State of Vermont

Information Security Standards

Standards and Best Practices

Table of Contents

1. Introduction

1.1. Authority

The Agency of Digital Services (ADS) is charged with providing "services for all activities directly related to information technology and cybersecurity, including telecommunications services, information technology equipment, software, accessibility, networks in State government, and the sharing of data and information within State government" (3 V.S.A. § 3301). ADS, in collaboration with its partners across state government, has established the following Information Security Standards. The standards promote the development, implementation, and operation of more secure information systems by establishing minimum levels of due diligence for information security. These standards facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.

1.2. Purpose

The standards in this document promote the development, implementation, and operation of more secure information systems by establishing minimum levels of due diligence for information security. These standards facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements. Additionally, these standards contain "Recommended Best Practices" that have been suggested to ensure information security. While non-mandatory, the best practices are recommended and should be considered in planning to help ensure future security and compliance.

1.3. Scope

Standards herein are required to be applied to information systems within the Executive Branch agencies and business units. Agencies are responsible for ensuring, through documented agreements, that all third parties acting on their behalf comply. In circumstances where these standards 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 Digital Services, or designee. The exception must be documented and kept on file for review by auditors or during a security assessment. Agency of Administration (AOA) Directive Memorandum 11.7, Electronic Communications and Internet Use, remains in effect.

1.4. Sources of Security Guidelines

These standards and recommended best practices have been developed referencing the following resources: The International Organization for Standardization (ISO) 27001 & 27002, The National Institute of Standards and Technology (NIST) Special Publications, and the SANS Institute recommended policy and best practices. In the event that guidance is not clear, NIST standards will be the default.

The items documented as Recommended Best Practices are not mandatory and do not need to be met by agencies to comply. 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. Most best practices included here will, over time, become the new mandatory minimum standards.

Prior to agency implementation of these standards, 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 standard identified below.

1.5. Required Training and Certification

State of Vermont employees are required to cultivate security awareness. In order to further that objective, all employees must complete security awareness training in accordance with the ADS and Department of Human Resources published schedule. Additionally, agencies may require additional trainings tailored to specific agencies or positions, according to agency policies or requirements from Federal agencies. All required trainings must be taken upon hire and then completed each year for the duration of employment. User accounts of any individual not in compliance with the training requirements may be disabled until the training requirements have been met.

1.6. Policy Exceptions

In circumstances where these standards 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 requesting Agency Secretary, appointing authority or designee, the CISO, and the Secretary of ADS, or designee. The exception must be documented and kept on file for review by auditors or during a security assessment and will require annual renewal.

1.7. Changes and Amendments

In order to ensure that the State of Vermont can continue to respond quickly to new or emerging security threats, this policy may be supplemented with ADS Cybersecurity Directives or Standards from time to time.

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" or the "Principle of Least Privilege" 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.

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 only need 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 Standard 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 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 inside and outside the State network.
3. Passwords must be no less than 12 characters in length, and contain a minimum of one uppercase letter, one lowercase letter, one special character, and one number.
4. User IDs and passwords must not be shared.
5. 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.
6. Users must not reveal passwords to anyone, including supervisors, family members or co-workers.
7. Management approval must be required for establishing each user ID and a process must be in place to remove or suspend user IDs or access which is no longer required to perform an assigned job function.
8. The construction and specifications of a password must be defined in any supplemental agency policies and must be of a complexity consistent with the information the user has access to.
9. A multi-factor authentication method (e.g. pin, secure token, or authenticator app) must be used to authenticate user access to information systems containing federally or industry protected data types where appropriate.
10. Passwords must be obfuscated on login to all information systems so that the password cannot be read from the screen.
11. Passwords must not be transferred or transmitted in an unsecure electronic format, such as email.

12. Vendor or other default supplied passwords for information systems must be changed immediately upon installation.
13. Passwords must be changed whenever there is a chance that the password or information system has been compromised.
14. Authentication must occur through encrypted channels using methods such as Kerberos, SSH, or SSL.
15. On any system that can store or log passwords, such as servers and clients, passwords must be stored in protected, encrypted files.
16. 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.
17. All passwords must be changed quarterly (every 90 days) 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 (Internal Revenue Service Publication 1075, Criminal Justice Information Services (CJIS) security policy, Minimum Acceptable Risk Standards for Exchanges (MARS-E), Health Information Portability and Accountability Act (HIPAA), etc.).
18. System passwords must be treated as confidential information, known to the least number of people possible. However, to maintain business continuity all system passwords must be documented and stored in a secure location with at least two individuals having access to said location.
19. 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.
    e. Maintaining logs of the special access privilege use on all/critical information systems.
20. Information systems must disable inactive accounts after 90 days of inactivity. This includes inactive user and computer objects.
21. Managed Service Accounts: Active Directory Managed Service Accounts and Group Managed Service Accounts should be used for service accounts where possible. These accounts will increase the security of the system and/or application by only allowing a specific system, or group of systems, access to the account's password in Active Directory.

2.1.1. Authentication Best Practices

1. Passphrases should be used in lieu of passwords. A passphrase is similar to a password in usage but is significantly longer for added security with a typical minimum of 16 characters.
2. For additional password and passphrase security, it is suggested that agencies follow the latest version of the NIST password recommendations. At time of signing, the latest

recommendations were found in NIST Special Publication 800-63-2 Electronic Authentication Guideline Revision 3.

3. Users of state information systems should be trained to not reuse their state account passwords for any other purpose.
4. Passwords should only be stored in protected and secure internal networks or an acceptable password manager, approved by ADS. Vendors and contractors do not require ADS approval but should attempt to follow this best practice.
5. The State of Vermont offers MFA for application access through the Microsoft portal for those with valid vermont.gov accounts.
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 will 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 standards prior to production deployment.
3. Authorization must be removed immediately upon departure or change in employee job duties. Managers must submit a ticket to ADS Service Desk by close of business on the day of change in status. Vendors and contractors must remove any account with access to State systems or other systems in support of the activities described in the contract. User accounts must automatically be logged after 60 days of inactivity and email check sent to their manager. After 90 days of inactivity, accounts must be automatically suspended, marked for review and possible deletion. Those accounts where the individual has an excused leave of absence (Medical, Military, etc.), the account shall be suspended and documented after the 60 days of inactivity or sooner but not deleted or removed.
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 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 successful and failed login attempts to information systems and granted and denied access to resources in accordance with Section 4.5 Log Management.
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 weekly and reviewed in detail as necessary.
3. Audit logs must be tamper-resistant. In all cases, access to the logs must be limited only to those requiring 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 standards 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 in 3.1.

The standard identified in Section 3.1 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 Section 2 Access Control.
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 entirely overwritten or destroyed according to standards in NIST Publication 800-88 and the Digital Media and Hardware Disposal Standard.

It is recognized that some exemptions in state, as well as Federal law may require encryption. Records officers are responsible for assuring that internal standards related to their respective agency records management programs include encryption requirements that comply with Section 5.3 Encryption. A log review process is mandatory. Two-factor authentication for access is required in accordance with Section 2 Access Control.

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 standard 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. Vendors and contractors may use this as guidance but when not adhering to this standard must have a documented process, based on NIST (or other State acceptable) standards, to meet these requirements.

4.1. Antivirus and Anti-Malware

1. All workstations and servers must have antivirus and anti-malware software enabled where available, except as a specific waiver has been granted by the Secretary of ADS, or designee.
2. All information systems with antivirus software must undergo at a minimum a weekly full system scan for viruses and malware.
3. Any infected information system must be handled in accordance with incident response procedures.
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 Section 5.4 Patch Management.
7. All antivirus and anti-malware signatures must be updated at least daily and software 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. Weekly scans required in the Antivirus and Anti-Malware Standard should be scheduled to occur automatically during nonbusiness hours.
3. Scan frequency should be increased to daily on critical or central systems.
4. Backups should be scanned and verified clean.

4.2. Workstation Management & Desktop Security

1. All workstations must be patched in accordance with Section 5.4 Patch Management. A weekly restart of all workstations is required to ensure that patches have been appropriately applied.
2. Workstations must be protected with anti-virus software to protect the machine against malware in accordance with Section 4.1 Anti-Virus & Anti-Malware.
3. Standard users must not have administrative rights access to their workstations in accordance with Section 2 Access Control. If privileged access is required, a separate privileged account should be created and used only for tasks requiring elevated privileges on that specific information system. Privileged accounts will not be used to elevate privileges for other accounts without documentation such as a service ticket or memorandum from a manager. In all cases, the privilege escalation should conform to role-based standards. These accounts shall be

documented, tracked, and authorized by ADS Shared Services or the contractor or vendor administrative process.

4. By default, workstations must not be configured to support peer to peer networking. A specific business use must be identified and approved by ADS 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 or other form of end point protection 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.
11. Workstations must use password logons and have passwords compliant with Section 2.1 Authentication.
12. Users must lock their workstation when leaving it unattended, and workstations must automatically lock after a maximum of 15 minutes. Once locked, workstations must require users to reauthorize via login credential.

4.3.Mobile Device Management

1. Mobile Devices must not be physically connected to agency owned equipment, unless specifically authorized by ADS for the purpose of managing State-owned mobile devices.
2. All State employees and contractors must not store State data on personally owned devices.
3. Information stored on portable devices must be protected in a manner commensurate with the classification of the information.
4. Mobile devices must be configured to include a password, pattern, or pin protected lock screen. All mobile devices must lock after no more than 5 minutes of inactivity.
5. Mobile device operating system and applications must be kept updated with the latest security patches.
6. 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 Section 2.1 Authentication.
7. Mobile devices must not be left unattended in uncontrolled access areas.
8. Storage devices such as hard disk drives and other media containing sensitive information must be physically secured under lock and key for storage purposes or destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information.

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 Section 2 Access Control. Server administrators must use privileged 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 an ADS-approved remediation plan to remain in service or will 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 and approved by the office of the Chief Technology Officer. Applications that create risk for the enterprise are subject to approval by ADS management.
7. There must be established Agency or Department procedures for approving or denying the attachment of peripheral devices to any server and all devices must be approved before installation.
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), login, logout, and failures of access in accordance with Section 4.5 Log Management. Additionally, logs should include any change in status to services enabled on the server.
9. Servers must be synchronized with one or more ADS approved network time device(s).
10. All web servers must point to State of Vermont approved record servers, to include Domain Name System (DNS) servers, using DNS Security Extensions (DNSSEC). All web servers must have a valid SPF record, register with the State of Vermont Domain Registration authority, and have valid certificates issued by the ADS Webmaster. Prior coordination must occur with the ADS Webmaster before beginning web server development. Vendors and contractors that manage web systems for the State must also comply with this standard.
11. The following standards must be applied to server management:
    a. Section 4.1 Anti-Virus & Anti-Malware
    b. Section 4.6 Information Backup
    c. Section 4.7 Security Zone and Network Security Management (local Area Network and Wide Area Network)
    d. Section 4.10 Remote Access
    e. Section 5.3 Encryption
    f. Section 5.4 Patch Management

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 Section 4.7 Security Zone and Network Security Management.

4.5.Log Management

1. Log data generated from servers, network devices (firewalls, switches, routers, etc.) and other devices/services must be maintained and preserved. 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 Section 2 Access Control.
4. Logs must be regularly reviewed and analyzed for indications of unauthorized or unusual activity. Suspicious activity (for example, unauthorized changes to security controls and failed or unauthorized access attempts), must be investigated, findings reported to ADS Security, 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 and/or federal 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. Critical security logs should be copied into a secure repository with access restricted to security log reviewing personnel and department IT managers.
5. Log files will be made available to the Vermont Security Operations Center (VTSOC) upon request for one time or automated export to the Security Information and Events Management (SIEM) console. Vendors and contractors do not need to follow this standard, but the State recommends they have their own system for log monitoring and aggregation.

4.6.Information Backup

1. Backups must be made based on the data stored in the information system and store the necessary data files and programs to recreate a viable workspace.
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 Section 5.3 Encryption.
3. System administrators and owners must coordinate with Enterprise Application Services (EAS) to test their backups at least annually to ensure information can be restored and to identify restoration constraints. Vendors and contractors must test backups to ensure they can provide services to the State.
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 standard.
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. At least three generations of backups must be maintained for each system.
8. 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.
2. System administrators and owners must coordinate with EAS to test their backups at least quarterly to ensure information can be restored and to identify restoration constraints.
3. Secure offline copies of backups should be created weekly to protect against malicious alteration of backup files.

4.7.Security Zone and Network Security Management (Local Area Network & Wide Area Network)

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 using 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. All network equipment (firewalls, MPLS, VLANs, hubs, switches, routers, wireless access points) must be managed to ensure that security zones are maintained.
7. All network equipment (firewalls, MPLS, VLANs, hubs, switches, routers, wireless access points) must be configured in accordance with Section 2 Access Control.
8. By default, all hardware switch ports must be turned off unless physical access is controlled to both endpoints of the physical connection.
9. Dynamic IP address assignments must be logged.
10. Static IP addresses must be inventoried and analyzed quarterly for changes.
11. 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.
12. Currently certified secure management software must be used for management of access points. At the time of signing, acceptable software must use or be based off SNMPv3 and SSH protocols.
13. The following sections also apply to security zone management:
    a. Section 4.5 Log Management
    b. Section 4.10 Remote Access
14. Firewall Rules: Firewall rulesets shall be reviewed annually with system owners and business owners to ensure current ruleset is updated and stale records are removed.

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.
4. Physical separation of security zones should be maintained. Virtual separation mechanisms (e.g. VMs and VLANs) may be used for segregating sub-zones within a security zone.
5. Network policy orchestration should be deployed to provide an automation and oversight component to all network and security policy activities.

4.8.Intrusion Detection

1. Intrusion Detection Systems (IDS) must be deployed to monitor external network traffic.
2. Intrusion detection signatures must be updated at least daily and software/firmware maintained at current vendor supported levels.
3. IDS must perform packet and protocol analysis, fragmented and packet stream reassembly, and detect attacks in real time to provide timely alerts and notification where technically feasible.
4. Logs must be maintained and reviewed in accordance with Section 4.5 Log Management.
5. Evidence and alerts of intrusion must be handled in accordance with incident response plans and the State incident response standard. Incident response plan/procedure must include

response to Intrusion Detection System (IDS) alerts. Vendors and contractors must have a policy and processes based on NIST (or other State acceptable) standards.

6. IDS must be monitored by appropriately trained and authorized staff.
7. All State of Vermont external network traffic must be appropriately configured to traverse the State's boundary firewalls, IDS, and Albert sensors.

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 Section 4.1 Anti-Virus & Anti-Malware.
2. Electronic records/data which by law are designated confidential or by a similar term, including federally or industry protected data (for example HIPAA, PII, and FTI) must be sent via encrypted e-mail.
3. E-mail must be retained in accordance with records retention schedules.
4. E-mail servers must be secured in accordance with Section 4.4 Server Management or in accordance with the tenant agreement with Microsoft. Vendors and contractors must have an email security 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 Section 2 Access Control.
7. Privileged-user access must be audited in accordance with Section 2 Access Control.
8. There will be no transfer of email records of a State employee or State vendor partner account if they move to a different agency or department within State government, unless specifically authorized by the Agency of departure.
9. State issued email may only be used to conduct State business and State business must not be conducted with a non-State email address.
10. State issued credentials may not be used to access other unaffiliated systems.

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 Section 2.1 Authentication.

2. Remote access users must not provide their password to anyone in accordance with Section 2.1 Authentication.
3. Remote access users must not allow another person to use their remote connection.
4. All VPN connections must be established using MFA. All exceptions must be approved by ADS management in conjunction with the system owner.
5. All remote access approvals must be documented, including purpose, conditions, duration and approved methods.
6. 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 or entity.
7. 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.
8. Personal equipment that is used to connect to the agency's networks must meet the security requirements of agency-owned equipment for remote access.
9. Remote access rights must be terminated immediately upon the departure of an employee or if their duties no longer require remote access.
10. State employees accessing agency or State networks to perform technical administration of servers or network equipment must use State-owned equipment.
11. 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

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 requests approval 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, and the system configuration matches current State standard requirements.
3. 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.
4. 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

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 Section 5.3 Encryption.
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. An authentication server must be used to authenticate for wireless access to non-guest State networks.
11. The access points shall support logging and review the logs shall be performed on a regular basis in accordance with Section 4.5 Log Management.
12. Wireless access points shall be located on the interior of any building where State-owned wireless access points are placed. Access points located near exterior walls or windows allow wireless networks to bleed outside of State controlled spaces.
13. No official State business, to include hosting servers, workstations, printers, etc., shall be conducted using the guest wireless access.
14. Wired connections should be used, when available, at all State workstation locations.
15. No entity may install or provision a wireless network without approval of ADS management.

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 access point 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 Section 4.7 Security Zone and Network Security Management.

4.12. Removable Media

1. Employees may only use authorized State of Vermont owned removable media in their work computers. Personally owned devices, including but not limited to tablets, printers, wireless access points/routers, personal digital assistants (PDAs), smart phones, and storage devices such as flash memory (USB flash drives, SD, MMC, XD, Compact Flash memory sticks), portable hard

drives, and MP3 players are prohibited for use with State of Vermont workstations or servers. Vendors and contractors may not store State data on removeable media.

2. State of Vermont owned removable media may not be connected to or used in computers that are not owned or leased by the State of Vermont without explicit permission from the Agency/Department IT manager. All permission granted will be documented.
3. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies.
4. Vendors or others requesting one-time access to the network for demonstration or training will work directly with the Helpdesk to ensure the appropriate security controls are in place and documented before connecting to the network. Individuals and firms under contract or agreement with the Agency must provide details of connectivity requirements and meet all State and Agency security standards and obtain written prior approval of the Agency IT Leader before connecting to the network.
5. When sensitive or exempt information is stored on removable media, it must be encrypted in accordance with Section 5.3 Encryption.
6. The use of personal internet-based applications for storage of State of Vermont data is strictly prohibited, unless specifically authorized by the Secretary of ADS and the requesting Agency Secretary/Department Commissioner. These applications may include, but are not limited to, Dropbox, Box, Google Docs, OneDrive, iCloud, etc.

4.12.1. Removable Media Best Practices

1. Removable media should be scanned for threats using a computer that is not connected to the State of Vermont-managed IT infrastructure before being used on any State-owned IT asset. This proactive approach to scanning for potential threats can limit the risk of removable media use within Agency/Department environments.

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 Officer (CIO) must approve a Business Case/Cost Analysis (an IT ABC form) for information technology (IT) procurement in accordance with current State policies.

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 follow: Agency of Administration Bulletin 3.5 and the IT Procurement Guideline.

3. Project sponsors should capture all Information Security costs at the time of IT ABC submission to ensure appropriate protective measures are integrated into the system development and/or procurement cycle.

5.2. Cloud Services

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

5.3. Encryption

1. In all cases where encryption is used, encryption protocol and strength must be up to date with current standards in NIST 800-175B at a minimum. At time of signing, the minimum acceptable encryption standard is AES 128-bit encryption.
2. All copies, including 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 encryption see Section 4.11 Wireless Access.

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 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 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 Special Publication 800-108, 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. System owners and administrators must deploy security patches to operating systems and applications upon testing and within the timeframe given. High and Critical vulnerabilities must be secured and closed within 30 days, medium vulnerabilities within 60 days, and low vulnerabilities within 90 days unless the agency has a signed risk acceptance form signed by the CISO or a Plan of Actions and Milestones (POA&M) is required for further testing of the security patch.
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. The standard ADS centralized patching solution must be used, unless specifically authorized in writing by the Secretary of ADS, or designee. Vendors and contractors will use a centralized system for patching systems.
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, compensating 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.
9. Unpatched systems that exceed the outlined standards, risk being disconnected from the State network until they are brought into compliance.

5.4.1. Patch Management Best Practices

1. High (or Critical and exploitable) severity 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 Section 5.3 Encryption.

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.
2. To ensure that development changes are approved before going into production, developers should not have administrative access to production servers.

5.6. Social Media/Information Distribution

1. Employees should refer to the full Social Media/Information Distribution Policy to answer any questions.

5.6.1. Authorization

1. Personal social media accounts should remain personal in nature and be used to share personal opinions or non-work-related information.
2. Employees should not participate on social media websites or other online forums on behalf of an agency unless authorized by the Secretary of their Agency or Secretary of Administration.
3. Employees must never use their State-provided email account or password in conjunction with a personal social media website or other online forums.

5.6.2. Confidentiality

1. Employees shall not post or release proprietary, confidential, sensitive or personally identifiable information or state government intellectual property on social media websites, online forums, or to external email addresses.

6. Cyber Risk Management

The goal of cyber risk management is to ensure that risk management of systems is an integral part of organizational functions. Cyber risk management is defined as the identification, assessment, and

prioritization of risks followed by a coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of malicious events to preserve the integrity of information and intangible assets.

6.1. Vulnerability Management

1. To ensure the security of critical State information, vulnerability management strategies will be put in place in State agencies and departments. Vulnerability management is the practice of identifying, classifying, remediating, and mitigating vulnerabilities in a system.
2. System and/or application vulnerabilities will be identified through vulnerability scans or security assessments performed by the ADS Security team. Vulnerability management includes both appropriate patching of vendor-identified vulnerabilities, as well as identification of poor security practices and architectural design weaknesses, which must be performed by system owners.
3. A notification of vulnerabilities identified through scans will be available to the IT managers or system administrators in charge of the system or application with the vulnerability.
4. Automated Vulnerability Assessments will run at minimum every 30 days. Administrators will be notified of the current state of their environment.
5. All devices that are capable of being scanned or installing a vulnerability management agent, currently the Nessus solution, must be enrolled in the vulnerability management Security Center for scanning and all new devices must be added to Security Center when being added to the network.
6. All network or system changes must be coordinated with the Vulnerability Management program to ensure scanning continues uninterrupted.
7. Vulnerabilities must be secured and closed within 30 days for high and critical vulnerabilities, 60 days for medium vulnerabilities, and 90 days for low vulnerabilities. If a vulnerability cannot be mitigated within the required timeframe, a POA&M will be required to track the vulnerability until closed. If the vulnerability cannot be remediated, a risk acceptance request form must be submitted by the requesting Agency/Department and approved by the CISO in accordance with the Vulnerability Scanning & Remediation Process. Risk acceptance must be reauthorized and renewed annually, initiated by Agency/Department request for continued acceptance.

6.2. Incident Management

1. Incident management describes the activities of an organization to identify, analyze, and correct hazards to restore services to normal as quickly as possible and to prevent a future reoccurrence.
2. All incident response must follow the Incident Response Standard.
3. All computer security incidents, including suspicious events, must be reported immediately (orally or via e-mail) to the Agency/Department IT manager and Department supervisor by the individual who witnessed/identified the breach.
4. The affected Agency/Department will coordinate with the office of the CISO and ADS personnel to mitigate, contain, and eradicate incidences according to the Incidence Response Plan.
5. All actions taken regarding an incident will be directed by ADS Security staff. Unintended consequences of well-meaning behavior can prohibit fully investigating an incident's root cause.

ADS will coordinate with affected Agency/Department leadership and IT managers to fully understand business impact of breaches in a timely manner.

6. The Secretary of ADS, or designee, shall be the only point of contact for public information dissemination and law enforcement coordination. All State of Vermont Employees must not publicize any information without explicit instructions from and coordination with the Secretary of ADS, or designee.

6.3. Disaster Recovery Plan/Contingency Planning

1. All critical systems must have a written plan on how to restore service in a timely manner in cases of emergency. Plans should include backup procedures, any redundant systems, and a list of persons to contact in an emergency.
2. Plans must be stored at minimum in both hard copy on site and an accessible off-site location to ensure the plan is still available in case of disaster.

7. 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 - a wireless network structure where devices can communicate directly with each other.

Auditing – is the process of ensuring Authorization and Authentication are correct on an information system.

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

Credentials – Any combination of email address or Active Directory username, and the password associated with the email address or username.

Data Leakage – the unauthorized transmission of data (or information) from within an organization to an external destination or recipient. This may be either through electronic or physical means.

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

Encryption – the process of encoding messages.

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

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.

Intrusion Detection System (IDS) - a device or software application that monitors network or system activities for malicious activities or Standard 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.

Mobile Device – A Portable Computing device with a primary local non-removable data storage, wireless networking interfaces, and an operating system not intended for Workstations.

Multifactor Authentication (MFA) - 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.

National Institute of Standards and Technology (NIST) - 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 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 – the connection to systems from a remote location. VPNs are generally used for remote access.

Separation of Duties (SoD) - 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 – the special requirements of powerful accounts within the IT infrastructure of an enterprise.

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

Virtual Local Area Network (VLAN) - 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