Citywide Cybersecurity Policy

Committee on Information Technology

The City and County of San Francisco (City) is dedicated to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. The following policy is intended to maintain and enhance 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 deployment. The Cybersecurity Policy supports the City's Cybersecurity Program established 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 departments, and commissions. Elected officials, employees, consultants, and vendors 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. Appoint a Departmental Information Security Officer (DISO) to coordinate cybersecurity efforts. Larger Departments may appoint a Chief Information Security Officer (CISO) to recognize the increased scope of responsibility.
2. 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.
3. Support cyber incident response as needed in accordance with Emergency Support Function 18 (ESF-18) Unified Cyber Command.
4. Conduct and update, at least annually, a department cybersecurity risk assessment. Departments with dedicated Risk Management staff may elect to integrate cybersecurity risk management into the department's Risk Management program.
5. Develop and update, at least annually, department cybersecurity requirements to mitigate risk and comply with legal and regulatory cybersecurity requirements. Department will develop and adopt cybersecurity requirements that should be equivalent to or greater than the citywide security requirements.
6. Participate in citywide cybersecurity forum meetings.

COIT Policy Dates

Approved: November 21, 2019
Next Review Date: FY 2020-2021

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 security architecture, creates a common understanding of shared or transferred risk when systems and infrastructure are connected, 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 cybersecurity risk to systems, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of infrastructure services.
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to respond to a cybersecurity event.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired by a cybersecurity event.

Departments, in consultation with the City Chief Information Security Officer (CCISO), may choose alternatives to the NIST Cybersecurity Framework. However, 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 NIST Special Publication 800-30, "Guide for Conducting Risk Assessments," risk assessment is the process of identifying, estimating, and prioritizing information security risks.[1] Assessing risk requires the careful analysis of threat and vulnerability information to determine

[1] ISO 31000 "Risk Management – Guidelines" is another framework for risk assessment.

the extent to which circumstances or events could adversely impact an organization [i.e. City departments] and the likelihood that such circumstances or events will occur.

The purpose of risk assessment 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
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 an approved cybersecurity framework, including NIST CSF, ISO 2700x, and CIS Top 20, and a risk-based approach, the City Services Auditor conducts readiness assessments to measure implementation.

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

CYBERSECURITY REQUIREMENTS

Departments are required to develop and update cybersecurity requirements to mitigate risk profiles and comply with legal and regulatory cybersecurity requirements. The City Chief Information Security Officer will develop baseline cybersecurity requirements to address the citywide risk profile. All proposed requirements will be reviewed and approved by the Architecture Policy and Review Board (APRB). Upon adoption by the APRB, Departments should subsequently develop cybersecurity requirements that should be equivalent to or greater than the citywide security requirements to address department risks. APRB should establish meaningful timelines for adoption based on the complexity of the proposed requirements.

City-wide cyber-security requirements shall not supersede State or Federal requirements that may apply to certain specific city departments.

-

ROLES AND RESPONSIBILITIES

1. **Department Heads** shall:
    a. Promote a culture of cybersecurity awareness and compliance with the City's cybersecurity policy. Department heads must remind their employees and contractors 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 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 Departmental Information Security Officer (DISO) or a Chief Information Security Officer

2. **City Chief Information Security Officer (CCISO)** shall:
   a. Establish and maintain a security team and function with the ability to identify, protect, detect, respond, and recover from attacks against City information resources.
   b. Develop and maintain a centralized incident response program capable of addressing major compromises of City information resources.
   c. Review Emergency Support Function 18 Unified Cyber Command annex annually and ensure it is updated as needed.
   d. Support departments' cyber emergency exercises and conduct periodic Citywide cybersecurity emergency exercise with City leaders.
   e. 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 the City's residual risk profile to City leadership.
   f. Develop cybersecurity risk assessment methodology and provide training to DISOs on conducting cybersecurity risk assessments.
   g. Provide guidance on building the security organization at the department level.
   h. Ensure that Departments' cybersecurity risk assessment results are protected adequately and access is restricted to limited City cybersecurity personnel.
   i. At least annually, develop and update citywide cybersecurity requirements to mitigate the City's residual risk profile, and comply with legal and regulatory cybersecurity requirements. All cybersecurity requirements will be approved by the Architecture Policy & Review Board (APRB) before going into effect.
   j. Support departments' implementation of citywide cybersecurity requirements.
   k. Support department DISOs in their cybersecurity responsibilities, including through the centralized incident response program, cybersecurity defense capabilities, and a citywide cybersecurity toolset.
   l. Organize citywide cybersecurity forum meetings.

3. **Departmental Information Security Officers (DISOs)** 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. Develop the necessary security organizations based on the available resources and budget.
   c. Inform the City Chief Information Security Officer 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.

d. Participate in the citywide cybersecurity round table meetings.
e. Conduct and update, at least annually, department cybersecurity risk assessments, and confidentially share results with the City Chief Information Security Officer.
f. Meet annually with department Disaster Preparedness Coordinator to review results of cyber risk assessment and update department COOP cyber appendix as needed. Departments with dedicated Emergency Management Functions shall review the results of their department's cyber-security risk assessments and update their incident response procedures as appropriate
g. Conduct, at least annually, department cybersecurity emergency exercise with department leadership, City partners, and critical third parties. Departments with dedicated Emergency Management Functions may elect to incorporate cyber-security as part of their department emergency exercises.
h. Develop and update, at least annually, department cybersecurity requirements to mitigate department risk profile and comply with legal and regulatory cybersecurity requirements, and confidentially share requirements with the City Chief Information Security Officer. Department requirements that should be equivalent to or greater than the citywide security requirements.
i. When appropriate, consult with the City Chief Information Security Officer when gathering the requirements for new information systems to ensure the security design is vetted before selection and deployment.

4. **Department of Emergency Management**
    a. Activate the city emergency operations center to coordinate response to emergency level cyber event as outlined in Emergency Support Function 18 Unified Cyber Command.
    b. Support Citywide cybersecurity emergency exercise for City leaders in coordination with the City Chief Information Security Officer.

5. **Department Disaster Preparedness Coordinators (DPC)**
    a. Train department leadership and cybersecurity incident response staff with Department and Emergency Operation Center roles and responsibilities
    b. Work with the DISO to adopt the reporting processes for Emergency Support Function 18 Unified Cyber Command.
    c. Participate, at least annually, in the department cybersecurity emergency exercise.

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

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

8. **City Services Auditor** shall:

a. Evaluate City cybersecurity efforts with regular readiness assessments and assist in the evaluation of cybersecurity audit controls.
b. Review, at least annually, department implementation plans for adoption of citywide and department-specific cybersecurity requirements.
c. Perform security testing for departments in alignment with the citywide cybersecurity requirements to validate that departments effectively implement the requirements.
d. Share results of this testing with the Department Head, and when requested, facilitate the discussion of potential risk reduction strategies between the department and the City CISO.

9. **City 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 accountable 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.
3. City Services Auditor shall evaluate City cybersecurity efforts and validate departments' implementation of the applicable security requirements.

EXCEPTIONS

No exceptions to this policy will be approved.

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/
- Cyber Safe SF which contains documentation for the CCSF cybersecurity requirements and ESF-18 Unified Cyber Command - https://sfgov1.sharepoint.com/sites/TIS-National-Cybersecurity-Awareness

DEFINITIONS

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