# CCSF - Cybersecurity Policy (DRAFT)

The City and County of San Francisco (CCSF) requires a cybersecurity policy with clear, consistent and achievable standards applicable to all City departments to ensure the security of public, sensitive, and confidential data and systems. A comprehensive cybersecurity program guides departments in the effort to successfully identify, protect, detect, respond and recover from incidents whether deliberate or accidental.

**PURPOSE AND SCOPE**

In order to safeguard CCSF the Cybersecurity Program is designed 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 secured and operational status
- ensure risk treatment is adequate and in alignment with the criticality of the information resource
- facilitate awareness of risk to our operations within the context of cybersecurity

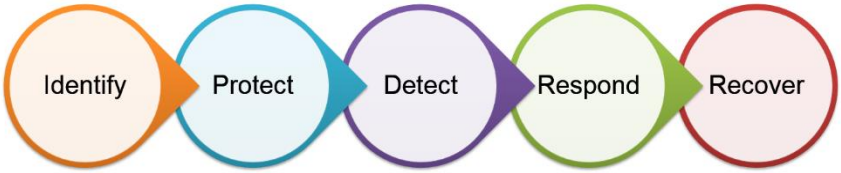
This policy applies to all information resources operated by or for the City and County of San Francisco and its component departments and commissions. Elected officials, employees, consultants, and vendors working on behalf of the City and County of San Francisco are required to comply with this policy.

**POLICY STATEMENT**

The Cybersecurity Policy lays the foundation for the City and County of San Francisco's (CCSF) Cybersecurity Program as a whole and demonstrates executive level support for the program. The program's charter, cybersecurity framework, policies, standards, and guidelines provide a risk-based approach to protect information resources essential to the effective and efficient government of the City and County.

Successful implementation of the policy relies heavily upon adoption of a framework on which to build the program. The Cybersecurity Framework, developed by the National Institute of Standards and Technology provides a methodology to secure CCSF information resources. It was designed to protect critical infrastructure and data. The Cybersecurity program will use the substantial body of documentation and processes developed by NIST.

**CYBER SECURITY PROCESS**



# CCSF - Cybersecurity Policy (DRAFT)

**POLICY REQUIREMENTS**

In order to adequately protect information resources, systems and data must be properly categorized based on information sensitivity and criticality to operations. Information resource classification drives the level of protection required for the system or data. This 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.

Departments shall

- Implement or consume central standards and services as they develop, such as access control and management, risk assessment and management, awareness and training, and data classification.
- Ensure their cybersecurity programs comply with the Cybersecurity Framework and the risk based approach. The core functions of the Cybersecurity Framework are:

*Identify*

- Asset Management (ID:AM) - The data, personnel, devices, systems, and facilities that enable the department to achieve business purposes are identified and managed consistent with their relative importance to department objectives and the department's risk strategy.
- Business Environment (ID:BE) - The department's mission, objectives, stakeholders, and activities are understood and prioritized to inform the context establishment of the risk assessment function.
- Governance (ID:GV) - The policies, procedures, and processes to manage and monitor the department's regulatory, legal, risk, environmental, and operational requirements are understood integrated into cybersecurity risk management process
- Risk Assessment (ID:RA) - The department understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), department assets, and individuals.
- Risk Management Strategy (ID:RM) - The department's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

*Protect*

- Access Control (PR:AC) - Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- Awareness and Training (PR:AT) - The department's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
- Data Security (PR:DS) - Information and records (data) are managed consistent with the department's risk strategy to protect the confidentiality, integrity, and availability of information.
- Information Protection Processes and Procedures (PR:IP) - Security policies, processes, and procedures are maintained and used to manage protection of

information systems and assets.

- Maintenance (PR:MA) - Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
- Protective Technology (PR:PT) - Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

*Detect*

- Anomalies and Events (DE:AE) - Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- Security Continuous Monitoring (DE:CM) -Information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Processes (DE:DP) - Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

*Respond*

- Response Planning (RS:RP) - Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- Communications (RS:CO) - Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- Analysis (RS:AN) - Analysis is conducted to ensure adequate response and support recovery activities.
- Mitigation (RS:MI) - Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- Improvements (RS:IM) - Department response activities are improved by incorporating lessons learned from current and previous detection/response activities.

*Recover*

- Recovery Planning (RC:RP) - Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- Improvements (RC:IM) - Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Communications (RC:CO) - Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

**ROLES AND RESPONSIBILITIES**

1. **Department Heads Shall**:
    a. Adequately 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 system.

   b. Consult with the City CISO to determine if their information technology activities warrant the appointment of Department Cybersecurity Officer or if a Security Liaison is adequate. All departments shall appoint an individual charged with the responsibility to coordinate risk management for information resources under the control of the department and ensure all information resources are properly categorized / classified.
   c. 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 Security 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. Represent their respective department at the quarterly CCSF Cybersecurity meeting.
   c. Provide periodic reports (monthly, quarterly, and ad hoc) on the status of their cybersecurity program and efforts to the City CISO.
   d. Inform the City CISO when there is an event which compromises the 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.
3. **City Chief Information Security Officer** 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. Ensure continued development and maintenance of Cybersecurity Policies, Standards, and Guidelines
   c. Develop and maintain a centralized incident response program capable of addressing major compromises of CCSF information resources.
   d. Investigate data and system compromises, identify the root cause, and develop remediation solutions in concert with the impacted department.
   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. Conduct quarterly citywide cybersecurity meetings.
4. **Chief Data Officer** shall work with the City CISO to develop and maintain an information classification system and support departments in their data classification efforts.
5. **Department Record Retention Managers** shall ensure that records are kept only for the required retention period and once expired it is disposed of through an approved method. If the system is unable to purge data no longer required due to technical limitations, this should be noted as a risk in the systems risk assessment and reasonable efforts should be made to update the system in future technology implementations. Compensating controls, such as encryption, should be explored to reduce the risk of exposure.
6. **City Services Auditor** shall support City cybersecurity efforts with regular reviews and assist in the development and exercise of cybersecurity audit controls.
7. **CCSF Employees, contractors, and vendors** must comply with cybersecurity practices and Acceptable Use Agreement, and timely report any incidents to the appropriate officials.

# CCSF - Cybersecurity Policy (DRAFT)

**COMPLIANCE**

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

**THIS POLICY TO BE REVIEWED ANNUALLY**