CCSF – DISASTER PREPAREDNESS, RESPONSE, RECOVERY AND RESILIENCY POLICY (DRAFT)

The City and County of San Francisco (CCSF) requires an IT-focused Disaster Preparedness, Response, Recovery and Resiliency (DPR^3) policy with clear, consistent and achievable standards applicable to all City departments that would ensure the delivery of public services during, and after, a disaster. A comprehensive IT-focused DPR^3 policy that guides departments on how to successfully prepare for, respond to, and recover from a disaster (either man-made or natural) is required to ensure that CCSF is ready to serve the public when disaster strikes.

PURPOSE AND SCOPE

The purpose of the COIT Disaster Preparedness, Response, Recovery and Resiliency (DPR^3) policy is to **define the requirements** for a baseline DPR^3 policy **applicable to all CCSF departments** that will lay the framework to recover IT Systems, Applications and Data from any type of disaster that causes a major outage. To ensure public services can be efficiently and effectively provided, the emphasis of this policy is to promote the resilience of CCSF's critical IT infrastructure, minimize the effects of a disaster upon departmental operations, and restore critical IT services. The **development, implementation, and regular testing** of disaster response, recovery and business resumption plans are critical to ensure a highly reliable and resilient IT infrastructure that performs as expected when most needed in an emergency.

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 COIT Disaster Preparedness, Response, Recovery and Resiliency (DPR^3) policy **requires all** City and County of San Francisco departments to develop and implement disaster-related planning for information technology systems and data, planning referred to herein as **IT Continuity of Operations Plans (IT COOP) or IT Emergency Response and Recovery Plans (IT ERRP)**. The IT COOP is a component of the larger departmental Continuity of Operations Plan; and the IT ERRP is a component of the departmental Emergency Response and Recovery Plan, hereinafter jointly referred to as IT COOP/ERRP. This DPR^3 policy outlines the requirements for preparedness, testing and redundancy to ensure the continuity of government operations and minimize disruption to vital public services. The policy provides citywide leaders and departmental managers with clear planning and preparation practices to build resiliency in order to mitigate risks.

Planning on how to effectively minimize, and recover from, the effects of a service-impacting disaster **must be coordinated citywide**, as success will rely upon the assistance, resources and expertise of multiple City agencies. Effective recovery is dependent on each City agency following agreed upon procedures and practices in order for the overall goals of timely response and recovery to be met.

CCSF – DISASTER PREPAREDNESS, RESPONSE, RECOVERY AND RESILIENCY POLICY (DRAFT)

POLICY REQUIREMENTS

1. IT COOP/ERRP drafts will be completed by July 2017. Final plans must be completed by July 2018 and updated at least biennially by each City department.
    a. Departments must include **a summary of systems and technologies**, assessment of redundancy needs and practices (planned and actual), along with the **identification of criticality** (high, medium, low).
    b. Departments must update its plans whenever departmental computing or telecommunications environments undergo significant changes.
    c. Such changes may include: physical facility, computer hardware/software, telecommunications hardware/software, telecommunications networks, application systems, organizational staffing and budgetary needs.
2. **All new City IT contracts, policies and procedures must incorporate disaster resiliency**. Existing contracts should be modified upon renewal to address disaster resiliency. If a department receives IT services from another department or an outside agency/vendor/organization, the department must make certain the DPR^3 policy requirements are addressed.
3. Each department shall develop (or revise) its IT COOP/ERRP to be in alignment with this COIT DPR^3 policy. A department must confirm its adherence to the COIT DPR^3 policy to the City Services Auditor (CSA) via annual submission of a DPR^3 policy compliance form. The CSA **may periodically audit** departmental IT COOP/ERRPs and test results for compliance with policy and standards.
4. **Each department is responsible and accountable for its own DPR^3 program**.
5. A departmental IT COOP/ERRP is primarily for departmental use.
    a. It should be adapted as necessary to meet individual departmental needs. However, all key business/departmental requirements shall be addressed in its plan.
    b. It must contain enough information to enable departmental management to be confident in the department's ability to resume mission-critical computing and telecommuting services and operations.
    c. It may contain references to another department's IT COOP/ERRP, or to a department's internal policy, standards or procedures manual.
6. Each department **shall test its IT COOP/ERRP at least annually**. The specific type, frequency and extent of the IT systems testing will depend upon:
    a. Criticality of business function
    b. Cost of executing the test plan
    c. Budget availability
    d. Complexity of information systems and components
    e. Results of prior testing
7. Each department shall **train its employees** to execute its IT COOP/ERRP. Training will consist of:
    a. Making employees aware of the need for an IT COOP/ERRP.
    b. Informing employees, as appropriate, of the existence of the plan and providing procedures to follow in the event of an emergency.
    c. Training all personnel with responsibilities identified in the plan to perform the appropriate disaster recovery/business resumption procedures.
    d. Providing the opportunity to practice disaster recovery/business resumption skills.

8. If two or more departments participate in operating/staffing a facility with IT Systems, they must develop a joint IT COOP/ERRP that meets their mutual needs and is in compliance with this COIT DPR[3] policy. Similarly, where departments are dependent on citywide networks and systems under the operation of the Department of Technology (DT), departments and DT must jointly coordinate service level needs and compliance, as appropriate based on the criticality of the system.
9. A department's IT COOP/ERRP shall include the following components:
    a. Communications: How will communications be accomplished during a major event? What contingencies and/or procedures are in place to communicate if/when landlines and/or cell service is down?
    b. IT Incident Response: Who is to be contacted, when and how? What immediate actions must be taken in the event of certain occurrences?
    c. IT Succession: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
    d. Criticality of Service List: List all IT Systems-dependent services provided categorized by high, medium and low criticality along with recovery timeframe requirements.
    e. Data Inventory and Security Assessment: Detail the data stored on the systems, its criticality, its confidentiality and adherence to SF Open Data Policy. The annual systems and dataset inventories can inform this step and are available on the open data portal.
    f. Data Backup and Restoration: Detail which data is backed up, the media to which it is saved, where that media is stored and how often the backup is done. Also describe how that data could be/will be recovered. How is data backed-up to a place outside of San Francisco's geological area and how often does it land in this distant place? How often are backups shipped, either physically or over a link, to the remote location?
    g. Drills and Testing: Departments need to document their drill plans, and the follow-up procedures from drills, for both data and critical systems. This should include devising action-items arising from the drill results along with procedures to implement the post-drill action items identified.
    h. Equipment Replacement: Describe what equipment is required to begin to provide services, list the order in which it is necessary and note where to purchase/obtain the equipment.
    i. Power Supply: Detail the power supply resources available to the department to maintain/restore power during, and after, an emergency. Provide details regarding the type and capacity of the power supply and the expected length of time the supply will last.
    j. Network and Telephony Connectivity: Detail the existing network and telephony systems in use and the redundancies and procedures in place to cope with an emergency and/or disaster.
    k. Cyber-Security: This component of a department's IT COOP/ERRP should adhere to the separate COIT Cyber-Security Policy.
10. **Department heads are responsible for ensuring compliance** with this policy.

*** Disaster Preparedness, Response, Recovery and Resiliency.** Includes, but is not limited to, the documentation, plans, policies and procedures that are required to restore normal operation to a City

department impacted by man-made or natural emergencies, outages or disasters. The key IT-related goals include:

- Resume critical processes and restore data.
- Safeguard data.
- Safeguard hardware, software and facilities.

ROLES AND RESPONSIBILITIES

1. **COIT:**
    a. Provide necessary support to Departments to enable them to develop and complete their IT COOP/ERRPs and provide ongoing policy guidance and oversight to ensure citywide consistency with DPR^3 standards and best practices.
2. **Department Head:**
    a. Responsible for ensuring compliance with this policy.
3. **Department CIO/IT Lead:**
    a. Responsible for development of IT COOP/ERRPs and ongoing testing and monitoring of DPR^3 compliance.
4. **Department Business Stewards/Owners:**
    a. Responsible for departmental business operations and compliance and specifying recovery time objectives.
5. **Department of Technology:**
    a. Responsible for developing and implementing IT COOP/ERRPs for Citywide IT infrastructure support, including, but not limited to, the citywide business network, internet connectivity, telecommunications and emergency radio communications, as well as assisting departments without internal IT staff with the development of their IT COOP/ERRPs.
6. **CSA Audits:**
    a. CSA Audits will periodically audit departmental IT COOP/ERRPs and test results for compliance with DPR^3 policy and standards.

AUTHORIZATION

SEC. 22A.3.(c) 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."

DEFINITIONS

Biennially: Once every two years.

Disaster Mitigation: Actions taken to reduce or eliminate the effects of a future emergency event.

Disaster Preparedness: Actions taken prior to an emergency event to ensure an effective response.

Disaster Response: Actions taken in response to an emergency. Efforts to minimize the hazards created by the disaster and fulfill the basic humanitarian needs of the affected population.

Disaster Recovery: Starts after the immediate threat to human life has subsided and its end goal is a return to normalcy.

Disaster Resiliency: The ability to recovery quickly from disasters and return to normalcy.

High / Medium / Low Criticality:

Importance of process for the department	Process dependency upon the IT System		
	Low Dependency	Medium Dependency	High Dependency
Low Importance	no criticality	no criticality	low criticality
Medium Importance	no criticality	low criticality	medium criticality
High Importance	low criticality	medium criticality	high criticality

IT Continuity of Operations Plan (COOP): Is a component of a Departmental Continuity of Operations Plan that ensures IT business processes can continue during a time of emergency or disaster by detailing the continuity procedures to be used during an emergency.

IT Emergency Response and Recovery Plan (ERRP): Is a component of a departmental Emergency Response and Recovery Plan that speaks to departmental IT processes and how they are available to support the responsibilities ascribed, beyond the normal operations of a department, in the CCSF Emergency Response Plan, and in accordance with applicable Federal, State and Local laws, regulations and Mayoral Executive Directives.

Mission Critical System: A system that is essential to the survival of a business or organization. When a mission critical system fails or is interrupted, business operations are significantly impacted.

Recovery Point Objective (RPO): The interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the maximum allowable threshold.

*Recovery Time Objective (RTO)***:** The duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

THIS POLICY TO BE REVIEWED ANNUALLY