 2024. The bid opening time still remains at 1:30PM EST.

No other changes.

INVOICE TO	SHIP TO
ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US	ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	See Exhibit A - Pricing Page				

*\* Please see Dell's Cost Proposal for more information.*

Comm Code	Manufacturer	Specification	Model #
81112501			

**Extended Description:**  
 See attached documentation for complete details.

**SCHEDULE OF EVENTS**

Line	Event	Event Date
1	Vendor Technical Questions due by 2:00PM EST	2024-03-01

# **REQUEST FOR PROPOSAL**

## **(WV ERP Board and CRFP ERP24\*01)**

### **TABLE OF CONTENTS**

- 1. Table of Contents**
- 2. Section 1: General Information and Instructions**
- 3. Section 2: Instructions to Vendors Submitting Bids**
- 4. Section 3: General Terms and Conditions**
- 5. Section 4: Project Specifications**
- 6. Section 5: Vendor Proposal**
- 7. Section 6: Evaluation and Award**
- 8. Certification and Signature Page**

### **SECTION 1: GENERAL INFORMATION**

#### **1.1. Introduction:**

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the “Purchasing Division”) is issuing this solicitation as a request for proposal (“RFP”), as authorized by W. Va. Code §5A-3-10b, for the WV Enterprise Resource Planning Board (hereinafter referred to as the “Agency”) to provide a cloud based single sign on solution to manage login profiles with efficiency and with top-notch security standards. This is a replacement for the current MyApps system used by the State of WV to manage users of Statewide systems.

The RFP is a procurement method in which vendors submit proposals in response to the request for proposal published by the Purchasing Division. It requires an award to the highest scoring vendor, rather than the lowest cost vendor, based upon a technical evaluation of the vendor’s technical proposal and a cost evaluation. This is referred to as a best value procurement. Through their proposals, vendors offer a solution to the objectives, problem, or need specified in the RFP, and define how they intend to meet (or exceed) the RFP requirements.

# **REQUEST FOR PROPOSAL**

(WV ERP Board and CRFP ERP24\*01)

## **SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS**

Instructions begin on next page.

## 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," "will," 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.

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

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: March 1, 2024 at 2:00PM EST

Submit Questions to: Tara L. Lyle  
2019 Washington Street, East  
Charleston, WV 25305  
Fax: (304) 558-3970  
Email: tara.l.lyle@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 electronically 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 \_\_\_\_\_ 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:

SOLICITATION NO.:

BID OPENING DATE:

BID OPENING TIME:

FAX NUMBER:

**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 WV OASIS (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: March 12, 2024 at 1:30PM EST

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.

This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-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 § 5A-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](http://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/vrc/Venpref.pdf](http://www.state.wv.us/admin/purchase/vrc/Venpref.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 of Israel. This certification is required by W. Va. Code § 5A-3-63.

# **REQUEST FOR PROPOSAL**

## **(WV ERP Board and CRFP ERP24\*01)**

### **SECTION 3: GENERAL TERMS AND CONDITIONS**

Terms and conditions begin on next page.

## 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.

*Dell acknowledges and accepts.*

**2. DEFINITIONS:** As used in this Solicitation/Contract, the following 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.

*Dell acknowledges and accepts.*

**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:

**Term Contract**

**Initial Contract Term:** The Initial Contract Term will be for a period of three (3) years. 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)

**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.

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

**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:

the contract will continue for \_\_\_\_\_ years;

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).

**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.

**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.

**Other:** Contract Term specified in \_\_\_\_\_  
Dell acknowledges and accepts.

**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.

Dell acknowledges and accepts.

**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.

**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.

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

**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.



**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.

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

Dell acknowledges and accepts.

**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 a 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.

Dell acknowledges and accepts.

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

**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.

Dell acknowledges and accepts.

**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 of 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:

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

**Automobile Liability Insurance** in at least an amount of: \_\_\_\_\_ per occurrence.

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

**Commercial Crime and Third Party Fidelity Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Cyber Liability Insurance** in an amount of: \$5,000,000.00 per occurrence.

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

**Pollution Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Aircraft Liability** in an amount of: \_\_\_\_\_ per occurrence.

Please see attached Memorandum of Insurance submitted within the proposal response.

**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.

Please see attached Memorandum of Insurance submitted within the proposal response.

**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.

Dell acknowledges and accepts.

**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 \_\_\_\_\_.

Liquidated Damages Contained in the Specifications.

Liquidated Damages Are Not Included in this Contract.

Dell acknowledges and accepts.

**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.

Dell acknowledges and accepts.

**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.

Please see attached exceptions regarding the State's requested pricing preference.

**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.

Dell acknowledges and accepts.

**15. PAYMENT METHODS:** 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.)

Dell acknowledges and accepts.

**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.

Please see attached clarifications pertaining to this section.

**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.

[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)

**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.

[Please see attached clarifications pertaining to this section.](#)

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

[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)

**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.

Dell acknowledges and accepts.

**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.

Dell acknowledges and accepts.

**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.

Dell acknowledges and accepts.

**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.

Dell acknowledges and accepts.

**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.

Please see attached clarifications pertaining to this section.

**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.

Dell acknowledges and accepts.

**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 [www.state.wv.us/admin/purchase/privacy](http://www.state.wv.us/admin/purchase/privacy).

Dell acknowledges and accepts.



**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-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.

**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.

[Dell acknowledges and accepts.](#)

**33. ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document 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.

[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)

Revised 8/24/2023

**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.

[Please see attached clarifications pertaining to this section.](#)

**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.

[Please see attached clarifications pertaining to this section.](#)

**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.

[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)



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

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.

Quarterly 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.gov](mailto:purchasing.division@wv.gov).  
[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)

**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.

[Dell acknowledges and accepts.](#)

**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 form referenced above.

[Dell acknowledges and accepts.](#)

**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.

Dell acknowledges and accepts.

**45. VOID CONTRACT CLAUSES:** This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

Dell acknowledges and accepts.

**46. ISRAEL BOYCOTT:** Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

Dell acknowledges and accepts.

**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) Brian Tatum , Account Executive

(Address) One Dell Way, Round Rock, TX 78682

(Phone Number) / (Fax Number) (440) 334-9419

(email address) Brian\_Tatum@Dell.com

**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.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Dell Marketing, L.P.

(Company)

Kiara Daniels

(Signature of Authorized Representative)

Kiara Daniels, Proposal Manager 4/2/2024

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

(512) 720-5068

(Phone Number) (Fax Number)

Kiara\_Daniels@Dell.com

(Email Address)

\*Please refer to Dell's Clarifications and Exceptions.

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

### SECTION 4: PROJECT SPECIFICATIONS

#### 4.1. Background and Current Operating Environment:

Currently the State of WV uses MyApps custom identity management system. This system was developed by the Auditor's office in 2008. This system was also used to manage user access when the WVOASIS system went live in 2013 for Budget, 2014 for Financials and starting in 2015 for the HRM, time and leave system.

There is now a need to standardize on a new platform that will allow the State to manage login profiles with greater efficiency and with greater security standards. The Enterprise Resource Planning Board is issuing this RFP to find a cloud based comprehensive single sign on solution for the use of many third-party applications to include CGI Advantage, UKG, Deighton, and other applications currently hosted and maintained by the ERP Board.

Dell acknowledges and accepts.

**4.2. Project Goals and Mandatory Requirements:** In the past three years the OASIS system has been requested to provide multiple forms of data to the critical agency system to include some of those listed above. This helps in the reduction of duplication of data, duplication of user entry of this data and to provide a central source for data. As this expands in the future, there needs to be a secure mechanism for user interaction. That user interaction we believe will come from a new cloud-based identity management system. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches.

**4.2.1. Goals and Objectives** – The project goals and objectives are listed below.

**4.2.1.1** Provide a state-wide solution for the ERP solution and supporting applications to provide a single sign on solution.

**4.2.1.2** Obtain a complete single sign solution that is cloud based and will provide robust security solutions to include encryption, logging, and provide common industry standard options for a single sign on solution.

**4.2.2. Mandatory Project Requirements** – The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

**4.2.2.1** The solution must be able integrate with our existing identity sources including Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Ultimate Kronos Group (UKG)

**4.2.2.2** The solution must provide a seamless migration path for users from our existing identity infrastructure.



# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

- 4.2.2.3 Authentication methods must include SAML2.0, SP(Service Provider) and IDP (Identity Provider) methods of authentication.
- 4.2.2.4 The solution presented must be cloud-based.

**4.3. Qualifications and Experience:** Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

*Dell acknowledges and accepts.*

**Qualification and Experience Information:** Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

- 4.3.1.1. Can apps integrate directly with the solution's Application Programming Interface (API) to perform restful Application Programming Interface calls such as reading user information, or making changes to user objects, group membership.
- 4.3.1.2. Indicate if the proposed solution provides the ability to create custom Application Programming Interface access policies and/or authorized servers. Provide details.
- 4.3.1.3. Indicate if your service/solution offers Application Programming Interface token management and creation. If the solution offers this capability, provide details on API token management and creation capabilities.
- 4.3.1.4. Describe the Application Programming Interface capabilities your solution offers for integration with custom applications and workflows.
- 4.3.1.5. How do you ensure the security and privacy of data transmitted through your Application Programming Interfaces?
- 4.3.1.6. Can your solution support standards like Open Authorization (OAuth) 2.0 and OpenID Connect for secure Application Programming Interface access?
- 4.3.1.7. Detail the scalability of your Application Programming Interface infrastructure to support high volumes of authentication and authorization requests.
- 4.3.1.8. Does your solution provide Remote Authentication Dial-In User Service (RADIUS) support that does not require on-premise components?
- 4.3.1.9. Indicate if the solution provides supported push notification. If so, what controls can be used to lower the risk of push fatigue attacks.
- 4.3.1.10. List the Multi-factor methods supported.
- 4.3.1.11. Does your service offer out of the box login flows that protect against brute-force attacks?
- 4.3.1.12. Indicate if the proposed service offers out of the box login flows that protect against brute-force attacks and describe the protection against these attacks.
- 4.3.1.13. Detail the authentication methods supported by your platform (e.g., Email Multi-Factor Authentication (MFA), Short Message/Messaging Service (SMS)

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

MFA, Biometric/Web Authentication API (WebAuthN), and define any other capabilities that the vendor offers.

- 4.3.1.14. How does your solution provide adaptive authentication based on risk assessment?
- 4.3.1.15. Can your solution integrate with third-party identity providers for federated authentication?
- 4.3.1.16. Indicate which authentication protocols the proposed solution supports (e.g., Security Assertion Markup Language (SAML) 2.0, OpenID Connect (OIDC), Remote Authentication Dial-In User Service (RADIUS). Identify any other authentication protocols the proposed solution offers.
- 4.3.1.17. Explain how your solution adapts authentication methods based on contextual factors like location and device.
- 4.3.1.18. How does your solution handle scenarios where a user has lost their primary authentication device?
- 4.3.1.19. Can the solution block access based on blacklisted Internet Protocol (IP) addresses or Geogrpahy (GEO) location?
- 4.3.1.20. Does the service identify, detect, and block suspicious authentication activity?
- 4.3.1.21. Does the solution perform behavior detection during authentication? (Example: Impossible Travel, Device context, Network Context,)
- 4.3.1.22. How does your platform detect and prevent unauthorized access?
- 4.3.1.23. Can your platform support attribute-based access control (ABAC) to dynamically adjust access based on user attributes?
- 4.3.1.24. Can your solution integrate with external identity providers to extend authorization capabilities?
- 4.3.1.25. Can your platform enforce access policies based on contextual factors such as, but not limited to time of day, location, and user behavior?
- 4.3.1.26. Describe your solution's approach to enforcing the principle of least privilege for user access.
- 4.3.1.27. How does your platform support session termination and re-authentication based on inactivity or specific triggers?
- 4.3.1.28. Does the solution have the ability to have isolated lower environments for the purposes of testing / development?
- 4.3.1.29. Does your solution provide multiple environments for testing purposes?
- 4.3.1.30. Does the solution allow automation of tasks through scripting or Application Programming Interface calls?
- 4.3.1.31. Do you offer flexible application integrations such as general Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and Open Authorization (Oauth) connectors?
- 4.3.1.32. Do you offer deployment assistance, documentation, or training to ensure a smooth transition to your platform?
- 4.3.1.33. Can the solution leverage Active Directory as the Identity Provider? If so, do agents need to be installed on our systems to facilitate that communication? Additionally, is your solution capable of syncing that information in real time?
- 4.3.1.34. If an agent is required to facilitate a connection between Active Directory and your service, please describe how that information is exchanged securely.



# **REQUEST FOR PROPOSAL**

## **(WV ERP Board and CRFP ERP24\*01)**

Additionally, please describe how redundancy and failover can be configured to ensure there is a constant flow of information.

- 4.3.1.35.** Does the solution support the ability to import password hashes from other Identity Providers (IDPs)? If so, describe what hashing algorithms are supported and how that process works.
- 4.3.1.36.** Do you have an administrator dashboard User Interface (UI) to manage users? Can you enforce a specific multi-factor type for administrative access?
- 4.3.1.37.** Does the solution support external federation? If so, how, and what Identity Providers (IdPs) are supported?
- 4.3.1.38.** How does your solution streamline user onboarding and offboarding processes?
- 4.3.1.39.** How does your platform handle role-based access control and user provisioning?
- 4.3.1.40.** What customization options are available for the user interface and branding?
- 4.3.1.41.** Are all Multi-Factor Authentication (MFA) factors available for use in authenticating a user prior to performing self-service password maintenance? (E.g., Forgot Password, Change Password, Account Unlock)
- 4.3.1.42.** During a password reset, does the solution compare the supplied new password against a public database of known-compromised credentials and blocked the use of compromised credentials?
- 4.3.1.43.** Describe the self-service features available to end-users for password resets and profile updates.
- 4.3.1.44.** How does your platform handle de-provisioning of user access when an employee leaves the organization?
- 4.3.1.45.** What mechanisms are in place to ensure that user access is granted or revoked promptly?
- 4.3.1.46.** Does your service integrate with third-party logging solutions? If so, what logging formats are supported (i.e. JavaScript Object Notation (JSON), Comma separated Variable (CSV), and define any other capabilities that the vendor offers. And are they sent in real-time?
- 4.3.1.47.** Does the solution provide reporting on authentication statistics (Single Sign On (SSO) attempts, Multi-Factor Authentication (MFA) enrollment, new user creation, lockouts, permission changes, password resets), and define any other capabilities that the vendor offers.
- 4.3.1.48.** How long are the logs maintained?
- 4.3.1.49.** Do you provide any ability to create or pull reports? Do you have any templates for executive type reports?
- 4.3.1.50.** Please provide the full list of security events and descriptions captured by your service.
- 4.3.1.51.** Explain the logging mechanisms in place to capture identity-related events and activities.
- 4.3.1.52.** How does your solution provide real-time alerts for security incidents and policy violations?
- 4.3.1.53.** Can your solution meet compliance requirements by generating audit trails and activity reports?

# **REQUEST FOR PROPOSAL**

## **(WV ERP Board and CRFP ERP24\*01)**

- 4.3.1.54.** What options are available for exporting logs and reports to external systems or Security information and event management (SIEM) solutions?
- 4.3.1.55.** Indicate and identify any countries where you provide services to clients outside of the United States (and US territories).
- 4.3.1.56.** Have there been any significant security breaches in the past 24 months? If so please provide documentation of how this breach occurred, how many accounts were involved, and the remedy/solution for the breach.
- 4.3.1.57.** Provide information on how clients are informed of maintenance and patch releases.
- 4.3.1.58.** Where does the solution reside?
- 4.3.1.59.** Describe how your service is compliant with Americans with Disabilities Act (ADA) standards and how you support screen readers and descriptive technology.
- 4.3.1.60.** Describe how your service provides failover and redundancy.
- 4.3.1.61.** What controls does your service have in place to prevent automated attacks?
- 4.3.1.62.** How does your solution ensure high availability and resilience in the face of unexpected outages or disasters?
- 4.3.1.63.** Provide your data backup and recovery strategies to safeguard against data loss?
- 4.3.1.64.** Describe your approach to continuous monitoring and threat detection within your identity infrastructure.
- 4.3.1.65.** Can your solution provide insights into user behavior anomalies that might indicate compromised accounts?
- 4.3.1.66.** How does your platform ensure data integrity and protection against unauthorized modifications of user attributes?
- 4.3.1.67.** Can sessions be configured to timeout? If so, what are the configurable parameters?
- 4.3.1.68.** Are sessions cleared upon logging off?
- 4.3.1.69.** Can active user sessions be forcibly terminated by administrators?
- 4.3.1.70.** Describe your approach to managing long-running sessions
- 4.3.1.71.** How does your platform manage user sessions in scenarios where users access applications from various locations?
- 4.3.1.72.** Explain how your solution assists administrators in remotely terminating active sessions when necessary.
- 4.3.1.73.** Does your solution integrate with Active Roles Server?
- 4.3.1.74.** Explain how your platform complies with industry standards and regulations related to data security and privacy.
  
- 4.3.1.75.** Vendor must provide three references of clients with similar requirements and user base. Vendor must provide contact information for each reference and current user count range. The estimated range should be greater than 30,000 users.

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

**4.4. Mandatory Qualification/Experience Requirements** – The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

**4.4.1.1.** Vendor must provide SSAE No. 18 SOC 1 Type 2 report results yearly to satisfy overall State of WV SOC1 requirements.

### SECTION 5: VENDOR PROPOSAL

**5.1. Economy of Preparation:** Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

**5.2. Incurring Cost:** Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

**5.3. Proposal Format:** Vendors should provide responses in the format listed below:

**5.3.1. Two-Part Submission:** Vendors must submit proposals in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.

**5.3.2. Title Page:** State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.

**5.3.3. Table of Contents:** Clearly identify the material by section and page number.

**5.3.4. Response Reference:** Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.

**Proposal Submission:** All proposals (both technical and cost) must be submitted to the Purchasing Division **prior** to the date and time listed in Section 2, Instructions to Vendors Submitting Bids as the bid opening date and time.

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

### SECTION 6: EVALUATION AND AWARD

- 6.1. Evaluation Process:** Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.
- 6.2. Evaluation Criteria:** Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the 100 points. Cost represents 30 of the 100 total points.

#### **Evaluation Point Allocation:**

The evaluation questions in Section 4.3 have been divided into three levels (High, Medium, and Low).

High Requirement Level (42 responses):	15 Points Maximum (each)
Medium Requirement Level (24 responses):	10 Points Maximum (each)
Low Requirement Level (8 responses):	5 Points Maximum (each)

A total of 910 points can be earned from responses to these evaluation questions.

Total Technical Score: 910 Points Possible

Total Cost Score: 390 Points Possible

**Total Proposal Score: 1300 Points Possible**

- 6.3. Technical Bid Opening:** At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.
- 6.4. Technical Evaluation:** The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

### 6.5. Proposal Disqualification:

6.5.1. **Minimum Acceptable Score (“MAS”):** Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

6.5.2. **Failure to Meet Mandatory Requirement:** Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

6.6. **Cost Bid Opening:** The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

We are requesting an initial contract term of three years, with the option to renew for three additional one-year periods. Please complete the pricing page for all six years.

6.7. **Cost Evaluation:** The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

**Cost Evaluation Formula:** Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

**Step 1:**  $\text{Lowest Cost of All Proposals} / \text{Cost of Proposal Being Evaluated} = \text{Cost Score Percentage}$

**Step 2:**  $\text{Cost Score Percentage} \times \text{Points Allocated to Cost Proposal} = \text{Total Cost Score}$

Example:

Proposal 1 Cost is \$1,000,000  
Proposal 2 Cost is \$1,100,000

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 –  $\$1,000,000 / \$1,000,000 =$  Cost Score Percentage of 1 (100%)  
Step 2 –  $1 \times 30 =$  Total Cost Score of 30

Proposal 2: Step 1 –  $\$1,000,000 / \$1,100,000 =$  Cost Score Percentage of 0.909091 (90.9091%)  
Step 2 –  $0.909091 \times 30 =$  Total Cost Score of 27.27273

**6.8. Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Dell Marketing, L.P.

(Company)

*Kiara Daniels*

Kiara Daniels, Proposal Manager

(Representative Name, Title)

(512) 720-5068

(Contact Phone/Fax Number)

4/2/2024

(Date)

**ADDENDUM ACKNOWLEDGEMENT FORM**  
**SOLICITATION NO.: CRFP ERP24\*02**

**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)

- |                                     |                |                          |                 |
|-------------------------------------|----------------|--------------------------|-----------------|
| <input checked="" type="checkbox"/> | Addendum No. 1 | <input type="checkbox"/> | Addendum No. 6  |
| <input checked="" type="checkbox"/> | Addendum No. 2 | <input type="checkbox"/> | Addendum No. 7  |
| <input type="checkbox"/>            | Addendum No. 3 | <input type="checkbox"/> | Addendum No. 8  |
| <input type="checkbox"/>            | Addendum No. 4 | <input type="checkbox"/> | Addendum No. 9  |
| <input type="checkbox"/>            | Addendum No. 5 | <input type="checkbox"/> | 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.

Dell Marketing, L.P.

Company

Kiara Daniels

Authorized Signature

4/2/2024

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.  
Revised 6/8/2012



## Legal Clarifications and Exceptions

---

Please see the following page for Dell's Clarification and Exceptions.



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

State of West Virginia  
 Centralized Request for Proposals  
 Info Technology

**Proc Folder:** 1376334 **Reason for Modification:**  
**Doc Description:** Identity Management Single Sign-On Solution  
**Proc Type:** Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2024-02-23	2024-03-12 13:30	CRFP 0947 ERP2400000002	1

**BID RECEIVING LOCATION**

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

**DOR**

**Vendor Customer Code:**  
**Vendor Name :**  
**Address :**  
**Street :**  
**City :**  
**State :** **Country :** **Zip :**  
**Principal Contact :**  
**Vendor Contact Phone:**  
**Extension:**

**FOR INFORMATION CONTACT THE BUYER**  
 Larry D McDonnell 304-558-2063  
 larry.d.mcdonnell@wv.gov

Vendor  
Signature X

FEIN#

DATE

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

Date Printed: Feb 23, 2024

Page: 1

FORM ID: WV-PRC-CRFP-002 2020\05

**ADDITIONAL INFORMATION**

The State of West Virginia Purchasing Division, is soliciting bids for the West Virginia Enterprise Resource Planning Board, to establish an open-end contract for a cloud based single sign on solution to manage login profiles, per the attached documentation. \*\*\*\*\*

ELECTRONIC SUBMISSION IS PROHIBITED FOR THIS RFP

INVOICE TO	SHIP TO
ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301	ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	See Exhibit A - Pricing Page				

Comm Code	Manufacturer	Specification	Model #
81112501			

**Extended Description:**  
See attached documentation for complete details.

**SCHEDULE OF EVENTS**

Line	Event	Event Date
1	Vendor Technical Questions due by 2:00PM EST	2024-03-01

Date Printed: Feb 23, 2024

Page: 2

FORM ID: WV-PRC-CRFP-002 2020\05

**REQUEST FOR PROPOSAL**  
(WV ERP Board and CRFP ERP24\*01)

## **TABLE OF CONTENTS**

- 1. Table of Contents**
- 2. Section 1: General Information and Instructions**
- 3. Section 2: Instructions to Vendors Submitting Bids**
- 4. Section 3: General Terms and Conditions**
- 5. Section 4: Project Specifications**
- 6. Section 5: Vendor Proposal**
- 7. Section 6: Evaluation and Award**
- 8. Certification and Signature Page**

## **SECTION 1: GENERAL INFORMATION**

### **1.1. Introduction:**

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the “Purchasing Division”) is issuing this solicitation as a request for proposal (“RFP”), as authorized by W. Va. Code §5A-3-10b, for the WV Enterprise Resource Planning Board (hereinafter referred to as the “Agency”) to provide a cloud based single sign on solution to manage login profiles with efficiency and with top-notch security standards. This is a replacement for the current MyApps system used by the State of WV to manage users of Statewide systems.

The RFP is a procurement method in which vendors submit proposals in response to the request for proposal published by the Purchasing Division. It requires an award to the highest scoring vendor, rather than the lowest cost vendor, based upon a technical evaluation of the vendor’s technical proposal and a cost evaluation. This is referred to as a best value procurement. Through their proposals, vendors offer a solution to the objectives, problem, or need specified in the RFP, and define how they intend to meet (or exceed) the RFP requirements.

Revised 07/01/2021

# **REQUEST FOR PROPOSAL**

## **(WV ERP Board and CRFP ERP24\*01)**

### **SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS**

Instructions begin on next page.

## 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," "will," 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.

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

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: March 1, 2024 at 2:00PM EST

Submit Questions to: Tara L. Lyle  
2019 Washington Street, East  
Charleston, WV 25305  
Fax: (304) 558-3970  
Email: tara.l.lyle@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 electronically 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 \_\_\_\_\_ 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:

SOLICITATION NO.:

BID OPENING DATE:

BID OPENING TIME: FAX  
NUMBER:

**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: March 12, 2024 at 1:30PM EST

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.

This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-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 § 5A-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](http://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/vrc/Venpref.pdf](http://www.state.wv.us/admin/purchase/vrc/Venpref.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 minorityowned 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 *wv*OASIS 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 of Israel. This certification is required by W. Va. Code § 5A-3-63.

# **REQUEST FOR PROPOSAL**

(WV ERP Board and CRFP ERP24\*01)

## **SECTION 3: GENERAL TERMS AND CONDITIONS**

Terms and conditions begin on next page.

## 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 following 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:

**Term Contract**

**Initial Contract Term:** The Initial Contract Term will be for a period of \_\_\_\_\_ three (3) years

\_\_\_\_\_. 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 \_\_\_\_\_ successive one (1) year periods or multiple three (3) 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)

**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.

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



**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:

the contract will continue for \_\_\_\_\_ years;

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).

**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.

**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.

**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.

**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.

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

**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.

**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.

**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 a 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:

**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 of 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:

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

**Automobile Liability Insurance** in at least an amount of: \_\_\_\_\_ per occurrence.

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

**Commercial Crime and Third Party Fidelity Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Cyber Liability Insurance** in an amount of: \_\_\_\_\_ per occurrence. \$5,000,000.00

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

**Pollution Insurance** in an amount of: \_\_\_\_\_ per occurrence.

**Aircraft Liability** in an amount of: \_\_\_\_\_ per occurrence.

**Please see Dell and/or Quest's Memoranda of Insurance submitted with this Proposal**

**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.

**Please see Dell and/or Quest's Memoranda of Insurance submitted with this Proposal**

**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 \_\_\_\_\_.

Liquidated Damages Contained in the Specifications.

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.~~

**\*While Dell appreciates the request for most favored pricing, we cannot contractually agree to this request at this time. However, we remain committed to providing competitive and fair terms for our valued Customers, such as the State.**

**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 METHODS:** Vendor must accept payment by electronic funds transfer and PCard. (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.

**\*Dell accepts this clause subject to this requested clarification herein.**

**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 provided the State will not be entitled for any refunds for purchases made prior to the date of cancellation by the State; however the State will keep any license/subscription purchases prior to the

cancellation through the end of the subscription period. 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.

\* Dell accepts this clause subject to the request clarification herein.

**20. TIME:** Time is of the essence regarding all matters of time 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:** To the extent the following warranties are extended by Quest, 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.  
\*Dell accepts this clause subject to the requested clarification herein.
- 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 [www.state.wv.us/admin/purchase/privacy](http://www.state.wv.us/admin/purchase/privacy).

**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-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.



**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 Document 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 **by Vendor** 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.

To the extent such claims arise out of Vendor's obligations as a reseller. 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.

\*Dell accepts subject to its requested clarification herein.

**36. INDEMNIFICATION:** To the extent such claims arise out of Vendor's obligations as a reseller. 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.

\*Dell accepts subject to its requested clarification herein.

**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:

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.

**□** Quarterly 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.gov](mailto:purchasing.division@wv.gov).

**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 form 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 § 5A-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 § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

**47. LIMITATION OF LIABILITY:** Except for State's obligations to pay for product, services, or Third Party Products, State's violation of the restrictions on use of Products and Services or Vendor's or its Affiliates' intellectual property rights, or Vendor's indemnity obligations as stated in the clause above titled "Indemnification", Vendor's (including its suppliers) and State's total liability arising out of any Dispute or any matter under this Contract, is limited to the amount State paid to Vendor during the 12 months before the date that the matter or Dispute arose for the Product, Services or both that are the subject of the Dispute, but excluding amounts received as reimbursement of expenses or payment of taxes. Vendor (and its suppliers) shall have no liability for any direct damages resulting from State's use or attempted use of Third-Party Software, Free Software or Development Tools, all defined in the EULA described in [www.dell.com/eula](http://www.dell.com/eula), or Third-Party Products. Except for State's payment obligations and violation of Vendor's or its Affiliates' intellectual property rights, neither Vendor (and its suppliers) nor State has liability to the other for special, consequential, exemplary, punitive, incidental or indirect damages, or for lost profits, loss of revenue, loss or corruption of data, loss of use or procurement of substitute products or services.

**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.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

\_\_\_\_\_  
(Company)

\_\_\_\_\_  
(Signature of Authorized Representative)

\_\_\_\_\_  
(Printed Name and Title of Authorized Representative) (Date)

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

(Phone Number) (Fax Number)

---

(Email Address)

Revised 8/24/2023

### SECTION 4: PROJECT SPECIFICATIONS

#### 4.1. Background and Current Operating Environment:

Currently the State of WV uses MyApps custom identity management system. This system was developed by the Auditor's office in 2008. This system was also used to manage user access when the WVOASIS system went live in 2013 for Budget, 2014 for Financials and starting in 2015 for the HRM, time and leave system.

There is now a need to standardize on a new platform that will allow the State to manage login profiles with greater efficiency and with greater security standards. The Enterprise Resource Planning Board is issuing this RFP to find a cloud based comprehensive single sign on solution for the use of many third-party applications to include CGI Advantage, UKG, Deighton, and other applications currently hosted and maintained by the ERP Board.

**4.2. Project Goals and Mandatory Requirements:** In the past three years the OASIS system has been requested to provide multiple forms of data to the critical agency system to include some of those listed above. This helps in the reduction of duplication of data, duplication of user entry of this data and to provide a central source for data. As this expands in the future, there needs to be a secure mechanism for user interaction. That user interaction we believe will come from a new cloud-based identity management system. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches.

**4.2.1. Goals and Objectives** – The project goals and objectives are listed below.

**4.2.1.1** Provide a state-wide solution for the ERP solution and supporting applications to provide a single sign on solution.

**4.2.1.2** Obtain a complete single sign solution that is cloud based and will provide robust security solutions to include encryption, logging, and provide common industry standard options for a single sign on solution.

**4.2.2. Mandatory Project Requirements** – The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor



# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

- 4.2.2.1 The solution must be able integrate with our existing identity sources including Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Ultimate Kronos Group (UKG)
- 4.2.2.2 The solution must provide a seamless migration path for users from our existing identity infrastructure.
- 4.2.2.3 Authentication methods must include SAML2.0, SP(Service Provider) and IDP (Identity Provider) methods of authentication.
- 4.2.2.4 The solution presented must be cloud-based.

**4.3. Qualifications and Experience:** Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

**Qualification and Experience Information:** Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

- 4.3.1.1. Can apps integrate directly with the solution's Application Programming Interface (API) to perform restful Application Programming Interface calls such as reading user information, or making changes to user objects, group membership.
- 4.3.1.2. Indicate if the proposed solution provides the ability to create custom Application Programming Interface access policies and/or authorized servers. Provide details.
- 4.3.1.3. Indicate if your service/solution offers Application Programming Interface token management and creation. If the solution offers this capability, provide details on API token management and creation capabilities.
- 4.3.1.4. Describe the Application Programming Interface capabilities your solution offers for integration with custom applications and workflows.
- 4.3.1.5. How do you ensure the security and privacy of data transmitted through your Application Programming Interfaces?
- 4.3.1.6. Can your solution support standards like Open Authorization (OAuth) 2.0 and OpenID Connect for secure Application Programming Interface access?

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

- 4.3.1.7. Detail the scalability of your Application Programming Interface infrastructure to support high volumes of authentication and authorization requests.
- 4.3.1.8. Does your solution provide Remote Authentication Dial-In User Service (RADIUS) support that does not require on-premise components?
- 4.3.1.9. Indicate if the solution provides supported push notification. If so, what controls can be used to lower the risk of push fatigue attacks.
- 4.3.1.10. List the Multi-factor methods supported.
- 4.3.1.11. Does your service offer out of the box login flows that protect against bruteforce attacks?
- 4.3.1.12. Indicate if the proposed service offers out of the box login flows that protect against brute-force attacks and describe the protection against these attacks.
- 4.3.1.13. Detail the authentication methods supported by your platform (e.g., Email Multi-Factor Authentication (MFA), Short Message/Messaging Service (SMS) MFA, Biometric/Web Authentication API (WebAuthN), and define any other capabilities that the vendor offers.
- 4.3.1.14. How does your solution provide adaptive authentication based on risk assessment?
- 4.3.1.15. Can your solution integrate with third-party identity providers for federated authentication?
- 4.3.1.16. Indicate which authentication protocols the proposed solution supports (e.g., Security Assertion Markup Language (SAML) 2.0, OpenID Connect (OIDC), Remote Authentication Dial-In User Service (RADIUS). Identify any other authentication protocols the proposed solution offers.
- 4.3.1.17. Explain how your solution adapts authentication methods based on contextual factors like location and device.
- 4.3.1.18. How does your solution handle scenarios where a user has lost their primary authentication device?
- 4.3.1.19. Can the solution block access based on blacklisted Internet Protocol (IP) addresses or Geogrphahy (GEO) location?
- 4.3.1.20. Does the service identify, detect, and block suspicious authentication activity?
- 4.3.1.21. Does the solution perform behavior detection during authentication? (Example: Impossible Travel, Device context, Network Context,)
- 4.3.1.22. How does your platform detect and prevent unauthorized access?
- 4.3.1.23. Can your platform support attribute-based access control (ABAC) to dynamically adjust access based on user attributes?
- 4.3.1.24. Can your solution integrate with external identity providers to extend authorization capabilities?
- 4.3.1.25. Can your platform enforce access policies based on contextual factors such as, but not limited to time of day, location, and user behavior?
- 4.3.1.26. Describe your solution's approach to enforcing the principle of least privilege for user access.
- 4.3.1.27. How does your platform support session termination and re-authentication based on inactivity or specific triggers?

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

- 4.3.1.28. Does the solution have the ability to have isolated lower environments for the purposes of testing / development?
- 4.3.1.29. Does your solution provide multiple environments for testing purposes?
- 4.3.1.30. Does the solution allow automation of tasks through scripting or Application Programming Interface calls?
- 4.3.1.31. Do you offer flexible application integrations such as general Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and Open Authorization (Oauth) connectors?
- 4.3.1.32. Do you offer deployment assistance, documentation, or training to ensure a smooth transition to your platform?
- 4.3.1.33. Can the solution leverage Active Directory as the Identity Provider? If so, do agents need to be installed on our systems to facilitate that communication? Additionally, is your solution capable of syncing that information in real time?
- 4.3.1.34. If an agent is required to facilitate a connection between Active Directory and your service, please describe how that information is exchanged securely. Additionally, please describe how redundancy and failover can be configured to ensure there is a constant flow of information.
- 4.3.1.35. Does the solution support the ability to import password hashes from other Identity Providers (IDPs)? If so, describe what hashing algorithms are supported and how that process works.
- 4.3.1.36. Do you have an administrator dashboard User Interface (UI) to manage users? Can you enforce a specific multi-factor type for administrative access?
- 4.3.1.37. Does the solution support external federation? If so, how, and what Identity Providers (IdPs) are supported?
- 4.3.1.38. How does your solution streamline user onboarding and offboarding processes?
- 4.3.1.39. How does your platform handle role-based access control and user provisioning?
- 4.3.1.40. What customization options are available for the user interface and branding?
- 4.3.1.41. Are all Multi-Factor Authentication (MFA) factors available for use in authenticating a user prior to performing self-service password maintenance? (E.g., Forgot Password, Change Password, Account Unlock)
- 4.3.1.42. During a password reset, does the solution compare the supplied new password against a public database of known-compromised credentials and blocked the use of compromised credentials?
- 4.3.1.43. Describe the self-service features available to end-users for password resets and profile updates.
- 4.3.1.44. How does your platform handle de-provisioning of user access when an employee leaves the organization?
- 4.3.1.45. What mechanisms are in place to ensure that user access is granted or revoked promptly?
- 4.3.1.46. Does your service integrate with third-party logging solutions? If so, what logging formats are supported (i.e. JavaScript Object Notation (JSON), Comma separated Variable (CSV), and define any other capabilities that the vendor offers. And are they sent in real-time?

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

- 4.3.1.47. Does the solution provide reporting on authentication statistics (Single Sign On (SSO) attempts, Multi-Factor Authentication (MFA) enrollment, new user creation, lockouts, permission changes, password resets), and define any other capabilities that the vendor offers.
- 4.3.1.48. How long are the logs maintained?
- 4.3.1.49. Do you provide any ability to create or pull reports? Do you have any templates for executive type reports?
- 4.3.1.50. Please provide the full list of security events and descriptions captured by your service.
- 4.3.1.51. Explain the logging mechanisms in place to capture identity-related events and activities.
- 4.3.1.52. How does your solution provide real-time alerts for security incidents and policy violations?
- 4.3.1.53. Can your solution meet compliance requirements by generating audit trails and activity reports?
- 4.3.1.54. What options are available for exporting logs and reports to external systems or Security information and event management (SIEM) solutions?
- 4.3.1.55. Indicate and identify any countries where you provide services to clients outside of the United States (and US territories).
- 4.3.1.56. Have there been any significant security breaches in the past 24 months? If so please provide documentation of how this breach occurred, how many accounts were involved, and the remedy/solution for the breach.
- 4.3.1.57. Provide information on how clients are informed of maintenance and patch releases.
- 4.3.1.58. Where does the solution reside?
- 4.3.1.59. Describe how your service is compliant with Americans with Disabilities Act (ADA) standards and how you support screen readers and descriptive technology.
- 4.3.1.60. Describe how your service provides failover and redundancy.
- 4.3.1.61. What controls does your service have in place to prevent automated attacks?
- 4.3.1.62. How does your solution ensure high availability and resilience in the face of unexpected outages or disasters?
- 4.3.1.63. Provide your data backup and recovery strategies to safeguard against data loss?
- 4.3.1.64. Describe your approach to continuous monitoring and threat detection within your identity infrastructure.
- 4.3.1.65. Can your solution provide insights into user behavior anomalies that might indicate compromised accounts?
- 4.3.1.66. How does your platform ensure data integrity and protection against unauthorized modifications of user attributes?
- 4.3.1.67. Can sessions be configured to timeout? If so, what are the configurable parameters?
- 4.3.1.68. Are sessions cleared upon logging off?
- 4.3.1.69. Can active user sessions be forcibly terminated by administrators?
- 4.3.1.70. Describe your approach to managing long-running sessions

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

- 4.3.1.71. How does your platform manage user sessions in scenarios where users access applications from various locations?
- 4.3.1.72. Explain how your solution assists administrators in remotely terminating active sessions when necessary.
- 4.3.1.73. Does your solution integrate with Active Roles Server?
- 4.3.1.74. Explain how your platform complies with industry standards and regulations related to data security and privacy.
  
- 4.3.1.75. Vendor must provide three references of clients with similar requirements and user base. Vendor must provide contact information for each reference and current user count range. The estimated range should be greater than 30,000 users.

**4.4. Mandatory Qualification/Experience Requirements** – The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

- 4.4.1.1. Vendor must provide SSAE No. 18 SOC 1 Type 2 report results yearly to satisfy overall State of WV SOC1 requirements.

### SECTION 5: VENDOR PROPOSAL

**5.1. Economy of Preparation:** Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

**5.2. Incurring Cost:** Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

**5.3. Proposal Format:** Vendors should provide responses in the format listed below:

**5.3.1. Two-Part Submission:** Vendors must submit proposals in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

**5.3.2. Title Page:** State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.

**5.3.3. Table of Contents:** Clearly identify the material by section and page number.

**5.3.4. Response Reference:** Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.

**Proposal Submission:** All proposals (both technical and cost) must be submitted to the Purchasing Division **prior** to the date and time listed in Section 2, Instructions to Vendors Submitting Bids as the bid opening date and time.

### SECTION 6: EVALUATION AND AWARD

**6.1. Evaluation Process:** Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.

**6.2. Evaluation Criteria:** Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the 100 points. Cost represents 30 of the 100 total points.

#### **Evaluation Point Allocation:**

The evaluation questions in Section 4.3 have been divided into three levels (High, Medium, and Low).

High Requirement Level (42 responses): 15 Points Maximum (each)

Medium Requirement Level (24 responses): 10 Points Maximum (each) Low

Requirement Level (8 responses): 5 Points Maximum (each)

A total of 910 points can be earned from responses to these evaluation questions.

Total Technical Score:

910 Points Possible

# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

Total Cost Score:

390 Points Possible

**Total Proposal Score: 1300 Points Possible**

**6.3. Technical Bid Opening:** At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

**6.4. Technical Evaluation:** The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

**6.5. Proposal Disqualification:**

**6.5.1. Minimum Acceptable Score (“MAS”):** Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

**6.5.2. Failure to Meet Mandatory Requirement:** Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

**6.6. Cost Bid Opening:** The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

We are requesting an initial contract term of three years, with the option to renew for three additional one-year periods. Please complete the pricing page for all six years.



# REQUEST FOR PROPOSAL

## (WV ERP Board and CRFP ERP24\*01)

**6.7. Cost Evaluation:** The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

**Cost Evaluation Formula:** Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

**Step 1:**  $\text{Lowest Cost of All Proposals} / \text{Cost of Proposal Being Evaluated} = \text{Cost Score Percentage}$

**Step 2:**  $\text{Cost Score Percentage} \times \text{Points Allocated to Cost Proposal} = \text{Total Cost Score}$

Example:

Proposal 1 Cost is \$1,000,000  
Proposal 2 Cost is \$1,100,000  
Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 –  $\$1,000,000 / \$1,000,000 = \text{Cost Score Percentage of } 1 \text{ (100\%)}$   
Step 2 –  $1 \times 30 = \text{Total Cost Score of } 30$

Proposal 2: Step 1 –  $\$1,000,000 / \$1,100,000 = \text{Cost Score Percentage of } 0.909091 \text{ (90.9091\%)}$   
Step 2 –  $0.909091 \times 30 = \text{Total Cost Score of } 27.27273$

**6.8. Availability of Information:** Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

# REQUEST FOR PROPOSAL

(WV ERP Board and CRFP ERP24\*01)

---

(Company)

---

(Representative Name, Title)

---

(Contact Phone/Fax Number)

---

(Date)

**Attachment A: Cost Sheet**

## One Identity LLC NDA

---

Please see the following page for One Identity LLC NDA.

## Mutual Nondisclosure Agreement

This Nondisclosure Agreement (the "NDA") is made between One Identity LLC ("**One Identity**") on behalf of itself and its subsidiaries and affiliates and the legal entity identified in the signature field below ("**Company**"). The parties plan to exchange Confidential Information (as defined below) to explore business opportunities and manage their business relationships with one another and desire to establish the obligations with respect to such exchange. One Identity and the Company agree as follows:

- (1) **Definitions.** "**Confidential Information**" means information or materials disclosed by one party (the "**Disclosing Party**") to the other party (the "**Receiving Party**") that are not generally available to the public and which, due to their character and nature, a reasonable person under like circumstances would treat as confidential and do not include information or materials that: (a) are generally known to the public, other than as a result of an unpermitted disclosure by the Receiving Party after the Effective Date (as defined below); (b) were known to the Receiving Party without an obligation of confidentiality prior to receipt from the Disclosing Party; (c) the Receiving Party lawfully received from a third party without that third party's breach of agreement or obligation of trust; or (d) are or were independently developed by the Receiving Party without use of the Disclosing Party's Confidential Information. One Identity's Confidential Information may include the Confidential Information of its subsidiaries and affiliates.
- (2) **Obligations.** The Receiving Party shall (a) not disclose the Disclosing Party's Confidential Information to any third party, except as permitted in subsection (3) below; (b) protect the Disclosing Party's Confidential Information from unauthorized use or disclosure by exercising at least the same degree of care it uses to protect its own similar information, but in no event less than a reasonable degree of care; (c) promptly notify the Disclosing Party of any known unauthorized use or disclosure of the Disclosing Party's Confidential Information; and (d) cooperate with the Disclosing Party in any litigation brought by the Disclosing Party against third parties to protect its proprietary rights.
- (3) **Permitted Disclosures.** Notwithstanding the foregoing, the Receiving Party may disclose the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent (a) to any of its affiliates, directors, officers, employees, consultants, contractors or representatives (collectively, the "**Representatives**"), but only to those Representatives that (i) have a "need to know" in order to carry out the purposes of this NDA or to provide professional advice in connection with this NDA; (ii) are legally bound to the Receiving Party to protect information such as the Confidential Information under terms at least as restrictive as those provided herein; and (iii) have been informed by the Receiving Party of the confidential nature of the Confidential Information and the requirements regarding restrictions on disclosure and use as set forth in this Section; (b) as may be required by operation of law or legal process, provided that the Receiving Party provides prior notice of such disclosure to the Disclosing Party unless expressly prohibited from doing so by a court, arbitration panel or other legal authority of competent jurisdiction. The Receiving Party shall be liable to the Disclosing Party for the acts or omissions of any Representatives to which it discloses Confidential Information which, if done by the Receiving Party, would be a breach of this NDA.
- (4) **Ownership and Relationship.** All Confidential Information disclosed under this NDA shall remain the property of the Disclosing Party and no license under any patent or other intellectual property right is granted or conveyed by this NDA or a disclosure hereunder. This NDA does not create any agency, partnership or business relationship between the parties.
- (5) **Term and Termination.** The effective date of this NDA shall be the date of Company's signature below (the "**Effective Date**") and shall survive until terminated by written notice from one party to the other. Termination of this NDA shall not relieve a party of its obligations hereunder which shall continue for a period of five (5) years from the date of the disclosure under this NDA. Upon written request from the Disclosing Party and at its option, the Receiving Party shall promptly return the Disclosing Party's Confidential Information or destroy such Confidential Information, each to the extent it is reasonable and practicable to do so.
- (6) **Miscellaneous.** (a) Monetary damages may be insufficient to fully compensate either party for its losses in the event the other violates the provisions of this NDA. In addition to seeking monetary damages, each party therefore shall be entitled to seek to enjoin the other party from violating or continuing to violate the provisions of this NDA. (b) Except in connection with a change of control or business reorganization of a party, or a party's sale of assets, neither party shall assign any of its rights or obligations under this NDA without the prior written consent of the other. (c) This NDA constitutes the entire agreement between the parties with respect to the subject matter hereof, and it supersedes any prior or contemporaneous written or oral agreement. (d) The invalidity or unenforceability of any provision of this NDA shall not affect the validity or enforceability of any other provision of this NDA. (e) This NDA shall not be modified except by written agreement of the parties. (f) This NDA shall be governed by the laws of the State of Washington without regard to its conflicts of laws principles. Any action seeking enforcement of this NDA or any provision hereof shall be brought exclusively in the state or federal courts located in Seattle, Washington. Each party hereby agrees to submit to the jurisdiction of such courts. (g) The headings of the paragraphs of this NDA are inserted for convenience only and shall not constitute a part hereof or affect in any way the meaning or interpretation of this NDA.

<b>One Identity:</b> <u>One Identity LLC</u>	<b>Company:</b> _____
<b>Address:</b> <u>20 Enterprise, Suite 100, Aliso Viejo, CA 92656</u>	<b>Address:</b> _____
<b>Authorized Signature:</b>  <u>Matt Goldberg</u>	<b>Authorized Signature:</b> _____
<b>Name:</b> <u>Assistant General Counsel</u>	<b>Name:</b> _____
<b>Title:</b> <u>Legal Department</u>	<b>Title:</b> _____
	<b>Date:</b> _____

Please return a Company executed NDA to [ContractsDepartment@Quest.com](mailto:ContractsDepartment@Quest.com).

## Memorandum of Insurance

---

Please see the following page for the Memorandum of Insurance.

MEMORANDUM OF INSURANCE					DATE 27-Mar-2024	
<p>This Memorandum is issued as a matter of information only to authorized viewers for their internal use only and confers no rights upon any viewer of this Memorandum. This Memorandum does not amend, extend or alter the coverage described below. This Memorandum may only be copied, printed and distributed within an authorized viewer and may only be used and viewed by an authorized viewer for its internal use. Any other use, duplication or distribution of this Memorandum without the consent of Marsh is prohibited. "Authorized viewer" shall mean an entity or person which is authorized by the insured named herein to access this Memorandum via <a href="https://marshdigital.marsh.com/marshconnect/viewMOI.action?clientId=362542334">https://marshdigital.marsh.com/marshconnect/viewMOI.action?clientId=362542334</a>. The information contained herein is as of the date referred to above. Marsh shall be under no obligation to update such information.</p>						
<b>PRODUCER</b> Marsh USA LLC dba Marsh Risk & Insurance Services ("Marsh")			<b>COMPANIES AFFORDING COVERAGE</b>			
<b>INSURED</b> Dell Technologies Inc. and all Subsidiaries One Dell Way - RR1-50 Round Rock Texas 78682 United States			Co. A Zurich American Insurance Company			
			Co. B American Guarantee and Liability Insurance Company			
			Co. C American Zurich Insurance Company			
			Co. D Syndicate 2623/623 at Lloyd's			
			Co. E			
			Co. F			
<b>COVERAGES</b>						
THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS MEMORANDUM MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS						
CO LTR	TYPE OF INSURANCE	POLICY NUMBER	POLICY EFFECTIVE DATE	POLICY EXPIRATION DATE	LIMITS LIMITS IN USD UNLESS OTHERWISE INDICATED	
A	<b>GENERAL LIABILITY</b> Commercial General Liability Occurrence	GLO699017800	01-Mar-2024	01-Mar-2025	GENERAL AGGREGATE USD 10,000,000 PRODUCTS - COMP/OP AGG USD 10,000,000 PERSONAL AND ADV INJURY USD 5,000,000 EACH OCCURRENCE USD 5,000,000 FIRE DAMAGE (ANY ONE FIRE) USD 5,000,000 MED EXP (ANY ONE PERSON) USD 10,000	
A	<b>AUTOMOBILE LIABILITY</b> Any Auto Hired Autos Non-Owned Autos	BAP699017700	01-Mar-2024	01-Mar-2025	COMBINED SINGLE LIMIT USD 5,000,000 BODILY INJURY (PER PERSON) BODILY INJURY (PER ACCIDENT) PROPERTY DAMAGE	
B	<b>EXCESS LIABILITY</b> Umbrella Form	AUC640818902	01-Mar-2024	01-Mar-2025	EACH OCCURENCE USD 15,000,000 AGGREGATE USD 15,000,000	
C A	<b>WORKERS COMPENSATION / EMPLOYERS LIABILITY</b> THE PROPRIETOR / PARTNERS / EXECUTIVE OFFICERS ARE Included	WC699017500-AOS WC699017600-MA, NE, WI	01-Mar-2024 01-Mar-2024	01-Mar-2025 01-Mar-2025	WORKERS COMP LIMITS Statutory EL EACH ACCIDENT USD 1,000,000 EL DISEASE - POLICY LIMIT USD 1,000,000 EL DISEASE - EACH EMPLOYEE USD 1,000,000	

D	Professional/E&O	B0509FINPT2350059	01-Jun-2023	01-Jun-2024	Each Claim/Aggregate (Claims Made)	USD \$15M excess of \$20M SIR

The Memorandum of Insurance serves solely to list insurance policies, limits and dates of coverage. Any modifications here to are not authorized.

<b>MEMORANDUM OF INSURANCE</b>	<b>DATE</b> 27-Mar-2024
--------------------------------	----------------------------

This Memorandum is issued as a matter of information only to authorized viewers for their internal use only and confers no rights upon any viewer of this Memorandum. This Memorandum does not amend, extend or alter the coverage described below. This Memorandum may only be copied, printed and distributed within an authorized viewer and may only be used and viewed by an authorized viewer for its internal use. Any other use, duplication or distribution of this Memorandum without the consent of Marsh is prohibited. "Authorized viewer" shall mean an entity or person which is authorized by the insured named herein to access this Memorandum via <https://marshdigital.marsh.com/marshconnect/viewMOI.action?clientId=362542334>. The information contained herein is as of the date referred to above. Marsh shall be under no obligation to update such information.

**PRODUCER**  
Marsh USA LLC dba Marsh Risk & Insurance Services ("Marsh")

**INSURED**  
Dell Technologies Inc. and all Subsidiaries  
One Dell Way - RR1-50  
Round Rock  
Texas 78682  
United States

**ADDITIONAL INFORMATION**

WITH THE EXCEPTION OF WORKERS COMPENSATION, ADDITIONAL INSURED APPLIES WHERE REQUIRED BY WRITTEN CONTRACT. WAIVER OF SUBROGATION APPLIES WHERE REQUIRED BY CONTRACT AND WHERE PERMITTED BY LAW.

The above referenced Errors & Omissions policy shall include technology/professional liability, and data protection liability (cyber liability) insurance providing protection against: (a) errors and omissions in the performance of professional services; (b) breaches of security; (c) violation or infringement of any right of privacy, breach of federal, state, or foreign security and/or privacy laws or regulations; and (d) data theft, damage, destruction, or corruption.

Crime #SAA E3917780500  
Insurer: Great American Insurance Company  
Effective 10/29/2023 - 10/29/2024  
Limit - \$15M \$2.5M Deductible

Excess Crime #DOXG71222032001  
Insurer: ACE American Insurance Company  
Effective 10/29/2023 - 10/29/2024  
Limit - \$10M xs \$15M

The Memorandum of Insurance serves solely to list insurance policies, limits and dates of coverage. Any modifications hereto are not authorized.





# CERTIFICATE OF LIABILITY INSURANCE

10/31/2024

DATE (MM/DD/YYYY)

10/30/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

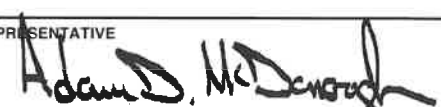
<b>PRODUCER</b> Lockton Insurance Brokers, LLC CA License #OF15767 Three Embarcadero Center, Suite 600 San Francisco CA 94111 (415) 568-4000	<b>CONTACT NAME:</b> PHONE (A/C No, Ext): E-MAIL ADDRESS:	FAX (A/C No):													
	<table border="1"> <thead> <tr> <th>INSURER(S) AFFORDING COVERAGE</th> <th>NAIC #</th> </tr> </thead> <tbody> <tr> <td>INSURER A : Federal Insurance Company</td> <td>20281</td> </tr> <tr> <td>INSURER B : Great Northern Insurance Company</td> <td>20303</td> </tr> <tr> <td>INSURER C : Lloyds of London</td> <td></td> </tr> <tr> <td>INSURER D : Chubb National Insurance Company</td> <td>10052</td> </tr> <tr> <td>INSURER E :</td> <td></td> </tr> <tr> <td>INSURER F :</td> <td></td> </tr> </tbody> </table>		INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A : Federal Insurance Company	20281	INSURER B : Great Northern Insurance Company	20303	INSURER C : Lloyds of London		INSURER D : Chubb National Insurance Company	10052	INSURER E :		INSURER F :
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A : Federal Insurance Company	20281														
INSURER B : Great Northern Insurance Company	20303														
INSURER C : Lloyds of London															
INSURER D : Chubb National Insurance Company	10052														
INSURER E :															
INSURER F :															
<b>INSURED</b> 1512384 Quest Software Inc. 10801 III N. Mopac Expressway, Suite 400 Austin TX 78759															

**COVERAGES** QUESO03      **CERTIFICATE NUMBER:** 18811382      **REVISION NUMBER:** XXXXXXXX

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
B	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:	N	N	3604-45-38	10/31/2023	10/31/2024	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000 \$
	<input checked="" type="checkbox"/> AUTOMOBILE LIABILITY ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY	N	N	7359-56-16	10/31/2023	10/31/2024	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ XXXXXXXX BODILY INJURY (Per accident) \$ XXXXXXXX PROPERTY DAMAGE (Per accident) \$ XXXXXXXX Comp/Coll Ded \$ 1,000
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED    RETENTION \$	N	N	7818-26-86	10/31/2023	10/31/2024	EACH OCCURRENCE \$ 25,000,000 AGGREGATE \$ 25,000,000 \$ XXXXXXXX
D	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below		N	71836917	10/31/2023	10/31/2024	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
C A	Primary Tech/E&O-Cyber Crime	N	N	B0146CYUSA2301294 8262-7803	10/31/2023 10/31/2023	10/31/2024 10/31/2024	\$10M \$5M

**DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)**  
 Freedom Mortgage is an Additional Insured with respect to liability arising out of the operations of the insured and to the extent provided by the policy language or endorsement issued or approved by the insurance carrier.

<b>CERTIFICATE HOLDER</b>  18811382 One Identity, LLC 20 Enterprise, Suite 100 Aliso Viejo CA 92656	<b>CANCELLATION</b> See Attachment  SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.  AUTHORIZED REPRESENTATIVE 
--	---

Tech E&O/Cyber:

Coverage: Primary Tech E&O/Cyber

Policy #: B0146CYUSA2301294

Carrier: Lloyds of London

Policy Term: 10/31/22 – 10/31/23

Limit: \$10M

Coverage: 1st Excess Tech E&O/Cyber

Policy #: B0146CYUSA2301915

Carrier: Lloyds of London

Policy Term: 10/31/22 – 10/31/23

Limit: \$10M xs \$10M

Coverage: 2nd Excess Tech E&O/Cyber

Policy #: EO5CABJ48P007

Carrier: Liberty Surplus Insurance Corporation

Policy Term: 10/31/22 – 10/31/23

Limit: \$10M xs \$20M

Coverage: 3rd Excess Tech E&O/Cyber

Policy #: 596738248

Carrier: Columbia Casualty Company

Policy Term: 10/31/22 – 10/31/23

Limit: \$10M xs \$30M

Coverage: 4th Excess Tech E&O/Cyber Quota Share A

Policy #: CYT27220105

Carrier: Canopus US Insurance

Policy Term: 10/31/22 – 10/31/23

Limit: \$5M po \$10M xs \$40M

Coverage: 4th Excess Tech E&O/Cyber Quota Share B

Policy #: XCE-00011M8-01

Carrier: Westfield Specialty Insurance Company

Policy Term: 10/31/22 – 10/31/23

Limit: \$5M po \$10M xs \$40M

## Proposal Legal Notes

---

Dell Technologies conducts operations through its subsidiaries and is the parent company to contracting legal entities Dell Marketing L.P. and EMC Corporation.

The contents of this response, including all elements of proposed pricing, performance level agreements and any referenced terms and conditions, apply only to direct purchases with Dell Technologies.

### Terms & Conditions

This proposal will remain valid for 30 days from the date of submission of the proposal. Final pricing and other legally binding contract terms must be agreed or confirmed between the parties.

Dell is submitting this proposal subject to the clarifications and exceptions to the CRFP 0947 ERP2400000002 Identity Management Single Sign-On Solution terms and conditions included herewith. Dell welcomes the opportunity to negotiate its request for clarifications and exceptions to the terms and conditions to reach a mutually acceptable governing agreement with State of WV Department of Administration Purchasing Division.

If the CRFP 0947 ERP2400000002 Identity Management Single Sign-On Solution allows State of WV Department of Administration Purchasing Division the discretion to reject a bid that takes exceptions to the CRFP 0947 ERP2400000002 Identity Management Single Sign-On Solution terms and conditions, Dell requests the opportunity to review and discuss its request for clarifications and exceptions with State of WV Department of Administration Purchasing Division further.

Dell has proposed a limitation of liability in line with industry standards for software and services contracts, and believes this provision is a fair allocation of risk, based on Dell's role as a reseller, and the State's direct contractual relationship with Quest.

### Disclaimer

This proposal (and information contained herein) is provided to you for information purposes only. Dell Technologies is not responsible for any errors or omissions relating to this proposal or that may occur as a result of the passage of time. In addition, Dell Technologies may improve or change this presentation or improve or change its products and service offerings from time to time, without updating this proposal. Please contact your sales representative for updates or additional information.

### Confidentiality

This proposal (and information contained herein) is Dell Technologies Confidential Information, and your access and use are subject to and governed by the terms of your written nondisclosure agreement with Dell Technologies. In the absence of an applicable, written nondisclosure agreement between you and Dell Technologies, your access and use of this proposal (and information contained herein) shall be limited as follows: you will maintain the confidentiality of the Dell Technologies Confidential Information with at least the same degree of care that you use to protect your own confidential information, but no less than a reasonable degree of care under the circumstances; you may use the Dell Technologies Confidential Information only for the business transaction between you and Dell Technologies ("Purpose"); you may disclose Dell Technologies Confidential Information only to your employees who have a need to know the information for the Purpose and are legally bound by similar nondisclosure terms; and you will not disclose Dell Technologies Confidential Information to any other employee or to a third party.

---

**Note**

This information may be exempt from disclosure under open records and/or freedom of information act (foia) statutes and regulations. Dell reserves all rights available to it under applicable law to appeal any disclosure to a third-party accordingly.