State of Vermont

Information Security Policies

Policies and Best Practices

August 4, 2017

August 4, 2017

Office of the Chief Information Security Officer

By	Changes	Version date
Darwin Thompson	Original draft	10/10/2016
Angela Leclerc	Updates from 11/28 Meeting	11/28/2016
John P Hunt	Cross references added from State Non-Functional Security Requirements Endnotes and Bibliography	12/16/2016
Seamus Loftus, John P Hunt	Added policies for Email Transfers and Cloud	1/15/2017
John P Hunt	Edits and Index additions	1/30/2017
John P Hunt	Draft 1 to DII Management for Review	1/30/2017
John P Hunt	Draft 1 added MFA Policy	3/14/2017
John P Hunt	Final for Review and Signature by CIO	3/14/2017
John P Hunt	Added Glossary of Terms	3/16/2017
Glenn Schoonover	Final Proof reading and re-formatting TOC	3/28/2017
Angela Leclerc	Remove reference to Department of Information & Innovation (DII) and replace with Agency of Digital Services (ADS)	8/4/17

Table of Contents

1 Executive Summary

The Agency of Administration / Agency of Digital Services (ADS) is charged with providing "direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government" (22 V.S.A. § 901).

ADS, in collaboration with its partners across state government, has established the following Information Security Policies. The policies promote the development, implementation, and operation of more secure information systems by establishing minimum levels of due diligence for information security. These policies facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.

These policies identify techniques associated with protecting and securely providing access to state information systems. Agencies may elect to exceed the minimums outlined in these policies to achieve their organizational security goals and requirements. Elements of these policies are interdependent and are intended to be implemented in their entirety.

Policies herein are required to be applied to information systems within the Executive Branch agencies and business units. Agencies are responsible for complying and ensuring, through documented agreements, all third parties acting on their behalf comply. In circumstances where these policies can/will not be implemented, agencies must document exceptions and indicate what compensating controls have been applied to adequately protect the information. The exception document must be signed by the Agency Secretary, appointing authority or designee, and the Secretary of Administration or designee. The exception must be documented and kept on file for review by auditors or during a security assessment.

These policies and recommended best practices have been developed using a combination of the following resources

- International Organization for Standardization (ISO) 27001 & 27002
- National Institute of Policy and Technology (NIST) recommended policy
- SANS Institute recommended policy and best practices

The items documented as *Recommended Best Practices* are not mandatory and do not need to be met by agencies to be in compliance. They are presented to provide additional information to agencies on opportunities to further enhance the security of their information systems. Agencies should take these into consideration for future planning, and to encompass areas of technology with emerging policy.

Prior to agency implementation of these policies they should carefully review the status of their agency's records and information management program with the Vermont State Archives and Records Administration (VSARA) and other stakeholders. A record is any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of agency business (1 V.S.A. § 317(b)). Proper classification will determine the level of controls required to adequately protect those records.

Based upon this review, the agency will be best able to evaluate the potential risk posed to their information systems and develop their mitigation strategy based on a combination of those risks and the policy identified below.

2 Access Control

To ensure critical data can only be accessed by authorized personnel, information systems controls and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job. Fundamental to a good access control mechanism is the requirement for strong user authentication, authorization, and auditing[i].

Authentication is the act of verifying the identity of a user or process. The most common method used to authenticate a user is a username and password combination.

Authorization is the act of allowing the identified user access to information for which they are authorized. Levels of authorization must be specific to the business needs of the organizations. Some positions may need only to view information, while others may be authorized to add, modify or delete information.

Auditing is the process of reviewing both authentication and authorization to be sure that only the correct people have been granted access to information and only the correct people have used their authorizations to access information.

The policy element identified below for authentication, authorization and audit must apply to all information systems, modifications to systems, and when evaluating new information systems.

2.1 Authentication

1. The classic paradigm for authentication systems[ii] identifies three factors as the cornerstone of authentication:
    a. Something you know (for example, a password)
    b. Something you have (for example, mobile device, RSA Token, an ID badge or a cryptographic key)
    c. Something you are (for example, a fingerprint or other biometric data)
2. Multi-factor or Two Factor Authentication (MFA) must be used to access and authenticate applications when working outside the Vermont Government network.
3. User IDs and passwords must not be shared.
4. The combination of a unique User ID and a valid password must be the minimum requirement for granting access to information except for that which is publicly viewable.
5. Users must not reveal passwords to anyone, including supervisors, family members or co-workers.
6. Management approval must be required for establishing each user ID and a process must be in place to remove or suspend user IDs that are no longer required to perform an assigned job function.
7. The construction and specifications of a password must be defined in agency policy and must be of a complexity consistent with the information the user has access to.

8. A multi-factor authentication method (e.g. pin, secure token) must be used to authenticate users access to information systems containing federally or industry protected data where appropriate.
9. Passwords must be obfuscated on login to all information systems so the password cannot be read from the screen.
10. Vendor or other default supplied passwords for information systems must be changed immediately upon installation.
11. Passwords must be changed whenever there is a chance that the password or information system has been compromised.
12. Authentication must occur through encrypted channels using methods such as Kerberos, SSH, SSL.
13. On servers and clients, passwords must be stored in protected, encrypted files.
14. Controls must be implemented to protect information systems from brute force password guessing attacks (e.g. lock out after predetermined number of incorrect attempts.) Controls must be commensurate with the associated risk to the information system.
15. All standard user passwords must be changed twice a year (every180 days), at minimum, to reduce the risk of compromise through guessing, and password cracking or other attack and penetration methods. Individual agency/department policies may be more restrictive to meet regulatory requirements (IRS 1075, CJIS, HIPAA, etc.).
16. Special Access Privileges: Procedures must be established to maintain documentation of special access privileges, including high-level privileges (e.g.: root access, administrator), system utilities requiring high-level privileges, and privileges that provide access to sensitive network devices, operating systems, or software application capabilities. Procedures must include:
    a. Specifying and documenting the purpose and acceptable use of special access privileges.
    b. Management approval for granting special access privileges.
    c. Requiring different accounts or different authentication tokens than those used with the individual’s regular user account.
    d. Specifying and documenting a procedure to remove special access privileges.

2.1.1 Authentication Best Practices

1. Passphrases may be used in lieu of passwords. A passphrase is similar to a password in usage, but is significantly longer for added security.
2. For additional password and passphrase security, it is recommended that agencies follow NIST Special Publication 800-63-2 Electronic Authentication Guideline.
3. Users of state information systems should be trained to not reuse their state account passwords for any other purpose.
4. Passwords should be composed of a variety of letters (upper and lower case), numbers and symbols and provide a minimum of 14 bits of entropy (See NIST 800-63-2) for a discussion of entropy).

5. The State of Vermont offers MFA for application access using Microsoft or Citrix products.
6. For secured access to information systems and applications, the authentication method should be consistent with the classification level of the information contained within.
7. Access to password-protected information systems should be timed out after an inactivity period. This inactivity period should be based on an information system risk assessment.

2.2 Authorization

1. Assignment of privileges/access to individuals must be based on job classification and function (role based). Individual unique identity must map to one or more identified roles.
2. Access to objects by default must be restricted via an access control mechanism. Access must be specifically granted to provide explicit access to objects within any information system. Access must be reviewed and modified in accordance with security policies prior to production deployment.
3. Authorization must be removed immediately upon departure or change in employee job duties.
4. Administrative rights to information systems must be tied to identified unique individuals. Administrative rights must be limited to only staff whose duties require it.

2.2.1 Authorization Best Practices

1. Agencies should identify roles and the appropriate access rights for each role and then assign roles to positions.
2. The administrator should be able to assign the appropriate role to a transfer or new hire so that the employee simply inherits the required access rights. Roles are usually additive so that users receive privileges based on the aggregated role assignments of their directory entries.

2.3 Audit of Access Control

1. All information systems must support logging of access including logins to the information system, and granted and denied access to resources in accordance with Log Management Policy.
2. Information systems containing exempt records and information must log all view, add, modify, and delete of information and all failed attempts to perform these actions unless specifically exempted by statute. Access logs must be monitored for access control violations daily and reviewed in detail as necessary.
3. Information systems must be reviewed at least every 90 days for inactive accounts.
4. Audit logs must be tamper-resistant. In all cases, access to the logs must be limited only to those with a need to access.

3 Information Asset Management

Under the Vermont Public Records Act (PRA), all agencies are responsible for managing records and information produced or acquired during agency business as public assets (1 V.S.A. § 315-320). In addition, each agency head is required to designate a member of his or her staff as records officer. Under state law, records officers are responsible for maintaining an active records management program for all agency records and information, regardless of format, in accordance with record schedules and other requirements established by the Vermont State Archives and Records Administration (VSARA) and ADS (3 V.S.A. § 218).

Within the context of information security, all record schedules issued to agencies since 2008 include public access requirements. A public access requirement is the availability of a record for public use and inspection pursuant to 1 V.S.A. § § 315-320. Unless exempt from public inspection and copying pursuant to 1 V.S.A. § 317, records are expected to be promptly produced for public inspection upon request. Public agencies must follow the procedure outlined in 1 V.S.A. § 318. The access requirements below represent actions agencies must take based on specific laws associated with the accessibility of their records.

Access	Description	Usage
Exempt	Records must not be provided for free and open examination pursuant to 1 V.S.A. §§ 315-320.	Assigned to records that are wholly exempt from public use and inspection pursuant to 1 V.S.A. § 317.
General	Records may be provided for free and open examination pursuant to 1 V.S.A. §§ 315- 320.	Assigned to records that are not exempt from public inspection and copying pursuant to 1 V.S.A. § 317.
Redact	Records contain specific information that must not be provided for free and open examination pursuant to 1 V.S.A. §§ 315- 320.	Assigned to records that contain specific information that is exempt from public inspection and copying pursuant to 1 V.S.A. § 317 and require exempt information to be redacted from the records prior to public use, inspection and/or copying.
Review	Records may be provided for free and open examination pursuant to 1 V.S.A. §§ 315- 320 but not always. Default value for general schedules, which require agencies to establish internal policies.	Assigned to records that are generally not exempt from public inspection and copying pursuant to 1 V.S.A. § 317 but, in limited circumstances, may be exempt. Internal review and/or policy is required.

Classification levels for information security purposes are driven by the above public access requirements. All electronically stored records and information, regardless of classification level, must be protected from unauthorized access to the information that could affect its confidentiality, availability or integrity. For example, a publicly available web site must still be protected from unauthorized access that could result in hacking or disruption of the information or availability of the information.

After completing a risk assessment and mapping the identified risks to the required assurance level, agencies can select appropriate technology that, at a minimum, meets the technical requirements for the required level of assurance. In particular, this document states specific requirements for each level. Therefore, even information systems handling only open data will comply with the minimum-security policy identified in this document. If a risk assessment is not accomplished, the data must be protected as if the records and information is *Exempt/Redact* as described below.

The policy identified below is for management and transfer of electronically stored records and information based on classification level.

3.1 Records and Information Classification Level

1. **General:** Access control must be in place to ensure data integrity. Change logging must be in place in accordance with the Access Control policy.
2. **Exempt/Redact:** All nonexempt controls plus access control must be in place to prevent unauthorized viewing. Access logging must be in place and data must be encrypted in transit. Disposal: media must be sanitized or destroyed.

It is recogonized that some exemptions in state, as well as Federal, law may require encryption. Records officers are responsible for assuring that internal policies related to their respective agency records management programs include encryption requirements that comply with the Encryption Policy. A log review process is mandatory. Two-factor authentication for access is required in accordance with the Access Control policy.

4 Communications & Operations Management

The goal of communications and operations management is to ensure the correct and secure operations of information processing. This section describes security policy and best practices for Antivirus and Malware, Workstation Management and Desktop Security, Mobile Device Management, Server Management, Log Management, Information Backup, Network Security Management, Intrusion Detection and Prevention, Email, Remote Access, and Wireless Access.

4.1 Antivirus and Anti-Malware

1. All workstations and servers must have antivirus *and* anti-malware software enabled where available.[iii]
2. All information systems with antivirus software must undergo at a minimum a monthly full system scan for viruses and malware.
3. Any infected information system must be handled in accordance with incident response procedures as established by ITSM.
4. Where technically possible, portable/mobile devices must also have antivirus protection.
5. Where technically possible, antivirus and anti-malware software must be centrally managed with ongoing updates and reporting.
6. Antivirus and anti-malware software must be maintained at current patch levels in accordance with the Patch Management Policy.
7. All antivirus and anti-malware signatures must be updated and maintained at current vendor supported and recommended levels.
8. Users must not be able to disable the antivirus and anti-malware software on their workstation or portable/mobile device.

9. All e-mail must be scanned at the e-mail gateway and upon arrival at the workstation. Infected e-mail messages must be isolated and remediated.

4.1.1 *Antivirus & Anti-Malware Best Practices*

1. Anti-malware solutions for workstations should be integrated with web browsing to scan for malicious web sites during browsing.
2. Monthly scans required in the Antivirus and Anti-Malware Policy should be scheduled to occur automatically.

4.2 Workstation Management & Desktop Security

1. All workstations must be patched in accordance with the Patch Management policy.
2. Workstations must be protected with anti-virus software to protect the machine against malware in accordance with Anti-virus and Anti-Malware Policy.
3. Users must not have administrative rights access to their workstations in accordance with the Access Control Policy.
4. By default, workstations must not be configured to support peer to peer networking. A specific business use must be identified and approved by management before enabling this technology.
5. By default, all network services and other non-essential services on workstations must be disabled. A specific business use must be identified and approved by management before enabling this technology
6. Each workstation must have a firewall installed and configured where technically feasible. It is acceptable to utilize the firewalls that come packaged with specific operating systems.
7. Workstations firewalls must be configured to default deny.
8. Workstations must not have deprecated (unsupported by vendor) operating systems or applications installed.
9. Workstations must only have licensed and approved applications installed.
10. Procedures must be established and followed to approve attachment of peripheral devices to the workstation; only approved devices must be attached.

4.2.1 *Workstation Management & Desktop Security Best Practice*

1. Secure workstation by using operating system locking features.
2. Secure workstation with a screensaver with password protection.

4.3 Mobile Device Management

1. Mobile Devices cannot be physically connected to agency owned equipment.
2. Agencies must instruct employees not to put exempt data on a personally owned portable device.

3. Information stored on portable devices must be protected in a way commensurate with the classification of the information and in accordance with the Protection of Information Assets Policy.
4. Where technically possible, security mechanisms on mobile devices must be used. These include encryption, remote tracking of the device for physical recovery, remote wipe and/or hard drive destruction, password or biometric protection, and automatic wipe after a predetermined number of failed password attempts in accordance with the Authentication Policy.
5. Mobile devices must not be left unattended in uncontrolled access areas.
6. Storage devices such as hard disk drives and other media containing sensitive information must be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information.

4.3.1 Mobile Device Management Best Practices

1. Secure mobile devices using locking features.
2. Use auto screen locking capabilities.

4.4 Server Management

1. All servers must be configured so that end users must not have administrative rights access to servers in accordance with the Access Control Policy. Server administrators must use named user accounts that tie actions back to a specific individual for performing administrative work. Generic name and shared accounts must not be used.
2. All default accounts (guest, admin, etc.) on servers must be disabled.
3. Servers must have a firewall installed and configured to block unneeded ports. It is acceptable to utilize the firewalls that come packaged with specific operating systems.
4. Servers with deprecated (unsupported by vendor or open source community) operating systems or applications must be on a path to be removed from production.
5. All unnecessary services must be disabled.
6. Servers must only have applications installed that are approved and authorized by the server owner.
7. There must be established procedures for approving or denying the attachment of peripheral devices to the server.
8. Servers must be set up to log security events that occur on the server. Logs must include activities allowed and activities denied, what system event occurred, when the event occurred, and who performed it, as well as privileged access events, (admin login, actions taken, root system or privileged account access and activity), log ins, log outs, and denials or failures of access in accordance with the Log Management Policy.
9. Servers must be synchronized with one or more network time device(s).
10. The following additional policies must be applied to server management:
    a. Antivirus and Anti-Malware Policy

b. Information Backup Policy

c. Security Zone and Network Security Management (local Area Network and Wide Area Network Policy

d. Remote Access Policy

e. Encryption Policy

f. Patch Management Policy

4.4.1 Server Management Best Practices

1. Configuration management and monitoring tools should be used to identify unapproved changes to server configuration files.
2. Application servers should not be used to store application data. Application data should be stored on a different server than the application server in accordance with the Security Zone and Network Security Management.

4.5 Log Management[iv]:

1. Log data from servers, network components (firewalls, switches, routers, etc.) and other devices/services must be ongoing. Events must be logged as they occur. Log data must be collected in its original form whenever technically possible but may also be collected in a normalized format for log aggregation.
2. Logs must be configured to capture security-related information in sufficient detail to recreate activity in support of incident investigations including, but not limited to, start up and shut down of audit functions, account logon and logoff activity, access to security relevant files, activities that modify, bypass, or negate security controls, failed attempts to access resources, and the use of privileged accounts.
3. Access to log files must be controlled in accordance with the Access Control Policy.
4. Logs must be regularly reviewed and analyzed for indications of unauthorized or unusual activity. Suspicious activity must be investigated, findings reported to appropriate management, and necessary follow-up actions taken.
5. Log data must, by default, be considered exempt until exempt information has been removed for public disclosure.
6. Logs must be retained in accordance with the state retention requirements for the information and information systems they are logging.

4.5.1 Log Management Best Practices

1. Log data should be collected to a centralized system with restricted physical and logical access.
2. Automated mechanisms should be used to integrate monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
3. Events not requiring immediate action should be identified and reviewed within 30 days.
4. Review of log information should include examination of attempts to gain unauthorized access, failed resource access attempts, unauthorized changes to security controls and suspicious network traffic patterns.

5. Critical security logs should be segregated from other log information with access restricted to security review personnel.

4.6 Information Backup[v]

1. Backups must be made based on the data stored in the information system.
2. An analysis process of the data classifications must define a backup cycle and document it as well as determining backup media selection and backup encryption methods in accordance with the Encryption Policy.
3. Backups must be tested at least annually to ensure information can be restored and to identify restoration constraints.
4. Copies of mission-critical data identified in business continuity and disaster recovery plans must be stored in a secured, offsite location. If backups are stored offsite using a third-party vendor, vendor practices must comply with state policies on data protection and must meet this policy.
5. Access to backups of mission critical data must be limited to personnel authorized to handle the most sensitive data being backed up.
6. Backups must be clearly and consistently labeled to facilitate restoration and testing and to guard against mishandling, loss, or accidental overwriting.
7. Media must be stored in compliance with manufacturer's storage requirements.

4.6.1 Information Backup Best Practice:

1. Automated back-up management software should be used to manage backups on information systems.

4.7 Security Zone and Network Security Management (Local Area Network & Wide Area Network)[vi]

1. A business needs analysis must be conducted to determine what network traffic is required for each information system.
2. Firewalls must be configured to deny all and allow only explicitly approved network traffic.
3. Internal state information systems and data must be separated from the public Internet through the use of a perimeter firewall.
4. Internal security zones must be established to segregate network traffic with differing security requirements from each other. These zones must segregate trusted local workstation networks from restricted server networks. Servers containing exempt data must be located within a restricted zone.
5. Public facing web applications must segregate applications within a DMZ.
6. Network equipment (firewalls, MPLS, VLANs, hubs, switches, routers, wireless access points) must be managed to ensure that security zones are maintained.
7. By default, all hardware switch ports must be turned off unless physical access is controlled to both endpoints of the physical connection.
8. Dynamic IP address assignments must be logged.

9. Virtual separation mechanisms (e.g. VM and VLAN) must only be used for segregation of machines with differing security requirements if security controls are in place to ensure segregation between security zones cannot be bypassed.
10. Network hubs/unmanaged switches are not permitted.
11. SNMPv3 or SSL/TLS must be used for management of access points.
12. The following policy areas also apply to security zone management:
    a. Log Management Policy
    b. Remote Access Policy

4.7.1 Security Zone and Network Security Management (Local Area Network & Wide Area Network) Best Practices

1. Security zones should be consistently managed and documentation of information exchanges between agencies and business partners should be in place.
2. Data for applications located in a DMZ should be segregated and stored within a protected security zone.
3. Critical security control devices should be segregated from the rest of the network.

Physical separation of security zones should be maintained. Virtual separation mechanisms (e.g. VM and VLAN) may be used for segregating sub-zones within a security zone.

4.8 Intrusion Detection[vii]:

1. IDS must be deployed to monitor external network traffic.
2. Intrusion detection signatures must be updated and maintained at current vendor supported levels.
3. IDS must perform packet and protocol analysis.
4. IDS must perform fragmented and packet stream reassembly.
5. IDS must detect attacks in real time to provide timely alerts and notification.
6. Logs must be maintained and reviewed in accordance with the Log Management Policy.
7. Evidence and alerts of intrusion must be handled in accordance with incident response plans and the statewide incident response policy. Incident response plan/procedure must include response to Intrusion Detection System (IDS) alerts.
8. IDS must be monitored by appropriately trained staff.

4.8.1 Intrusion Prevention Systems Best Practices

1. IDS should be deployed to monitor internal network traffic.
2. IDS may be combined with Intrusion Prevention System (IPS) features. This solution should be deployed with caution due to potential uncontrolled interruption of network traffic.
3. Behavioral based IPS should be used to block attacks that are only detectable because of changes in the normal operational state.

4.9 E-mail

1. Virus and spam filtering must be implemented on email gateways in accordance with the Antivirus and Anti-Malware Policy.
2. Records/Data which by law are designated confidential or by a similar term, including federally or industry protected data (HIPAA, FERPA, CJI, etc.) electronic data must be sent via encrypted e-mail.
3. Copies of e-mail must be retained in accordance with records retention schedules.
4. E-mail servers must be secured in accordance with the Server Management Policy.
5. E-mail accounts must be connected to individual users. Where a group e-mail account exists, primary ownership of and responsibility for that account must be assigned to an individual.
6. Access controls must be implemented to maintain integrity and confidentiality in accordance with the Access Policy.
7. Privileged-user access must be audited in accordance with the Audit of Access Control Policy.
8. No transfer of email records of a state employee if they move to a different agency or department within state government.

4.9.1 E-mail Best Practices

1. E-mail systems should be monitored for data leakage.
2. E-mail systems should facilitate eDiscovery processes.

4.10 Remote Access

1. All remote access methods must support authentication of unique users in accordance with the Authentication Policy.
2. At no time, must any remote access user provide their password to anyone in accordance with the Authentication Policy.
3. At no time, must any remote access user allow another person to use their remote connection.
4. All remote access approvals must be documented, including purpose, conditions, duration and approved methods.
5. Split tunneling or dual homing must not be permitted at any time if remote access is accomplished using personally-owned equipment. If state-owned equipment is used, split tunneling or dual homing must only be permitted if the remote network is under the complete control of the connecting person.
6. All computers that are connected directly to an agency’s internal networks via remote access technologies must use the most up-to-date anti-virus software, operating system and application patches.
7. Personal equipment that is used to connect to the agency's networks must meet the security requirements of agency-owned equipment for remote access.

8. Remote access rights must be terminated immediately upon the departure of an employee or if their duties no longer require remote access.
9. State employees accessing agency or state networks to perform technical administration of servers or network equipment must use state owned equipment.
10. Contracts with third parties such as vendors, partners, and contractors requiring remote access must specify security requirements for connectivity. Third party equipment used to connect to an agency's networks must meet the requirements of agency-owned equipment for remote access. Remote access must be terminated immediately upon the completion or termination of a contract, termination of the partner relationship, or termination of an individual's employment with the vendor, partner or contractor.

4.10.1 Remote Access Best Practices[viii]:

1. Equipment not owned and supported by the state should not be connected via remote access technologies to the state network or agency resources.
2. If an agency decides to allow equipment not owned by the state to connect to the network, the agency should implement solutions to ensure that antivirus and patch levels are current prior to connection to the network or agency resource.
3. Agencies should consider providing employees with a bootable USB or CD that contains an agency-approved image. This would allow the employee to load the image and to work remotely without accessing or storing information directly to a personal computer.
4. Where VPN solutions are utilized, agencies should use a VPN solution that forces the user to limit all interactions to the agency network while the VPN connection is open.
5. Individuals accessing state resources via a web-based application using their personally owned equipment should maintain that equipment with current operating system and application patch levels and antivirus software.

4.11 Wireless Access[ix]:

1. Industry supported wireless standard 802.11 must be used by wireless access points.
2. The decision of whether, and how, guest access will be allowed must be documented. Guest access via a wireless entry point must be configured to only allow Internet access but prevent access to internal network resources.
3. For non-guest access the Wireless Protected Access2 (WPA2) protocol with AES encryption must be deployed for data encryption to further protect transmitted information.
4. Comprehensive security assessments and inventory of wireless access must be performed at regular and random intervals. Assessments must include validating that unauthorized access points do not exist in the agency and testing the boundaries of wireless access.
5. Data must be encrypted in transit in accordance with the Encryption Policy.
6. Access points must be placed in physically secure or hidden areas to prevent unauthorized physical access and user manipulation.
7. Non-default SSID must be used for wireless networks. SSIDs must not reveal information about the network, agency name or location.
8. Nonessential management protocols must be disabled on access points.

9. The “ad hoc mode” for 802.11 on wireless clients must be disabled when technically possible.
10. Administrative access to manage the wireless device must only be enabled via a dedicated wired management VLAN. Access to administrative functions must be disabled via the wireless interface.
11. If the access point supports logging, turn it on and review the logs on a regular basis in accordance with the Log Management Policy.

4.11.1 Wireless Access Best Practices

1. External boundary protection should be implemented around the physical perimeter of buildings containing access points. These protections include locating access points on interior walls and, wherever possible, using enterprise class systems that use controller based AP configuration management.
2. Guest access should be restricted such that only authorized guests have access.
3. A firewall should be placed between the wired infrastructure and the wireless network in accordance with Security Zone and Network Security Management.

5 Information Systems Acquisition, Development and Management

The goal of information systems acquisition, development and management is to ensure that security is an integral part of information systems. Information systems are defined as computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the state’s shared computing and network infrastructure.

5.1 Business Case Standard

1. The Chief Information Officers (CIO) must approve a Business Case/Cost Analysis (an IT ABC form) for information technology (IT) procurement with lifecycle costs over $500,000.

5.1.1 Business Case Best Practices

1. An IT ABC form should be completed to document the value proposition of all IT investments.
2. For general requirements and guidelines regarding acquisition of IT goods and services please go to: Agency of Administration Bulletin 3.5 and the IT Procurement Guideline.

5.2 Cloud Services

1. Agency of Digital Services will be the central source for contracts with public and private cloud services and cloud service providers.

5.3 Encryption[x]

1. In all cases where encryption is used, encryption protocol and strength must be Advanced Encryption Standard (AES) 128-bit or stronger. If AES 128-bit is not technically possible, triple DES (3DES) must be used until AES 128-bit or stronger is available.
2. Backup and archive copies of exempt information must be encrypted. Encryption of exempt information must be at the storage media level, at the database level, or at the application level. Encrypted backup and archive media must support data restoration and disaster recovery and support various backup media types used by the state.
3. Encryption must be deployed at a level (e.g. file, folder, database, application, full disk) that is commensurate with the risk and compliance requirements of the information being stored.
4. Encryption for USB flash-drives and hard drives must either use password and encryption capabilities built into the device or must be encrypted using host-based encryption software at the time data is stored on the device.
5. Key management or escrow processes must be used when using a key-based data encryption system.
6. Encryption keys suspected of having been compromised must be replaced immediately.
7. For wireless see Wireless Access Policy

5.3.1 Encryption Best Practices

1. Records/Data which by law are designated confidential or by a similar term including federally or industry protected data (HIPAA, FERPA, CJI, etc.) should be encrypted using AES 256-bit or stronger encryption
2. Backup and archive media encryption should integrate seamlessly with backup processes and devices.
3. NIST recommendations in Storage Encryption Technologies for End User Devices NIST should be reviewed and used where applicable.
4. Encryption keys should not be used to encrypt data across multiple systems, storage devices, etc.
5. Periodic cryptographic key changes and retirement of old keys (for example: archiving, destruction, and revocation as applicable) should be practiced.
6. Key-management procedures that require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key) should be implemented.
7. NIST document Key Derivation Using Pseudorandom Functions NIST sp800-108 should be reviewed for more information on encryption keys and key management.

5.4 Patch Management

1. All operating systems and commercial off-the-shelf/open source software must be patched and maintained at current vendor supported levels.
2. Agencies must deploy security patches to operating systems and applications upon release unless the agency follows a documented procedure for testing and deploying security patches within an identified timeframe.
3. Operating System and commercial off-the-shelf/open source software for which the vendor/open source community no longer provides security patches is considered deprecated and must be remediated with documented controls or removed from production.
4. Wherever possible, automated patching systems must be implemented to automatically update operating systems and applications.
5. Automated patching systems must log which information systems have received the patches and audit for information systems that have been missed.
6. An application update management process must be implemented to ensure the most up-to-date approved patches and application updates are installed for all software.
7. Custom developed applications must be tested on a defined schedule for vulnerabilities and updated to correct identified vulnerabilities.
8. If no patch is available, other controls must be implemented, such as turning off services or capabilities related to the vulnerability; adapting or adding access controls, e.g. firewalls, at network borders; increased monitoring to detect or prevent actual attacks; raising awareness of the vulnerability; keeping an audit log of all procedures undertaken; evaluating the technical vulnerability management process in order to ensure its effectiveness; and addressing high-risk information systems first.

5.4.1 Patch Management Best Practice[xi]:

1. High Risk Security patches should be applied immediately after appropriate testing or within 72 hours.

5.5 Information System Development Lifecycle

1. Access to operating system, source code, and operational or production application software/program directories, locations, and configuration files must be managed, limiting access to authorized individuals.
2. When developing, or modifying information systems, a change control management process must be used to require authorization to initiate or make changes to the system, test and accept the changes, and move changes into production.
3. New or updated information systems must include adequate system documentation and ensure that system documentation is readily available to support the staff responsible for operating, securing and maintaining new and updated information systems.
4. Separate development, test and production environments must be used to protect production systems from development work and testing.

5. Procurement of information systems designed to store, access or in any way handle exempt information must include requirements that information located on or transferred to or from these systems can be encrypted in accordance with the Encryption Policy.

5.5.1 Information System Development Life Cycle Best Practices

1. Separation of duties between system developers and operations should be maintained, including between the following roles system administration and system auditing; system development and system change; system operations and system security administration.

6 Glossary

Access Control – controls based on job duties and responsibilities added to systems and process that limit the usability and capability of those systems and processes. Access Control requires authentication and authorization.

Ad hoc mode - Ad-hoc mode refers to a wireless network structure where devices can communicate directly with each other.

Authentication – is the act or process of showing an identity to be true.

Authorization – is the act of specifying specific rights to an identity for systems and processes.

Bulletin 3.5 – the procurement and contracting procedures for the State of Vermont. See http://aoa.vermont.gov/bulletins/3point5

Data leakage – per the SANS Institute, Data Leakage is the unauthorized transmission of data (or information) from within an organization to an external destination or recipient. This may be electronic, or may be via a physical method.

DMZ - refers to a subnetwork that exposes an organizations external services to the internet.

Encryption – the process of encoding messages

Exception document – generally a document that requests a policy be set aside for a specific reason. The exception document outlines risks associated with not following a policy

Exempt – a classification of a record. A document/record not provided for free and open examination.

External boundary – the physical perimeter for use for wireless access

IDS - An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.

IT ABC Form – The State of Vermont in-take form for IT Projects

ITSM – Information Technology Service Management

Multi-factor Authentication - Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity for a login or other transaction.

NIST - NIST is the National Institute of Standards and Technology, a unit of the U.S. Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

Password - A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource

Patch Management – the processes around patches. A patch is piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bugfixes or bug fixes, and improving the usability or performance.

Redact – to censor or obscure text in a document for security purposes

Remote access – connection to systems from a remote location. VPNs are generally used for remote access.

Separation of Duties (SoD) - is the concept of having more than one person required to complete a task. In business, the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error. SoD is also a capability of identity and access management systems.

Spam – Unsolicited or inappropriate messages sent on the Internet to many recipients

Special Access Privileges – Within identity and access management, it is focused on the special requirements of powerful accounts within the IT infrastructure of an enterprise.

User IDs - A user ID is the unique name that you use to identify oneself with access to a computer service.

VLAN - A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network

VM – virtual machine

VPN – virtual private network

Wireless – computer networking using radio signals

7 Bibliography

Enterprise Architecture State of Vermont. (2015). *Non-functional Requirements.* Montpelier Vermont.

ISO/IEC. (2011). *ISO/IEC 25010:2011(E) Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models.* Geneva, Switzerland: IS0 / IEC.

Joint Task Force Tranformation Initiative. (04/30/2013). *Security and Privacy Controls for Federal Information Systems (NIST 800-53 Rev. 4).* National Institute of Standards and Technology.

Statewide Information Security Standards, November 2009, Enterprise Security Office, security.office@state.or.us, http://oregon.gov/das/EISPD/ESO

8 Endnotes

[i] 6.7.108 **Security** Hosting & General Security Services System Hardening "Network device configurations will be hardened by performing the following:

- Disabling telnet access.
- Controlling Simple Network Management Protocol (SNMP) access to devices.
- Controlling access to devices using Terminal Access Controller Access Control System Plus (TACACS+).
- Turn off unneeded services.
- Perform appropriate level of logging."

[ii] 6.7.133 **Security** Security General Strong Authentication Hosting Service Provider will use strong authentication to provide enhanced protection against unauthorized access to Vermont's web application environments using Hosting Service Provider's adaptive access capabilities. The service will review Vermont's business and security requirements to implement appropriate Hosting Service Provider adaptive access policies and implement in Vermont's selected Non-Production Environment within the identified Enhanced Security Services Environments. Production implementation will take place upon Vermont's successful testing and sign off on the service in a Non-Production Environment.

[iii] 6.7.104 Security Hosting & General Security Services Protection Against Malicious Code Hosting Service Provider will license and install third party Service Provider anti-virus and anti-spam products to scan all employee and the State email and inbound attachments that traverse either the State's dedicated servers located at Hosting Service Provider's Data Centers.

[iv] 6.7.125 **Security** Security General Security Logging Hosting Service Provider will log security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to the Environment or Hosting Service Provider Programs, as well as system alerts, console messages, and system errors. The Hosting Service Provider implements controls to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten. Security-related log entries will capture the following information: date, time, time zone, user account name and/or IP address, original value, location of change (hostname, filename, table name), new value (other than password).

[v] 6.7.56 **Security** Database Security Backup & Recovery Hosting Service Provider will employ the use of dedicated backup servers

[vi] 6.3.21 **Security** Network WAN Hosting Service Provider will use VPN devices in a site-to-site (network-to-network) topology leveraging the public Internet or dedicated links.

6.3.22 **Security** Network WAN Hosting Service Provider will implement Internet Protocol Security (IPsec) as part of an overall VPN strategy to secure data between endpoints on the Management Link by employing tunneling and encryption to facilitate data privacy.

6.3.23 **Security** Network WAN Hosting Service Provider will pre-configure Hosting Service Provider-provided VPN(s) to provide the following levels of encryption and authentication, in accordance with the IPSec standard: Data encryption using 168-bit Triple Des or AES256, Hashed Message Authentication Codes (HMAC) with a SHA-1 algorithm.

6.3.24 **Security** H3.1.54 Network WAN The standard Network Connectivity between Hosting Service Provider and the State will be through a hardware VPN provided by Hosting Service Provider.

6.3.25 **Security** Network WAN Hosting Service Provider will provide access to the Environment will be via a virtual private network (VPN) connection. Hosting Service Provider will provide the State with the number and type of VPNs required.

6.3.26 **Security** Network WAN Hosting Service Provider will specify, design and deliver a network transport to allow Hosting Service Provider personnel to access a Hosting Service Provider environment, e.g., Transaction Link. The DMZ at the Hosting Service Provider Data

Centers will be connected through VPN tunnels that terminate on the Hosting Service Provider firewalls. For all other Hosting Service Provider Data Centers, the HPISN DMZ will connect to the Hosting Service Provider Data Center network via a direct link though a Firewall Interconnect Network (FIN).

6.3.27 **Security** Network WAN Hosting Service Provider will configure the VPN device based on the State's network topology and Hosting Service Provider policies. The Hosting Service Provider-provided VPN will have two interfaces, external and internal. Hosting Service Provider will use both interfaces (dual-arm mode), but will support a configuration that uses only one interface (single-arm mode).

6.3.28 **Security** Network WAN The external interface will be connected to a switch between the State's border router and firewall.

6.3.29 **Security** Network WAN The VPN device external interface will be connected to a firewall DMZ interface.

6.3.30 **Security** Network WAN The VPN Device external interface will not be directly connected to the Internet. The external untrusted interface should be connected to the Internet behind the State's boarder router to enable the State to apply Access Control Lists (ACLs) to secure the State’s Environment from unsolicited traffic.

[vii] 6.7.60 **Security** Database Security Media Storage Hosting Service Provider will employ intrusion detection systems to provide continuous surveillance for intercepting and responding to security events as they are identified.

[viii] 6.7.41 **Security** Database Security Access Control Remote access for Hosting Service Provider employees and subcontractors requires all connections to the Hosting Service Provider network from a non-Hosting Service Provider location to use either an IPSec or SSL-encrypted VPN,

[ix] 6.26.225 **Security** Security General PII Standards "Project participants and other individuals will not transmit or store any Personally Identifiable Information (PII) using storage publicly available, over the Internet or any wireless communication device, unless:

1) PII is “de-identified” in accordance with 45 C.F.R § 164.514(b) (2),

2) Encrypted in accordance with applicable law, including the American Recovery and Reinvestment Act of 2009 and as required by policies and procedures established by the State."

[x] 6.26.211 **Security** Security General Encryption Database data will be encrypted at the file system layer.

6.26.212 **Security** Security General Encryption Data stored on file systems will be encrypted.

[xi]6.13.157 **Security** Maintenance and Operations Application Support Solutions will have critical security patches applied within 24 hours of the patch release.

6.13.158 **Security** Maintenance and Operations Application Support Solutions will support automated patch deployment.