CYBERSECURITY AWARENESS AND TRAINING STANDARD - DRAFT

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

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:

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

SCOPE

This standard applies to all CCSF information systems users. These users 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 shall participate in cybersecurity awareness training, including:

a) All users are required to take annual cybersecurity awareness training in the form of Computer-Based-Training (CBT) or instructor led workshops.
b) All new users are required to take mandatory cybersecurity awareness training in the form of the CBT or instructor led workshops.
c) 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 Cybersecurity Liaison 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.

ROLES AND RESPONSIBILITIES

1.1 City Chief Information Security Officer (CISO)

- Facilitate implementation of effective cybersecurity awareness and training programs at departments.
- 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 add to or customize this baseline training to meet departmental needs.

1.2 Department Heads

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

1.3 Departmental Cybersecurity Officers / Liaisons

- Organize cybersecurity awareness training and other awareness activities at 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 to track cybersecurity awareness training participation within their departments.

1.4 Departmental HR

- Maintain records of annual training completion for employees.

1.5 City Services Auditor

- Assess compliance with this standard.

1.6 Users

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

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

AUTHORIZATION

SEC. 22A.3. of the City's Administrative Code states, "COIT shall review and approve the recommendations of the City CIO for ICT standards, policies and procedures to enable successful development, operation, maintenance, and support of the City's ICT."