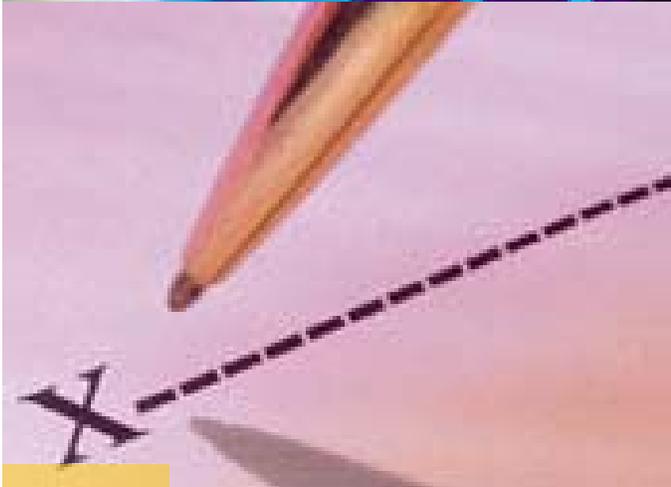


STATEWIDE INFORMATION SECURITY STANDARDS



Statewide Information Security Standards

November 2009

Enterprise Security Office

(503) 378-6557

security.office@state.or.us

<http://oregon.gov/das/EISPD/ESO>

DAS
DEPARTMENT OF
ADMINISTRATIVE
SERVICES
ENTERPRISE INFORMATION
STRATEGY AND POLICY DIVISION

| By | Changes | Version date |
|---|--|----------------------------|
| Amy McLaughlin, Richard Woodford, Shaun Gatherum | Original draft created | 6/30/2009 |
| Agencies Review & Comment | Comments added and addressed | 8/2009 |
| ESO | All comments addressed and edits made | 10/1/09 |
| State CIO Review | No comments no changes | 10/12/09 |
| EISAB | Out for review & comment | 10/13/09 – 10/23/09 |

TABLE OF CONTENTS

| | |
|--|----|
| Executive Summary | 3 |
| 1. Access Control..... | 4 |
| 2. Information Asset Management | 7 |
| 3. Communications & Operations Management | 8 |
| 4. Information Systems Acquisition, Development and Management | 17 |
| 5. Approval | 20 |

Executive Summary

Department of Administrative Services (DAS) has established the following Statewide Information Security Standards for information systems security. The standards promote the development, implementation, and operation of more secure information systems by establishing minimum levels of due diligence for information security. The standards facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum-security requirements. DAS has the responsibility for developing and overseeing the implementation of statewide standards, and policies on information security under the authority of Oregon Revised Statute 182.122.

These standards identify techniques associated with protecting and securely providing access to the State's information systems. Agencies may elect to exceed these minimum security standards to achieve their organizational security goals and requirements. These specific standards are interdependent and are intended to be implemented in their entirety.

The standards are required to be applied to information systems within the Executive Branch agencies. Agencies are responsible for complying with these standards and ensuring, through documented agreements, all third parties acting on their behalf comply. In circumstances where the 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 director. In instances where the risk is low and is accepted by the agency, the situation must be documented, signed by the agency director, and kept on file for review by auditors or during a security assessment.

These Statewide Information Security Standards and recommended best practices have been developed using a combination of the following resources:

- International Organization for Standardization (ISO) 27001 & 27002
- National Institute of Standards and Technology (NIST) recommended standards
- SANS Institute recommended standards and best practices
- Burton Group recommended methodologies 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 with the standards. 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 standards.

Prior to an agency implementation of these standards they should carefully review their information asset classification to determine the level of controls required to adequately protect those information assets. 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 standards identified below.

1. Access Control

To ensure critical data can only be accessed by authorized personnel, information systems controls and processes shall 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.

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 shall 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 standards identified below for authentication, authorization and audit shall apply to all information systems, modifications to systems, and when evaluating new information systems.

1.1. Authentication Standards:

- 1.1.1 The combination of a unique User ID and a valid password shall be the minimum requirement for granting access to information except for that which is publicly viewable.
- 1.1.2 Policy shall be established directing users not to reveal passwords to anyone, including supervisors, family members or co-workers.
- 1.1.3 Management approval shall be required for establishing each user ID and a process shall be in place to remove or suspend user IDs that are not longer required to perform an assigned job function
- 1.1.4 The construction and specifications of a password shall be defined in agency policy and shall be of a complexity consistent with the information the user has access to.
- 1.1.5 A multi-factor authentication method (e.g.: pin, secure token) shall be used to authenticate users to the data¹ for information systems containing level 4 data²
- 1.1.6 Passwords shall be redacted on login to all information systems so the password cannot be read off of the screen.
- 1.1.7 Vendor supplied passwords for information systems shall be changed immediately upon installation.
- 1.1.8 Passwords shall be changed whenever there is a chance that the password or information system has been compromised.
- 1.1.9 Authentication shall occur through encrypted channels using methods such as Kerberos (preferably Kerberos 5.0 or higher), SSH, SSL, etc.
- 1.1.10 On servers and clients, passwords shall be stored in protected, encrypted files.
- 1.1.11 Controls shall be implemented to protect information systems from brute force password guessing attacks (e.g. lock out after predetermined number of incorrect attempts.) Controls shall be commensurate with the associated risk to the information system.

¹ NIST Special Publication 800-63 Electronic Authentication Guideline.

² Statewide Information Asset Classification Policy #107-004-050

1.1.12 Special Access Privileges: Procedures shall 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 shall include:

- 1.1.12.1. Specifying and documenting the purpose and acceptable use of special access privileges.
- 1.1.12.2. Management approval for granting special access privileges.
- 1.1.12.3. Requiring different accounts or different authentication tokens than those used with the individual's regular user account.
- 1.1.12.4. Specifying and documenting a procedure to remove special access privileges.

1.2. Authentication Recommended Best Practices:

- 1.2.1 Passphrases may be used in lieu of passwords. A passphrase is similar to a password in usage, but is significantly longer for added security, fourteen characters minimum.
- 1.2.2 For additional password and passphrase security, it is recommended that agencies follow NIST Special Publication 800-63 Electronic Authentication Guideline.
- 1.2.3 Users of state information systems should be trained to not reuse their state account passwords for any other purpose.
- 1.2.4 Passwords should be composed of a variety of letters (upper and lower case), numbers and symbols³.
- 1.2.5 For secured access to information systems and applications, passwords should be of a length consistent with the classification level of the information contained within.
- 1.2.6 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.

1.3. Authorization Standards:

- 1.3.1 Assignment of privileges/access to individuals shall be based on job classification and function (role based). Individual unique identity shall map to one or more identified roles.
- 1.3.2 Access to objects by default shall be restricted via an access control mechanism. Access shall be specifically granted to provide explicit access to objects within any information system. Access shall be reviewed and modified in accordance with security policies prior to production deployment⁴.
- 1.3.3 Authorization shall be removed immediately upon departure or change in employee job duties.
- 1.3.4 Administrative rights to information systems shall be tied to identified unique individuals. Administrative rights shall be limited to only staff whose duties require it.

1.4. Authorization Recommended Best Practices:

- 1.4.1 Agencies should identify roles and the appropriate access rights for each role and then assign roles to positions.

³ NIST Special Publication 800-118 Guide to Enterprise Password Management (Draft)

⁴ Identity and Privacy Strategies, Reference Architecture Technical Position, Burton Group.

- 1.4.2 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.⁵

1.5. Audit of Access Control Standards:

- 1.5.1 All information systems shall support logging of access including logins to the information system, and granted and denied access to resources in accordance with Log Management Standards Section 3.9.
- 1.5.2 Information systems containing level 4⁶ data shall log all view, add, modify and delete of information and all failed attempts to perform these actions. Access logs shall be monitored for access control violations daily and reviewed in detail as necessary.
- 1.5.3 Information systems shall be reviewed at least every 90 days for inactive accounts⁷.
- 1.5.4 Audit logs shall be tamper-resistant. In all cases, access to the logs shall be limited only to those with a need to access.

⁵ Identity and Privacy Strategies, Reference Architecture Technical Position, Burton Group
⁶ Statewide Information Asset Classification Policy #107-004-050
⁷ NIST 800-53, PCI Standard

2. Information Asset Management

The goal of information asset management is that information assets are identified, properly classified, protected throughout their lifecycles and that all assets have a nominated owner. Owners shall be identified for all assets and the responsibility for the maintenance of controls shall be assigned. Levels of protection of information are driven by classification level. Information, like other assets, shall be properly managed from its creation to disposal. As with other assets, not all information has the same value or importance to the agency and therefore information requires different levels of protection. Information asset classification and data management are critical to ensure that the state's information assets have a level of protection corresponding to the sensitivity and value of the information asset. The classification of information is governed by the Information Asset Classification Policy # 107-004-050.

All electronically stored assets, regardless of classification level, must be protected from unauthorized access to the information that could affect its confidentiality, availability or integrity⁸. For example, a publicly available Level 1 "Published" web site must still be protected from unauthorized access that could result in hacking or disruption of the information or availability of the information. Therefore, even information systems handling only Level 1 and Level 2 information will comply with the minimum-security standards identified in this document.

The standards identified below are for handling and transmitting information based on the classification level of the information.

2.1. Protection of Information Assets Standards:

- 2.1.1 **Level 1:** Access control shall be in place to prevent unauthorized changes. Access logging shall be in place to identify what was changed and who changed it in accordance with the Access Control standards in section 1.
- 2.1.2 **Level 2:** All Level 1 standards apply. Access control shall be in place to prevent unauthorized viewing. Access logging shall be in place to identify unauthorized attempts.
- 2.1.3 **Level 3:** All level 2 standards apply. Information shall be encrypted at rest and in transit in accordance with the Encryption Standards in section 4.4. Alternatively, information shall be housed in a secured facility behind a minimum of two constantly locked sets of doors. A documented, authorized person shall grant access to Level 3 information. Self-service authorization is never permissible. Electronic information shall be encrypted before removing from the secured facility. Electronic information shall not be sent via unencrypted e-mail. Disposal of media storing Level 3 data shall be sanitized in accordance with the Sustainable Acquisition and Disposal of Electronic Equipment (e-Waste/Recovery) Policy #107-009-0050. Agencies may elect to destroy media rather than sanitize.
- 2.1.4 **Level 4:** All Level 3 standards apply. A log review process is mandatory. Information shall be removed from the secure location within a facility only with documented authorization and tracking. Two-factor authentication for access is required in accordance with the Access Control standards in Section 1.

2.2. Handling of Information Assets Standards:

- 2.2.1 **Level 1:** Level 1 information stored on electronic media shall be protected from unauthorized changes to, or deletion of, the original "published" document.
- 2.2.2 **Level 2:** All Level 1 standards apply. Information stored on paper shall not be left unattended in open or public areas.

⁸ Statewide Information Asset Classification Policy #107-004-050

- 2.2.3 **Level 3:** All Level 2 standards apply. Information stored on paper shall be maintained in locked file cabinets or in a locked room with access restricted to only those individuals who have a business need to access and utilize the information. Information shall not be left unattended on desktops and shall be locked away at the end of each business day.
- 2.2.3.1. Information transmitted verbally shall be communicated only between those people with a business need to know the information. Processes for protecting verbal communications shall include, but not be limited to, closing doors, lowering voices, checking the surrounding areas for people who may overhear sensitive information, and not leaving information on voice mail systems. Information shall not be discussed on speakerphones or other electronic media during conference calls unless: All authorized parties participating in the call have been authenticated, all authorized participating parties have previously verified that no unauthorized persons are in such proximity that they might overhear the conversation, the conference call is made in an area of the building that is secure (i.e. offices or conference rooms where the door can be closed and conversations cannot be overheard through thin walls.), and all parties involved shall openly identified⁹
- 2.2.4 **Level 4:** All Level 3 standards apply. Level 4 information stored on paper shall be maintained in locked file cabinets and in a locked room with access restricted to only those individuals who have a business need to access and utilize the information. Access to Level 4 information stored on paper shall be logged each time it is accessed. Level 4 information shall not be left unattended on desktops and shall be locked away immediately after use.

3. Communications & Operations Management

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

3.1. Antivirus and Anti-malware Standards:

- 3.1.1 All workstations and Windows based servers shall have antivirus/anti-malware software installed upon them.
- 3.1.2 All information systems with antivirus software shall undergo at a minimum a monthly full system scan for viruses and malware.
- 3.1.3 Any information system with a virus, Trojan, etc. shall be removed from the network, and handled in accordance with incident response procedures.
- 3.1.4 Where technically possible, portable devices shall also have antivirus protection.
- 3.1.5 Where technically possible, antivirus/anti-malware software shall be centrally managed with ongoing updates and reporting.
- 3.1.6 Antivirus/anti-malware software shall be maintained at current patch level in accordance with the Patch Management Standards in section 4.6.
- 3.1.7 All antivirus/anti-malware signatures shall be updated and maintained at current vendor supported and recommended levels.

⁹ ISO 27002 10.8.1 Information exchange policies and procedures & 10.8.5 Business information systems

- 3.1.8 End users shall not be able to disable the antivirus/anti-malware software on their workstation or portable device.
- 3.1.9 All e-mail shall be scanned at the e-mail gateway and upon arrival at the workstation. Infected e-mail messages shall be isolated and remediated.

3.2. Antivirus & Anti-malware Recommended Best Practices:

- 3.2.1 Anti-malware solutions for workstations should be integrated with web browsing to scan for malicious web sites during browsing.
- 3.2.2 Monthly scans required in the Antivirus and Anti-malware Standards in section 3.1 should be scheduled to occur automatically.

3.3. Workstation Management & Desktop Security Standards:

- 3.3.1 All workstations shall be patched according to patch management standards identified in accordance with Patch Management standards in section 4.6.
- 3.3.2 Workstations shall use encryption in accordance with the level of asset stored on the machine and as identified in the Asset Management and Encryption sections of this document.
- 3.3.3 Workstations shall be protected with anti-virus software to protect the machine against malware in accordance with Antivirus and Anti-malware Standards in section 3.1.
- 3.3.4 End users shall not have administrative rights access to their workstations in accordance with the Access Control Standards in section 1.
- 3.3.5 By default, workstations shall not be configured to support peer to peer networking. A specific business use must be identified and approved by management before enabling this technology.
- 3.3.6 By default all network services on workstations shall be disabled unless there is a business reason to enable them.
- 3.3.7 Each workstation shall have a firewall installed and configured. It is acceptable to utilize the firewalls that come packaged with specific operating systems.
- 3.3.8 Workstations firewalls shall be configured to default deny.
- 3.3.9 Workstations shall not have a deprecated (unsupported by vendor) operating systems or applications installed.
- 3.3.10 Workstations shall only have authorized applications installed on them.
- 3.3.11 Procedures shall be established and followed to approve attachment of peripheral devices to the workstation; only approved devices shall be attached.

3.4. Workstation Management & Desktop Security Best Practice:

- 3.4.1 Where possible, files shall be stored to a network shared drive, not to local drives. When files are stored on local drives for offsite work, they shall be transferred to the network shared drive upon return to the office.

3.5. Mobile Device Management Standards:

- 3.5.1 Agencies that choose to allow employees to connect personally owned portable devices (cameras, I-phones, USB drives, etc) to agency owned equipment shall provide an exception and approval process by which the agency grants and documents approval to attach the equipment.
- 3.5.2 Agencies shall instruct employees not to put Level 3 and Level 4¹⁰ data on a personally owned portable device.
- 3.5.3 Information stored on portable devices shall be protected in a way commensurate with the classification of the information and in accordance with the Protection of Information Assets Standards in section 2.1.
- 3.5.4 Equipment, information or software shall not be taken off-site without prior authorization.
- 3.5.5 Information shall be transported on mobile devices only in accordance with the statewide Transporting Information Assets (107-004-100) and Controlling Portable and Removable Storage Devices (107-004-051) policies.
- 3.5.6 Where technically possible, security mechanisms on mobile devices shall 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 Standards in section 1.1.
- 3.5.7 Mobile devices shall not be left unattended in uncontrolled access areas.
- 3.5.8 Processes shall be established to provide for appropriate disposal or reuse of personally owned equipment used for state business.
- 3.5.9 Storage devices such as hard disk drives and other media (tapes, diskettes, CDs, DVDs, Personal Digital Assistant (PDAs), Smartphone, or other devices that store information) containing sensitive information shall be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information. For disposal of electronic equipment, refer to the Statewide Policy 107-009-0050 on Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy).

3.6. Mobile Device Management Recommended Best Practices:

- 3.6.1 Only state owned mobile devices should be connected to state owned computing equipment.
- 3.6.2 Where possible, agencies should utilize processes to either identify or prevent unauthorized use of unapproved portable devices.
- 3.6.3 Where possible, lock-down cables should be used on portable devices even in access-controlled areas.

3.7. Server Management Standards:

- 3.7.1 All servers shall be configured so that end users shall not have administrative rights access to servers in accordance with the Access Control Standards in section 1. Server administrators shall use named user accounts that tie actions back to a specific individual for performing administrative work. Generic name and shared accounts shall not be used.
- 3.7.2 Where technically possible all default accounts (guest, admin, etc) on servers shall be disabled.

¹⁰ Statewide Information Asset Classification Policy #107-004-050

- 3.7.3 Where technically possible each server shall have a firewall installed and configured to block unneeded ports. It is acceptable to utilize the firewalls that come packaged with specific operating systems.
- 3.7.4 Servers with deprecated (unsupported by vendor or open source community) operating systems or applications installed shall be remediated with documented controls or removed from production.
- 3.7.5 Servers shall be configured to run only required services. All unnecessary services shall be disabled.
- 3.7.6 Servers shall only have applications installed that are approved and authorized by the server owner.
- 3.7.7 There shall be established procedures for approving or denying the attachment of peripheral devices to the server.
- 3.7.8 Servers shall be set up to log security events that occur on the server. Logs shall 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 Standards in section 3.9.
- 3.7.9 Servers shall be synchronized with one or more network time device(s).
- 3.7.10 The following additional standards shall be applied to server management:
 - 3.7.10.1. Antivirus and Anti-malware Standards section 3.1
 - 3.7.10.2. Information Backup Standard section 3.11
 - 3.7.10.3. Security Zone and Network Security Management (local Area Network and Wide Area Network Standards section 3.13
 - 3.7.10.4. Remote Access Standards section 3.19
 - 3.7.10.5. Encryption Standards section 4.4.
 - 3.7.10.6. Patch Management Standards section 4.6

3.8. Server Management Recommended Best Practices:

- 3.8.1 Configuration management and monitoring tools should be used to identify unapproved changes to server configuration files.
- 3.8.2 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 (local Area Network and Wide Area Network Standards in section 3.13

3.9. Log Management Standards:

- 3.9.1 Log data from servers, network components (firewalls, switches, routers, etc.) and other devices/services shall be ongoing. Events shall be logged as they occur. Log data shall be collected in its original form whenever technically possible but may also be collected in a normalized format for log aggregation.
- 3.9.2 Logs shall 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.

- 3.9.3 Access to log files shall be controlled in accordance with the Access Control Standards in section 1.
- 3.9.4 Logs shall be regularly reviewed and analyzed for indications of unauthorized or unusual activity. Suspicious activity shall be investigated, findings reported to appropriate management, and necessary follow-up actions taken.
- 3.9.5 Log data shall, by default, be considered Level 3 until Level 3 information has been removed for public disclosure. If logs contain personally identifiable information (PII) as defined in ORS 646A 600 and in any applicable federal or industry regulations (HIPAA, FERPA, etc), privacy of the log information shall be protected in accordance with the most restrictive applicable regulations and laws.
- 3.9.6 Logs shall be retained in accordance with the state retention requirements for the information and information systems they are logging. Where no specific retention rules apply, logs shall be kept for six months to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Logs pertaining to ongoing information security incidents shall be preserved as long as necessary to complete and close the investigations.

3.10. Log Management Recommended Best Practices:

- 3.10.1 Log data should be collected to a centralized system with restricted physical and logical access.
- 3.10.2 Automated mechanisms should be used to integrate monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
- 3.10.3 Events not requiring immediate action should be identified and reviewed within 30 days.
- 3.10.4 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.
- 3.10.5 Critical security logs should be segregated from other log information with access restricted to security review personnel.

3.11. Information Backup Standards

- 3.11.1 Information systems and the classification levels of the data stored upon them, time-criticality of business processes, business continuity plans, legal, regulatory, contractual obligations and retention requirements shall be analyzed to determine the frequency with which backups need to be made, the backup media types, and encryption requirements. The analysis process shall define a backup cycle and document it as well as determining backup media selection and backup encryption methods in accordance with the Encryption Standards Section 4.4 and the requirements in the State Information Security Plan section 6.0.
- 3.11.2 Backups shall be tested to ensure information can be restored and to identify restoration constraints.
- 3.11.3 Copies of mission-critical data identified in business continuity and disaster recovery plans shall be stored in a secured, offsite location. If backups are stored offsite using a third-party vendor, vendor practices shall comply with state policies on data protection and shall meet these standards.

- 3.11.4 Access to backups of mission critical data shall be limited to personnel authorized to handle the most sensitive data being backed up.
- 3.11.5 Backups shall be clearly and consistently labeled to facilitate restoration and testing and to guard against mishandling, loss, or accidental overwriting.
- 3.11.6 Media shall be stored in compliance with manufacturer's storage requirements.

3.12. Information Backup Recommended Best Practice:

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

3.13. Security Zone and Network Security Management (Local Area Network & Wide Area Network) Standards:

- 3.13.1 A business needs analysis shall be conducted to determine what network traffic is required for each information system.
- 3.13.2 Firewalls shall allow only explicitly approved network traffic.
- 3.13.3 Internal state information systems and data shall be separated from the public Internet through the use of a perimeter firewall.
- 3.13.4 Internal security zones shall be established to segregate network traffic with differing security requirements from each other. These zones shall segregate trusted local workstation networks from restricted server networks. Public facing web applications shall segregate those applications within a DMZ zone. Servers containing level 3 or level 4¹¹ data shall be located within a restricted zone.
- 3.13.5 Network equipment (firewalls, MPLS, VLANs, hubs, switches, routers, wireless access points) shall be managed to ensure that security zones are maintained.
- 3.13.6 By default all hardware switch ports shall be turned off unless physical access is controlled to both endpoints of the physical connection.
- 3.13.7 DHCP address assignments shall be logged.
- 3.13.8 Virtual separation mechanisms (eg. VM and VLAN) shall 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.
- 3.13.9 The following standards areas also apply to security zone management:
 - 3.13.9.1. Log Management Standards in section 3.9
 - 3.13.9.2. Remote Access Standards in section 3.19

3.14. Security Zone and Network Security Management (Local Area Network & Wide Area Network) Recommended Best Practices:

- 3.14.1 Security zones should be consistently managed and documentation of information exchanges between agencies and business partners should be in place.
- 3.14.2 Data for applications located in a DMZ zone should be segregated and stored within a protected security zone.
- 3.14.3 Network hubs should be avoided for network extension, switches should be used instead.

¹¹ Statewide Information Asset Classification Policy #107-004-050

- 3.14.4 Critical security control devices should be segregated from the rest of the network.
- 3.14.5 Non-encrypted protocols such as SNMPv1 or SNMPv2 should not be used. SNMPv3 or SSL/TLS should be used for management of access points.
- 3.14.6 Physical separation of security zones should be maintained. Virtual separation mechanisms (eg. VM and VLAN) may be used for segregating sub-zones within a security zone.

3.15. Intrusion Detection Standards:

- 3.15.1 IDS shall be deployed to monitor external network traffic.
- 3.15.2 Intrusion detection signatures shall be updated and maintained at current vendor supported levels.
- 3.15.3 IDS shall perform packet and protocol analysis.
- 3.15.4 IDS shall perform fragmented and packet stream reassembly.
- 3.15.5 IDS shall detect attacks in real time to provide timely alerts and notification.
- 3.15.6 Logs shall be maintained and reviewed in accordance with the Log Management Standards in section 3.9.
- 3.15.7 Evidence and alerts of intrusion shall be handled in accordance with incident response plans and the statewide incident response policy. Incident response plan/procedure shall include response to IDS alerts.
- 3.15.8 IDS shall be monitored by appropriately trained staff.

3.16. Intrusion Prevention Systems Recommended Best Practices:

- 3.16.1 IDS should be deployed to monitor internal network traffic.
- 3.16.2 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.
- 3.16.3 Behavioral based IPS should be used to block attacks that are only detectable because of changes in the normal operational state.

3.17. E-mail Standards:

- 3.17.1 Virus and spam filtering shall be implemented on email gateways in accordance with the Antivirus and Anti-malware Standard in section 3.1.
- 3.17.2 Level 3 or Level 4¹² electronic data shall not be sent via unencrypted e-mail
- 3.17.3 Copies of e-mail shall be retained in accordance with data retention schedules.
- 3.17.4 E-mail servers shall be secured in accordance with the Server Management Standards in section 3.7
- 3.17.5 E-mail accounts shall be connected to individual users. Where a group e-mail account exists, primary ownership of and responsibility for that account shall be assigned to an individual.
- 3.17.6 Access controls shall be implemented to maintain integrity and confidentiality in accordance with the Access Standards in section 1.

¹² Statewide Information Asset Classification Policy #107-004-050

- 3.17.7 Privileged-user access shall be audited in accordance with the Audit of Access Control Standards in section 1.

3.18. E-mail Recommended Best Practices:

- 3.18.1 E-mail systems should be monitored for data leakage.
- 3.18.2 E-mail systems should facilitate eDiscovery processes.

3.19. Remote Access Standards:

- 3.19.1 All remote access methods shall support authentication of unique users in accordance with the Authentication Standards in section 1.1.
- 3.19.2 At no time shall any remote access user provide their password to anyone in accordance with the Authentication Standards in section 1.1.
- 3.19.3 At no time shall any remote access user allow another person to use their remote connection.
- 3.19.4 All remote access approvals shall be documented, including purpose, conditions, duration and approved methods.
- 3.19.5 Split tunneling or dual homing shall 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 shall only be permitted if the remote network is under the complete control of the connecting person.
- 3.19.6 All computers that are connected directly to an agency's internal networks via remote access technologies shall use the most up-to-date ant-virus software and operating system and application patches.
- 3.19.7 Personal equipment that is used to connect to the agency's networks shall meet the security requirements of agency-owned equipment for remote access.
- 3.19.8 Remote access rights shall be terminated immediately upon the departure of an employee or if their duties no longer require remote access.
- 3.19.9 State employees accessing agency or state networks to perform technical administration of servers or network equipment shall use state owned equipment.
- 3.19.10 Contracts with third parties such as vendors, partners, and contractors requiring remote access shall specify security requirements for connectivity. Third party equipment used to connect to an agency's networks shall meet the requirements of agency-owned equipment for remote access. Remote access shall 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.

3.20. Remote Access Recommended Best Practices:

- 3.20.1 Equipment not owned and supported by a State of Oregon agency should not be connected via remote access technologies to the state network or agency resources.
- 3.20.2 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.
- 3.20.3 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.

- 3.20.4 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.
- 3.20.5 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.

3.21. Wireless Access Standards:

- 3.21.1 Industry supported wireless access standards 802.11 shall be used by wireless access points.
- 3.21.2 The decision of whether, and how, guest access will be allowed shall be documented. Guest access via a wireless entry point shall be configured to only allow Internet access but prevent access to internal network resources.
- 3.21.3 For non-guest access the Wireless Protected Access2 (WPA2) protocol with AES encryption shall be deployed for data encryption to further protect transmitted information. Current versions of IEEE standards are 802.11, 802.11a, 802.11b, 802.11e, 802.11g, 802.11i and 802.11n.
- 3.21.4 Comprehensive security assessments and inventory of wireless access shall be performed at regular and random intervals. Assessments shall include validating that unauthorized access points do not exist in the agency and testing the boundaries of wireless access.
- 3.21.5 Data shall be encrypted in transit in accordance with the Encryption Standards in section 4.4.
- 3.21.6 Access points shall be placed in physically secure or hidden areas to prevent unauthorized physical access and user manipulation.
- 3.21.7 Non-default SSID shall be used for wireless networks. SSIDs shall not reveal information about the network, agency name or location.
- 3.21.8 Nonessential management protocols shall be disabled on access points.
- 3.21.9 The "ad hoc mode" for 802.11 on wireless clients shall be disabled when technically possible.
- 3.21.10 Administrative access to manage the wireless device shall only be enabled via a dedicated wired management VLAN. Access to administrative functions shall be disabled via the wireless interface.
- 3.21.11 If the access point supports logging, turn it on and review the logs on a regular basis in accordance with the Log Management Standards in section 3.9.

3.22. Wireless Access Recommended Best Practices:

- 3.22.1 External boundary protection should be implemented around the physical perimeter of buildings containing access points. These protections include locating access points interior walls and, wherever possible, using enterprise class systems that use controller based AP configuration management.
- 3.22.2 Guest access should be restricted such that only authorized guests have access.
- 3.22.3 A firewall should be placed between the wired infrastructure and the wireless network in accordance with the Security Zone and Network Security Management (Local Area Network and Wide Area Network Standards in section 3.13

4. 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 in ORS 182.122 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.” This section describes security standards and best practices for Emerging Technologies, Business Cases, Encryption, Patch Management, and Information Systems Development Lifecycle.

4.1. Emerging Technologies Recommended Best Practices:

- 4.1.1 Agencies using or considering Voice Over IP (VOIP) for telephone service should review the [NIST Special Publication 800-58 Security Considerations for Voice Over IP Systems](#)
- 4.1.2 Agencies using or considering using a cloud computing environment should review the NIST Presentation on [Effectively and Securely Using the Cloud Computing Paradigm](#)

4.2. Business Case Standard:

- 4.2.1 A business case shall be developed for system development and implementation projects over \$500k per Department of Administrative Services IT Investment and Review (IRR) requirements.

4.3. Business Case Recommended Best Practices:

- 4.3.1 A business case should be completed to justify custom information system development projects.
- 4.3.2 For general requirements and guidelines regarding acquisition of IT goods and services and the IT Investment Review and Approval process please go to: <http://www.oregon.gov/DAS/EISPD/IRR.html>.

4.4.

Encryption Standards:

- 4.4.1 In all cases where encryption is used, encryption protocol and strength shall be Advanced Encryption Standard (AES) 128-bit or stronger. If AES 128-bit is not technically possible, triple DES (3DES) shall be used until AES 128-bit or stronger is available.
- 4.4.2 Backup and archive copies of Level 3 and Level 4 information shall be encrypted. Encryption of Level 3 and Level 4 information shall be at the storage media level, at the database level, or at the application level (see standards below). Encrypted backup and archive media shall support data restoration and disaster recovery and support various backup media types used by the state.
- 4.4.3 Encryption shall 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.
- 4.4.4 Encryption for USB flash-drives and hard drives shall either use password and encryption capabilities built into the device or shall be encrypted using host-based encryption software at the time data is stored on the device.
- 4.4.5 All information Levels 1-4 transmitted in accordance with the Wireless Access Standards in section 3.21.

- 4.4.6 Key management or escrow processes shall be used when using a key-based data encryption system.
- 4.4.7 Encryption keys suspected of having been compromised shall be replaced immediately.

4.5. Encryption Recommended Best Practices:

- 4.5.1 Level 3 and Level 4¹³ data should be encrypted using AES 256-bit or stronger encryption
- 4.5.2 Backup and archive media encryption should integrate seamlessly with backup processes and devices.
- 4.5.3 NIST recommendations in [Storage Encryption Technologies for End User Devices NIST sp800-111](#) should be reviewed and used where applicable
- 4.5.4 Encryption keys should not be used to encrypt data across multiple systems, storage devices, etc.
- 4.5.5 Periodic cryptographic key changes and retirement of old keys (for example: archiving, destruction, and revocation as applicable) should be practiced.
- 4.5.6 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.
- 4.5.7 NIST document [Key Derivation Using Pseudorandom Functions NIST sp800-108](#) should be reviewed for more information on encryption keys and key management.
- 4.5.8 NIST document [Using Approved Hash Algorithms NIST sp800-107](#) should be reviewed for more information on encryption algorithms and key strength.

4.6. Patch Management Standards:

- 4.6.1 All operating systems and commercial off-the-shelf/open source software shall be patched and maintained at current vendor supported levels unless there is a documented business reason for not applying a specific patch.
- 4.6.2 Agencies shall immediately 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.
- 4.6.3 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 shall be remediated with documented controls or removed from production.
- 4.6.4 Wherever possible, automated patching systems shall be implemented to automatically update operating systems and applications.
- 4.6.5 Automated patching systems shall log which information systems have received the patches and audit for information systems that have been missed.
- 4.6.6 An application update management process shall be implemented to ensure the most up-to-date approved patches and application updates are installed for all software.
- 4.6.7 Custom developed applications shall be tested on a defined schedule for vulnerabilities and updated to correct identified vulnerabilities.
- 4.6.8 If no patch is available, other controls shall be implemented, such as turning off services or capabilities related to the vulnerability; adapting or adding access controls, e.g.

¹³

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.¹⁴

4.7. Patch Management Recommended Best Practice:

- 4.7.1 Security patches should be applied immediately after appropriate testing or within 72 hours.

4.8. Information System Development Lifecycle Standards:

- 4.8.1 Access to operating system, source code, and operational or production application software/program directories, locations, and configuration files shall be managed, limiting access to authorized individuals.
- 4.8.2 When developing or modifying information systems, a change control management process shall be used to require authorization to initiate or make changes to the system, test and accept the changes, and move changes into production.
- 4.8.3 New or updated information system shall 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.
- 4.8.4 Procurement of information systems designed to store, access or in any way handle information classified at level 3 or level 4¹⁵ shall include requirements that information located on or transferred to or from these systems can be encrypted in accordance with the Encryption Standards in section 4.4.

4.9. Information System Development Life Cycle Recommended Best Practices:

- 4.9.1 Separate development, test and production environments should be used to protect production systems from development work and testing.
- 4.9.2 Segregation 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.
- 4.9.3 The early steps in the SDLC process through implementation are closely tied to the stages of project management as outlined in the Project Management Book of Knowledge (PMBOK), the state of Oregon's designated approach to project management. Key tasks should be considered for each step of the Information Security SDLC as defined by the National Institute of Standards and Technology (NIST) in the SDLC web site and brochure (<http://csrc.nist.gov/groups/SMA/sdlc/index.html>).

¹⁴ ISO 12.6.1

¹⁵ Statewide Information Asset Classification Policy #107-004-050

5. Approval

By: _____
Scott Harra, Director, DAS

Date

By: _____
Dugan Petty, State Chief Information Officer, DAS

Date

By: _____
Theresa Masse, State Chief Information Security Officer, DAS

Date