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

Personnel Security Policy and Procedure (PS-1)

Table of Contents

1.0. Purpose

This policy establishes the Office of Information Technology's personnel security policy and procedures governing screening and access to the State's information technology systems and assets. It is a system of policies and procedures which seek to manage the risk of permanent, temporary, and contract staff trusted with access to State of Maine information systems and assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data. This policy corresponds to the Personnel Security (PS) Control Family, of the National Institute of Standards and Technology (NIST) Special Publication 800-53.

2.0. Scope

2.1. This document applies to all State of Maine personnel, both employees and contractors with access to:

- 2.1.1. Executive Branch Agency information assets, irrespective of location; and
- 2.1.2. 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 Partner:

- 4.1.1. In collaboration with OIT and IT Procurement, holds all vendors/partners for externally hosted Information Assets accountable to this Policy, within the vendor/partner's span-of-control.
- 4.1.2. Ensures agency personnel are aware of all applicable penalties for noncompliance, including the personnel sanctions identified in Section 8.8 of this policy.
- 4.1.3. Develops and implements agency-level policy and procedures, to meet any additional, pertinent personnel security regulatory compliance requirements.
- 4.1.4. Ensures position risk designations are updated and applied accurately.
- 4.1.5. Develops agency level personnel security policy and procedure as required by state and federal law.

4.2. OIT Information Security:

- 4.2.1. Owns, executes, and enforces this Policy and Procedure.
- 4.2.2. Ensures that all OIT personnel are aware of all applicable penalties for non-compliance.

4.3. IT Procurement:

- 4.3.1. Ensures vendor contracts stipulate that third-party personnel are subject to the requirements identified in 8.7, Third-Party Personnel Security.

4.3.2. In collaboration with the Agency Business Partner, holds all third-party providers (including vendors, contractors and other supplier organizations providing information system development, IT services, network and security management, suppliers, and partners for externally-hosted Information Assets) accountable to this Policy.

4.3.3. Third-party providers are responsible for managing third-party personnel in accordance with this policy.

5.0. Management Commitment

Management is committed to following this document.

6.0. Coordination Among Agency Entities

The Office of Information Technology coordinates personnel security with agencies to ensure the security of State of Maine information assets in accordance with Executive Order 25 FY 20/21[1] and Title 5, Chapter 163 §1971-1985.[2] Agencies and OIT coordinate to meet all state and federal audit documentation and reporting compliance requirements.

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. The following procedures are designed to satisfy the security control requirements of this Policy (Personnel Security) as outlined in NIST Special Publication 800-53, Internal Revenue Service Publication 1075, Centers for Medicare & Medicaid Services Minimum Acceptable Risk Standards for Exchanges 2.0, Criminal Justice Information (see Definitions) Services Security Policy, Health Insurance Portability and Accountability Act Security Rule, and to satisfy State and Federal law.

8.2. Position Risk Designations (PS-2)

8.2.1. OIT works with agencies to determine if positions will have access, or the substantial possibility of access, to data types that have been classified by OIT and the Agency as having a personally identifiable information (PII) (see Definitions) Impact Level of High (see also the corresponding Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP) (see Definitions) category Red for examples of state and federally-protected data

[1] https://www.maine.gov/governor/mills/sites/maine.gov.governor.mills/files/inline-files/EO%2082%2025.pdf
[2] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

types in this category, such as: Federal Tax Information (FTI) (see Definitions), protected health information (PHI) (see Definitions), Social Security Administration (SSA) data, criminal justice information (CJI), Financial/Credit Card Information, etc.).

8.2.2. Individuals, including State of Maine employees, contractors, and third-party personnel, with potential access to data types classified as having a High PII impact level/TLP Red (CJI, PHI, FTI, SSA or any other state or federally protected data types) must be screened to at least the minimum standards specified by law and regulations.

8.2.3. When a position's responsibilities or access levels change so that the position has access or the substantial possibility of access to data types that have been classified by OIT as having a High PII Impact Level/TLP Red data or other similarly protected data types, the individual must be screened to at least the minimum standards specified by law and regulations.

8.2.4. The method for determining examination and screening requirements for all OIT positions is outlined in the Bureau of Human Resources' (BHR) Human Resources Policy and Practices Manual.[3]

8.3. **Personnel Screening (PS-3)**

8.3.1. As outlined in the federal Immigration Reform and Control Act of 1986 the State of Maine is required to hire only U.S. citizens, and aliens who are authorized to work in the U.S.

8.3.2. As per the BHR Policy and Practices Manual, Form I-9 must be completed within three business days of the date of hire. To complete Form I-9, the employee must provide certain documents to establish both the employee's identity and eligibility for employment.

8.3.3. All personnel are subject to, at minimum, a state criminal background check.

8.3.3.1. In the event the background check reveals a prior criminal conviction, the criminal record may legitimately be considered pursuant to and using the screening criteria specified by BHR.

8.3.4. Fingerprint-based Background Checks - Access to CJI: The State of Maine has adopted the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy as its minimum-security requirement for CJI. All Information Systems developed, acquired, or utilized as a service by OIT containing CJIS-regulated information incorporate this security standard. The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to FBI CJIS Division systems and

[3] https://www.maine.gov/bhr/state-hr-professionals/rules-policies/policy-practices-manual

information and to safeguard CJI. All entities with access to, or who operate in support of, the FBI CJIS Division's services and information must comply with the FBI's CJIS Security Policy and its minimum-security requirement for the safeguarding of CJI. This includes personnel and contractors of State of Maine agencies.

8.3.4.1. Fingerprint-based background checks are required for all personnel and contractors that have unescorted access to areas where CJI is processed (i.e. OIT/Department of Public Safety (DPS) Datacenter or telco rooms), or they have network access, system or security administrative privileges to systems that store or process CJI.

8.3.4.2. The CJIS Information Security Officer (ISO), within the DPS, Maine State Police, is responsible for ensuring adherence to the CJIS Security Policy. The CJIS ISO performs a national criminal history record check initially, and every five years thereafter for personnel with access or the substantial possibility of access to CJI. Fingerprint-based background checks are processed through either the State Identification Bureau or a local law enforcement agency; prints are forwarded to the CJIS ISO to conduct the fingerprint-based background check. Upon completion, the CJIS ISO provides a response of pass/fail to the OIT ISO contact, who notifies the appropriate OIT supervisor. OIT is responsible for registering all personnel and contractors with approved access to CJI for the appropriate level of CJIS Security Awareness Training in CJIS Online.

8.3.4.3. Disqualifiers for access to CJI data are determined by the CJIS ISO.

8.3.5. Fingerprint-based Background Checks - Access to FTI: IRS Publication 1075, requires local agencies to establish a personnel security program that ensures background investigations are completed to the appropriate level for any individual who will have access to FTI as part of their job duties, both current and prospective applicants, employees, and contractors. Agencies must comply with federal and state compliance standards and minimum background check requirements to implement these requirements (see MRSA Title 5, Chapter 163 §1986[4] for OIT's governing statute; other agency business partners are responsible for establishing their own statutory and regulatory compliance requirements for fingerprint-based background checks). The OIT requirements are as follows:

8.3.5.1. All OIT employees with access to FTI are subject to local and federal background checks, FBI fingerprint-based criminal history record checks (CHRC).

8.3.5.2. All necessary steps are taken before an employee is allowed access to FTI.

8.3.5.3. The suitability background check is favorable.

8.3.5.4. Current employees must submit to a background check upon implementation of this policy and every 10 years thereafter.

[4] https://legislature.maine.gov/statutes/5/title5sec1986.html

8.3.5.5. OIT performs an FBI fingerprint-based CHRC upon hiring, and every five years, for personnel who have access or the substantial possibility of access to FTI, starting within the calendar year of enactment of the State implementation law (see Title 5, Chapter 163 §1986).[5]

8.3.5.6. OIT uses the suitability criteria guidance provided by BHR for determining suitability standards for access to FTI. These factors assist the agency with determining suitability for access to FTI.

8.3.6. Agencies may impose additional screening requirements within the law, provided they are not less stringent than the minimum federal standards articulated above for applicable data types. Agencies are also responsible for ensuring that an appropriate review of contractor background checks are completed as specified in the contract.

8.3.7. Upon receipt of the results of a background check report for State employees, BHR refers criminal history conviction information to agency management, who determines if the potential or current employee should gain or retain access to controlled data (see Definitions).

8.3.7.1. Agency management makes a final decision after considering the above-listed factors relevant to the potential or current employee's employment on a case-by-case basis.

8.3.7.2. Agency management determines whether hiring the individual would potentially threaten the safety and well-being of State of Maine data, information assets, and/or employees and the public due to the threat to information assets. A determination that an employee is not suitable to access PII, CJI, FTI, SSA, PHI and/or other controlled data may result in dismissal or removal from a position requiring access to those.

8.3.7.3. Notwithstanding the foregoing, should a position not requiring access to PII, CJI, FTI, SSA, PHI, and/or other controlled data be open and available, the employee may be reassigned to this position, subject to the business needs of the agency and the capabilities of the employee.

8.3.7.4. BHR is consulted before a final decision is made.

8.3.8. Employees may be rescreened when transferring position and at the agency's discretion. When an employee moves from one position to another, the higher level of clearance (i.e., national over State only) should be adjudicated.

8.3.9. Commencement of individual employment for OIT includes completing the OIT Pre-hire and orientation checklist and guidelines' (See Appendix B).

[5] https://legislature.maine.gov/statutes/5/title5sec1986.html

8.4. Personnel Terminations (PS-4, PS-4(2))

8.4.1. Termination of individual employment from OIT includes completing the 'Exit interview checklist for OIT (See Appendix B).

8.4.1.1. State of Maine employee and contractor supervisors must complete the requirements of this form for personnel leaving State of Maine employment. This form accounts for:

8.4.1.1.1. Disabling information system access prior to or during the personnel termination process/action;

8.4.1.1.2. Terminating/revoking any authenticators/credentials associated with the individual;

8.4.1.1.3. Conducting exit interviews that include a discussion of non-disclosure of information security and privacy information;

8.4.1.1.4. Retrieving all security-related, information systems-related organizational property;

8.4.1.1.5. Retaining access to organizational information and information systems formerly controlled by the terminated individual; and

8.4.1.1.6. Notifying OIT via the ticket system User Request form within one (1) calendar day.

8.4.2. As determined by agency management and approved by BHR, employees terminated for cause are immediately escorted out of the organization.

8.5. Personnel Transfers (PS-5)

8.5.1. For personnel transfer, the sending agency, the receiving agency, and OIT jointly define the access requirements over the 30 days prior to the transfer, in accordance with the Access Control Policy and Procedures[1] and the Access Control Procedures for Users,[2] and changes in operational and regulatory compliance requirements.

8.5.2. Within one (1) business day of the transfer, OIT is notified by either the sending agency, or the receiving agency, via the enterprise ticketing system.

8.5.3. Based upon regulatory requirements, the sending agency, the receiving agency, and OIT jointly decide on the following

8.5.3.1. The disposition of the legacy (prior to the transfer) directory account, email, records, and access rights to information assets;

8.5.3.2. The creation of the new (following the transfer) directory account, email, records, and access rights to information assets; and

8.5.3.3. The extent of access, if any, to the legacy (prior to the transfer) email, records, and information assets, that is allowed to the personnel following the transfer.

[1] https://www.maine.gov/oit/policies/AccessControlPolicy.pdf
[2] https://www.maine.gov/oit/policies/AccessControlProceduresForUsers.pdf

8.5.4. Based upon regulatory requirements, and the access rights to information assets necessary for the new position (following the transfer), the receiving agency, OIT, the Attorney General's Office, and the Bureau of Human Resources jointly decide on any additional screening that may be required for the transferring personnel.

8.6. Access Agreements (PS-6)

8.6.1. Prior to accessing controlled data, personnel complete confidentiality and security training as required by the regulating entity. Additionally, enterprise security awareness training is repeated annually as a baseline for all employees, as specified in Security Awareness Training Policy and Procedures.[6]

8.6.1.1. Security Awareness Training includes signing of the Rules of Behavior.[7]

8.6.2. Depending on what categories of controlled data personnel have access to, additional training may need to be conducted and agreements, including nondisclosure agreements, or other documents completed.

8.7. Third-Party Personnel Security (PS-7)

8.7.1. Third-party personnel consist of contractors and subcontractors who provide or are subject to provide services to a State of Maine agency under an identified interconnection security agreement, memorandum of understanding/agreement, or contract. Third-party personnel who could access State of Maine information assets are required to meet the same personnel security screening criteria and requirements as State of Maine employees. Requirements for third-party personnel are stipulated in their contract.

8.7.1.1. All third-party personnel are subject to, at the minimum, a state criminal background check. Third-party personnel who have access, or the substantial possibility of access, to data types that have been classified by OIT as having a PII Impact Level of High/TLP category Red are also subject to additional security screening requirements as stipulated above for compliance with state and federal laws, regulations, or policies.

8.7.1.2. The Safeguard Contract Language from IRS Publication 1075 is incorporated within all contracts that involve access to FTI, systems which contain those, or Maine Revenue Service information systems.

8.7.1.3. Agency management in conjunction with the OIT ISO, determines if a position involves access, or the substantial possibility of access, to State of Maine information technology systems, or to data types that have been classified by OIT as having a PII Impact Level of High/TLP

[6] https://www.maine.gov/oit/policies/SecurityAwarenessTrainingPolicy.pdf
[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RulesofBehavior.pdf

category Red, that reside on those systems.

8.7.2. Third-party personnel access to state and federally protected data types designated as PII impact Level of High/TLP Red requires prior approval from the appropriate federal entity. Agencies are responsible for receiving the appropriate approvals prior to allowing third-party personnel access.

8.7.3. Third-party personnel are responsible for notifying the immediate State of Maine supervisor of the personnel, as well as agency management, of personnel transfers and/or terminations within 15 calendar days so OIT can secure confidential information and equipment.

8.7.4. Third-party personnel are required to comply with the same security requirements, laws, regulations, and policies as State of Maine personnel.

8.7.4.1. Agency staff overseeing the work of third parties shall be responsible for communicating and enforcing applicable laws, as well as State and agency security policies, and procedures. Agencies must monitor third-party provider compliance.

8.7.4.2. Non-disclosure Agreements must be signed by authorized representatives of the third-party before any information technology services are delivered.

8.7.4.3. State confidential data and information assets must not be released to third parties without properly executed contracts and confidentiality agreements. These contracts must specify conditions of use and security requirements and the access, roles, and responsibilities of the third-party before access is granted.

8.7.5. IT Procurement works with the Agencies to ensure compliance with third-party personnel requirements.

8.8. Personnel Sanctions (PS-8)

8.8.1. For State of Maine employees, failure to comply with the procedures identified in this policy may result in progressive discipline up to and including dismissal.

8.8.2. For State of Maine contractors and non-State of Maine personnel, failure to meet and comply with security policies and procedures may result in removal of the individual's ability to access and use State of Maine data and systems, as well as whole or partial termination of the contract depending on the nature of the breach. Employers of non-State of Maine personnel will be notified of any violations.

8.8.3. In addition, for contractors, the failure to maintain the State's minimum-security standards during the term of the contract, including renewals, will result in whole or partial termination of the contract, depending on the nature of the breach.

8.8.4. 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.

9.0. Document Details

9.1. Initial Issue Date: 07 December 2022
9.2. Latest Revision Date: 02 December 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[8]
9.6. Waiver Process: Waiver Policy[9]
9.7. Distribution: Internet[10]

10.0. Review

10.1. 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

11.1. OIT 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 a minimum of 6 years after withdrawal or replacement and then destroyed in accordance with guidance[11] 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

12.1. Under the Maine Freedom of Access Act (FOAA),[12] 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 Maine 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 person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the State.

13.0. Definitions

13.1. Controlled Data: Information that law, regulation, or policy requires to have safeguarding or disseminating controls, special handling safeguards, or protection

[8] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[9] https://www.maine.gov/oit/policies/waiver.pdf
[10] https://www.maine.gov/oit/policies-standards
[11] https://www.maine.gov/sos/arc/records/state/GS1Administrative.pdf
[12] https://legislature.maine.gov/statutes/1/title1sec402.html

from unauthorized disclosure. All controlled data is TLP: Red, but not all TLP: Red data is controlled. Includes but is not limited to FTI, CJI, and PHI.

13.2. Criminal Justice Information (CJI): CJI is the abstract term used to refer to all of the Federal Bureau of Investigations (FBI) Criminal Justice Information Services (CJIS) provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any PII), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to, data used to make hiring decisions.

13.3. Federal Tax Information (FTI)

13.3.1. 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 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 PII.

13.3.2. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as SSA, Federal Office of Child Support Enforcement, Bureau of the Fiscal Service, or Centers for Medicare and Medicaid Services, or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement.

13.3.3. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through an authorized secondary source.

13.4. 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.).

13.5. 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. 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.

13.6. Traffic Light Protocol (TLP): OIT subscribes to the U.S. Department of Homeland Security CISA Traffic Light Protocol[13] classification levels. See the Risk Assessment Policy and Procedures (RA-1)[14] for a description of the classification levels.

14.0. Abbreviations

14.1. BHR: Bureau of Human Resources
14.2. BYOD: Bring Your Own Device
14.3. CHRC: Criminal History Record Checks
14.4. CISA: Cybersecurity and Infrastructure Security Agency
14.5. CJA: Criminal Justice Agencies
14.6. CJI: Criminal Justice Information
14.7. CJIS: Criminal Justice Information Services
14.8. DPS: Department of Public Safety
14.9. FBI: Federal bureau of Investigation
14.10. FTI: Federal Tax Information
14.11. IRC: Internal Revenue Code
14.12. ISO: Information Security Officer
14.13. NCJA: Noncriminal Justice Agencies
14.14. NIST: National Institute of Standards and Technology
14.15. OIT: Office of Information Technology
14.16. PHI: Protected Health Information
14.17. PII: Personally Identifiable Information
14.18. PS: Personnel Security
14.19. SID: Security Identifier
14.20. SSA: Social Security Administration
14.21. TLP: Traffic Light Protocol

[13] https://www.us-cert.gov/tlp
[14] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RiskAssessmentPolicyProcedure.pdf

Appendix A: OIT Pre-hire and orientation checklist and guidelines

Supervisor:	**Report Org (4-digit billing code):**	
Name:	**Position:**	**Start Date:**

Check One: ____ State Employee ____ Contractor

Item #	Description (see next page for guide)	Date	Initial	Form/Letter/Email Completed
Prior to first day, supervisor collaborates with BHR and OIT for:				
1.	Background Check And I-9			
2.	REQUEST FOR SECURITY BADGE (This Also Pertains to Contractors)			
3.	Telephone Access Code – Pin			
4.	Telephone Work Order			
5.	SECURID			
6.	Set Up Exchange E-Mail (New/Modify/Delete User Request Form)			User Ticket# Footprints# Footprints#
7.	Cellular Phone or Smartphone			
First day, supervisor works with BHR and employee to:				
8.	IT Policy			
9.	BYOD			
10.	Security and Privacy Awareness Training Including Rules of Behavior			
11.	Work Rule – State Owned Equipment			

Prior to first day:

- **Background check and I-9:** Prior to being offered a position, all potential State of Maine employees are subject to a state background check and I-9. The Personnel Office conducts these.
- **Request for physical access badge:** Please open a physical access request[15] for a new badge (instructions).[16] On their start date, please send the new hire to see the Enterprise Security Team for a badge photo. They will issue a physical access badge as long as the above has been completed and approved.
- **Telephone Access Code:** Complete on-line form[17] indicating the limit for the telephone ID. Limits are 0 = International, 1 = North America, 2 = New England, 3 = Maine.
- **Telephone Work Order:** Initiate a Telephone Work Order Request ticket.[18]
- **SecurID**: For employees that will remote access State of Maine information assets, initiate a SecurID ticket.[19]
- **New/Modify User and Computer request:** Initiate a User Request ticket at New/Modify/Delete User Form to set up Active Directory (email), printers, distribution list, application access, and request device. The device is ordered on the same footprints ticket as the user request.
- **Request phone/smartphone:** If an employee requires a cellular phone or smartphone, complete the State Cellular Request Form.[20]

First day:

- **Bring your own device (BYOD):** If the employee wishes to use their own cell phone or smartphone for work-related functions and/or to access State of Maine information assets, including the SOM AIRE network, Intune and Lookout must be installed. Instructions and the request form are found at the Mobile Device Portal.[21] See the Mobile Device Policy[22] for more details.
- **IT Policy**: The Personnel Office will have the employee acknowledge the IT Policy.[23] For contractors, the supervisor will ensure that the contractor acknowledges the IT Policy.
- **Security and Privacy Awareness training:** Enterprise Security Awareness training is automatically pushed out to new Agency personnel with e-mail addresses. Agencies are responsible for the delivery of enterprise security awareness training for any agency personnel without a state e-mail address.

[15] https://footprints.state.me.us/footprints/security.html
[16] https://footprints.state.me.us/footprints/help/tutorials/security-request.pdf
[17] http://inet.state.me.us/oit/eforms/access-codes/index.html
[18] https://footprints.state.me.us/footprints/telco.html
[19] http://footprints.state.me.us/footprints/rsa.html
[20] https://stateofmaine.sharepoint.com/:w:/r/sites/MaineIT/Shared%20Documents/Employee%20Forms/state-cellular-request-form02122018.doc?d=wa7617f0b99164835912e64bc4cf5e1af&csf=1&web=1&e=PfXcST
[21] https://stateofmaine.sharepoint.com/sites/MaineIT/SitePages/Mobile/Mobile-Devices.aspx
[22] https://www.maine.gov/oit/policies/MobileDevicePolicy.pdf
[23] https://www.maine.gov/bhr/sites/maine.gov.bhr/files/inline-files/DAFSITPolicy.pdf

Appendix B: Exit interview checklist for OIT

Contingency Plan Participation:

Employee holds a position of responsibility in the following contingency plans:	Yes	No
Incident Response Policy and Procedures (IR)		
Contingency Planning Policy and Procedures (CP)		
Business Continuity and Disaster Recovery Policy		

Have these roles been reassigned? Yes____ No_____

Office and Confidential Files

Have the following been collected?	Yes	N/A	Date
Office sensitive files			
Confidential information			
Protected information			

Computing Equipment Asset Inventory

Has the employee returned the following?	Yes	N/A	Date
Laptop/desktop			
Mobile phone			
SecurID Key			
Flash Drives			
External Hard Drives			
Printers			
ID Badge			
Keys			
Security alarm codes			
Voice mail password			
Laptop security cable lock			
Other computing office equipment			

Access Termination

Have the following been completed?	Yes	N/A	Date
OIT ticket to modify/delete user			
Procedure for Handling Files and Email of Departing or Transferring Users[24] (internal only)			

Transition Period and plan

Have the following been completed?	Yes	N/A	Date
Transfer of knowledge			
Transfer of accounts			
Location of electronic files			

[24] http://inet.state.me.us/foaa/documents/ProcedureforHandlingFilesandEmailofDepartingorTransferringUsers.pdf