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

Rules of Behavior (PL-4)

Table of Contents

1.0. Purpose

The purpose of this document is to describe the responsibilities and expected behavior of those using State of Maine information or information assets (see Definitions). The rules of behavior (RoB) apply to both general and privileged users and are based on controls established by the National Institute of Standards and Technology (NIST) 800-53 Rev. 4. This document is not intended to replace or address standards for professional conduct outside 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

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

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

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 to re-sign the Acknowledgment Forms.

6.0. Procedures

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

6.2. General Rules (PL-4, PL-4(1))

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

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

6.2.1.2. Read and comply with all State of Maine, Department of Administrative and Financial Services (DAFS), and Office of Information Technology (OIT) policies and procedures.

6.2.1.3. Read and comply with the State of Maine Personal Use of Social Media Policy,[1] the State of Maine Policy and Work Rules Concerning the Use of State Information and Technology (IT) Equipment and Resources,[2] the State of Maine E-Mail Usage and Management Policy(intranet only),[3] and the State of Maine Policy Against Harassment.[4]

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.[5]

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);[6]

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

6.2.1.7. Properly secure all nonpublic State information and information assets in accordance with their Traffic Light Protocol (TLP) (See Data Classification Policy)[7], in all areas, at work and remotely, and in any form (for example, digital, paper, or other).

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), in accordance with the Data Classification Policy[8].

6.2.1.9. Only access sensitive or confidential information (see Definitions) necessary to perform job functions and only use such information for the purposes for which it was collected and in accordance with all applicable security controls.

6.2.1.10. Take all necessary precautions to properly classify State information assets (in accordance with the Risk Assessment Policy and Procedures)[9] and safeguard such assets in accordance with applicable Federal and State policies and procedures from

[1] https://www.maine.gov/bhr/state-hr-professionals/rules-policies/policy-practices-manual/Personal-Use-of-Social-Media
[2] https://www.maine.gov/bhr/sites/maine.gov.bhr/files/inline-files/DAFSITPolicy_0.pdf
[3] http://inet.state.me.us/dafs/policies/emailsystem.html
[4] https://www.maine.gov/bhr/sites/maine.gov.bhr/files/inline-files/Policy_Statement_Against_Harassment_July_2011.pdf
[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityPolicy.pdf
[6] https://www.maine.gov/oit/policies/SecurityAwarenessTrainingPolicy.pdf
[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[9] https://www.maine.gov/oit/policies/RiskAssessmentPolicy&Procedure.pdf

unauthorized access, disclosure, use, modification, destruction, theft, disclosure, loss, damage, or abuse.

6.2.1.11. Report any loss, compromise, or unauthorized use of State information and information assets immediately upon discovery or 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 to the Information Security Office. Security weakness includes unexpected system behavior, which can result in the unintentional disclosure of information or exposure to security threats.

6.2.1.15. Sign and comply with agency-specific nondisclosure and confidentiality agreements.

6.2.1.16. Only access system utilities that are made available due to a legitimate business case.

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,[10] and User Device and Commodity Application Policy).[11]

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

6.2.1.20. Comply with rules supplemental to 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 the 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.

6.2.2.4. Share credentials.

[10] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemAndServicesAcquisitionPolicy.pdf
[11] https://www.maine.gov/oit/policies/UserDeviceCommodityAppPolicy.pdf

6.2.2.5. Use nonstandard software or equipment (see the User Device and Commodity Application Policy).[12]
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 (such as sending chain letters via email, playing streaming videos, games, music, and so on).
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 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 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 (for example, social media accounts such as Twitter, Facebook, personal blog, chat room, electronic mail addresses, internet protocol (IP) network addresses, and so forth) 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 (sales discounts, marketing, and similar materials), setting up a personal business or website, or signing up for personal memberships.
6.2.2.19. Conduct State business through non-Maine.gov account(s). This prohibition applies irrespective of whether the device is State-issued, or otherwise.
6.2.2.20. Use personal email accounts on State-issued devices.

[12] https://www.maine.gov/oit/policies/UserDeviceCommodityAppPolicy.pdf

6.2.2.21. Use State information assets in violation of State law (Title 21-A M.R.S. § 32(3) 3)[13] to advocate for or against a candidate for Federal office, a constitutional office, an elective municipal, a 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).[14]

6.2.2.22. Use State information assets in violation of State law (5 MRSA c. 164, Sec. 1)[15] with certain exceptions, State law now makes it a crime to contract with a company, using, obtaining, or purchasing information and/or communications technology and services included on the Prohibited Technologies List.[16]

6.2.2.23. Use unapproved and unprotected non-State devices, such as mobile phones that have not been officially approved in accordance with the Mobile Device Policy,[17] to conduct State business.

6.2.2.24. Post, upload, or communicate any personal opinions or defamatory, scandalous, offensive, libelous, pornographic, or otherwise illegal or unsanctioned material to any State agency 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.

6.2.2.25. Post, upload, or share any nonpublic State information (TLP:Red, TLP:Amber, TLP:Green) on any public website or social media/networking website. The unauthorized access or disclosure of sensitive or confidential information (TLP:Red, TLP:Amber) via any method or medium, including social media and networking sites, may result in criminal penalties including fines, and imprisonment (see the Data Classification Policy[18] for more information on 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.

---

[13] https://legislature.maine.gov/statutes/21-A/title21-Asec32.html
[14] https://www1.maine.gov/bhr/sites/maine.gov.bhr/files/inline-files/csbull13-1M.pdf
[15] https://legislature.maine.gov/backend/App/services/getDocument.aspx?documentId=107394
[16] https://www.maine.gov/oit/prohibited-technologies
[17] https://www.maine.gov/oit/policies/MobileDevicePolicy.pdf
[18] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.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 Acknowledgement Form 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 (in other words, "root") access must be limited to as small a group as possible, based on the principle of least privilege (see Definitions). For example, the "root" account should not be used for tasks that can be completed using a nonprivileged account.

6.3.6. Any administrators must first login as themselves (general 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 asset 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.,[19] or other applicable legal authority.

6.4.2. 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 information technology equipment or resources (including all mobile devices subject to the Mobile Device Policy,[20] including both bring-your-own and State-issued devices): antivirus/antimalware software, firewalls, host and network intrusion protection and intrusion detection systems, vulnerability management systems, database and application monitoring systems, data loss prevention,

[19] https://www.mainelegislature.org/legis/statutes/1/title1ch13sec0.html
[20] https://www.maine.gov/oit/policies/MobileDevicePolicy.pdf

web and e-mail content filtering systems, activity monitoring; and other related technologies necessary to secure the State's information assets.

6.4.3. As permissible by law, State agency information security monitoring systems and their authorized personnel have the right to monitor, audit, review, block, and log:
6.4.3.1. Traffic sent or received by users of State information assets,
6.4.3.2. Network traffic stemming from or sent to agency networks, systems, applications, databases, or other information assets, and
6.4.3.3. Traffic directed at State information assets from external sources.

7.0. Document Details

7.1. Initial issue Date: June 24, 2020
7.2. Latest Revision Date: October 16, 2024
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[21]
7.6. Waiver Process: Waiver Policy[22]
7.7. Distribution: Internet[23]

8.0. Review

This document is reviewed triennially and whenever substantive changes are made to policies, procedures, or other authoritative regulations that affect it. Individuals who have signed a previous version of the RoB must read and re-sign the policy when it is revised or updated.

9.0. 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 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

Under FOAA, certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as to security plans, procedures, or risk assessments. Information contained in these records may be disclosed to the State 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

[21] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[22] https://www.maine.gov/oit/policies/waiver.pdf
[23] https://www.maine.gov/oit/policies-standards

person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the State.

11.0. Definitions

11.1. Confidential Information: Information that is protected 1) under any other Federal or State law or regulation intended to protect sensitive information, or 2) by order, resolution, or determination of a court or administrative board or other administrative body, and 3) as protected from disclosure under Federal or State law or regulation. It also includes sensitive information used or held by an agency, the unauthorized access, use, or disclosure of which could result in considerable loss or harm. 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 the Data Classification Policy[24] for more information on TLP data classification levels).

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

11.3. Malicious Code: Unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Classifications of malicious code include viruses, worms, and Trojan horses.

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

11.5. Traffic Light Protocol: OIT subscribes to the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP)[25] classification levels. OIT's four classification levels can be found in section 7.0 of the Data Classification Policy.[26]

12.0. Abbreviations

12.1. CISA: Cybersecurity and Infrastructure Security Agency
12.2. CISO: Chief Information Security Officer
12.3. DAFS: Department of Administrative and Financial Services

[24] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[25] https://www.us-cert.gov/tlp
[26] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf

12.4. IP: Internet Protocol
12.5. NIST: National Institute of Standards and Technology
12.6. OIT: Office of Information Technology
12.7. PIN: Personal Identification Number
12.8. PIV: Personal Identity Verification
12.9. RoB: Rules of Behavior
12.10. TLP: Traffic Light Protocol

Appendix A: General User Rules Acknowledgment Form

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 Rules 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 Rules of Behavior 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(s), password(s), passcode(s), Personal Identity Verifications (PIVs), personal identification 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. Not knowingly use privileged access without a legitimate business need on any system or software. Notify system owners immediately when privileged access is known to be 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), PIVs, 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