Tennessee Department of the Treasury (Treasury)
Comprehensive Cybersecurity Approach Framework

Treasury Information Services

June 21, 2023

Contents

1 Organizational and Management Practices

1.1 Security Program Governance

Treasury leadership has assigned roles and responsibilities for information security across its organization. This includes, but is not limited to, the following: documenting, disseminating, and periodically updating a formal information security program that addresses purpose, scope, roles, responsibilities, applicable laws and regulations, and the implementation of policies, standards, and procedures.

1.2 Confidentiality Agreements

Implement confidentiality or non-disclosure agreements with contractors and external entities to ensure the agency's needs for protection of classified information is met.

Treasury executes confidentiality and/or non-disclosure agreements with all contractors and external entities at the time of contract award. Signed/countersigned agreements are mandatory prior to the beginning of contract execution.

Treasury's Employee Guidebook (guidebook) outlines employee responsibilities concerning confidentiality and the handling of sensitive information. The employee guidebook is to be read by each new hire and signed on their first day. Additionally, secure transmittal / transportation of sensitive data is addressed within each RFP. Employees are always instructed to transmit data through secure mean, and to address with IS Security of any concerns that have with transmitting and receiving sensitive information.

1.3 Risk Assessments

A review process at planned intervals is implemented to ensure the continuing suitability and effectiveness of the agency's approach to managing information security.

Treasury has contracted with Dynetics, Inc. (Dynetics) of Huntsville, AL to provide comprehensive security evaluations. The most recent evaluation took place July 3, 2015 through July 22, 2015. Please see **Appendix A** for details of their findings.

Treasury IS Security will be revitalizing the ISO 27001/2 security framework and possibly moving to NIST standards in the FY 2024 year.

Treasury utilizes services from STS for vulnerability scanning of Treasury servers hosted by STS. Reports are provided weekly through the portal. Additionally, STS scans all publically facing services from outside the State network annually.

1.4 System Security

A formal document that provides an overview of the security requirements for agency information systems and describes the security controls in place (or planned) for meeting those requirements is maintained.

Treasury Servers are built from a baseline server image that meets the minimum standard of security required. As services are added to the servers, they are done so in a secure manner.

Treasury workstations are built from department images that meet the minimum standard security required. As additional programs and software is installed, they are evaluated to ensure security is not compromised.

1.5 System Certification

An assessment of the security controls in place for existing systems and those planned for new systems is conducted at least once each year. Assessment tools are readily available through security organizations, like National Institute of Standards and Technology (NIST), SysAdmin, Audit, Network, Security (SANS) Institute, and other reputable sources. The agency's security team reviews and approves actions taken to correct any deficiencies identified. Responsible technical or operational management are included in the review process.

Treasury's Servers are scanned by STS Security to identify any vulnerabilities on the listed on the MS-ISAC advisory. Security works with STS and Treasury

Server Administrators to address the vulnerabilities and mitigate any found risks.

1.6 Configuration Change Control

Changes made to information systems are controlled and documented. The changes are reviewed and approved in accordance with written policy and procedures, including a process for emergency changes.

Configuration management for Concord level is managed via Treasury's software development lifecycle configuration management process (see **Appendix B – Concord Configuration Management Process**).

Treasury follows a standard ServiceNow-based procedure for system changes requiring such requests to be submitted by the business owner of the system. Lifecycle of the request is documented within the ServiceNow ticket.

Changes to Servers are first completed in a test environment to ensure continued functionality after the change. Changes to workstations are made to a test group of workstations composed of approximately 10% of the total number of workstations, before being applied department wide.

1.7 Security Categorization

Procedures to classify systems and information that is stored, processed, shared, or transmitted with respect to the type of data (e.g., confidential or sensitive) and its value to critical business functions are in place.

Treasury does not employ a multi-tiered document security classification system. Rather, Treasury policy is to treat all information containing personally identifiable information (PII) as confidential and sensitive.

Treasury's policy for transmission of confidential and sensitive email may be found within the Employee User Responsibilities – Security of Confidential and Sensitive Information section within the Employee Handbook **(See Appendix D – Employee Handbook).**

1.7.1 Storage of Information

Confidential and sensitive information may only be stored in secure directories with access defined under least privileges policy. All Treasury workstations use encryption at rest to protect the sensitivity of data on the workstation. Treasury File servers also uses encryption at rest technology to ensure protection of data.

1.7.2 Processing of Information

Processing of information follows guidelines set forth in the “clean desk” subsection of Employee User Responsibilities – Security of Confidential and Sensitive Information section within the Employee Handbook.

1.7.3 Sharing of Information

Treasury’s policy is to not share PII with any other entity except as required by job function and approved by supervisor. The sharing of information between State departments is governed via guidelines set forth in Employee User Responsibilities – Security of Confidential and Sensitive Information section within the Employee Handbook.

1.7.4 Transmission of Information

Destruction of media containing PII is governed within the Employee User Responsibilities – Security of Confidential and Sensitive Information section within the Employee Handbook.

Media is specified as hardcopy and hard drives. However, no such guidance is offered for thumb drives, CDs, DVDs, etc.

1.7.4.1 Electronic

Transmission of confidential and sensitive information may only take place in keeping with Section 1.7.3 and may only take place via secure means including, but not limited to Secure File Transfer Protocol (SFTP), secure email, Hypertext Transfer Protocol Secure (HTTPS), or encrypted external devices.

1.7.4.2 Hardcopy

Sharing of hardcopy information may only take place in keeping with Section 1.7.3. Scanning or printing of hardcopy information is governed under Employee User Responsibilities – Security of Confidential and Sensitive Information section within the Employee Handbook. Additionally, Treasury employees are instructed to follow division protocols for securing confidential information in hard copy.

1.8 Vulnerability Scanning

A regular occurring (e.g., bi-annual, quarterly, monthly) process using specialized scanning tools and techniques that evaluates the configuration, patches, and services for known vulnerabilities is employed.

Currently reports from Windows Server Update Services (WSUS) and Ivanti Protect are review by IS Security to identify servers and workstations that are lacking in the latest patches, this is done monthly. STS does weekly scanning of Treasury Servers, hosted in their environment as well as the Treasury caged space and provides reports of vulnerabilities found. Nessus scanning tools are utilized to identify vulnerabilities and missing patches.

2 Personnel Practices

2.1 Security Awareness

Training is provided to all employees and contractors on an annual basis that addresses acceptable use and good computing practices for systems they are authorized to access. Content of training is based on the agency’s policies addressing issues, such as, privacy requirements, virus protection, incident reporting, Internet use, notification to staff about monitoring activities, password requirements, and consequences of legal and policy violations.

Since 2013, Treasury has utilized State of Tennessee Strategic Technology Solutions (STS) SANS "Securing the Human" video series to conduct training. New employees are required to watch the Treasury Security video as part of their new hire orientation. Department-wide classroom training occurs on a 12-month cycle every October, with online capabilities for remote users. Treasury utilizes online training to deliver its information and training specific to security policies. Please see **Appendix E – Online Security Training** for details about this training.

2.2 Human Resources Security

Policies and procedures that address purpose, scope, roles, responsibilities, and compliance to support personnel security requirements, such as access rights, disciplinary process, etc. are in place.

HR to provide document name for these procedures.

2.3 Position Categorization

Procedures for identifying system access needs by job function and screening criteria for individuals performing those functions are in place.

Treasury Security works with the supervisors to create security profiles for each role. Once a role's profile has been verified as correct, that profile will be mirrored for future hires into that same role.

2.4 Personnel Separation

A process to terminate information system and physical access and ensure the return of all agency-related property (keys, id badges, etc.) when an individual changes assignments or separates from the agency is developed and implemented.

Treasury Security policy is to be notified immediately upon receipt of an employee's termination or resignation notice. Policy requires a ServiceNow ticket be filed for documenting the departure of the user. If that user is assigned a laptop, Treasury Security will collect the laptop before end of business day on the user's last day. Additionally, per that ServiceNow TASK, that user is de-provisioned within Active Directory (AD) and outside network connectivity is revoked immediately upon termination.

2.5 Third Party or Contractor Security

Personnel security requirements for third-party providers and procedures to monitor compliance are in place. Requirements are included in acquisition-related documents, such as service-level agreements, contracts, and memorandums of understanding.

All third party or contractor personnel are required to sign a Server Access Control Form explicitly stating terms of use. Upon signing of this document, contractors are given minimum necessary access to only those servers required to perform their task. Completion of that task triggers a de-provisioning of that contract per the approach shown in 2.4 Personnel Separation above.

2.6 Personnel Screening

Employee history and/or a background check is performed on employees who work with or have access to confidential or sensitive information or critical systems.

All candidates considered for hire by Treasury must complete a background check prior to receiving an offer. Additionally, existing employees may also be required to complete a background check as a condition of promotion or advancement. Although these processes are owned by HR, Security must verify with HR that this check has been satisfactorily completed before provisioning any employee accounts. Security is adding this verification as a component of the New User Image work flow.

3 Physical Security Practices

3.1 Physical and Environmental Program

Policy and procedures that address the purpose, scope, roles, responsibilities, and compliance for physical and environmental security, such as security perimeter and entry controls, working in secure areas, equipment security, cabling security, fire detection and suppression, room temperature controls, etc. are in place.

Andrew Jackson Building Physical Access Security - All entry points are monitored by Walden Security Guards. All employees must badge in and receive a green light in the system. Badges are given to employees and access is request by HR and Facilities Management through General Services. All guest are required to sign in on the Ground Floor. The guest goes through a metal detector and bags are examined. Treasury occupies all of Floor 14 and 15. Floor 13 is split between Treasury and Revenue. Access to Treasury areas in the Andrew Jackson Building are restricted Treasury Employees only. The Records Management area is further restricted to Records Management and a select few Infrastructure and Security personnel. The Infrastructure and Security area is restricted to INFS only personnel, however the area is required to be unlocked during business hours.

Data Center North and **Data Center South** policies can be found on OIR's intranet at http://oir.intranet.tn.gov/sites/oir.intranet.tn.gov/files/policy/policy-attach/DataCenter-Physical-Security-Policies_v2.1.pdf

Clover Bottom Disaster Recovery Site - Access is controlled by physical keys and an alarm system.

3.2 Physical Access Monitoring

The need for monitored access to business areas is evaluated. In monitored areas, records for approved personnel access and sign-in sheets for visitors are maintained. Logs are periodically reviewed, violations or suspicious activities are investigated, and action is taken to address issues.

Treasury utilizes the standard card scanning system as provided by the Department of General Services. Access/egress reports are available on an as-need basis.

Physical access to secure areas within Treasury is limited to those who need it. This access is reviewed biannually.

3.3 Physical Access Control

Physical access to facilities containing information systems is controlled and individual’s authorization is verified before granting access.

Physical access to secure areas within Treasury are limited to those who need it. Access is reviewed biannually.

Physical access to Data Center North is controlled by authorization list and limited to those who need it.

Data Center South security is not documented here as there are no Treasury-owned assets in place there.

3.4 Environmental Controls

The necessary environmental controls, based on a requirements assessment, which includes but is not limited to backup power to facilitate an orderly shutdown process, fire detection and suppression, temperature and humidity controls, water damage detection and mitigation are provisioned and properly maintained.

The above controls are in place and operational for Data Center North and Data Center South~~.~~

For assets housed within the Andrew Jackson Building, the utility server room is protected with fire detection and suppression only. Backup power, temperature/humidity controls, and water damage controls are not in place within this server room. This is seen as an acceptable risk as there are no production services housed within it.

3.5 Secure Disposal of Equipment

Processes are in place to permanently remove any sensitive data and licensed software prior to disposal.

Upon de-provision of servers, desktops, and laptops, their hard disk drives are removed and placed in a secure area until audit has reviewed. After audit, the hard disk drives are disposed of by shredding.

4 Data Security Practices

4.1 Disaster Recovery Planning

A Disaster Recovery Plan (DRP) is in place that supports the current business continuity needs of the agency. The DRP plans for the recovery of technology and communications following any major event that disrupts the normal business environment, provides for periodic updating and testing of the plan, and its documentation includes, but is not limited to:

- Regularly updated information about where copies of the plan reside, including appropriate off-site locations.

For each new system implemented, disaster tests are planned and conducted. Documentation for that testing may be found in the DR_Planning folder of IICC51. Newer tests are documented in Recovery Planner, Treasury's Business Continuity tool.

Information about previous actual incidents and after action reports may be found in the DR_Planning \wip\yyyy as well as in Recovery Planner.

Infrastructure, during new or replacement system implementation, creates disaster plans specific to the implementation and criticality of the systems covered. Disaster recovery plans for Implementations can be provided by either the vendor, OIR, within the state data centers, or a mix of both.

Infrastructure is in the process of trying to formalize their plans, since some are in disparate documents. These plans will reside in RecoveryPlanner.

If Disaster Recovery is hosted by a vendor, that vendor is required by contract to have a minimum of one test per year per system and provide the test results to Treasury showing they can meet the Recovery Time Objectives (RTO).

Disaster Recovery plans are managed within a hosted solution and are backed up offsite as a component of that service.

- Training for appropriate personnel.

Treasury has employed a training program for new employees, new managers, and individuals with changes of responsibility regarding disaster recovery plans and notifications. During testing, individuals meet as part of the testing group to understand their roles.

It is stated policy that tabletop exercises and tests are to be completed for all areas and Treasury systems on a repetitive cycle.

4.2 Information Back-up

Backup copies of information and software are completed on a routine schedule, tested regularly, and stored off-site.

Treasury Data volumes are copied to a second offsite location daily.

Treasury's critical servers and specific sensitive files are backed up daily to a disk-to-disk device that, in turn, replicates information in near real time to a second offsite location.

Backups are tested on an as-need basis.

4.3 Monitoring

System logging, and routine procedures to audit logs, security events, system use, systems alerts or failures, etc. are implemented and log information is in placed where it cannot be manipulated or altered.

Treasury employs Citrix Edgesight for monitoring the Citrix environment and the logging of events.

Treasury employs Citrix Netscaler for the logging of failed and successful log on attempts to Citrix..

Treasury has created group policies to govern event logging configurations.

Treasury uses Kiwi Syslog to maintain logs of connections made through the Firewall for all connections inbound and outbound.

4.4 Data Classification

Policies and processes to classify information in terms of its value, legal requirements, sensitivity, and criticality to the organization are in place.

Treasury treats all data containing PII as confidential and sensitive. Retention requirements are guided by Legal.

4.5 Access Controls

Policies and procedures are in place for appropriate levels of access to computer assets. Access controls include, but are not limited to:

- Password management, including the use of strong passwords, periodic password change, and restriction of sharing access and/or passwords. System access is authorized according to business need and password files are not stored in clear text or are otherwise adequately protected.

  System access is managed by user ID / password (UID/PWD) combination. The access granted a specific UID/PWD pair is managed by group policy. Treasury employs OIR domain-level policy.

- Wireless access restrictions are in place, with organizational control over access points, prohibition and monitoring against rogue access points, appropriate configuration of wireless routers and user devices, and policy, procedure, and training for technical staff and users are in place.

  Users may see and attach to specific wireless access points if they have security rights to do so. However users must supply and be authenticated via a UID/PWD pair to utilize any wireless local area network (WLAN).

- Secure remote access procedures and policies are in place, and are known and followed by users.

  Secure remote access is provided to appropriate resources via Pulse Secure, formally Juniper VPN. Users are validated via a 2-part login and after authentication, are allowed access to appropriate resources (See 4.5 Access Controls above) via encrypted communications.

- Mobile and portable systems and their data are protected through adequate security measures, such as encryption and secure passwords, and physical security, such as storing devices in a secure location and using cable locking devices.

  Portal systems such as laptops employ encrypted hard disk drives keyed to the users' UID/PWD pair. Absence of the correct UID/PWD pair leaves the portable device in an unusable state.

  Treasury policy is for employees to keep assigned equipment on their person at all times.

  Per policy, mobile phones integrated into Treasury resources are required to be encrypted. Mobile phone are enrolled into the State's Mobile Device Management system to enforce minimum standards.

- The tracking of access and authorities, including periodic audits of controls and privileges is in place.

  Group / privilege audits take place by application and on a yearly schedule. Employee change in job duties automatically triggers individual group/privilege audit.

- Networks challenge access requests (both user and system levels) and authenticate the requester prior to granting access.

  No resource access is granted within any of Treasury's systems except via AD authentication.

4.6 Least Privilege

Configuration to the lowest privilege level necessary to execute legitimate and authorized business applications is implemented.

Least privilege is employed throughout Treasury and reviewed through system audits on an annual basis. During such audits, access is reviewed by specific, named resources and based upon defined criteria are either approved or revoked.

4.7 Data Storage and Portable Media Protection

Policies and procedures to protect data on electronic storage media, including CDs, USB drives, and tapes are in place. Procedures include labels on media to show sensitivity levels and handling requirements, rotation, retention and archival schedules, and appropriate destruction/disposal of media and data.

All data containing PII is consider confidential and sensitive and is managed under guidelines as set forth above. Additionally, all external drives are formatted and encrypted with Microsoft Windows Bitlocker Drive Encryption (Bitlocker) for increased security.

5 Information Integrity Practices

5.1 Identification and Authentication

Policies and procedures for identification and authentication to address roles and responsibilities, and compliance standards are in place.

As part of the hiring process, hiring managers submit ServiceNow tickets for their new hires. Details regarding roles/responsibilities are managed within that ticket and dictate AD group membership and other program access.

5.2 User Identification and Authentication

Information systems/applications uniquely identify and authenticate users when it is appropriate to do so.

Treasury relies on AD authentication to unique identify users. For remote access, Treasury relies on Citrix' RSA dual-factor authentication. Passwords changes are mandated every 90 days. For laptops connecting to the Treasury network, a VPN solution with dual-factor authentication is used.

5.3 Device Identification and Authentication

Information systems/applications identify and authenticate specific devices before establishing a connection with them.

User authentication and group membership is provided by AD. Application and device access is determined by the user’s AD group membership. Workstations must be enrolled inactive directory to allow user access.

5.4 Malicious Code Protection

A regular patching process has been implemented to protect against malicious code. The process is automated when possible.

Treasury relies on Symantec Endpoint Protection (SEP) to provide protection from the injection of malicious code. SEP updates the endpoints automatically ensuring the latest protection for devices.

WSUS and Shavlik are used for enterprise patch management.

5.5 Intrusion Detection

Tools and techniques are utilized to monitor intrusion events, detect attacks, and provide identification of unauthorized system use.

Treasury leverages STS’s IDP/IDS Intrusion detection and prevention system on the perimeter of the state’s network. OIR alerts us of any intrusions that may impact Treasury operations.

Treasury has separate firewalls (3) on the inside of the network that protect each site. These firewalls prevent access to Treasury systems from other agencies within the state network.

5.6 Security Alerts and Advisories

The appropriate internal staff members receive security alerts/advisories on a regular basis and take appropriate actions in response to them.

SEP is configured to alert emails alerts to appropriate groups when an infection is found.

STS emails out advisories on new and emerging threats that may have an impact on State systems.

See 5.6 Intrusion Detection above.

5.7 Secure System Configuration

The security settings on systems are configured to be appropriately restrictive while still supporting operational requirements. Non-essential services are disabled or removed when their use is not necessary as to eliminate unnecessary risk.

Treasury servers are configured to provide minimal operational requirements.

Treasury has configured Citrix policies to restrict access to local PC drives, printers, and removable media to complement its log off and disconnect timers.

5.8 Software and Information Integrity

Information systems/applications detect and protect against unauthorized changes to software and information.

Software configuration and data changes are secured to specific AD groups. Requests for changes to configuration are submitted through and managed by Treasury's ServiceNow Change Request process.

5.9 Information Input Accuracy, Completeness, and Validity

Information systems/applications check data inputs for accuracy, completeness, and validity.

Treasury applications check for data validity as part of their adherence to business requirements. Defects found during development are resolved in accordance with Treasury's software development lifecycle (SDLC). Defects found after go-live are resolved through Treasury's Change Request process.

5.10 Flaw Remediation

Information system/application flaws are identified, reported, and corrected.

Defects found during development are resolved in accordance with Treasury's software development lifecycle (SDLC). Defects found after go-live are resolved through Treasury's Change Request process.

6 Software Integrity Practices

6.1 System and Services Acquisition

Policies and procedures for system and services acquisition are in place to address roles and responsibilities, and processes for compliance checking.

6.1.1 Identity Authentication

6.1.2 Application Privileges

Treasury has policies and procedures in place to makes ensure users only get the rights to applications needed for their specific job. Privileges may be revoked by a security administrator at any time.

6.1.3 Input Validation

See 5.10 - Information Input Accuracy, Completeness, and Validity above

6.2 Software Integrity Practices

Policies and procedures associated with system and services acquisition and product acceptance are in place.

- Software Usage Restrictions – Controls or validation measures to comply with software usage restrictions in accordance with contract agreements and copyright laws are in place.

  Lansweeper Software Inventory and Audit (Lansweeper) identifies and lists all current software in our environment. Treasury reviews this list for compliance on a quarterly basis.

- User Installed Software – An explicit policy governing the downloading and installation of software by users is in place.

  AD group membership denies users of the privileges required to install software on Treasury assets. Requests for software installs are managed via a change request process in ServiceNow with any resulting install performed by system administrators.

- Outsourced Information System Services – Controls or validation measures to ensure that third-party providers of information system services employ adequate security controls in accordance with applicable laws, policies and established service level agreements are in place.

  No information systems are currently outsourced at Treasury. However, access and change requests made by any partner follow standard review and approval process.

- Developer Security Testing – A security test and evaluation plan is in place, implemented, and documents the results. Security test results may be used in support of the security certification process for the delivered information system.

  Developers making public facing applications have their applications tested by STS Security before STS Networking will make the application available to the public. Developers maintain a continuous learning environment as part of their development set in their IPP.

  Per page 42 of the Employee Guidebook, "In order to protect the security of the state network, employees must follow the following guidelines:

  1. Employees may not attach hardware or load software on a Treasury-issued computer or electronic device.

  2. Employees issued laptops must take their laptop with them to be available for disaster recovery. They must secure the laptop when transporting, such as locking the laptop in the trunk of the car or securing in a non-visible location while in transit. The device should not remain in the vehicle when it is not occupied.

  3. If an employee knows or learns of any misuse of a state-issued computer or electronic device, they must notify their supervisor or Internal Audit."

7 Personal Computer Security Practices

Personal computing devices include desktops, laptops, notebooks, tablets, Personal Device Assistants (PDA), and other mobile devices.

Personal devices are not allowed on Treasury's network. If a need is demonstrated, Treasury will issue a secure device.

All Treasury devices are employ Bitlocker encryption and are are scheduled for virus patches through SEP. Treasury employs Ivanti and WSUS security patch management.

Treasury employs Apple's standard feature for remotely locking, finding, and wiping Iphones and Ipads.

Treasury does not have any non-Treasury devices with active sync enabled.

Treasury uses the State's MDM solution to track mobile device security settings.

7.1 Device Hardening

Operating system and application level updates, patches, and hot fixes are applied as soon as they become available and are fully tested. Services on the computing devices are only enabled where there is a demonstrated business need and only after a risk assessment.

Windows patches are tested a day after release. If no issues are reported they are approved department wide the Friday after patch Tuesday. Out of band updates that are not prioritized as critical are approved with the next month's cycle.

Servers are patched monthly with out of cycle security patches installed as soon as practical.

7.2 Lock-Out for Inactive Computing Devices

The automatic locking of the computing device after a period of inactivity is enforced.

Treasury users have an inactivity lock out time on their computer of 10 minutes or less.

8 Network Protection Practices

8.1 Network Protection

Network and communication protection policies and procedures are in place. These documents outline the procedures to authorize all connections to network services. Authorization is based on an evaluation of sensitive or critical business applications, classification of data stored on the system, and physical location of the system (e.g., public area, private access, secure access, etc.).

Treasury policy is to allow only Treasury-issued and approved vendor devices access to Treasury networks.

8.2 Boundary Protection

Equipment designed for public access (i.e. Web servers dispensing public information) is protected. These are segregated from the internal networks that control them. Access into internal networks by authorized staff is controlled to prevent unauthorized entry.

Citrix Netscaler (perimeter Secure Socket Layer (SSL) appliance) in conjunction with token-based RSA dual-factor authentication provides Treasury remote users secure, appropriate access to the Treasury network and Treasury systems.

Public facing devices in the STS environment are positioned in a DMZ zone, separating them from internal devices.

8.3 Protect and Secure Network Infrastructure

Policies and procedures for technology upgrades, network equipment (e.g., servers, routers, firewalls, switches), patches and upgrades, firewall and server configurations, and server hardening are in place.

Treasury IS routinely reviews hit counts on Firewalls and removes rules with zero hit counts after being disabled for an undisclosed amount of time.

8.4 Transmission Integrity and Confidentiality

Data is protected from unauthorized disclosure during transmission. Data classification is used to determine what security measures to employ, including encryption or physical measures.

Sensitive data should be encrypted when in transit. SFTP processes are setup through OIR. Encrypted point to point tunnels are set up between locations and vendors accessing Treasury resources. Pulse Secure utilizes SLL encryption for employees to have remote access. When sending sensitive emails Treasury employees are directed to send with [secure email] in the subject line, this forces TLS encryption.

Treasury leverages OIR's SFTP site to securely retrieve and deliver files to vendors

Treasury Bloomberg server has its own internal STFP server to securely deliver daily trade files to the vendor.

8.5 Remediation Process

Treasury's remediation framework is centered around:

- Identify
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy
- Protect
  - Access Control
  - Awareness and Training
  - Data Security
  - Information Protection / Procedures

    - Maintenance
    - Protective Technology
- Detect
    - Anomalies and events
    - Continuous monitoring
    - Detection process
- Respond
    - Response planning
    - Communications
    - Analysis
    - Mitigation
    - Improvements
- Recover
    - Recovery
    - Improvement
    - Communication

9 Incident Response Practices

9.1 Incident Response

Incident response policies and procedures consistent with applicable laws and state policies are in place. These include but are not limited to identification of roles and responsibilities, investigation, containment and escalation procedures, documentation and preservation of evidence, communication protocols, and lessons learned.

When a Treasury IS person learns of an Incident, the first action is to perform a full scan of the computer using the Symantec Endpoint Protection software. If an infection is found, the computer is removed from the network. The computer is then reimaged and reissued to the user. There is not a documented process for this.

9.2 Incident Reporting

Proper incident reporting policies and procedures are in place. These include training employees and contractors to identify and report incidents, the reporting of incidents immediately upon discovery, and preparation and submission of follow-up written reports.

From the Employee Guidebook page 44.

Employee Must Notify of Computer Symptoms

An employee must call the Help Desk immediately if their computer has any of the following symptoms:

- Receipt of an anti-virus alert;
- The browser is going to unwanted websites or random websites and these sites cannot be closed;
- The employee’s password does not work; or
- Co-workers receive an email message from the employee that the employee did not send.

Employees and vendors are instructed to forward suspected “spam” emails to Spam.Abuse@tn.gov

10 Alignment with Standards

Treasury is using the ISO 27001/2 framework to identify and test alignment with policies and procedures. ISO Sorts are performed each month to test separate sections of the plan.

10.1 ISO 27001 (International Organization for Standardization – IT Security Techniques, Information Security Management Systems Requirements)

Treasury has previously run ISO 27001 tests and wishes to restart this effort. Due to its age, all previous work must be reviewed before it can be used again.