State of Maine
Department of Administrative and Financial Services
Office of Information Technology (OIT)

Configuration Management Policy and Procedures (CM-1)

Table of Contents

1.0. Purpose

This document outlines the State of Maine (SOM) Office of Information Technology (OIT) Policy and Procedures for ensuring appropriate configuration methods are applied in maintaining SOM information assets (see Definitions). This document corresponds to the Configuration Management[1] Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0. Scope

2.1. This document applies to

- 2.1.1. All SOM personnel, both employees and contractors;
- 2.1.2. Executive Branch Agency information assets, irrespective of location; and
- 2.1.3. Information assets from other State government branches that use Executive Branch managed services.

3.0. Conflict

If this document conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Roles and Responsibilities

4.1. Agency Business Partners

- 4.1.1. In collaboration with OIT Information Asset Owners and I.T. Procurement, hold contracted other parties that host State information assets accountable to this Policy and Procedures.
- 4.1.2. Develop and implement Agency-level policy and procedures to meet any additional statutory requirements or Agency-specific controls.

4.2. OIT Change Advisory Board Chairs

- 4.2.1. Develops, maintains, and enforces requirements of Configuration Management, in alignment with the Change Management Policy.[2]

4.3. OIT Client Technology Services

- 4.3.1. Uses a configuration manager to enforce software standards for end points.
- 4.3.2. Provides customer support for the installation of approved applications on end-user devices.

4.4. OIT Enterprise Architecture and Policy

- 4.4.1. Develops and maintains a list of approved technologies for use by the State Executive Branch and the State wide area network.

[1] https://nvd.nist.gov/800-53/Rev4/family/Configuration%20Management
[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf

4.5. OIT Information Asset Owners
- 4.5.1. Comply with this Policy and Procedures in regard to configuration management.
- 4.5.2. In collaboration with Agency Business Partners and I.T. Procurement, hold contracted other parties that host State information assets accountable to this Policy and Procedures.

4.6. I.T. Procurement
- 4.6.1. In collaboration with Agency Business Partners and Information Asset Owners, hold contracted other parties that host State information assets accountable to this Policy and Procedures.

4.7. OIT Information Security Office
- 4.7.1. Owns, executes, and enforces this Policy and Procedures.
- 4.7.2. Provides oversight of the security functions of the State's Security Information and Event Management system.

4.8. OIT Network Services
- 4.8.1. Enforces controls of network infrastructure devices connecting to State resources.

4.9. OIT Computing and Infrastructure Services
- 4.9.1. Maintains a workflow for managing trusted PKI certificates.

5.0. Management Commitment

The State of Maine is committed to following this Policy and Procedures.

6.0. Coordination Among Agency Entities

The various divisions within OIT, as well as the Agency Business Partners, will cooperate with OIT in executing this Policy and Procedures. OIT handles most of the security control requirements of this Policy as part of its Change Management processes. Configuration Management is attained through effective, risk-based, Change Management processes, in conjunction with continuous monitoring by the Information Security Office, and other divisions within OIT.

7.0. Compliance

7.1. For State of Maine employees, failure to comply with this document may result in progressive discipline, up to and including dismissal.

7.2. For State of Maine contractors and non-State of Maine personnel, failure to comply may result in removal of the individual's ability to access, and use, State of Maine data and systems. Employers of contractors will be notified of any violations.

7.3. Personnel are also subject to any applicable penalties for statutory requirements compliance violations. Depending on the requirement, and the nature of the violation, penalties could include fines and/or criminal charges.

8.0. Procedures

8.1. Baseline Configuration (CM-2)

8.1.1. OIT Information Asset Owners develop, document, and maintain a current baseline configuration of the information systems under their purview. Baseline configurations serve as a basis for all builds, releases, and/or changes to information systems. Maintaining baseline configurations requires creating new baselines as information systems change over time. To the maximum extent possible, baseline configurations are dictated by standards bodies (such as, the CIS Benchmarks,[3] IRS Safeguards Benchmarks,[4] etc.), or by trusted product vendors (such as, Microsoft, Oracle, etc.).

8.1.2. Any consumer device with an operating system seeking to attach to the State wide area network must meet the following minimum criteria:

8.1.2.1. Supported operating systems: Windows, Android, iOS, Chrome OS, MacOS;

8.1.2.2. All critical operating system and Security patches have been applied within the previous 30 calendar days;

8.1.2.3. Have an anti-malware listed in the Leaders quadrant of the latest Gartner Magic Quadrant for Endpoint Protection Platforms (EPP), and *not* blacklisted by any arm of the U.S. Federal Government; and

8.1.2.3. The anti-malware data file updated within the previous 15 calendar days.

8.1.3. Network Services uses various network administration products to enforce controls of devices on the network as directed by the Chief Information Security Officer.

8.1.3.1. For any device connected to the State wide area network, OIT must have at least read-only access.

8.1.3.2. Any device connected to the wide area network may be quarantined, and/or disconnected, and/or impounded, for any reason, including, but not limited to: Potential Malware, device type and configuration not in alignment with OIT standards, adverse impact to the network, excessive bandwidth utilization, or non-payment of OIT Network charges, etc.

8.1.4. **Baseline Configuration Reviews and Updates (CM-2(1)):** OIT Information Asset Owners review, and update, the baseline configuration of information systems as an integral part of information system component installation and upgrades. This review is undertaken at least once every calendar year, as well as when configuration changes are made due to critical security patches, upgrades, and emergency changes (e.g., unscheduled changes, system crashes, and replacements of critical components). Any and all security

[3] https://www.cisecurity.org/cis-benchmarks/
[4] https://www.irs.gov/privacy-disclosure/safeguards-program

patching and emergency changes are subject to the Change Management Policy.[5] All major changes are subject to either the Application Deployment Certification Policy,[6] or the Infrastructure Deployment Certification Policy.[7]

8.1.5. **Baseline Configuration Retention of Previous Configurations (CM-2(3)):** As part of standard Change Management, OIT Information Asset Owners retain at least one previous stable version of the baseline configuration of all information systems to support rollback.

8.1.6. **Baseline Configuration for Development and Test Environments (CM-2(6)):** OIT Information Asset Owners maintain baseline configurations of development and test environments, that are managed separately from the operational (production) baseline configurations.

8.1.7. **Baseline Configurations for Systems, Components, or Devices for High-Risk Areas (CM-2(7)):**

8.1.7.1. OIT Managers refer to travel guidance set by the U.S. Secretary of State and consult with the Information Security Office, prior to approving work outside the United States by any OIT personnel or contractor. Agencies should establish similar controls.

8.1.7.2. When agency personnel travel, and/or engage in remote work, abroad, especially high-risk areas, OIT issues extra-hardened (more stringent configuration settings (see Definitions)), and stripped-down devices (notebooks and phones) to such agency personnel. These devices do *not* have any app that is not, strictly speaking, relevant to the mission at hand.

8.1.7.3. Upon personnel's return to Maine, these devices (i.e., notebooks and phones) are reset to factory defaults before being returned to the OIT device fleet.

8.2. **Configuration Change Control (CM-3)**

8.2.1. Any changes to the baseline configuration is undertaken strictly according to the Change Management Policy.[8] This involves the systematic proposal, justification, implementation, testing, review, and disposition of changes, including system upgrades and modifications. This also includes emergency changes to remediate suddenly-discovered vulnerabilities. The Change Advisory Board must approve all changes, without exception. Auditing of changes includes activities before and after changes are made, and the actual steps required to implement such changes.

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf
[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ApplicationDeploymentCertification.pdf
[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/Infrastructure-Deployment-Certification.pdf
[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf

8.2.2. Any configuration change proposal is explicitly reviewed for its security impact, as well as its potential impact to end-users.

8.2.3. For any information asset, all configuration change decisioning, as well as the implementation details, are documented, and the resulting audit trail is retained for as long as OIT remains invested in that information asset.

8.2.4. Change Management logs are available for review reactively as part of any troubleshooting, and incident response/management.

8.2.5. Coordination and oversight of the configuration change control is provided by the Change Advisory Board on a weekly basis.

8.2.6. **Automated Notification and Prohibition (CM-3(1)):**

8.2.6.1. All configuration changes are documented in the enterprise ticketing application.

8.2.6.2. For each configuration change, all stakeholders (identified by their email addresses) are explicitly identified in the change ticket, and each of them receives automated notification for every change in the ticket.

8.2.6.3. Any proposed changes that are not yet approved by the Change Advisory Board are clearly flagged as Not-Yet-Approved.

8.2.6.4. No actual configuration change may proceed without the explicit approval of the Change Advisory Board.

8.2.6.5. All relevant details of the proposed change must be documented within the change ticket. This is an essential pre-requisite for approval by the Change Advisory Board.

8.2.6.6. All stakeholders are automatically notified through email when approved changes are completed.

8.2.7. **Test, Validate, Document Changes (CM-3(2)):** OIT Information Asset Owners test, validate, and document changes to information assets before implementing the changes to the operational (production) systems. The burden of initiating, and coordinating, the testing, validation, and documentation rests with the Change Initiator, who represents the Information Asset Owner. Individuals and groups conducting such tests understand and comply with the information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes.

8.2.8. **Automated Change Implementation (CM-3(3)):** To the maximum extent possible, OIT Information Asset Owners employ automated mechanisms to implement changes to the current configuration baselines, and deploy the updated baselines across the enterprise. Such automation tools include Microsoft System Center Configuration Manager, Chef, Puppet, Docker, etc.

8.2.9. **Security Representative (CM-3(4)):** The Information Security Office has a permanent representative on the Change Advisory Board.

8.2.10. **Automated Security Response (CM-3(5)):** Logs are ingested into the enterprise Security Information and Event Manager, and are monitored by a third-party vendor. Suspicious behavior discovered generates an email alert to the Information Security Office. This is a cause for immediate investigation by the Chief Information Security Officer.

8.2.11. **Cryptography Management (CM-3(6)):** There exists a strictly controlled process for generating, tracking, and renewing trusted OIT Public Key Infrastructure (PKI, see Definitions) certificates. This is based upon best practices of the Microsoft Windows Server Active Directory Certificate Services, and is built into the enterprise Active Directory.

8.3. Security Impact Analysis (CM-4)

8.3.1. The Change Advisory Board analyzes changes to the information system to determine potential security impacts prior to change implementation. The standing member of the Information Security Office on the Change Advisory Board conducts security impact analyses. Security impact analyses include, at a minimum, assessments of risk to forecast the impact of the changes, and to determine if additional security controls are necessary. Security impact analyses are scaled in accordance with the security categories of the information systems.

8.3.2. **Separate Test Environments (CM-4(1)):** OIT Information Asset Owners analyze changes to the information system in a separate test environment before implementation in an operational (production) environment. Information Asset Owners probe security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

8.3.3. **Verification of Security Functions (CM-4(2)):** After an information system is changed, OIT Information Asset Owners check the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome to meeting the security requirements for the system. Any anomaly is escalated to the Information Security Office.

8.4. Access Restrictions for Change (CM-5)

8.4.1. OIT defines, documents, approves, and enforces access restrictions associated with configuration changes to information systems, per the Access Control Policy.[9]

[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf

8.4.2. Only authorized system administrators can make configuration changes, including upgrades and modifications.

8.4.3. Detailed records of administrative access are maintained for the lifetime of an information asset. This is to ensure that configuration change control is implemented, and to support after-the-fact actions, should any unauthorized changes be discovered.

8.4.4. **Automated Access Enforcement and Auditing (CM-5(1)):** OIT enforces strict administrative access restrictions and has hired a third-party vendor to conduct log analysis in the Security Information and Event Manager. Dashboards can be created in the Security Information and Event Manager to provide on demand reporting as required.

8.4.5. **Review System Changes (CM-5(2)):** The Information Security Office monitors alerts provided by a third-party vendor who monitors the Security Information and Event Manager for suspicious behavior that may be a security concern.

8.4.6. **Signed Components (CM-5(3)):** The OIT Computing Infrastructure and Services division maintains a well-defined workflow for managing trusted PKI certificates. See the Identification and Authentication Policy[10] (Intranet only) for further details. Any information asset managed by OIT explicitly prevents the installation of certain sensitive components without first verifying that the sensitive component has been digitally signed by a trusted PKI certificate. The list of such sensitive components includes device firmware (including the Basic Input Output System and/or the Unified Extensible Firmware Interface), operating system patches and service packs, device drivers, and any security system component (such as anti-malware, remote virtual private network, multifactor authenticator, mobile device manager, etc.).

8.4.6.1 In general, exportation of the PKI private key is prohibited. More specifically, it is universally prohibited for client devices and general users. However, for certain enumerated administrative use cases, it is permitted by exception. For each permitted administrative use case, both the generation and consumption of the exported private key is executed by system administrators. Some of the permitted use cases include:

8.4.6.1.1 As an access token in boot media to provision net-new client devices. Provisioned devices are then issued their own discrete certificates.

8.4.6.1.2 Configuration of web and application servers that utilize a certificate installed on another server; and

[10] http://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf

8.4.6.1.3 Hosting by trusted external partners in the Maine.gov namespace.

8.4.7. **Limit Production/Operational Privileges (CM-5(5)):** Only authorized system administrators can make configuration changes in the production/operational instance. OIT enforces strict administrative access restrictions and implements auditing of said enforcement via log analysis in the Security Information and Event Manager. All OIT Managers (the managers of the various information asset teams) review, and re-evaluate, system administrator privileges at each employee transition, and as part of the annual performance management cadence.

8.4.8. **Limit Library Privileges (CM-5(6)):** Only authorized system administrators can make configuration changes to software resident within software libraries, and source control repositories. All OIT Managers (the managers of the various information asset teams) review, and re-evaluate, system administrator privileges at each employee transition, and as part of the annual performance management cadence.

8.5. **Configuration Settings (CM-6)**

8.5.1. OIT Information Asset Owners establish, document, and implement Common Secure Configurations (see Definitions) for information assets, using either industry standards bodies (such as, the National Institute of Standards and Technology,[11] CIS Benchmarks,[12] IRS Safeguards Benchmarks,[13] etc.), or trusted product vendors (such as Microsoft, Oracle, etc.). The purpose is to arrive at the most restrictive mode consistent with operational requirements.

8.5.2. Any deviation from the established configuration settings must go through an explicit waiver from the Chief Information Security Officer. Approval for such a waiver is contingent upon furnishing a non-trivial business case, and demonstrating suitable compensating controls.

8.5.3. **Respond to Unauthorized Changes (CM-6(2)):** Logs are ingested into the enterprise Security Information and Event Manager, and are monitored by a third-party vendor. Any suspicious behavior detected triggers an email alert to the Information Security Office. This is a cause for immediate investigation by the Chief Information Security Officer. Depending upon the outcome of that investigation, the original configuration settings (i.e., the state prior to the unauthorized changes) may be restored, and/or the affected information asset may be quarantined, and/or the affected information system may be

[11] https://www.nist.gov/
[12] https://www.cisecurity.org/cis-benchmarks/
[13] https://www.irs.gov/privacy-disclosure/safeguards-program

temporarily taken out of service, and/or a potential disciplinary action may be initiated.

8.6. Least Functionality (CM-7)

8.6.1. OIT Information Asset Owners configure information assets to provide only the essential capabilities, commensurate with agency customer business requirements. OIT Information Asset Owners disable functions, ports, protocols, and services not explicitly required for executing agency business customer business requirements.

8.6.2. To the maximum extent feasible under budgetary constraints, information assets are configured and optimized for the narrowest range of functions. Any function not strictly relevant for that narrow purpose is disabled.

8.6.3. As part of setting the baseline configuration (integral part of Deployment Certification, see 8.1.4 above), all information assets undergo a rigorous review with respect to enabled functions and settings. Functions often disabled include Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing, unused or unnecessary physical and logical ports, Universal Serial Bus, Bluetooth, File Transfer Protocol, etc. This ultimately limits unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling.

8.6.4. The Information Security Office, in collaboration with Network Security Services, routinely utilizes network scanning tools, intrusion detection and prevention systems, and end-point protections, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, ports, protocols, and services.

8.6.5. **Periodic Review (CM-7(1)):** The Information Security Office uses Tenable Nessus[14] to audit select information asset configurations as outlined in Vulnerability Scanning Procedure (RA-5).[15] Any non-essential function and service detected by such audits is jointly reviewed between the Information Security Office and the operational division to determine if the baseline configuration could be further tightened (by disabling unnecessary and/or unused functions, ports, protocols, and services). The Chief Information Security Officer provides the final decision.

8.6.6. **Prevent Program Execution (CM-7(2)):** All OIT-managed information assets prevent program execution in accordance with enterprise policies behind the anti-malware agent resident on that information asset.

[14] https://www.tenable.com/products/nessus
[15] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/VulnerablityScanningProcedure.pdf

8.6.7. **Unauthorized Software Blacklisting (CM-7(4)):**

8.6.7.1. OIT Client Technology Services use a configuration manager to check the network to remove software from end points. The configuration manager can be used for continuous monitoring of the network for the existence of unauthorized software.

8.6.7.2. OIT Client Technology Services customer service representatives use a collaboration wiki tool article for guidance on installing software on state-managed computers.

8.6.7.3. The OIT Enterprise Architecture Policy Team uses a new technology onboarding process to approve new software. The OIT Enterprise Architecture Policy Team maintains a list of approved technologies for use on the network.

8.7. **Information System Component Inventory (CM-8)**

8.7.1. OIT Enterprise Data Services maintains an Enterprise Asset Inventory that documents all information assets, both hardware and software. This inventory is kept updated by the various OIT operational teams, as an integral part of managing any change. Reviewing and updating the inventory is pegged to any substantial change in any information asset. The inventory also includes contact names, both technical and business.

8.7.2. For any information asset whose monthly subscription is billed back, there exists a fiscal incentive for the Agency Business Management and the OIT Account Managers to scrutinize the monthly bills, and vet the business needs of information assets on a monthly basis.

8.7.3. **Updates during Installations and Renewals (CM-8(1)):** OIT Information Asset Owners update the Enterprise Asset Inventory as an integral part of component installations, removals, and updates.

8.7.4. **Automated Unauthorized Component Detection (CM-8(3)):** Network Services employs the Cisco Identity Services Engine to detect unauthorized information assets. When unauthorized information assets are detected, access to the State wide area network is disabled from that information asset.

8.7.5. **Accountability Information (CM-8(4)):** The Enterprise Asset Inventory identifies the names and emails of individuals responsible and accountable for administering each of the information assets.

8.7.6. **No Duplicate Accounting of Components (CM-8(5)):** The Enterprise Asset Inventory enforces unique primary key requirements, which prevents duplicate accounting of information assets.

8.7.7. **Centralized Repository (CM-8(7)):** As stated above (8.7.1), OIT maintains a centralized Enterprise Asset Inventory, which documents all information assets, both hardware and software. Each asset includes contact names and emails, both technical and business, in order ensure accountability. This inventory is kept updated by the various OIT operational teams, as an integral part of managing any change.

8.7.8. **Automated Location Tracing (CM-8(8)):** OIT Client Technology Services selectively deploys the Absolute[16] location tracing app on some sensitive devices that reside outside of OIT data centers. For the most part, these are fraud investigator and/or healthcare worker laptops.

8.7.9. **Assignment of Components to Systems (CM-8(9)):** In terms of the granularity of tracking components of information systems, by default, OIT Information Asset Owners track all hardware and software assets that exist on their own, including virtual servers.

8.8. Configuration Management Plan (CM-9)

8.8.1. Each of the OIT Information Asset Owners maintains their own configuration management plans for the information assets under their purview. Such plans explicitly include roles and responsibilities. For instance, there exists a dedicated configuration management team within the OIT Client Technology Services department, which owns, executes, and enforces the configuration of the OIT workstation fleet.

8.8.2. The execution of the actual configuration management, and any changes, strictly follows the Change Management Policy.[17] The configuration management approval process explicitly includes designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems.

8.8.3. Each of the OIT Information Asset Owners explicitly identifies configuration items throughout the system development lifecycles for the information assets under their purview. They define the configuration items for the information system, and place the configuration items under configuration management. While configuration management applies to all stages of the system development lifecycle, it is especially important during the development/acquisition phase. However, as information systems continue through the system development life cycle, new configuration items may be

[16] https://www.absolute.com/
[17] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf

identified, and some existing configuration items may no longer need to be under configuration control.

8.8.4. Each of the OIT Information Asset Owners explicitly protects their configuration plans from unauthorized disclosure and modification.

8.9. Software Usage Restrictions (CM-10)

8.9.1. Within its fleet, OIT Client Technology Services uses software, and associated documentation, in accordance with contract agreements and copyright laws.

8.9.2. OIT Client Technology Services explicitly blocks the usage of peer-to-peer file sharing and any third party cloud storage services on its device fleet (both operating system executable, as well as pure browser apps, across workstations, tablets, and phones) to prevent unauthorized distribution, display, performance, or reproduction of copyrighted work.

8.9.3. Software license tracking is accomplished by a combination of manual and automated methods. This is the responsibility of the OIT Client Technology Services division.

8.9.4. **Open-source Software (CM-10(1)):** Open-source software is allowed on a case-by-case basis, but with the explicit message to the consumers identifying the inherent risks. All of this, and more, is documented in both the System and Services Acquisition Policy,[18] and the User Device and Commodity Application Policy.[19]

8.10. User-Installed Software (CM-11)

8.10.1. End-users do *not* have administrative access to the OIT-issued user devices assigned to them unless there is an agency-defined legitimate business need to do so. Therefore, end-users *cannot* install software that requires administrative access on client devices. However, once a software has been installed, end-users may download some extensions and plug-ins which do *not* require additional administrative access.

8.10.2. Only system administrators can install software on server devices.

8.10.3. Enforcement, and audit, of this provision is executed via continuous, automated monitoring, and ingestion of all systems logs into the enterprise Security Information and Event Manager.

8.10.4. **Alerts for Unauthorized Installations (CM-11(1)):**

[18] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemAndServicesAcquisitionPolicy.pdf
[19] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/UserDeviceCommodityAppPolicy.pdf

8.10.4.1. For OIT-managed phones, unauthorized installation of software is flagged by Lookout,[20] managed by OIT Computing Infrastructure and Services.

8.10.4.2. For OIT-managed servers, unauthorized installation of software is flagged by the Splunk[21] Security Information and Event Manager, managed by the Information Security Office.

9.0. Document Details

9.1. Initial Issue Date: 18 December 2020
9.2. Latest Revision Date: 20 March 2024
9.3. Point of Contact: Enterprise.Architect@Maine.Gov
9.4. Approved By: Chief Information Officer, OIT
9.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[22]
9.6. Waiver Process: Waiver Policy[23]
9.7. Distribution: Internet[24]

10.0. Review

This document will be reviewed triennially, and when substantive changes are made to Policies, Procedures, or other authoritative regulations affecting this document.

11.0. Records Management

Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and Directives* records management categories. They will be retained for three (3) years, and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

12.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA), certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures, or risk assessments. Information contained in these records may be disclosed to the Legislature, or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

[20] https://www.lookout.com/
[21] https://www.splunk.com/
[22] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[23] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/Waiver.pdf
[24] https://www.maine.gov/oit/policies-standards

13.0. Definitions

13.1. *Configuration Settings:* The set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the securityof information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections.

13.2. *Common Secure Configurations:* Also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides, etc. These provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB). The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings.

13.3. *Information Asset:* A discrete, identifiable piece of information technology, including hardware, software, and firmware. Information assets include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), input/output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, sensors), operating systems, virtual machines, middleware, business applications, system software, development tools, and miscellaneous related utilities.

13.4. *PKI (Public Key Infrastructure):* A set of roles, policies, hardware, software, and procedures that manages digital certificates. The purpose of a PKI is to facilitate the secure electronic transfer of information. More specifically, it is an arrangement that binds public keys with respective identities of entities (like people and organizations).

14.0. Abbreviations

14.1. EPP: Endpoint Protection Platforms
14.2. FOAA: Freedom of Access Act
14.3. NIST: National Institute of Standards and Technology
14.4. OIT: Office of Information Technology
14.5. PKI: Public Key Infrastructure
14.6. SCAP: Security Control Automation Protocol
14.7. SOM: State of Maine
14.8. USGCB: United States Government Configuration Baseline