



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

CYBER-CYBERSECURITY AWARENESS-2019

STATE CYBERSECURITY & HOMELAND SECURITY

Annual Cybersecurity Awareness Training Policy

Date of Last Revision 10/01/18

Governor's Office
(401) 574-8495

1. Purpose

- a. The threat to State digital systems and sensitive data from criminals, hackers and hostile entities increases daily. The presence of the digital threat requires that those accessing Enterprise systems and working with sensitive data be trained to protect the security and promote the resiliency of State networks and data. A high percentage of threats begin with human error from a lack of basic knowledge regarding the protection of digital assets and sensitive data. To ensure all State of Rhode Island Executive Branch employees are properly educated on the growing cybersecurity threats and risks associated with digital presence, and aware of the requirements for data protection, the State must implement annual cybersecurity awareness training to change the digital culture within State government while helping the State manage risks associated to cybersecurity. Additionally, due to the uncertainty of the cybersecurity threat, applicable training may be required as deemed necessary. This policy is not intended for the general population that accesses electronic government services or applications.

2. Applicability

- a. The Annual Cybersecurity Awareness Training Policy, and applicable training as required, applies to all State Executive Branch Agencies and State employees, whether permanent, non-permanent, contract, full or part-time, with access rights to State networks, data, computers and systems operated by the State or maintained on behalf of the State.
- b. State Cybersecurity and Homeland Security, in conjunction with the State of Rhode Island's Division of Human Resources, shall identify and provide an interactive solution for delivering annual cybersecurity awareness training and applicable training, as required, for all Executive Branch end users. Special Note on Collective Bargaining Agreements

3. Definitions

- a. **Agency:** Any department, agency, division, or unit of the State of Rhode Island Executive Branch.
- b. **End User:** Individual employed by the State, whether permanent, non-permanent, contract, full or part-time, with access to State networks, data, computers and systems operated by the State or maintained on behalf of the State.

- c. **Learning Management System:** Software application for the administration, documentation, tracking, reporting and delivery of educational courses or training programs.

4. Procedures for Compliance

- a. Cybersecurity awareness training and applicable trainings, in accordance with the requirements outlined in this policy:
 - (i.) Employees will have 6 months to complete the annual cybersecurity awareness training curriculum.
 - (ii.) Monthly reminders will be sent to employees that have not completed the training modules assigned to them within the training portal.
 - (iii.) Employees will receive a notification at the 5-month mark informing them that they are at risk of exceeding the training deadline.
 - (iv.) Employees who exceed the 6-month deadline will be required to complete their annual cybersecurity training before operating a state computer.
- b. Executive Branch employees progress will be tracked automatically through the training portal. Training records shall be retained in accordance with the Division of Human Resources Learning Management System (LMS) records retention requirements.

5. Repercussions for Noncompliance

- a. State Cybersecurity and Homeland Security shall ensure that all Executive Branch employees receive annual cybersecurity awareness training and will monitor the overall cybersecurity education effort through the State of Rhode Island's Executive Branch.
- b. Any employee who willfully disregards this policy will receive an email of non-compliance, with leadership copied for awareness. It is the responsibility of Agency leadership to ensure that their employees comply with the training requirements in this policy and complete their assigned annual cybersecurity awareness training and other cybersecurity training, as required, per this policy.

6. Signatures



Division Director

10/1/18
Date



Director of Administration

10/1/18
Date

