Cybersecurity Awareness & Training Standard

Committee on Information Technology

The City and County of San Francisco is dedicated to building a strong cybersecurity program to support, maintain, and secure its information and systems. The Cybersecurity Awareness and Training Standard is an implementing standard of the Citywide Cybersecurity Policy.

PURPOSE AND SCOPE

This document establishes the City and County of San Francisco (CCSF) Cybersecurity Awareness and Training Standard. The standard will help CCSF mitigate cybersecurity risks by training users, documenting the training, and communicating with them about cybersecurity best practices.

The goals of the Cybersecurity Awareness and Training Standard include:

1. Improving user awareness of the need to protect technology, information, and systems.
2. Ensuring users clearly understand their responsibilities for protecting information and systems.
3. Ensuring users are knowledgeable about CCSF cybersecurity policies, standards, guidelines, procedures and practices.
4. Developing user knowledge and skills so they can perform their jobs securely.
5. Ensuring that CCSF complies with federal, state and local government regulations and other requirements.

This standard applies to all CCSF information systems users with access to critical systems. These users may include: officers, elected officials, employees (including permanent civil service, exempt, temporary, full and part time, and provisional), consultants, vendors, interns, volunteers, or any other individual working on behalf of the City and County of San Francisco. These individuals are referred to collectively as "users" for purposes of this standard.

REQUIREMENTS

Users of CCSF information systems with access to critical systems shall participate in cybersecurity awareness training, including:

1. All users are required to take annual cybersecurity awareness training in the form of Computer- Based-Training (CBT) or instructor led workshops.
2. All new users are required to take mandatory cybersecurity awareness training in the form of the CBT or instructor led workshops.
3. Awareness reinforcement and additional training may be provided through newsletters, posters, phishing campaigns, screensavers, webcasts, workshops and national cybersecurity related events.

Records of training completion are required to be retained by and accessible to the Departmental Information Security Officer (DISO) and departmental human resources (HR) staff. Records shall be retained for a minimum of 2 years from last date of completion, or longer depending on departmental requirements.

COIT Policy Dates
Approved: 11/21/2019
Next Review Date: FY 2020-21

ROLES AND RESPONSIBILITIES

All Users of CCSF Information Systems

- Complete required annual training and participate in other awareness events.

City Chief Information Security Officer (CCISO)

- Work with the Department of Human Resources (HRD) to facilitate implementation of effective cybersecurity awareness and training programs citywide.
- Provide a cybersecurity awareness and training platform departments may utilize to comply with this standard.
- Publish annual role-based baseline cybersecurity awareness training. Departments may customize their training program to meet departmental needs.

Departmental Information Security Officers (DISOs) or Chief Information Security Officer

- Organize cybersecurity awareness training and other awareness activities for designated staff in their respective departments.
- Ensure the department's cybersecurity awareness and training program meets the regulatory and compliance requirements of the department and this standard.
- Work with departmental HR staff or other position designated by the department to track cybersecurity awareness training participation within their departments.

Department of Human Resources (HRD)

- Work with the City Chief Information Security Officer (CCISO) to facilitate implementation of effective cybersecurity awareness and training programs citywide.
- Provide a cybersecurity awareness and training platform that departments may utilize to comply with this standard.
- Work with departmental HR staff or other position designated by the department to track cybersecurity awareness training participation within their departments.

Departmental Human Resources Staff, or other staff responsible for managing training

- Maintain records of annual training completion for employees.

Department Heads

- Ensure compliance with this standard and program in their departments.

City Services Auditor

- Assess compliance with this standard.

COMPLIANCE

A department may restrict access to information systems of any user who fails to comply with the annual awareness training requirement, until the requirement is met.

REFERENCES

I. City Cybersecurity Policy
II. NIST Special publication 800-50
III. NIST Special publication 800-16