Division of Enterprise Technology Strategy and Services

ETSS Policy 950.2
Awareness and Training (AT)

Publish Date: 22 July 2026
Effective Date: 22 July 2026
Last Review: 21 July 2026

doa.entsec@doit.ri.gov

1. Purpose

Establish policy for implementing a comprehensive security awareness and training program that ensures all Network Resource privileged users, administrators, or users with access to Non-Public Classified Data systems understand their security responsibilities, recognize current threats, and are adequately trained to perform their assigned roles in a secure manner. The program provides ongoing awareness of cybersecurity risks—such as phishing, password management, insider threats, incident response, and data handling—and equips personnel with the knowledge and skills necessary to safeguard confidentiality, integrity, and availability of State of Rhode Island information systems and data.

This policy directly supports the Govern and Protect functions of the NIST Cybersecurity Framework (CSF) 2.0 by embedding security responsibilities into workforce culture and ensuring personnel are trained to implement protective safeguards effectively. Additionally, this policy incorporates Complementary User Entity Controls (CUECs) by explicitly recognizing the shared responsibility between enterprise security teams and agency personnel. The policy also aligns with the State's ETSS Security and Risk Program (PM-1), which establishes a statewide risk management framework based on NIST Risk Management Framework (RMF) and NIST SP 800-53 moderate baseline, by ensuring that awareness and training controls (AT family) are consistently implemented, maintained, and measured across all agencies and users under the coverage of Enterprise Technology Strategy and Services (ETSS) technology outlined in the applicability section.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments[1] (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "Agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Non-Public Classified Data
Any data that is not public (including private, sensitive, or confidential data as defined

by associated federal regulations and denoted by ETSS data classification labels). Non-Public Classified Data requires additional security controls, such as access restrictions and encryption.

Network Resources

Information processing systems, system components, devices, and data that are accessible via the local area network or State intranet. Network Resources include:

a. Data, information, and files (in storage and in transmission).
b. Desktop computers.
c. State issued mobile devices (e.g., laptops, tablets, notebooks, smartphones).
d. Peripheral devices (e.g., printers, scanners, fax machines, monitors).
e. Software, hardware, and network equipment (e.g., applications, phone systems, servers, routers, switches).

4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)
Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

Moderate Risk Systems (IAL2)
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. ***[IAL1, IAL2]*** **Awareness and Training Policy and Procedures (AT-1).** The agency will develop, document, disseminate to designated personnel defined in the applicable system security plan, review, and annually update an awareness and training policy and procedures.

4.2. ***[IAL1, IAL2]*** **Literacy Training and Awareness (AT-2).** The agency will:

1. Provide security and privacy awareness training to information system users, including managers, senior executives, and contractors, as part of initial training for new users, when required with information system changes, and annually thereafter. On an enterprise level, annual security awareness training that includes security risks associated with enterprise-wide activities, as well as ETSS information system security-related policies, standards, and procedures, will be provided to all state network users. Strategic and periodic use of additional training methods (e.g. email, posters, National Cybersecurity Awareness Month) should be leveraged, as necessary, to provide awareness of current security threats and re-enforce good security practices.

2. Incorporate lessons learned from security or privacy incidents into literacy training and awareness techniques.

4.2.1. ***[IAL1, IAL2]*** **Insider Threat (AT-2.2).** The agency will include literacy training regarding the recognition of potential indicators of insider threats such as repeated attempts to access systems not relevant to job duties, unexplained access to financial resources, and workplace violence or harassment.

4.2.2. ***[IAL2]*** **Social Engineering and Mining (AT-2.3).** The agency will include literacy training regarding the recognition and reporting of potential and actual instances of social engineering and social mining (e.g. how to communicate concerns of employees and management through agency channels).

4.3. ***[IAL1, IAL2]*** **Role-Based Training (AT-3).** Privileged users, third-party providers, and stakeholders should be trained, as appropriate, to understand their roles and responsibilities in securing information systems and data in accordance with ETSS and agency policies, procedures, agreements, and guidelines. The agency will:

1. Provide personnel with roles or security-related duties and responsibilities critical to maintaining the security, operational, and technical integrity of information systems with role-based training. Role-based training will be tailored to their assigned duties and must be completed prior to authorizing access to the information system to perform their assigned duties, when required due to information system changes, and annually thereafter. Roles that may require role-based training include, but are not limited to, agency leaders and senior management, system owners, security and privacy officers and engineers, acquisition and procurement officials, network architects, system and software developers and engineers, system/network/database administrators, personnel with contingency planning and incident response duties, and personnel with access to PII and other confidential or sensitive data.

2. Update role-based training content annually. Training should be based on changes to technology and current and emerging threats that are relevant to the role.

3. Incorporate lessons learned from security incidents or breaches into role-based training.

4.4. ***[IAL1, IAL2]*** **Training Records (AT-4).** The agency will:

1. Document security awareness and training activities of all information system users. Enterprise-level training will be recorded by the information system used to provide the training.

2. Retain training records for a minimum of five (5) years after termination, transfer, or separation, in accordance with federal or state laws, regulations, or compliance requirements. See *State of Rhode Island Department of State General Records Retention Schedule GRS9* for more information.

5. Approval / Review Signature:

Nathan Loura
Digitally signed by Nathan Loura
Date: 2026.07.22 09:23:21 Z

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services (ETSS)

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.07.22 08:31:09 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services (ETSS)