City and County of San Francisco

Committee on Information Technology

Committee on Information Technology Monthly Meeting

May 21, 2026

Agenda

1. Call to Order by Chair
2. Roll Call
3. General Public Comment
4. Approval of the Meeting Minutes from April 16, 2026
5. Review of the Web Portal Naming and Maintenance Standard – (Discussion Item)
6. Review of the Draft Amendments to the Data Custodian Policy – (Discussion Item)
7. Review the Draft Unmanned Aircraft System (Drone Technology) Policy – (Discussion Item)
8. Chair Update
9. Chief Information Officer Update
10. Adjournment

Item Number 3

General Public Comment

Discussion Item

Item Number 4

Approval of Minutes from April 16, 2026

Action Item

Item Number 5

Web Portal Naming and Maintenance Standard Review

Digital Services

Discussion Item

Department of Technology (DT) and Digital Services (DS)

Web Portal Naming and Maintenance Standard

City Administrator's Office
Digital Services
May 21, 2026

Overview

We have passed both the Domain Management and Subdomain Management Standards through this body. We now present Portal Naming and Maintenance Standards to further our aims to:

- Increase trust in City websites
- Ensure website security and reliability
- Prepare the City to comply with the State Law AB1637 in 2029

Policy Development Process

- **February 2026:** Policy Review Board
  - Introduction of key points and goals of the policy draft
- **April 2026: Policy Review Board**
  - Updated draft policy circulated review and feedback
- **May 2026: Full COIT**
  - Introduction of policy via presentation and open to discussion and feedback
- **Summer 2026: Full COIT**
  - Item for vote at COIT

Policy overview

Portal naming and management key points

- Establishes naming and URL standards for all City portals (custom-built and SaaS) to ensure a consistent, trustworthy public-facing digital presence

- Defines an approval and governance process requiring departments to coordinate with Digital Services and DT when developing and launching new portals

- Mandates accessibility, official labeling, and a public portal listing on SF.gov so residents can easily use and find City portals

Portal Definitions

Custom portals

A *custom portal* is developed exclusively for the City and County of San Francisco by internal staff or a design-build vendor. It may be hosted on-premise, in DT's cloud, or by a vendor. In the past, custom portals have typically had either a unique URL or a xyz.sfgov.org URL.

Custom built by staff:
- housing.sfgov.org
- careers.sf.gov
- Dbiweb02.sfgov.org/dbipts

Custom built by vendors
- pay.sfgov.org
- sfcitypartner.sfgov.org

SAAS portals

A *SaaS portal* uses standard commercial functionality hosted and maintained by a software product company, and available to other jurisdictions or private-sector users. SaaS portals have historically used the software product's URL, with an indicator that the instance belongs to San Francisco (e.g., sf.company.com or company.com/sanfrancisco).

Examples of SaaS portals:
- Data.sfgov.org
- Sanfrancisco.nextrequest.com
- Sfpl.bibliocommons.com
- apm.activecommunities.com/sfrecpark

Naming Standards

Custom portals

A clear, short, plain-English third-level name that describes their purpose like careers.sf.gov.

- Consult Digital Services and DT about portal naming to ensure clarity and avoid duplicates.
- All custom portals should be clearly marked as official websites of the City and County of San Francisco, on the portal itself.

SAAS portals

SaaS portals should use "sanfrancisco" or "sf" in the second or third-level subdomain, like sanfrancisco.nextrequest.com

- When multiple City departments use the same SaaS product, each department should include both "sanfrancisco" (or "sf") and a department identifier, following the provider's naming convention
- Departments should coordinate with DS when onboarding a SaaS product to ensure naming consistency across instances.
- SaaS portals should offer clear indicators of their official status wherever possible

City Portal Public List

Departments must provide Digital Services with a list of their existing portals within 90 days of this policy being passed at COIT.

When submitting the list, Departments must include the following information:

- Portal URL
- Portal type (SaaS or custom)
- A 1–2 sentence description, suitable for translation into threshold languages, of who the portal is for and what it does
- Responsible department owner email and role

Digital Services will create and maintain a public list of City portals on SF.gov. As new SaaS or custom portals are created, owners must notify Digital Services so that the public list can be kept current.

Governance and Compliance

- Each portal must have designated technical and content owners in the respective department.
- Portals that are found to be non-compliant with this standard, including portals that are not listed, improperly named, or lack appropriate official labeling, may be required to remediate.
- COIT and Digital Services will review this standard periodically to ensure it remains aligned with evolving state law, City policy, and best practices in digital government.

Accessibility Standards and Maintenance

- As with all City web properties, portals must meet the Digital Accessibility and Inclusion Standard (DAIS) for all pages outside of any login wall. This requirement applies not only at initial launch but for any subsequent updates or upgrades over time.
- For custom portals, the department takes responsibility for DAIS compliance in conjunction with any contracted vendors.
- For SaaS portals, this responsibility primarily falls to the SaaS provider and must be addressed in the terms of the contract.

Policy Summary

1. Submit a list of existing portals to COIT and Digital Services within 90 days of this policy passing at COIT.

2. Follow the domain application process when launching any new portal, including proposed name, business justification, accessibility plan, and designated owners.

3. Notify Digital Services and COIT when onboarding any new SaaS portal, to ensure it's added to the public portal list and naming is coordinated.

4. Maintain ongoing compliance, including accessibility (DAIS) standards and self-certification by designated technical and content owners.

Appendix

Resources

- ICANN Domain Name Registration Process
- Canada's DNS services management summary
- California domain registration
- UC Berkeley domain registration policy, including procedures and responsibilities

Item Number 6

Review Draft Amendments to the Data Custodian Policy

Department of Technology

Discussion Item

COIT Data Custodian and Policy Amendments
Department of Technology

May 21, 2026

Overview of Policy & Proposed Amendments

Data Custodian and Stewardship Policy was adopted in October 2021 to define DT's and departments' roles for custody of data on DT-managed infrastructure

Problem:

- Ambiguity of policy defining DT as the "Infrastructure Manager/Custodian" of department's data
- For public records requests, this could be interpreted as giving DT the responsibility to respond to requests for other departments' data
- But DT doesn't have the legal authority to make disclosure and redaction decisions for other departments' data

Proposed Solution:

- Define DT as "Infrastructure Manager"
- Define Departments as "Data Custodians"
- Clarify that being a "Data Custodian" for public-records purposes requires having the legal authority to decide on disclosures

Background

- The Sunshine Ordinance Task Force recently requested that DT explain "why the department feels it is neither the custodian nor in custody of the requested records as described by the Sunshine Ordinance."
- The Sunshine Ordinance uses the term "custodian of a public record" but does not define it.
- The California Public Records Act also does not define "custodian."
- Recent court cases* suggest a definition where the "custodian" for public-records purposes must have both:
    1) Custody or control of the records and
    2) Legal authority to decide on disclosure.

* *Consolidated Irrigation District v. Superior Court*, *City of San Jose v. Superior Court*, and *Anderson-Barker v. Superior Court*

Various Improvements to the Original Policy

1. "Data processing" clarified: narrowed to technical processing needed to operate/secure DT-managed infrastructure *(p.1)*
2. Clarifies what "DT-managed" means: removed "technical oversight" and defined DT-managed infrastructure as systems DT operates/administers (helps clarify cases like AWS Connect). *(p.1)*
3. "Operational management of information" reframed: DT manages the systems that store/transmit information—not the information itself. *(p.2)*
4. Removed "data sets" from DT duties: DT's responsibility now covers
5. databases and enterprise information systems (not department data). *(p.3)*
6. Confirmed department control of data design: Data Custodians decide on how data is organized and structured unless otherwise agreed with DT. *(p.4)*
7. Protected existing agreements: policy does not supersede department-specific MOUs/operating agreements unless explicitly stated. *(p.4)*

Questions

Item Number 7

Review Draft Unmanned Aircraft System (Drone Technology) Policy

Department of Technology

Discussion Item

2026 Employee Unmanned Aircraft System (UAS) Policy

Enabling Safe, Coordinated, and Scalable City UAS Operations

Department of Technology
Emerging Technologies Division
May 21, 2026

Drafting Process

Partners:

1. DT (lead)
2. COIT (strategy + Chapter 19B alignment)
3. DataSF (data governance)

Timeline:

February 2025 - June 2025: Initial scoping & issue identification at DT Drone Group

July 2025 - December 2025:

- Department 1:1s SFPD, SFFD, SFPUC, DEM, PRT, DPW, DBI, SFO, SHF
- Monthly Drone Policy Working Group meetings

February 2026 – April 2026: Draft policy introduced to and discussed at COIT PRB

April 2026: Draft policy distributed to CIOs and IT leads for feedback

Why this update, why now?

Context changes since 2019

1. Drone use is expected to grow across departments and use cases

2. The policy landscape has evolved—overlaps with Chapter 19B

3. The risk environment has also changed, increasing the need for coordination through UTM/Remote ID and emergency operations (Emergency Operation Center/Incident Command System)

Limitations of the 2019 Drone Policy

1. The 2019 Policy was time-limited and subject to an evaluation.

2. Implementation surfaced compliance frictions (e.g., transparency).

3. Departments need a flexible, guardrails-based framework beyond a fixed list of pre-approved use cases.

4. Operational data needs aren’t well supported (e.g., livestream-only guidance vs. legitimate needs for data retention, access, and sharing).

What's new?

What's New (Brief Overview)

1. From “pre-authorized use cases” → **flexible framework**
2. Clear path to comply via **19B Surveillance Technology Policies**
3. Data handling aligned with **Data Management Policy**
4. Stronger coordination during **emergencies**
5. Groundwork for **airspace coordination / future Unmanned Aircraft Traffic Management (UTM)**
6. Strengthened governance: **Citywide drone group + dept managers**
7. Simpler yet meaningful transparency **requirements**

Key change #1: From Use Cases to Guardrails

2019

Defined, COIT-approved departmental use cases

1. Drone use limited to "**authorized use cases**" listed **by department**

2. Departments **could not use drones for any reason outside those authorized use cases**.

2026

Departments define and maintain their own authorized use-case list

1. Departments assessed their **use cases**.

2. Use cases must be documented in a STP where required by Chapter 19B (or otherwise authorized under applicable department or City legal authority).

Key change #2: Chapter 19B Alignment

2019

Separate departmental Drone Policy always needed

1. Participating departments were **required to adopt a departmental drone policy** reflecting the City template/requirements.

2. The drone policy is the controlling document for use cases and requirements.

2026

Separate departmental UAS Policy not always needed

1. Departments whose UAS operations are governed by a **STP do not necessarily need** to **draft/maintain a separate UAS Policy**

2. **Alternative pathway to "collectively implement" the UAS policy requirements:**
   - **STPs +**
   - **Internal operating procedures +**
   - **Contract terms**

Key change #3: Data Governance

2019 Minimize and contain UAS data

1. **Prefer livestream / don't retain** and avoid keeping raw archives longer than needed

2. **Restrict access** and **generally prohibit sharing raw data across departments** (limited exceptions for processing/cleanup, exigent public safety, or legal requirement).

2026 UAS data as a City asset

1. **Align UAS data to City data management + classification standards** and assign accountable roles (**Data Steward / Privacy Officer**).

2. Enable controlled sharing through secure access and documented authority.

Key change #4: Simplified Transparency

2019 Event-by-event public notice

1. **Pre-flight public posting:** publish a **flight summary 24 hours in advance** (plus on-site **signage**) for non-emergency flights.

2. **Emergency exception with after-action notice:** emergencies don't require advance posting, but must be **posted within 48 hours after** the flight.

2026 Program-level + routine reporting

1. **Ongoing public reporting:** post program information and publish a **monthly UAS flight log** (with limited exceptions for operational security/law enforcement sensitivity).

2. **Internal accountability records:** maintain detailed internal documentation (e.g., flight staffing/roles) for audits/investigations, alongside public-facing reporting.

Key change #5: Enhances City Coordination

NEW

Thank you

Item Number 8

Chair Update

Discussion Item

Item Number 9

Chief Information Officer Update

Discussion Item

Adjournment