Management Directive
Commonwealth of Pennsylvania
Governor's Office

Management Directive 535.09 Amended – Information Technology Security Trainings

Date: May 3, 2023

By Direction of:

Neil R. Weaver, Secretary of Administration

Contact Agency: Office of Administration
Information Technology
Enterprise Information Security Office (EISO)
Phone: 717-772-4240, RA-CISO@pa.gov

This directive sets forth policy, responsibilities, and procedures that agencies must follow for all Authorized Users to receive Information Technology (IT) Security Training Courses at least once per calendar year.

1. PURPOSE.

To establish policy, responsibilities, and procedures regarding the minimum requirement that all Authorized Users of IT Resources receive IT Security Training Courses at least once per calendar year.

2. SCOPE.

This directive applies to all Authorized Users in departments, offices, boards, commissions, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction.

3. OBJECTIVE.

Provide IT Security Training Courses to Authorized Users to promote security best practices and consistent organizational behavior by providing guidance on incidents of fraud and by promoting consistency in mitigating IT security risks.

4. DEFINITIONS.

a. Authorized User. Commonwealth of Pennsylvania employees, contracted resources, consultants, volunteers, or any other users who have been granted access to, and are authorized by the Commonwealth to use, Commonwealth IT Resources.

b. **Commonwealth Network.** A collection of servers, mainframes, networking devices, and IT Resources that are interconnected, either by a cable, wireless connection, or logically, and are physically or operationally controlled and security-managed by the Commonwealth or a contracted third-party vendor on behalf of the Commonwealth.

c. **Fraud Awareness and Prevention Training.** Training on the types of intentional deception often engaged in by others pretending to be something they are not.

d. **IT Administrator Acceptable Use Training.** Training targeted for Privileged Users who are trusted with rights and abilities beyond those granted to normal users.

e. **IT Resources.** Equipment or interconnected systems or subsystems of equipment, networks, or services used to receive, input, store, process, manipulate, control, manage, transmit, display and/or output information, including, but not limited to: computers, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, Intranet, email, ancillary equipment, software, firmware, cloud-based services, systems, networks, platforms, plans, data, training materials, documentation, and social media websites.

f. **IT Security Awareness and Acceptable Use Training.** Training targeted to educate Authorized Users on potential security threats and the safeguards, including Information Technology and Physical Security, required to handle those threats for the purpose of protecting IT Resources and information.

g. **IT Security Training Courses.** Includes enterprise courses (IT Security Awareness and Acceptable Use Training, IT Administrator Acceptable Use Training, and Fraud Awareness and Prevention Training). In addition, there may be other job or role-related required trainings, for example: trainings on Criminal Justice Information Services (CJIS), Federal Tax Information (FTI), or Health Insurance Portability and Accountability Act (HIPAA).

h. **Physical Security.** Actions and activities designed to ensure the protection of IT Resources from physical threats such as unauthorized access, theft, vandalism, and natural disasters.

i. **Privileged User.** Authorized Users who have elevated access, with the ability to create, modify, and delete electronic resources, data, and system configurations.

5. POLICY.

a. All Authorized Users are required to complete applicable mandatory IT Security Training Courses, at a minimum, once every calendar year. All new Authorized Users will receive applicable mandatory IT Security Training Courses as part of new employee orientation.

b. All Authorized Users assigned an IT Security Training Course must complete the training within 21 calendar days of Commonwealth Network login activity or be subject to Active Directory account suspension for non-compliance.

c. IT Security Training Courses include enterprise courses (IT Security Awareness and Acceptable Use Training, IT Administrator Acceptable Use Training, and Fraud Awareness and Prevention Training). These enterprise trainings shall address Physical Security and IT security-based best practices, policies, procedures, and standards, as well as the importance of protecting confidential and sensitive information. In addition to the above, there may be other job or role-related required trainings, such as trainings on CJIS, FTI, or HIPAA. The completion of IT Security Training Courses is also a requirement of many state and federal regulations.

d. Managers will ensure that Authorized Users under their supervision are aware of, assigned, and complete the mandatory IT Security Training Courses. This includes ensuring new users who require other job or role-related required trainings are enrolled, assigned, and complete those training courses upon hire and annually thereafter. Managers shall ensure when an Authorized User is assigned IT Security Training Courses to complete, that such trainings are completed within 21 calendar days of Commonwealth Network login activity.

e. The Office of Administration (OA), Human Resources and Management, Bureau of Talent Development, will work with agency training coordinators and agency managers to ensure all Authorized Users have completed IT Security Training Courses.

f. Agency and Delivery Center Information Security Officers (ISOs), in conjunction with agency training officers, shall be responsible for maintaining and reviewing IT Security Training Course reports and reporting compliance to OA. Enterprise learning management tools will be used to provide reports of agency and employee compliance.

g. Employees or volunteers who fail to successfully complete assigned IT Security Training Courses, may be subject to the temporary or permanent removal of access or elevated privileges, and/or disciplinary action, up to and including termination of employment, as applicable, depending on the circumstances of the incident.

h. Contracted resources or consultants who fail to successfully complete assigned IT Security Training Courses, may be subject to the temporary or permanent removal of access or elevated privileges, and/or corrective action, up to and including termination of engagement, other action under the terms of the applicable contract, or suspension or debarment under the Contractor Responsibility Program.

6. RESPONSIBILITIES.

a. OA.

(1) EISO and the Bureau of Talent Development are responsible for developing the content of IT Security Training Courses and distributing that content in any form (i.e., computer-based training, classroom, video, etc.) necessary to reach all Authorized Users.

(2) EISO and the Bureau of Talent Development are responsible for tracking, compiling, and sharing reports of compliance to agency supervisors, monthly and as requested.

(3) The Bureau of Talent Development shall issue system generated email reminders to all Authorized Users who fail to complete their assigned enterprise courses. Supervisors will receive a copy of the system generated email to alert them of their Authorized User's non-compliance.

(4) EISO may suspend an Authorized User's account if the training is not completed within 21 calendar days.

b. Agencies.

(1) Ensure that all Authorized Users receive and complete IT Security Training Courses, as required.

(2) Ensure new users who require other job or role-related trainings are enrolled, assigned, and complete those trainings upon hire and annually thereafter.

(3) As appropriate, identify the roles that require additional specialized trainings (job or role-related) and share that information with EISO.

(4) When notified that an Authorized User has not completed the required IT Security Training Courses, notify the Authorized User of the non-compliance.

c. Authorized Users. Complete IT Security Training Courses based on their roles as outlined in the directive, but at a minimum of once each calendar year as directed by OA and the agency.

7. PROCEDURES.

a. EISO and the Bureau of Talent Development will coordinate the development of the yearly IT Security Training Courses.

b. The Bureau of Talent Development will communicate the availability of the yearly IT Security Training Courses to Authorized Users.

c. Authorized Users will complete required IT Security Training Courses at a minimum once each calendar year, as directed.

This directive replaces, in its entirety, *Management Directive 535.09 Amended*, dated January 25, 2022.