

Supplement N:

State Architecture and Computing Standards Requirements

State Security and Privacy Requirements

State IT Computing Policy Requirements

State Data Handling Requirements

Contents

State Architecture and Computing Standards Requirements.....	1
State Security and Privacy Requirements	1
State IT Computing Policy Requirements.....	1
State Data Handling Requirements	1
1. Overview and Scope.....	4
2. State Architecture and Computing Standards Requirements.....	4
2.1. Requirements Overview	4
2.1.1. State of Ohio Standards	4
2.1.2. Offeror Responsibilities	4
2.1.3. State Infrastructure Services	5
2.2. Compute Requirements	5
2.2.1. Client Computing.....	6
2.2.2. Server / OS	6
2.2.3. Ohio Cloud: Hypervisor Environment.....	6
2.3. Storage and Backup Requirements	6
2.3.1. Storage Pools	6
2.3.2. Backup.....	6
2.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN).....	7
2.5. Application Requirements	7
2.5.1. Application Platforms.....	7
2.5.2. Open API's.....	7
2.5.3. SOA (Service Oriented Architecture).....	7
2.6. Database Platforms.....	8
2.7. Enterprise Application Services.....	8
2.7.1. Health and Human Services: Integrated Eligibility	8
2.7.2. The Ohio Business Gateway (OBG).....	8
2.7.3. IT Service Management	8
2.8. Productivity, Administrative and Communication Requirements	9
2.8.1. Communication Services.....	9
3. General State Security and Information Privacy Standards and Requirements.....	9
3.1. State Provided Elements: Contractor Responsibility Considerations.....	10
3.2. Periodic Security and Privacy Audits	11
3.3. Annual Security Plan: State and Contractor Obligations	11
3.4. State Network Access (VPN).....	12
3.5. Security and Data Protection.....	13
3.6. State Information Technology Policies.....	13
4. State and Federal Data Privacy Requirements.....	14
4.1. Protection of State Data	14
4.2. Handling the State's Data.....	15
4.3. Contractor Access to State Networks Systems and Data	16
4.4. Portable Devices, Data Transfer and Media	17
4.5. Limited Use; Survival of Obligations	17
4.6. Disposal of PI/SSI	17
4.7. Remedies.....	17
4.8. Prohibition on Off-Shore and Unapproved Access.....	17
4.9. Background Check of Contractor Personnel.....	18
4.10. Federal Tax Information	18
5. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues	20
5.1. General.....	20
5.2. Actual or Attempted Access or Disclosure.....	20

5.3.	Unapproved Disclosures and Intrusions: Contractor Responsibilities.....	20
5.4.	Security Breach Reporting and Indemnification Requirements	21
6.	Security Review Services.....	21
6.1.	Hardware and Software Assets	21
6.2.	Security Standards by Device and Access Type.....	22
6.3.	Boundary Defenses.....	22
6.4.	Audit Log Reviews	22
6.5.	Application Software Security.....	22
6.6.	System Administrator Access.....	22
6.7.	Account Access Privileges	23
6.8.	Additional Controls and Responsibilities.....	23

1. Overview and Scope

This Supplement shall apply to any and all Work, Services, Locations and Computing Elements that the Contractor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State and any access of State resources in conjunction with delivery of work.

This scope shall specifically apply to:

- Major and Minor Projects, Upgrades, Updates, Fixes, Patches and other Software and Systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State;
- Any systems development, integration, operations and maintenance activities performed by the Contractor;
- Any authorized Change Orders, Change Requests, Statements of Work, extensions or Amendments to this agreement;
- Contractor locations, equipment and personnel that access State systems, networks or data directly or indirectly; and
- Any Contractor personnel, or sub-Contracted personnel that have access to State confidential, personal, financial, infrastructure details or sensitive data.

The terms in this Supplement are additive to the Standard State Terms and Conditions contained elsewhere in this agreement. In the event of a conflict for whatever reason, the highest standard contained in this agreement shall prevail.

2. State Architecture and Computing Standards Requirements

2.1. Requirements Overview

Offerors responding to State issued statement of work (SOW) requests, and as Contractors performing the work following an award are required to propose solutions that comply with the standards outlined in this document. In the event of a conflict with any published Standard, a variance may be requested, and the Offeror must show sufficient business justification for the variance request. The Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve / deny the variance request.

2.1.1. State of Ohio Standards

The State has a published Core Technology Stack as well as Enterprise Design Standards as outlined in this document and, due to State preferences, are subject to improvements and change. The State also provides numerous IT Services in both the Infrastructure and Application categories, as outlined in the State's IT Services Catalog at: <http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx>

2.1.2. Offeror Responsibilities

Offerors can propose on-premise or cloud-based solutions. When proposing on-premise solutions, vendors must comply with State requirements including using the State's Virtualized Compute Platform. Unless otherwise specified in the SOW request, offerors proposing on-premise solutions are required to install third party applications on State provided compute platforms. Dedicated server platforms are not compliant with the State's Virtualization Requirements.

Hardware and storage (memory, speeds, cpu and other configuration details) should be proposed to adhere to established State standards (generally VMware based system images for x86 environments) and or virtualized Oracle Exadata/Exalogic frames and components unless otherwise specified in the SOW Request.

In addition, Offerors are required to take advantage of all published IT Application Services where possible, i.e. Enterprise Service Bus, Content Management, Enterprise Document Management, Data Warehousing, Data

Analytics and Reporting and Business Intelligence. When dedicated Application components are required, i.e. Application Servers, Databases, etc., they should comply with the Core Technology standards.

2.1.3. State Infrastructure Services

The State of Ohio’s Office of Information Technology Infrastructure Services Division (OIT/ISD) will be responsible for providing the technical infrastructure platform as a service to the Contractor and will host the Contractor developed software and operating solution following the conclusion of the project for on-premise solutions. In general, this service includes the following:

- Primary Computing Facility: State of Ohio Computing Center (secure Tier III capable facility)
- Alternate/Disaster Recovery Center: Ohio Based Secure Tier II facility
- Redundant Networking between State facilities and Data Centers (Metro-E to 10Gb/s OARnet)
- Physical and Infrastructure Security Services
- Redundant Power, Cooling, Fire Suppression and onsite Redundant UPS/Power Generation
- Servers, Storage, Networking Devices, Firewalls, Security Appliances, Vulnerability and Virus Scanning to the operating system prompt
- Binding SLAs regarding performance, availability, reliability, provisioning and systems administrative access

The State of Ohio will provide ITIL based services in support of the Contractor as follows:

State Infrastructure Responsibility Matrix	
<p>Asset Management</p> <ul style="list-style-type: none"> ▪ Hardware Asset Tracking ▪ Software Asset Tracking ▪ Logistics Support ▪ Inventory Capture and Maintenance <p>Service Desk</p> <ul style="list-style-type: none"> ▪ Help Desk Operations ▪ Help Desk Tools ▪ Service Desk Processes 	<p>Enterprise Security Management</p> <ul style="list-style-type: none"> ▪ Emergency Response Service ▪ Threat Analysis ▪ Managed Intrusion/Detection/Prevention ▪ System Security Checking ▪ Security Advisory and Integrity ▪ Malware Defense Management ▪ Vulnerability Management ▪ ID Management ▪ Security Policy Management ▪ Security Compliance Support ▪ Security Audit
<p>Server Management</p> <ul style="list-style-type: none"> ▪ Platform Support (Tools/Processes Procedures) ▪ Unix/Intel Servers ▪ Incident Management ▪ Server Operations ▪ High Availability ▪ File Management <p>Storage Planning</p> <ul style="list-style-type: none"> ▪ Capacity Management ▪ Storage Performance Management 	<p>Data Center and Wide Area LAN/WAN Management</p> <ul style="list-style-type: none"> ▪ Enterprise Internet Services ▪ Regulatory/Change Management ▪ Network Engineering ▪ Standards ▪ LAN/WAN Management ▪ Network Operations and Management ▪ Network Capacity/Availability Management ▪ Network HW/SW Management ▪ Network Security ▪ Network M/A/C/D
<p>Data Center Architecture Planning</p> <ul style="list-style-type: none"> ▪ Hardware/Facilities Planning ▪ Unix/Intel Servers ▪ Platform Configuration Management ▪ Performance Management ▪ Capacity Management ▪ Batch Operations/Scheduling ▪ Storage Management ▪ Backup/Restore ▪ Media Management, Media Operations, Offsite Storage 	<p>Data Center Facilities Management</p> <ul style="list-style-type: none"> ▪ Site Maintenance and Operations ▪ Site Availability Management ▪ Routine Maintenance and Upgrades ▪ Non-Technical Services (parking lot, landscaping, snow removal etc.)

2.2. Compute Requirements

2.2.1. Client Computing

Offerors **must not** propose solutions that require custom PC's, Laptops, Notebooks etc. Unless otherwise specified in the SOW request, the State will source its own Client computing hardware and the Offeror's proposed solutions are required to be compatible with the State's hardware.

2.2.2. Server / OS

Offerors **must** propose solutions that comply with the State's supported Server / OS versions.

The following are the State's Required Server and OS versions.

Table 1 – Supported Server/OS versions

Operating System	Version	Edition
Microsoft Windows Server	2012, 2012 R2	Standard, Enterprise, & Datacenter
RedHat Linux	7	Enterprise
SUSE Linux	11	Enterprise
IBM AIX	7.1	
Oracle Enterprise Linux		Enterprise

When Offerors are proposing on-premise solutions, these solutions must comply with the State's supported Server Compute Platforms.

The State hosts and manages the Virtual Server hardware and Virtualization layer. The State is also responsible for managing the server's Operating System (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of Capacity Disk Storage. Customers can request up to 8 vCPUs and 24GB of RAM.

For Ohio Benefits and the Ohio Administrative Knowledge System (OAKS) – Exalogic Version 2.0.6.0.2

2.2.3. Ohio Cloud: Hypervisor Environment

2.3. Storage and Backup Requirements

2.3.1. Storage Pools

The State provides three pools (tiers) of storage with the ability to use and allocate the appropriate storage type based on predetermined business criticality and requirements. Storage pools are designed to support different I/O workloads.

When Offerors are proposing on-premise solutions, these solutions *must* take advantage of the State's Storage Service Offerings.

The pools and their standard use cases are below:

Table 2 – State Supported Storage Pools

Storage Pool	Availability	Performance	Typical Applications
Performance	Highest	Fast	Performance pool suited for high availability applications, with high I/O (databases).
General	High	Fast	General pool suitable for file servers, etc.
Capacity	High	Average	Capacity pool suitable for file servers, images and backup / archive). Not suited for high random I/O.

2.3.2. Backup

When Offerors are proposing on-premise solutions, these solutions *must* take advantage of the State's Backup Service Offering.

Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of customer data. It also provides for necessary restores due to data loss or corruption. The option of performing additional backups, archiving, restoring or retrieving functions is available for customer data. OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site. All critical production systems must also use the State's DR facility.

2.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN)

Offerors **must** propose solutions that work within the State's LAN / WAN infrastructure.

The State of Ohio's One Network is a unified solution that brings together Design, Engineering, Operations, Service Delivery, Security, Mobility, Management, and Network Infrastructure to target and solve key Government challenges by focusing on processes, procedures, consistency and accountability across all aspects of State and Local Government.

Ohio One Network can deliver an enterprise network access experience for their customers regardless of location or device and deliver a consistent, reliable network access method.

The State provides a high bandwidth internal network for internal applications to communicate across the State's LAN / WAN infrastructure. Normal traffic patterns at major sites should be supported.

Today, the State's WAN (OARnet) consists of more than 1,850 miles of fiber-optic backbone, with more than 1,500 miles of it operating at ultrafast 100 Gbps speeds. The network blankets the state, providing connectivity to all State Government Agencies.

The State of Ohio Network infrastructure utilizes private addressing, reverse proxy technology and Network Address Translation (NAT). All applications that are to be deployed within the infrastructure must be tolerant of these technologies for both internal product interaction as well as external user access to the proposed system, infrastructure or application.

The State Network team will review applications requirements involving excessive bandwidth (i.e. voice, video, telemetry, or applications) deployed at remote sites.

2.5. Application Requirements

2.5.1. Application Platforms

When Offerors are proposing on-premise solutions, these solutions *must* be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.)

2.5.2. Open API's

Proposed vendor applications must be developed with standards-based Open API's. An open API is an [application program interface](#) that provides programmatic access to software applications. Proposed vendor applications must describe in detail all available features and functionality accessible via APIs.

2.5.3. SOA (Service Oriented Architecture)

When Offerors are proposing on-premise solutions, these solutions *must* be developed using a standards-based Service Oriented Architecture (SOA) model.

2.6. Database Platforms

Proposed vendor application designs must run on databases that comply with the State's supported Database Platforms.

- DB2 Version 10
- SQL 2012 or higher
- ORACLE 11g and 12C
- Exadata Version 11.2.3.2.1

2.7. Enterprise Application Services

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outline in the IT Services Catalog available at:

<http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx>

At a minimum, proposed vendor application designs that include the following Application Services *must* use the Application IT Services outlined in the IT Services Catalog.

2.7.1. Health and Human Services: Integrated Eligibility

The Integrated Eligibility Enterprise platform provides four key distinct technology domains / capabilities:

- Common Enterprise Portal – includes User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability
- Enterprise Information Exchange – includes Discovery Services (Application and Data Integration, Master Data Management (MDM) Master Person Index and Record Locator Service), Business Process Management, Consent Management, Master Provider Index and Security Management
- Analytics and Business Intelligence – Integration, Analysis and Delivery of analytics in the form of alerts, notifications and reports
- Integrated Eligibility – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs

2.7.2. The Ohio Business Gateway (OBG)

The Ohio Business Gateway (OBG) offers Ohio's businesses a time-and money-saving online filing and payment system that helps simplify business' relationship with Government agencies.

- New Business Establishment – Provides a single, portal based web location for the establishment of new businesses in Ohio, file with the required State agencies and ensure that business compliance requirements of the State are met.
- Single Point Revenue and Fee Collection - Manage payments to State's payment processor (CBOSS) and broker payment to multiple agencies while creating transaction logs and Business Customer "receipts".
- One-Stop Filing and Forms - Provides guides and forms to Business Users through complex transactions that have multiple steps, forms and / or filing requirements for users on procedures to complete the process including Agencies and (if applicable) systems they will need to interact with.
- Scheduling and Reminders - Notify Business Customers of a particular event that is upcoming or past due (Filing due) using a "calendar" or "task list" metaphor.
- Collections and Confirmations – Provides a Payment Card Industry (PCI) certified web-based payment solution that supports a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, and cash payments.

2.7.3. IT Service Management

ServiceNow, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk workflow based application which provides flexibility and ease of use. The IT Service Management Tool provides workflows aligning with ITIL processes such as Incident Management, Request Fulfillment, Problem Management, Change Management and Service Catalog.

2.8. Productivity, Administrative and Communication Requirements

2.8.1. Communication Services

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outlined in the IT Services Catalog available at:

<http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx>

At a minimum, proposed vendor application designs that include the following Communication Services **must** use the Communication Services outlined in the IT Services Catalog.

Exchange

- Exchange Mail
- Office 365
- Skype for Business Instant Messaging & Presence
- Enterprise Vault
- Clearwell eDiscovery
- Exchange Web Services
- Bulk Mailing
- External Mail Encryption
- Outbound Fax
- Mobile devices

EDI/Application Integration/Medicaid EDI

Lyris Listserv

On-premise application based FAX: eFAX

Fax2Mail is a “hosted” fax solution that allows agencies to seamlessly integrate inbound and outbound Fax with their existing desktop E-mail and back-office environments. Fax2Mail is a “cloud-based” solution.

Voice over Internet Protocol (VoIP)

The CBTS VoIP service, which is open to all agencies, boards, commissions, local governments and state supported education institutions, as well as State of Ohio Cooperative Purchasing Program members, provides core telephony, voice mail, collaboration, video, audio, and auto attendant functions to eligible customers. Optional services including ACR, IVR, Call Center Solutions and SIP Trunking are also available.

3. General State Security and Information Privacy Standards and Requirements

The Contractor will be responsible for maintaining information security in environments under the Contractor’s management and in accordance with State IT Security Policies. The Contractor will implement an information security policy and security capability as set forth in this agreement.

The Contractor’s responsibilities with respect to Security Services will include the following:

- Provide vulnerability management Services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed.
- Support the implementation and compliance monitoring for State IT Security Policies.
- Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Manage and administer access to the systems, networks, System software, systems files and State data, excluding end-users.
- Provide support in implementation of programs to educate State and Contractor end-users and staff on security policies and compliance.
- Install and update Systems software security, assign and reset passwords per established procedures, provide the State access to create User ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assist in processing State security requests, perform security reviews to confirm that adequate security procedures are in place on an ongoing basis, and provide incident investigation support (jointly with the State), and provide environment and server security support and technical advice.
- Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.
- Perform physical security functions (e.g., identification badge controls, alarm responses) at the facilities under the Contractor's control.
- Prepare an Information Security Controls Document. This document is the security document that is used to capture the security policies and technical controls that the Contractor will implement, as requested by the State, on Contractor managed systems, supported servers and the LAN within the scope of this agreement. The Contractor will submit a draft document for State review and approval during the transition period.

The State will:

- Develop, maintain and update the State IT Security Policies, including applicable State information risk policies, standards and procedures.
- Provide a State Single Point of Contact with responsibility for account security audits;
- Support intrusion detection and prevention and vulnerability scanning pursuant to State IT Security Policies;
- Provide the State security audit findings material for the Services based upon the security policies, standards and practices in effect as of the Effective Date and any subsequent updates.
- Assist the Contractor in performing a baseline inventory of access IDs for the systems for which the Contractor has security responsibility;
- Authorize User IDs and passwords for the State personnel for the Systems software, software tools and network infrastructure systems and devices under Contractor management;
- Approve non-expiring passwords and policy exception requests, as appropriate.

3.1. State Provided Elements: Contractor Responsibility Considerations

The State is responsible for Network Layer (meaning the internet Protocol suite and the open systems interconnection model of computer networking protocols and methods to process communications across the IP network) system services and functions that build upon State infrastructure environment elements, the Contractor shall not be responsible for the implementation of Security Services of these systems as these shall be retained by the State.

To the extent that Contractor's access or utilize State provided networks, the Contractor is responsible for adhering to State policies and use procedures and do so in a manner as to not diminish established State capabilities and standards.

The Contractor will be responsible for maintaining the security of information in environment elements that it accesses, utilizes, develops or manages in accordance with the State Security Policy. The Contractor will implement information security policies and capabilities, upon review and agreement by the State, based on the Contractor's standard service center security processes that satisfy the State's requirements contained herein.

The Contractor's responsibilities with respect to security services must also include the following:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Provide vulnerability management services including supporting remediation for identified vulnerabilities as agreed.
- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Support OIT in the implementation, maintenance and updating of statewide data security policies, including the State information risk policies, standards and procedures.
- Managing and administering access to the systems, networks, Operating Software or System Software, (including programs, device drivers, microcode and related code supporting documentation and media that: 1) perform tasks basic to the functioning of data processing and network connectivity; and 2) are required to operate Applications Software), systems files and the State Data.
- Supporting the State in implementation of programs to raise the awareness of End Users and staff personnel as to the existence and importance of security policy compliance.
- Installing and updating State provided or approved system security Software, assigning and resetting passwords per established procedures, providing the agency access to create user ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assisting in processing the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency's assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules, as they are made known by the State, are not compromised.
- Performing physical security functions (e.g., identification badge controls, alarm responses) at the facilities under Contractor control.

3.2. Periodic Security and Privacy Audits

The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue or finding be discovered the following resolution path shall apply:

- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

3.3. Annual Security Plan: State and Contractor Obligations

The Contractor will develop, implement and thereafter maintain annually a Security Plan for review, comment and approval by the State Information Security and Privacy Officer, that a minimum must include and implement processes for the following items related to the system and services:

- Security policies

- Logical security controls (privacy, user access and authentication, user permissions, etc.)
- Technical security controls and security architecture (communications, hardware, data, physical access, software, operating system, encryption, etc.)
- Security processes (security assessments, risk assessments, incident response, etc.)
- Detail the technical specifics to satisfy the following:
 - Network segmentation
 - Perimeter security
 - Application security and data sensitivity classification
 - PHI and PII data elements
 - Intrusion management
 - Monitoring and reporting
 - Host hardening
 - Remote access
 - Encryption
 - State-wide active directory services for authentication
 - Interface security
 - Security test procedures
 - Managing network security devices
 - Security patch management
 - Detailed diagrams depicting all security-related devices and subsystems and their relationships with other systems for which they provide controls
 - Secure communications over the Internet

The Security Plan must detail how security will be controlled during the implementation of the System and Services and contain the following:

- High-level description of the program and projects
- Security risks and concerns
- Security roles and responsibilities
- Program and project security policies and guidelines
- Security-specific project deliverables and processes
- Security team review and approval process
- Security-Identity management and Access Control for Contractor and State joiners, movers, and leavers
- Data Protection Plan for personal/sensitive data within the projects
- Business continuity and disaster recovery plan for the projects
- Infrastructure architecture and security processes
- Application security and industry best practices for the projects
- Vulnerability and threat management plan (cyber security)

3.4. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including the secure sockets layer (SSL) protocol and public key authentication, signing and encryption. In addition, any remote access solution must use Secure Multipurpose Internet Mail Extensions (S/MIME) to provide encryption and non-repudiation services through digital certificates and the provided PKI. Multi-factor authentication is to be employed for users with privileged network access by leveraging the State of Ohio RSA solution.

3.5. Security and Data Protection.

All Services must also operate at the [moderate level baseline] as defined in the National Institute of Standards and Technology (“NIST”) 800-53 Rev. 3 [moderate baseline requirements], be consistent with Federal Information Security Management Act (“FISMA”) requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. Additionally, they must provide the State’s systems administrators with 24x7 visibility into the services through a real-time, web-based “dashboard” capability that enables them to monitor, in real or near real time, the Services’ performance against the established SLAs and promised operational parameters.

3.6. State Information Technology Policies

The Contractor is responsible for maintaining the security of information in environment elements under direct management and in accordance with State Security policies and standards. The Contractor will implement information security policies and capabilities as set forth in Statements of Work and, upon review and agreement by the State, based on the Offeror’s standard service center security processes that satisfy the State’s requirements contained herein. The Offeror’s responsibilities with respect to security services include the following:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency’s review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Managing and administering access to the Operating Software, systems files and the State Data.
- Installing and updating State provided or approved system security Software, assigning and resetting administrative passwords per established procedures, providing the agency access to create administrative user ID’s, suspending and deleting inactive logon IDs, researching system security problems, maintaining network access authority, assist processing of the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency’s assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules are not compromised.
- Where the Contractor identifies a potential issue in maintaining an “as provided” State infrastructure element with the more stringent requirement of an agency security policy (which may be federally mandated or otherwise required by law), identifying to agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:
- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hours. This notification shall not minimize the more stringent Service Level Agreements pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

The Contractor will comply with State Security and Privacy policies and standards. For purposes of convenience, a compendium of links to this information is provided in the Table below.

State of Ohio Security and Privacy Policies

Item	Link
Statewide IT Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx
Statewide IT Bulletins	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITBulletins.aspx
IT Policies and Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx
DAS Standards (Computing and??)	100-11 Protecting Privacy), (700 Series – Computing) and (2000 Series – IT Operations and Management) http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASpolicies/tabid/463/Default.aspx

4. State and Federal Data Privacy Requirements

Because the privacy of individuals’ personally identifiable information (PII) and State Sensitive Information, generally information that is not subject to disclosures under Ohio Public Records law, (SSI) is a key element to maintaining the public’s trust in working with the State, all systems and services shall be designed and shall function according to the following fair information practices principles. To the extent that personally identifiable information in the system is “protected health information” under the HIPAA Privacy Rule, these principles shall be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in the system that is not “protected health information” under HIPAA, these principles shall still be implemented and, when applicable, aligned to other law or regulation.

All parties to this agreement specifically agree to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to work associated with this SOW request including but not limited to:

- United States Code 42 USC 1320d through 1320d-8 (HIPAA);
- IRS 1075 pertaining to FTI data;
- Code of Federal Regulations, 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945,45 CFR164.502 (e) and 164.504 (e);
- Ohio Revised Code, ORC 173.20, 173.22, 1347.01 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5101.572, 5112.21, and 5111.61; and
- Corresponding Ohio Administrative Code Rules and Updates.
- Systems and Services must support and comply with the State’s security operational support model which is aligned to NIST 800-53 Revision 3.

4.1. Protection of State Data

Protection of State Data. To protect State Data as described in this agreement, in addition to its other duties regarding State Data, Contractor will:

- Maintain in confidence any personally identifiable information (“PI”) and State Sensitive Information (“SSI”) it may obtain, maintain, process, or otherwise receive from or through the State in the course of the Agreement;
- Use and permit its employees, officers, agents, and independent contractors to use any PI/SSI received from the State solely for those purposes expressly contemplated by the Agreement;

- Not sell, rent, lease or disclose, or permit its employees, officers, agents, and independent contractors to sell, rent, lease, or disclose, any such PI/SSI to any third party, except as permitted under this Agreement or required by applicable law, regulation, or court order;
- Take all commercially reasonable steps to (a) protect the confidentiality of PI/SSI received from the State and (b) establish and maintain physical, technical and administrative safeguards to prevent unauthorized access by third parties to PI/SSI received by Contractor from the State;
- Give access to PI/SSI of the State only to those individual employees, officers, agents, and independent contractors who reasonably require access to such information in connection with the performance of Contractor's obligations under this Agreement;
- Upon request by the State, promptly destroy or return to the State in a format designated by the State all PI/SSI received from the State;
- Cooperate with any attempt by the State to monitor Contractor's compliance with the foregoing obligations as reasonably requested by the State from time to time. The State shall be responsible for all costs incurred by Contractor for compliance with this provision of this subsection;
- Establish and maintain data security policies and procedures designed to ensure the following:
 - a) Security and confidentiality of PI/SSI;
 - b) Protection against anticipated threats or hazards to the security or integrity of PI/SSI; and
 - c) Protection against the unauthorized access or use of PI/SSI.

4.1.1. Disclosure

Disclosure to Third Parties. This Agreement shall not be deemed to prohibit disclosures in the following cases:

- Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether PI/SSI or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process, Contractor will promptly notify the State (unless prohibited from doing so by law, rule, regulation or court order) in order that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor will also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State. If, in the absence of a protective order, Contractor is compelled as a matter of law to disclose the information provided by the State, Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, Contractor will advise and consult with the State and its counsel as to such disclosure and the nature of wording of such disclosure) and Contractor will use commercially reasonable efforts to obtain confidential treatment therefore;
- To State auditors or regulators;
- To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations; or
- To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

4.2. Handling the State's Data

The Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect that data from unauthorized disclosure, modification, or destruction. "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State. To accomplish this, the Contractor must adhere to the following principles:

- Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of the State Data.
- Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability.

- Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as detect and respond to those threats and vulnerabilities.
- Maintain appropriate identification and authentication processes for information systems and services associated with State Data.
- Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.
- Implement and manage security audit logging on information systems, including computers and network devices.

4.3. Contractor Access to State Networks Systems and Data

The Contractor must maintain a robust boundary security capacity that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these points, and disable all others.

To do this, the Contractor must:

- Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.
- Use two-factor authentication to limit access to systems that contain particularly sensitive State Data, such as personally identifiable data.
- Assume all State Data and information is both confidential and critical for State operations, and the Contractor's security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of that data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.
- Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access the State's Data, as well as attacks on the Contractor's infrastructure associated with the State's data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State's Data.
- Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State Data is stored. The method of securing the State Data must be appropriate to the situation and may include erasure, destruction, or encryption of the State Data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this Contract.
- Have a business continuity plan in place that the Contractor tests and updates at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains the State's Data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State's Data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the State's Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.
- Not allow the State's Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract properly. Even then, the Contractor may permit such only if adequate security measures are in place to ensure the integrity and security of the State Data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas.

- Ensure that portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, the State's Data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network.
- Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

4.4. Portable Devices, Data Transfer and Media

Any encryption requirement identified in this Supplement means encryption that complies with National Institute of Standards Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number. Any sensitive State Data transmitted over a network, or taken off site via removable media must be encrypted pursuant to the State's Data encryption standard ITS-SEC-01 Data Encryption and Cryptography.

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such to the State in writing as quickly as reasonably possible. The Contractor also must maintain an incident response capability for all security breaches involving State Data whether involving mobile devices or media or not. The Contractor must detail this capability in a written policy that defines procedures for how the Contractor will detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access State Data or the infrastructure associated with State Data.

To the extent the State requires the Contractor to adhere to specific processes or procedures in addition to those set forth above in order for the Contractor to comply with the managed services principles enumerated herein, those processes or procedures are set forth in this agreement.

4.5. Limited Use; Survival of Obligations.

Contractor may use PI/SSI only as necessary for Contractor's performance under or pursuant to rights granted in this Agreement and for no other purpose. Contractor's limited right to use PI/SSI expires upon conclusion, non-renewal or termination of this Agreement for any reason. Contractor's obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

4.6. Disposal of PI/SSI.

Upon expiration of Contractor's limited right to use PI/SSI, Contractor must return all physical embodiments to the State or, with the State's permission; Contractor may destroy PI/SSI. Upon the State's request, Contractor shall provide written certification to the State that Contractor has returned, or destroyed, all such PI/SSI in Contractor's possession.

4.7. Remedies

If Contractor or any of its representatives or agents breaches the covenants set forth in these provisions, irreparable injury may result to the State or third parties entrusting PI/SSI to the State. Therefore, the State's remedies at law may be inadequate and the State shall be entitled to seek an injunction to restrain any continuing breach. Notwithstanding any limitation on Contractor's liability, the State shall further be entitled to any other rights or remedies that it may have in law or in equity.

4.8. Prohibition on Off-Shore and Unapproved Access

The Contractor shall comply in all respects with U.S. statutes, regulations, and administrative requirements regarding its relationships with non-U.S. governmental and quasi-governmental entities including, but not limited to the export control regulations of the International Traffic in Arms Regulations ("ITAR") and the Export Administration Act ("EAA"); the anti-boycott and embargo regulations and guidelines issued under the EAA, and the regulations of the U.S. Department of the Treasury, Office of Foreign Assets Control, HIPPA Privacy Rules and other conventions as described and required in this Supplement.

The Contractor will provide resources for the work described herein with natural persons who are lawful permanent residents as defined in 8 U.S.C. 1101 (a)(20) or who are protected individuals as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the U.S. It also includes any governmental (federal, state, local), entity.

The State specifically excludes sending, taking or making available remotely (directly or indirectly), any State information including data, software, code, intellectual property, designs and specifications, system logs, system data, personal or identifying information and related materials out of the United States in any manner, except by mere travel outside of the U.S. by a person whose personal knowledge includes technical data; or transferring registration, control, or ownership to a foreign person, whether in the U.S. or abroad, or disclosing (including oral or visual disclosure) or transferring in the United States any State article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic missions); or disclosing (including oral or visual disclosure) or transferring data to a foreign person, whether in the U.S. or abroad.

It is the responsibility of all individuals working at the State to understand and comply with the policy set forth in this document as it pertains to end-use export controls regarding State restricted information.

Where the Contractor is handling confidential employee or citizen data associated with Human Resources data, the Contractor will comply with data handling privacy requirements associated with HIPAA and as further defined by The United States Department of Health and Human Services Privacy Requirements and outlined in <http://www.hhs.gov/ocr/privacysummary.pdf>

It is the responsibility of all Contractor individuals working at the State to understand and comply with the policy set forth in this document as it pertains to end-use export controls regarding State restricted information.

Where the Contractor is handling confidential or sensitive State, employee, citizen or Ohio Business data associated with State data, the Contractor will comply with data handling privacy requirements associated with the data HIPAA and as further defined by The United States Department of Health and Human Services Privacy Requirements and outlined in <http://www.hhs.gov/ocr/privacysummary.pdf>.

4.9. Background Check of Contractor Personnel

Contractor agrees that (1) it will conduct 3rd party criminal background checks on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no Ineligible Personnel will perform Sensitive Services under this Agreement. "Ineligible Personnel" means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, or money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (b) has been convicted of a felony.

"Sensitive Services" means those services that (i) require access to Customer/Consumer Information, (ii) relate to the State's computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities ("Sensitive Services").

Upon request, Contractor will provide written evidence that all of Contractor's personnel providing Sensitive Services have undergone a criminal background check and are eligible to provide Sensitive Services. In the event that Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

4.10. Federal Tax Information

Contract Language for General Services

4.10.1. Performance

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

1. All work will be done under the supervision of the Contractor or the Contractor's employees.
2. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract.
Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.
3. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
4. The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
5. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
6. All computer systems receiving, processing, storing, or transmitting Federal Tax Information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
7. No work involving Federal Tax Information furnished under this Contract will be subcontracted without prior written approval of the IRS.
8. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
9. The agency will have the right to void the Contract if the Contractor fails to provide the safeguards described above.

4.10.2. Criminal/Civil Sanctions

1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a

result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.

3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

4.10.3. Criminal/Civil Sanctions

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations provided for the performance of any work under this Contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with Contract safeguards

5. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues

5.1. General

If over the course of the agreement a security or privacy issue arises, whether detected by the State, a State auditor or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of any Contracted service associated with this agreement, the Contractor must:

- notify the State of the issue or acknowledge receipt of the issue within two (2) hours;
- within forty-eight (48) hours from the initial detection or communication of the issue from the State, present an potential exposure or issue assessment document to the State Account Representative and the State Chief Information Security Officer with a high level assessment as to resolution actions and a plan;
- within four (4) calendar days, and upon direction from the State, implement to the extent commercially reasonable measures to minimize the State's exposure to security or privacy until such time as the issue is resolved; and
- upon approval from the State implement a permanent repair to the identified issue at the Contractor's cost; and

5.2. Actual or Attempted Access or Disclosure

If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any PI/SSI by Contractor or any of its subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into Contractor's or any of its subcontractor's facilities or secure systems (collectively "Intrusion"), Contractor must immediately:

- Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized Disclosure or Intrusion;
- Investigate and determine if an Intrusion and/or Disclosure has occurred;
- Fully cooperate with the State in estimating the effect of the Disclosure or Intrusion's effect on the State and fully cooperate to mitigate the consequences of the Disclosure or Intrusion;
- Specify corrective action to be taken; and
- Take corrective action to prevent further Disclosure and/or Intrusion.

5.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

Contractor must, as soon as is reasonably practicable, make a report to the State including details of the Disclosure and/or Intrusion and the corrective action Contractor has taken to prevent further Disclosure and/or Intrusion. Contractor must, in the case of a Disclosure cooperate fully with the State to notify the effected persons as to the fact of and the circumstances of the Disclosure of the PI/SSI. Additionally, Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies having jurisdiction to investigate a Disclosure and/or any known or suspected criminal activity.

- Where the Contractor identifies a potential issue in maintaining an “as provided” State infrastructure element with the more stringent of an Agency level security policy (which may be Federally mandated or otherwise required by law), identifying to Agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hour. This notification shall not minimize the more stringent Service Level Agreements pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

5.4. Security Breach Reporting and Indemnification Requirements

- In case of an actual security breach that may have compromised State Data, the Contractor must notify the State in writing of the breach within two (2) hours of the Contractor becoming aware of the breach and fully cooperate with the State to mitigate the consequences of such a breach. This includes any use or disclosure of the State data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Contract by an employee, agent, or subcontractor of the Contractor.
- The Contractor must give the State full access to the details of the breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate. The Contractor must document all such incidents, including its response to them, and make that documentation available to the State on request.
- In addition to any other liability under this Contract related to the Contractor’s improper disclosure of State data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year’s identity theft protection service on behalf of any individual or entity whose personally identifiable information is compromised while it is in the Contractor’s possession. Such identity theft protection must provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individuals’ credit history through those services.

6. Security Review Services

As part of a regular Security Review process, the Contractor will include the following reporting and services to the State:

6.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this should include:

- Deviations to hardware baseline
- Inventory of information types by hardware device
- Software inventory against licenses (State purchased)
- Software versions and then scans of versions against patches distributed and applied

6.2. Security Standards by Device and Access Type

The Contractor will:

- Document security standards by device type and execute regular scans against these standards to produce exception reports
- Document and implement a process for deviation from State standards

6.3. Boundary Defenses

The Contractor will:

- Work with the State to support the denial of communications to/from known malicious IP addresses*
- Require remote login access to use two-factor authentication
- Support the State's monitoring and management of devices remotely logging into internal network
- Support the State in the configuration firewall session tracking mechanisms for addresses that access OAKS

6.4. Audit Log Reviews

The Contractor will:

- Work with the State to review and validate audit log settings for hardware and software
- Work with the State to devise and implement profiles of common events from given systems to both reduce false positives and rapidly identify active access
- Provide requirements to the State to configure operating systems to log access control events
- Design and execute bi-weekly reports to identify anomalies in system logs
- Ensure logs are written to write-only devices for all servers or a dedicated server managed by another group.

6.5. Application Software Security

The Contractor will:

- Perform configuration review of operating system, application and database settings
- Ensure software development personnel receive training in writing secure code

6.6. System Administrator Access

The Contractor will

- Inventory all administrative passwords (application, database and operating system level)
- Implement policies to change default passwords in accordance with State policies, particular following any transfer or termination of personnel (State, existing MSV or Contractor)
- Configure administrative accounts to require regular password changes
- Ensure service level accounts have cryptographically strong passwords
- Store passwords in a hashed or encrypted format
- Ensure administrative accounts are used only for administrative activities
- Implement focused auditing of administrative privileged functions
- Configure systems to log entry and alert when administrative accounts are modified
- Segregate administrator accounts based on defined roles

6.7. Account Access Privileges

The Contractor will:

- Review and disable accounts not associated with a business process
- Create daily report that includes locked out accounts, disabled accounts, etc.
- Implement process for revoking system access
- Automatically log off users after a standard period of inactivity
- Monitor account usage to determine dormant accounts
- Monitor access attempts to deactivated accounts through audit logging
- Profile typical account usage and implement or maintain profiles to ensure that Security profiles are implemented correctly and consistently

6.8. Additional Controls and Responsibilities

The Contractor will meet with the State no less frequently than annually to:

- Review, Update and Conduct Security training for personnel, based on roles
- Review the adequacy of physical and environmental controls
- Verify the encryption of sensitive data in transit
- Review access control to information based on established roles and access profiles
- Update and review system administration documentation
- Update and review system maintenance policies
- Update and Review system and integrity policies
- Update and Implement Risk Assessment Policies and procedures
- Update and implement incident response procedures