



Data Custodian and Stewardship Policy

Committee on Information Technology

PURPOSE AND SCOPE

The purpose of this policy is to:

- Designate Department of Technology (DT) as infrastructure manager (Custodian) performing data processing (Infrastructure Manager) for DT-managed IT assets.
- Designate City departments as data owners (Owners).
- Outline roles and responsibilities each party has in connection with this policy.

All other policies covering the authorized use of CCSF computing resources are still in effect, as are all regulations (e.g., HIPAA, CJIS, Sunshine Ordinance, Data Retention, etc.) which protect the confidentiality and integrity of data entrusted to CCSF departments.

This policy applies to DT-managed networks, hardware, software, storage, external cloud environments, SaaS and the data (database records, video, chat, phone, etc), where DT has direct administration and/or technical oversight. This is to be distinguished from a shared enterprise technology contract or agreement managed by DT whereby multiple departments may use the same Enterprise Agreement but manages or administers their technical implementations or instances separately from each other, including DT.

POLICY STATEMENT

The Department of Technology (DT) is and will at all times remain the “Custodian” of data transmitted, uploaded, accessed, or stored on DT managed City IT infrastructure. **Each Department is the “Owner” of the Department’s data and is responsible for any data practices governing access, segregation, and retention. Data ownership responsibilities belong to Departments, subject to the other related policies referenced below.** Further, DT will not share, record, transmit, alter, or delete information belonging to CCSF departments, except that DT will share and transmit information in response to a request from the City Attorney, Controller, or Ethics Commission related to investigation or a request from the City Attorney related to litigation.

POLICY DETAILS

The Department of Technology (DT) provides secure management of citywide Information Technology (IT) infrastructure including connectivity, networking, operational systems email/voice services, and software business applications. IT management includes the operational management of information stored in database tables, scanned images, audio recording, video recording, messages, emails, and other data types. City departments utilize the DT infrastructure to automate business processes and delivery high-quality public services.

COIT Policy Dates

Approved: October 21, 2021

During system administration and maintenance, DT performs operations necessary to support the infrastructure services, including IT security, management, and system performance tuning. DT has implemented and will maintain appropriate technical and organizational security measures for the storage and processing of data. These measures consider the nature, scope and purpose of data (production, development, test, disaster recovery and operational snapshots, backups, failover) and are intended to protect data against the risks inherent managing IT infrastructure, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to data. DT has implemented access controls, transmission encryption, disaster recovery, security protection and monitoring to protect data stored on the DT managed infrastructure.

DATA SECURITY AND PRIVACY EXPECTATIONS

DT takes its responsibilities regarding the security and privacy of information held in City enterprise platforms very seriously. On an annual basis, DT employees sign the DT Information Technology Employee Confidentiality Acknowledgement that certifies that DT employees will only access information/data on DT managed infrastructure, in the performance of job duties and for no other purpose. Additionally, DT has established CCSF cybersecurity practices and policies to govern DT's role in supporting, maintaining, and securing critical infrastructure and data systems.

Data belongs to the owning department, and it is DT's policy to hold such records as confidential information in accordance with applicable laws, policies, and procedures. In limited circumstances, exceptions to this policy may occur when necessary to comply with valid investigatory and legal requests.

Departments will provide DT with data security requirements (such as PII, CJIS, CLETS, POS) in order to secure data against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation, or misuse; and accidental loss, destruction, or damage. Data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department.

ROLES AND RESPONSIBILITIES

- **Department of Technology – Infrastructure Manager/Custodian**
 - Responsible for implementing the technical infrastructure and architecture for the shared enterprise platform.

- Establishes processes to sustain the security, integrity, transport and storage of data.
 - Maintains day-to-day operational and administrative management responsibility for databases, data sets, and enterprise information systems (O365) supported by DT.
 - Performs system maintenance to ensure availability and continuity of services.
 - Ensures access to enterprise applications and data is authorized and change management practices are applied in partnership with Data Owners.
 - Alerts, performs technical diagnosis and resolves faults in underlying software and hardware that could impact data quality, integrity, and consistency.
 - Manages all City data as confidential information and the release of which is only authorized by the owning department.
 - As Custodians of Departments' data, DT performs vendor risk-assessments and network scanning/monitoring to protect the infrastructure, data and services.
- **City and County of San Francisco Departments – Data Owner**
 - Creates, edits, defines access and deletes data in accordance with the department's business purposes and processes as well as retention policies.
 - Governs data retention for information.
 - Ensures effective local protocols are in place to guide appropriate use, quality, availability and integrity of data.
 - Complies with all legal, regulatory, and data policies and procedures. This includes responsibility for the classification of data in accordance with COIT's Data Classification Standard.
 - Works proactively with Infrastructure Manager to define the scope and limitations of security and access.

COMPLIANCE

All CCSF users (employees, temporary workers, contractors, vendors, interns, or volunteers) of DT-managed resources are responsible for complying with this policy. An employee who consistently fails to comply with this policy may be subjected to appropriate disciplinary action.

RELATED POLICIES

- [Citywide Data Classification Standard Policy](#)
- [Citywide Cybersecurity Policy](#)
- [Department of Human Resources Employee Handbook](#)
- [SFGovTV's Programming Policy](#)

- DT Citywide: City Attorney Lit Hold Procedure – 75-0003
- DT Information Technology Employee Confidentiality Acknowledgement that certifies that DT employees will only access information/data maintained by DT as required for the performance of assigned duties and for no other purpose.