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

Rules of Behavior (PL-4)

Table of Contents

1.0. Purpose

1.1. The purpose of this document is to describe the responsibilities and expected behavior of those using State of Maine information or information assets. The rules of behavior (RoB) apply to both general and privileged users and are based on controls established by NIST 800-53 Rev. 4.[1] This document is not intended to replace or address standards for professional conduct outside of the information security context. This document represents the baseline security controls; additional RoB may be necessary for different types of controlled data based on State and Federal law, regulation, and policy.

2.0. Scope

2.1. This document applies to all State of Maine personnel, both employees and contractors, with access to Executive Branch information assets, irrespective of location, or information assets from other State government branches that use the State network;

3.0. Conflict

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

4.0. Management Commitment

4.1. The State of Maine is committed to following this document.

5.0. Personnel Acknowledgment

All personnel must sign the appropriate Acknowledgment Forms (General Users and Privileged Users) indicating that they have read, understand and agree to abide by the RoB prior to gaining access to systems and data. Personnel are also required to read the RoB when they are revised or updated and re-sign the Acknowledgment Form.

6.0. Procedures

6.1. The following serve as the baseline RoB for all general users, as well as additional rules for privileged users that are implemented to meet security planning requirements.

6.2. **General Rules (PL-4 to include CE-1).**

6.2.1. **All users <u>MUST</u>**:

6.2.1.1. Take personal responsibility to protect State information and information systems.

[1] https://nvd.nist.gov/800-53/Rev4/control/PL-4

6.2.1.2. Read and comply with all State of Maine, Department of Administrative and Financial Services and OIT policies and procedures.

6.2.1.3. Read and comply with the State of Maine Personal Use of Social Media Policy, the Policy and Work Rules Concerning the Use of State Information and Technology (I.T.) Equipment and Resources, the E-Mail Usage and Management Policy, and the State Policy Against Harassment.

6.2.1.4. Comply with all OIT policies that relate to the use of information or information systems, specifically the OIT Information Security Policy.

6.2.1.5. Comply with all information security training requirements as determined by the Information Security Office (see the Security Awareness and Training Policy and Procedures);[2]

6.2.1.6. Comply with any directions from supervisors and system administrators concerning access to, and use of, State information and information systems.

6.2.1.7. Properly secure all State information and information assets that are non-public in nature in accordance with its data classification (TLP: Green, Amber and Red) in all areas, at work and remotely, and in any form (e.g. digital, paper etc.).

6.2.1.8. Ensure that mobile media and devices that contain sensitive or confidential information (TLP Amber and TLP: Red) follow the mandate that this information must be in a protected environment at all times, or it must be encrypted; if clarification is needed as to whether an environment is adequately protected, users must seek guidance from the Chief Information Security Officer (CISO).

6.2.1.9. Only access sensitive or confidential information necessary to perform job functions (i.e., on a need-to-know basis) and only use such information for the purposes for which it was collected in accordance with all applicable security controls.

6.2.1.10. Take all necessary precautions to properly classify State information assets (in accordance with Risk Assessment Policy and Procedures[3]) and safeguard such assets in accordance with applicable federal and state policies and procedures from unauthorized access, disclosure, use, modification, destruction, theft, disclosure, loss, damage, or abuse.

[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-awareness-training-policy.pdf
[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/risk-assessment-policy-procedure.pdf

6.2.1.11. Report any loss, compromise, or unauthorized use of State information and information assets immediately upon discovery/detection in accordance with OIT policies and procedures.

6.2.1.12. Comply with federal and state laws, regulations, and OIT policies, standards, and procedures governing the protection of federally and state-protected data types (TLP: Amber and TLP: Red).

6.2.1.13. Comply with agency-specific procedures and protocols while transferring files, including OIT-approved, information system-implemented encryption mechanisms to protect the confidentiality and integrity of confidential data types.

6.2.1.14. Report any suspected or confirmed information security incidents or security weakness to the appropriate agency personnel and the Information Security Office. Security weakness includes unexpected system behavior, which may result in the unintentional disclosure of information or exposure to security threats.

6.2.1.15. Sign and comply with agency-specific non-disclosure and confidentiality agreements.

6.2.1.16. Only access system utilities which are made available due to a legitimate business case for the specific utility.

6.2.1.17. Lock computer screens when away from the computer.

6.2.1.18. Install and use only authorized software as determined by the Information Security Office on State of Maine information assets (see System and Services Acquisition Policy and Procedures, coming soon, and User Device and Commodity Application Policy[4]).

6.2.1.19. Exercise caution and follow appropriate security awareness training protocols for accessing emails, attachments, hypertext links, etc., to verify that information received is from trusted and secure sources.

6.2.1.20. Comply with supplemental rules, beyond the ones listed above, for specific systems, as needed.

6.2.1.21. Adhere to any additional agency-specific rules and requirements.

6.2.2. **All users must <u>NOT</u>**:

6.2.2.1. Share or disclose sensitive or confidential information, except as authorized in the user's official duties and with formal agreements that ensure all authorized third-parties will adequately protect this information.

6.2.2.2. Attempt to access any information asset for which they do not have express authorization.

6.2.2.3. Divulge remote connection methods and protocols.

[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/user-device-commodity-app-policy.pdf

6.2.2.4. Share credentials.

6.2.2.5. Use non-standard software or equipment (see the User Device and Commodity Application Policy).[5]

6.2.2.6. Make unauthorized changes to information or information systems.

6.2.2.7. Insert any removable media into a State device without ensuring that it does not contain malware.

6.2.2.8. Click on links or open attachments sent via email or text message from untrusted sources.

6.2.2.9. Engage in activity that may degrade the performance of information assets, deprive an Authorized user access to resources, or obtain extra resources beyond those allocated.

6.2.2.10. Engage in activities that could cause congestion, delay, or disruption of service to any state information resource (e.g., sending chain letters via email, playing streaming videos, games, music, etc.).

6.2.2.11. Allow others to use their account.

6.2.2.12. Access other users' accounts.

6.2.2.13. Circumvent security measures.

6.2.2.14. Download, install, or execute utilities such as password crackers, packet sniffers, or port scanners that reveal or exploit security weaknesses.

6.2.2.15. Download or transfer State of Maine information to any non-State device.

6.2.2.16. Communicate officially on behalf of a State agency and/or State government, or post or upload any content to a State agency website or social media account, unless such communication is part of the user's official job duties and has received prior management permission and authorization.

6.2.2.17. Use State information resources that result in user identity displayed or documented as affiliated with the State of Maine (e.g., social media accounts such as Twitter, Facebook, personal blog, chat room, newsgroup, electronic mail addresses, IP network addresses, etc.) and produce the appearance of an official communication representing the State of Maine or result in a display or recording of the participant's identity as affiliated with the State of Maine.

6.2.2.18. Use a State agency e-mail address to create personal commercial accounts for the purpose of receiving notifications (e.g., sales

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/user-device-commodity-app-policy.pdf

discounts, marketing, etc.), setting up a personal business or website, or signing up for personal memberships.

6.2.2.19. Use personal email accounts to conduct State business, regardless of whether the device is State-issued or otherwise.

6.2.2.20. Use personal email accounts on State-issued devices.

6.2.2.21. Use State information assets in violation of state law (Title 21-A M.R.S. § 32(3) 3) to advocate for or against a candidate for federal office, a constitutional office, an elective municipal, county or State office, including leadership positions in the Senate and House of Representatives, or to solicit contributions required by law to be reported to the Commission on Governmental Ethics and Election Practices. State law makes it a crime to use a computer system operated by a State department or agency to do any of the above (see BHR Civil Service Bulletin 13.1M).[6]

6.2.2.22. Use unapproved and unprotected non-State devices, such as mobile phones that have not been officially approved in accordance with the Mobile Device Policy,[7] to conduct State business.

6.2.2.23. Post, upload or communicate any personal opinions or defamatory, scandalous, offensive, libelous, pornographic, or otherwise illegal or unsanctioned material to any State agency and/or State government website or social media account, or use State information assets to do the same on any personal website or social media account.

6.2.2.24. Post, upload, or share any non-public State information (TLP: Green, Amber or Red) on any public website or social media/networking website. The unauthorized access or disclosure of sensitive or confidential information (TLP: Amber or TLP: Red) via any method or medium, including social media and networking sites, may result in criminal penalties including fines, and/or imprisonment (see definition section for examples of TLP data types).

6.3. **Rules for Privileged Users.**

6.3.1. Privileged users have network accounts with elevated privileges that grant them greater access to State information assets than non-privileged (general) users. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators. The compromise of a privileged user account may expose the State's information assets to a high level of risk; therefore, privileged user accounts require additional safeguards.

[6] https://www1.maine.gov/bhr/sites/maine.gov.bhr/files/inline-files/csbull13-1M.pdf

6.3.2. Due to privileged access rights, privileged users must comply with RoB standards higher than ordinary users and sign an additional Acknowledgment Form for Privileged Users (Appendix B).

6.3.3. The RoB Acknowledgment Form for Privileged Users is an addendum to the RoB for all general users. It provides mandatory requirements for the appropriate use and handling of OIT information systems and assets for all privileged users, including State employees, contractors, and other staff who possess privileged access to OIT information systems and assets.

6.3.4. Each Agency must maintain a list of Privileged Users, the privileged accounts those users have access to, the permissions granted to each privileged account, and the authentication technology or combination of technologies required to use each privileged account.

6.3.5. System Administration account (i.e. 'root') access must be limited to as small a group as possible based on the Principle of Least Privilege. For example, the 'root' account should not be used for tasks that can be completed via a non-privileged account.

6.3.6. Any administrators must first login as themselves (ordinary user) before escalating privileges to that of an administrator.

6.4. **Expectation of Privacy:**

6.4.1. Users of State information assets have no expectation of privacy while accessing OIT or State agency computers, networks, e-mail, or any other State information assets and may be monitored, recorded and audited. Any State information assets must be used with the understanding that such use may not be secure, is not private, is not anonymous, and may be subject to disclosure under the Maine Freedom of Access Act (FOAA), 1 MRSA § 400 et seq., or other applicable legal authority.

6.4.2. In order to protect State information assets against information security threats and ensure compliance with the State and agency-specific policies, as well as applicable contractual, regulatory, and statutory requirements, State agencies have the right to implement the following security monitoring technologies and systems on any State-owned I.T. equipment and resources (including all mobile devices subject to the Mobile Device Policy,[8] including BYOD and state-issued devices): anti-virus/anti-malware software, firewalls, host and network intrusion protection and intrusion detection systems, vulnerability management systems, database and application monitoring systems, data loss prevention, web and e-mail content filtering systems; and any other related technologies necessary to secure the State's information assets.

[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/mobile-device-policy.pdf

6.4.3. As permissible by law, State agency's information security monitoring systems and their authorized personnel have the right to monitor, audit, review, block, and log any traffic sent or received by users of State information assets, and any network traffic stemming from or sent to agency networks, systems, applications, databases, or other information assets, as well as any traffic directed at the State's information assets from external sources.

7.0. Document Details

7.1. Initial issue Date: 24 June 2020
7.2. Latest Revision Date: 24 June 2020
7.3. Point of Contact: Enterprise.Architect@Maine.Gov
7.4. Approved By: Chief Information Officer, OIT
7.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[9]
7.6. Waiver Process: Waiver Policy[10]

8.0. Review

8.1. This document must be reviewed at least annually, and when substantive changes are made to Policies, Procedures, or other authoritative regulations affecting this document. Individuals who have signed a previous version of the RoB must read and re-sign when the RoB are revised or updated.

9.0. Records Management

9.1. 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.

10.0. Public Records Exceptions

10.1. Under the Maine Freedom of Access Act, 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.

[9] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[10] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf

11.0. Definitions

11.1. *Confidential Information*: Confidential information includes any sensitive information that is protected under any other federal or state law or regulation intended to protect such information, or by order, resolution or determination of a court or administrative board or other administrative body, as well as any information designated as confidential and protected from disclosure under federal or state law or regulation. It also includes sensitive information used or held by an agency where considerable loss or harm could occur because of unauthorized access, use, or disclosure of this information. Statutory or regulatory penalties, notification provisions, or other mandates could also result if the information is accessed, used, or disclosed in an unauthorized manner (See definition below for TLP data classification levels, and System and Services Acquisition Policy and Procedures [coming soon] appendices for data types by classification level,).

11.2. *Federal Taxpayer Information (FTI):* FTI consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is received directly from the IRS (or obtained through an authorized secondary source), covered by the confidentiality protections of the Internal Revenue Code (IRC), and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI may contain personally identifiable information (PII).

Source: IRS Publication 1075.[11]

11.3. *Information Asset*: Used interchangeably with *Information System*. A discrete, identifiable piece of information technology, including hardware, software, firmware, systems, services, and related technology assets used to execute work on behalf of OIT or another State agency. (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30).

11.4. *Principle of Least Privilege:* A security principle where users are assigned the minimal access necessary to perform their job responsibilities. Access is granted for the shortest duration possible.

11.5. *Protected Health Information (PHI):* PHI means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. It includes information that is protected by the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act") and the federal regulations published at 45 C.F.R. parts 160 and 164 (collectively "HIPAA"). This definition excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, in employment records held by a covered entity in it its role as employer, and regarding a person who has been deceased for more than 50 years.

[11] https://www.irs.gov/pub/irs-pdf/p1075.pdf

Source: 45 CFR § 160.103.[12]

11.6. *Personally Identifiable Information (PII):* Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). It also includes personal information protected from disclosure under federal or state privacy laws.

Source: NIST CSRC Glossary.[13] Maine state law does not define PII, but rather provides a more limited definition of "personal information" within the context of the Maine Notice of Risk to Personal Data Act (see 10 M.R.S. §1347).[14]

11.7. *Traffic Light Protocol (TLP)*: The Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP) is used by OIT for the classification of PII impact level. OIT's four data, communication, or network classification levels are as follows:

1.1.1. Public (TLP: White): Non-sensitive, suitable for public consumption (PII with no impact level (i.e., Not Applicable); Public announcements or other publicly suitable information; Resources exposed to the Internet.

1.1.2. Internal (TLP: Green): Suitable for State Employees and contractors only, but not sensitive. Examples include, but are not limited to: PII with no impact level (i.e., Not Applicable); Employee newsletters or announcements, etc.; Internal memorandums not classified as "sensitive"; Subnets containing OIT Intranet servers; direct telephone line numbers to agency staff; and aggregated data.

1.1.3. Sensitive (TLP: Amber): Suitable for State Employees and select contractors only. Examples include, but are not limited to: PII of a low or moderate confidentiality impact level; Infrastructure information (IP addresses, server names, etc.); Information that would be embarrassing to the agency or the State if released; OIT File-servers, File-Shares, and their associated subnets; information exempt from disclosure pursuant to the Maine Freedom of Access Act (Title 1MRSA Chapter 13); information received from and/or about a business (tax information, business plans); security plans; network architecture.

1.1.4. Restricted (TLP: Red): Suitable for select State Employees and contractors only, access granted only on a need to know basis. Data must be encrypted at rest and in flight. Examples include, but are not limited to: PII of a high confidentiality impact level (e.g., Federal Tax Information, Social Security Administration data, Affordable Care Act data, Protected Health Information (PHI), PCI-DSS, driver's license or state identification card information, debit and credit card information, child welfare and legal information about minors and other types of federally-protected data and information, etc.).

[12] https://www.govinfo.gov/content/pkg/CFR-2017-title45-vol1/pdf/CFR-2017-title45-vol1-sec160-103.pdf
[13] https://csrc.nist.gov/glossary
[14] http://legislature.maine.gov/legis/statutes/10/title10sec1347.html

Appendix A: Acknowledgment Form for General Users

Signing this Acknowledgment Form below confirms that you, as a user of State of Maine information assets, have read, understood, and agree to comply with the Rules of Behavior. Users are required to sign the Acknowledgment Form prior to gaining access to State of Maine information systems and data. Attempting to engage in any of the unauthorized actions in the Rules of Behavior is prohibited and such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal or civil penalties.

I, _____, acknowledge that I have read, understand, and agree to abide by the State of Maine Information Technology Rules of Behavior. I understand that violations of these Rules of Behavior and information security policies and standards may result in disciplinary action and that these actions may include termination of employment; removal or disbarment from work on State contracts or projects; revocation of access to state and/or federal tax information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that I must read and re-sign when the Rules of Behavior are revised or updated.

_____ _____

Signature Date

_____

Agency

Appendix B: Privileged User Acknowledgment Form

Signing this Acknowledgment Form below confirms that you, as a privileged user of State of Maine information assets, have read, understood, and agree to comply with the Rules of Behavior for Privileged Users as described below. Attempting to engage in any of the unauthorized actions in the RoB for Privileged Users is prohibited and such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal or civil penalties.

I understand that as a Privileged User, I **must**:

1. Use Privileged User accounts appropriately for their intended purpose and only when required for official administrative actions;

2. Protect all Privileged User account passwords, passcodes, Personal Identity Verification (PIV), personal identified numbers (PINs) and other login credentials used to access information systems;

3. Comply with all system/network administrator responsibilities in accordance with other applicable policies;

4. Notify system owners immediately when privileged access is no longer required;

5. Properly protect all sensitive and confidential information and securely dispose of information no longer needed in accordance with sanitization policies;

6. Report all suspected or confirmed information security incidents to the OIT Information Security Office immediately and my supervisor as appropriate; and

7.Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a Privileged User, I **must not**:

1. Share Privileged User account(s), password(s), passcode(s), PINs and other login credentials;

2. Install, modify, or remove any system hardware or software or security settings without official written approval or unless it is part of my official job duties;

3. Remove or destroy system audit logs or any other security event log information unless authorized by appropriate official(s) in writing;

4.Tamper with audit logs of any kind. Note: In some cases, tampering can be considered evidence and can be a criminal offense punishable by fines and possible imprisonment;

5. Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls for unauthorized purposes;

6. Knowingly introduce unauthorized code, Trojan horse programs, malicious code, viruses, or other malicious software into OIT information systems or networks;

7. Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses;

8. Use Privileged User account(s) for day-to-day communications and other non-privileged transactions and activities;

9. Elevate the privileges of any user without prior approval from the system owner;

10. Use privileged access to circumvent OIT policies or security controls;

11. Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals;

12. Use a Privileged User account for Web access except in support of administrative related activities;

13.Use systems (either government issued or non-government) without the following protections in place to access sensitive or confidential OIT information:

a. Antivirus software with the latest updates,

b. Anti-spyware and personal firewalls,

c. A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access, and

d. Approved encryption to protect sensitive or confidential information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

I, _____, acknowledge that I have read, understand, and agree to abide by the State of Maine Information Technology Rules of Behavior for Privileged Users. I understand that violations of these Rules of Behavior and information security policies and standards may result in disciplinary action and that these actions may include termination of employment; removal or disbarment from work on State contracts or projects; revocation of access to state and/or federal tax information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that I must read and re-sign when the Rules of Behavior are revised or updated.

_____ _____

Signature Date

_____

Agency