# Citywide Technology Resilience Standard
Committee on Information Technology

The City and County of San Francisco (City) is dedicated to implementing and operating resilient systems and architectures, supporting access to critical services for the city, departments, and or public in the event of human-caused or natural disasters.

**PURPOSE AND SCOPE**

The Citywide Technology Resilience Standard is required for City Disaster Preparedness, Response, Recovery, and Resilience (DPR3) Policy compliance. The Citywide DPR3 Policy requires the City Chief Information Officer (CCIO) and City Chief Information Security Officer (CCISO) to develop achievable Technology Resilience Standards that ensure the delivery of public services during and after a disaster.

The requirements identified in this document apply to all technology platforms and services operated by or for the city. All departments, commissions, elected officials, employees, contractors, partners, bidders, and vendors working on behalf of the City are required to comply with this policy.

Department's IT leadership, operational and technology teams, emergency/disaster management professionals, and liaisons are responsible for implementing the following requirements.

**RESILIENCE REQUIREMENTS**

City departments must adopt the following minimum Resilience requirements. Departments should develop technology resilience requirements **equivalent to or greater than** these citywide requirements.

**City Systems Requiring Resilience Planning**

The resilience standard applies to the following types of technology:

- **On-Premises IT Infrastructure -** Software systems, databases, and hardware infrastructure deployed and housed from within a city facility. Department staff administers and maintains the Department's IT platforms and infrastructure. Only authorized staff within the department can access the software and data which system access is local to the department's local area network.
- **Hybrid Cloud IT Infrastructure** - Hybrid cloud refers to a mixed computing, storage, and software service environment comprising on-premises infrastructure, private cloud service, or a public cloud. A hybrid Cloud is a combination of public and private clouds, usually orchestrating a single IT solution between both.
- **Cloud IT Infrastructure (i.e., IaaS, PaaS) and Software as a Service (SaaS) -** Cloud computing delivers IT infrastructure and business application services through the Internet. These resources include data storage, servers, databases, networking, and software.
- **Technology Infrastructure** - The components of Technology Infrastructure are made up of interdependent elements, such as network components, servers, operating systems, and appliances.
- **Operational Technology (OT)** - Hardware or software that detects or causes a change through the direct monitoring and control of industrial equipment, assets, processes, and events. OT is common

in Industrial Control Systems (ICS) such as a Supervisory control and data acquisition (SCADA) system or building management system.

**System Analysis and Prioritization**

All technology business systems must be inventoried, with information describing the business purpose, user base, stored or processed data, and any regulatory requirements documented.

Departments will conduct a Business Impact Analysis (BIA) for each inventoried IT business system to understand the impact of a disaster/interruption on business operations, the dependencies for recovery, and recovery objectives. The completed BIAs are one component of a Department's IT Continuity of Operations Plan (COOP)/Disaster Recovery Plans (DRPs).

- TheA BIA will establish each system's Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
    - ***RTO*** *is the maximum* ***tolerable downtime*** *duration needed for a system to recover and be restored to normal from a disaster and become available for use after an incident. For example, if a critical public safety application must be recovered and available within 30 minutes before a significant public safety impact occurs, it the Department sets has an RTO of 30 minutes for that technology business system in the BIA.*
    - ***RPO*** *is the maximum* ***tolerable amount*** *duration of data loss before an unacceptable impact occurs. For example, if no more than 15 minutes of transactional data loss be tolerated data for a critical public health application can continue to be collected and restored manually for up to 4 hours, but there is no way to retain more than 4 hours without losing needed data, resulting in an adverse impact on public health, it has , the Department sets an RPO of 4 hours15 minutes for that technology business system in the BIA.*
- The BIA will categorize each system in Tier 1 through Tier 4.
    - **Tier 1 –** The department cannot operate without this service/technology, even for a short period of time (less than 1 hour). The impact on the business operations and potential data loss is incredibly significantly high, *e.g., disruption to public safety systems, city-managed Lifelines, radio Infrastructure, city and department Networks, and enterprise technology/applications*. Tier 1 systems require RTO of 0 to 4 hours and RPO of less than 15 minutes.
    - **Tier 2 –** The department can operate without this service/technology for a short period of time. The impact on the business and potential data loss are high. Tier 2 systems require RTO between 4 and 24 hours and RPO of less than 1 hour.
    - **Tier 3 –** The department could can work around the loss of this service/technology for a longer period days or perhaps a week. Still, . Eeventually, the process service/technology would have to be resumed for business operations and needs to be restored to normal use to prevent a financial, customer, operational, or legal/regulatory impact. Tier 3 systems require RTO and RPO less than 14 days.
    - **Tier 4 –** The department can operate without this service/product for an extended period, during which theis operation service/technology will be supported through backup/ alternative methods. Tier 4 systems require RTO and RPO less than 30 days.
- Department Head and CIO/IT Director will approve the BIA.

**Resilience Requirements**

The following Resilience requirements must be implemented for each business system tier for all types of technology platforms:

| Tier level | Resilience Strategy | Resilience Testing Frequency | Resilience Testing Type |
|---|---|---|---|
| Tier 1 | High Availability (HA) at the primary site, Active-Active (hot site), and offline backup (e.g., Immutable backup)<br><br>*For hot site, mirrored systems reside at the secondary/DR site, and most DR failover processes are automated. ~~for~~* ***RTO is ~~between~~ 0 to 4 hours ~~hrs~~ and RPO ~~in~~ is less than 15 minutes ~~mins~~***<br><br>~~*Example: Controller Payroll System.*~~ | Annually | Failover/ Failback or Parallel |
| Tier 2 | High Availability (HA) at the primary site, Active-Prepared (warm site), and offline backup<br><br>*For warm sites, pre-built DR systems are available for manual activation with active database replication. ~~for~~* ***RTO is between 4 to 24 hours ~~hrs~~ and RPO ~~for~~ is less than 1 hour.***<br><br>~~*Example: DEM 911 CAD.*~~ | Bi-Annually (Once every two years) | Failover/ Failback or Parallel |
| Tier 3 | Active-Passive with active database replication and offline backup<br><br>*The database is replicated and available for DR, but IT infrastructure will have to be procured~~,~~ and software installed from system backups. ~~for~~* ***RTO and RPO ~~in~~ are less than 14 ~~business~~ calendar days.***<br><br>~~*Example: JUSTIS System*~~ | Two - three years after successful test and restore from backup | Test the actual restore procedures from the data backup |
| Tier 4 | Cold Site (offline backups)<br><br>*For cold sites, no DR systems are available for recovery. The database will be restored from offline backups which are copies of the data set taken at a pre-determined point-in-time. IT infrastructure will need to be procured and installed, and software and configuration will be installed from backups. ~~for an~~* ***RTO and RPO ~~in~~ are less than 30 ~~business~~ calendar days.***<br><br>~~*Example: Telephone Billing System*~~ | Two - three years after successful test and restore from backup | Test the actual restore procedures from the data backup |

**Requirements for Cloud-based or Externally Hosted Technologies:**

Cloud-based or externally hosted technologies rely on the vendor for disaster recovery for business applications and databases. To ensure the availability of City services, departments will work with their procurement staff and the Office of the Purchaser to include the following requirements for any Hybrid Cloud, Cloud IT, or SaaS request for proposal (RFP), vendor contracts, and service level agreements as defined in the table below.

| Tier level | Resilience Vendor Reporting |
|---|---|
| Tier 1 | RTO less than 4 hours.<br>RPO less than 15 minutes.<br>Vendor to provide Resilience Test Report to the department annually.<br>If possible, the vendor will invite the department to participate in the vendor Resilience Test to validate Resilience capabilities. |
| Tier 2 | RTO less than 24 hours.<br>RPO less than 1 hour.<br>Vendor to provide Resilience Test Report to the department annually.<br>If possible, the vendor will invite the department to participate in the vendor Resilience Test to validate Resilience capabilities. |
| Tier 3 | RTO and RPO less than 14 days<br>If possible, the vendor to provide the Resilience Test Report to the department bi-annually. |
| Tier 4 | RTO and RPO less than 30 days<br>If possible, the vendor to provide the Resilience Test Report to the department bi-annually |

**ROLES AND RESPONSIBILITIES**

Citywide DPR3 Policy establishes roles and responsibilities of Operational and Technology teams and Emergency/Disaster Management professionals.

- Department Operational and Technology teams shall:
  - Build and implement Resilience by following the requirements defined in this standard
  - Coordinate with department emergency/disaster management professionals to ensure IT COOP/DRPs are current and complete Resilience testing on a specified regular schedule

- Department Emergency/Disaster Management Professionals shall:
  - Support a department's implementation and adherence to Citywide Resilience requirements by working with technology teams and leadership
  - Coordinate with department leadership and necessary operational or technology teams to update and maintain IT COOP/DRPs
  - Facilitate technology Resilience testing by coordinating with technology and operational teams on a regular schedule
- Department of Technology, Office of Cybersecurity - Technology Risk and Resilience Team
  - Provide needed guidance and resources for implementation, for example, BIA, IT COOP, and DR Test Plan templates, to all City departments
  - Create and maintain a central online Technology Risk and Resilience system to track the department's Resilience Standard implementation progress and support IT COOP annual review/updates
  - Report to COIT on non-compliance
- Office of City Purchaser and Department Procurement Specialists
  - Support inclusion of Resilience requirements during the procurement process

**IMPLEMENTATION REQUIREMENTS**

- Department must inventory their systems within three months and conduct a BIA within six months after this standard's publication date and annually after that
- Department must develop a Resilience implementation plan for Tier 1 and Tier 2 systems within 12 months of this standard's publication date
- Department must implement and test Resilience for Tier 1 systems within 12 months and Tier 2 systems within 15 months after this standards publication date and annually after that
- Departments should consider implementing Resilience for Tier 3 systems within 24 months after this standard's publication date and bi-annually after that

**EXCEPTIONS**

Exceptions to the standards shall be approved case-by-case basis by COIT Policy Review Board.

Citywide Technology Resilience requirements shall not supersede State or Federal requirements that may apply to specific city departments.