Citywide Cybersecurity Policy

Committee on Information Technology

The City and County of San Francisco is dedicated to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. The following policy is intended to establish key elements of a citywide cybersecurity program.

PURPOSE AND SCOPE

The COIT Cybersecurity Policy lays the foundation for the City's Cybersecurity Program as a whole and articulates executive level support for the effort. Cybersecurity operations across the City are in different stages of operation. The Cybersecurity Policy will help build the City's Cybersecurity Program in order to:

- protect our connected critical infrastructure
- protect the sensitive information placed in our trust
- manage risk
- continuously improve our ability to detect cybersecurity events
- contain and eradicate compromises, restoring information resources to a secure and operational status
- ensure risk treatment is sufficient and in alignment with the criticality of the information resource
- facilitate awareness of risk to our operations within the context of cybersecurity

The requirements identified in this policy apply to all information resources operated by or for the City and County of San Francisco and its component departments and commissions. Elected officials, employees, consultants, and third parties working on behalf of the City and County of San Francisco are required to comply with this policy.

POLICY STATEMENT

The COIT Cybersecurity Policy requires all departments to:

1. Adopt a cybersecurity framework as a basis to build their cybersecurity program. The City recommends adopting the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a methodology to secure information resources.
2. Adopt citywide cybersecurity requirements upon their publication.
3. Conduct and update, at least annually, a department cybersecurity risk assessment.
4. Develop and update, at least annually, department cybersecurity requirements to mitigate risk profiles and comply with legal and regulatory cybersecurity requirements. Department cybersecurity requirements can be equivalent to or greater than the citywide security requirements.
5. Provide management level support to conduct cybersecurity operations.
6. Appoint a Departmental Cybersecurity Officer or security liaison to coordinate cybersecurity efforts.
7. Participate in citywide cybersecurity roundtable meetings.

COIT Policy Dates

Approved: November 17, 2016
Next Review Date: FY 2017-18

CYBERSECURITY FRAMEWORK

The Cybersecurity Policy requires all departments to adopt a cybersecurity framework to guide their operations.

In order to adequately protect information resources, systems and data must be properly categorized based on information sensitivity and criticality to operations. A risk based methodology standardizes the security architecture, creates a common understanding of shared or transferred risk when systems and infrastructure are interconnected, and makes securing systems and data more straightforward.

The NIST framework provides five elements to a cybersecurity program.

Function	Description
Identify	Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities.
Protect	Develop and implement the appropriate safeguards to ensure delivery of infrastructure services.
Detect	Develop and implement the appropriate activities to identify the occurrence of a cyber security event.
Respond	Develop and implement the appropriate activities to respond to a cyber security event.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired by a cyber security event.

Departments in consultation with the City Chief Information Security Officer (CISO) may choose alternatives to the NIST Cybersecurity Framework but all departments shall implement or consume central standards and services from their respective framework, such as access control and management, risk assessment and management, awareness and training, and data classification.

CYBERSECURITY RISK ASSESSMENT

As defined in the NIST Special Publication 800-30 – Guide for Conducting Risk Assessments, risk assessment is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization [i.e. CCSF departments] and the likelihood that such circumstances or events will occur.

The purpose of risk assessments is to inform decision makers and support risk responses by identifying: (i) relevant threats to [departments] …; (ii) vulnerabilities both internal and external to [departments]; (iii) impact (i.e., harm) to [departments] that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

To ensure their cybersecurity programs comply with the Cybersecurity Framework and the risk-based approach, the City Services Auditor will conduct readiness assessments to measure implementation.

Readiness assessments will align with the NIST framework and enable departments to determine their current cyber security capabilities, set individual goals for a target state, and establish a plan for improving and maintaining cyber security programs. Readiness assessments will also assist the Department of Technology and the Controller in the efficient and effective planning of cyber security activities.

ROLES AND RESPONSIBILITIES

1. **Department Heads** shall:
    a. Promote a culture of cybersecurity awareness and compliance to City's cybersecurity policy. Department heads must remind employees and contractors in their departments about the City's Cybersecurity policies, standards, procedures, guidelines and best practices.
    b. To the extent resources allow, budget and staff the cybersecurity function for systems procured, operated, or contracted by their respective departments to ensure that all systems and the data contained by them are protected in accordance with the category / classification of the data and systems.
    c. Designate a cybersecurity officer or liaison in the case of smaller departments. Departments should consult with the City's Chief Information Security Officer (CISO) to determine if their information technology activities warrant the appointment of a Department Cybersecurity Officer or if a Security Liaison is adequate.
    d. When appropriate, consult with the City CISO office when gathering the requirements for new information systems to ensure that the security design is vetted before selection and deployment.

2. **Department Cybersecurity Officers / Liaisons** shall:
    a. Ensure information resources are properly protected through risk treatment strategies that meet the acceptable risk threshold for the category / classification of the information resource.
    b. Inform the City CISO when there is an event which compromises the control, confidentiality, integrity, or availability of a system or data involving Personally Identifiable Information, Regulatory Protected Information (such as HIPAA or Social Security Numbers), and/or data that is not considered public as soon as practical.
    c. Participate in the citywide cybersecurity round table meetings.
    d. Conduct and update, at least annually, department cybersecurity risk assessment.
    e. Develop and update, at least annually, department cybersecurity requirements to mitigate department risk profile and comply with legal and regulatory cybersecurity requirements.

f. Develop an implementation plan for adoption of citywide cybersecurity requirements and department-specific cybersecurity requirements within 12 months from the publication of this policy.

3. **City Chief Information Security Officer** (CISO) shall:
    a. Ensure that Department, Commission, and the Centralized Information Technology Cybersecurity Programs employ a risk based assessment and treatment program, and regularly report the status of CCSF's residual risk profile to City leadership.
    b. Develop cybersecurity risk assessment methodology and provide training to Department Cybersecurity Officers / Liaisons on conducting cybersecurity risk assessments.
    c. Develop and update, at least annually, citywide cybersecurity requirements to mitigate CCSF's residual risk profile and comply with legal and regulatory cybersecurity requirements. The first set of cybersecurity requirements to be developed within 6 months from the publication of this policy.
    d. Develop and maintain a centralized incident response program capable of addressing major compromises of CCSF information resources.
    e. Establish and maintain a Security Operations Center with the capability to identify, protect, detect, respond, and recover from attacks against CCSF information resources.
    f. Support departments' implementation of citywide cybersecurity requirements. Support department Cybersecurity Officers/ Liaisons in their cybersecurity responsibilities, including through centralized incident response program, cybersecurity defense capabilities, and citywide standard cybersecurity toolset.
    g. Organize citywide round table cybersecurity meetings.

4. **COIT and Mayor's Budget Office** shall:
    a. To the extent possible, adequately support and fund City and Department's cybersecurity operations in alignment with the risk assessment.

5. **Chief Data Officer** shall:
    a. Work with the City CISO to develop and maintain an information classification system and support departments in their data classification efforts.

6. **City Services Auditor** shall:
    a. Support City cybersecurity efforts with regular readiness assessments and assist in the development and exercise of cybersecurity audit controls.
    b. Review, at least annually, department implementation plans for adoption of citywide cybersecurity requirements and department-specific cybersecurity requirements.
    c. Perform security testing for departments in alignment with the citywide cybersecurity requirements.

7. **CCSF Employees, contractors, and vendors** shall:
    a. Comply with cybersecurity practices, requirements, and Acceptable Use Agreement, and promptly report any incidents to the appropriate officials.

COMPLIANCE

To the extent resources allow:

1. Department Heads are responsible for ensuring that systems procured, operated, or contracted by their respective department or commission meet the appropriate security protections required by the system's risk category /classification, in addition to any regulatory requirements.
2. Employees, consultants, and vendors shall ensure that information resources are appropriately and securely utilized, administered, and operated while authorized access is granted, according to the Acceptable Use Policy.

EXCEPTIONS

No exceptions will be approved to this policy.

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."

REFERENCES

NIST Cybersecurity Framework Website - http://www.nist.gov/cyberframework/

DEFINITIONS

For a list of definitions please refer to: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf