Attachment 9

Contingency Planning Policy - ITAM-0615

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

Subject:	Contingency Planning Policy	Item Number:	ITAM-0615
Owner:	Department of General Services	Adoption Date:	MM/DD/20YY
Approver(s):	County Board of Supervisors	Review Date:	MM/DD/20YY
Version:	1.0	Page:	Page **1** of **7**

I. Purpose

To ensure that normal County Information Technology (IT) resources and information systems are available during times of disruption of services.

II. Audience

The primary audience for this policy is Information Technology Professionals (County executives, managers, employees, contractors, vendors, and third parties) whose responsibilities include managing, administering, and operating County networks or systems.

III. Scope

This policy applies to any Information System that electronically generates, receives, stores, processes, or transmits County-owned data, whether the system is hosted on the County network or by a third-party provider. Additionally, these provisions apply to anyone doing business as the County and/or in support of the County that is provisioned access to County Networks or systems. This includes employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties, collectively referred to hereafter as “agents”.

IV. Definitions

See ITAM-0602, Glossary of Definitions

V. Policy

It is the policy of the County Board of Supervisors that:

Central IT and Departments must have a plan in place to minimize the risk of disruption to services due to system unavailability. Contingency planning details the necessary procedures required to protect the continuing performance of business functions and services, including IT services, during an outage to successfully restore and operate systems and business functions during significant disruption. Creation, maintenance, and annual testing of a plan will minimize the impact of recovery and loss of information assets caused by events ranging from a single disruption of business to a disaster. Planning and testing provides a foundation for a systematic and orderly resumption of all computing services within an agency when disaster strikes.

Primary Components of an IT Contingency Plan are:

- Identification of a disaster/contingency team.
- Definitions of recovery team member responsibilities.
- Documentation of each critical system including:
    - Purpose

    - ▪ Hardware
    - ▪ Operating System
    - ▪ Application(s)
    - ▪ Data
    - ▪ Supporting network infrastructure and communications
    - ▪ Identity of person responsible for system restoration
- System restoration priority list.
- Description of current system back-up procedures.
- Description of back-up storage location.
- Description of back-up testing procedures (including frequency).
- Identification of disaster recovery site including contact information.
- System Recovery Time Objective (RTO).
- System Recovery Point Objective (RPO).
- Procedures for system restoration at backup and original agency site.

The following outlines the minimum security control requirements which all County information systems must adhere to in order to operate in a production environment:

1. CONTINGENCY PLAN

County IT or Departmental IT shall:

a. Develop a contingency plan for critical information systems, in direct guidance and association with the information system owner, that:

i. Identifies essential missions and business functions and associated contingency requirements.

ii. Provides recovery objectives, restoration priorities, and metrics.

iii. Addresses contingency roles, responsibilities, assigned individuals with contact information.

iv. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.

v. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

vi. Is reviewed and approved by the County CIO, and information system's owner management on at least an annual basis.

b. Distribute copies of contingency plans to key contingency personnel, identified by name and/or by business role.

c. Coordinate contingency planning activities with incident handling activities.

d. Update the contingency plan to address changes to the business owner's mission, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

e. Communicate contingency plan changes to key contingency personnel identified by name and/or by business role.

f. Protect the contingency plan from unauthorized disclosure and modification.

2. CONTINGENCY TRAINING

County IT or Departmental IT shall:

a. Provide contingency training to information system users (all departments, offices, including the commissions, districts, and Board of Supervisors) consistent with assigned roles and responsibilities

b. Ensure designated personnel receive contingency training at least biannually of assuming a contingency role or responsibility, and when required by information system changes.

3. CONTINGENCY PLAN TESTING

County IT or Departmental IT, along with County information systems owners, shall:

a. Test the contingency plan for the information system, as determined by the mission critical nature of the business system(s) no less than annually.

b. Use strategic and tactical planning during testing to simulate a production information system to determine the effectiveness of the plan and the organizational readiness to execute the plan.

c. Review the contingency plan test results.

d. Initiate corrective actions, as needed.

e. Coordinate contingency plan testing with organizational elements responsible for related plans; plans related to contingency plans for information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans.

4. ALTERNATE STORAGE SITE

County IT or Departmental IT, in direct guidance and association with the County information system owner, shall:

a. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.

b. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

c. Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

d. Identify and document potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

5. ALTERNATE PROCESSING SITE

County IT or Departmental IT, in direct guidance and association with the County information system owner, shall:

a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of the information system operations for essential missions/business functions within the time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.

b. Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the agreed upon time period for transfer/resumption.

c. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.

d. Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

e. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

f. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with County business objectives and availability requirements.

6. TELECOMMUNICATIONS SERVICES

County IT or Departmental IT shall:

a. Establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within agreed upon recovery timeframes when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

b. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with agreed upon recovery objectives and availability requirements.

c. Request Telecommunications Service Priority for all telecommunications services used for security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

7. INFORMATION SYSTEM BACKUP

County IT or Departmental IT, in direct guidance and association with the County information system owner, shall:

a. Conduct backups of user-level information contained in the information system defined by frequency consistent with recovery time and recovery point objectives.

b. Conduct backups of system-level information contained in the information system defined by frequency consistent with recovery time and recovery point objectives.

c. Conduct backups of information system documentation including security-related documentation defined by frequency consistent with recovery time and recovery point objectives.

d. Protect the confidentiality, integrity, and availability of backup information at storage locations.

e. Test backup information to verify media reliability and information integrity.

8. INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

County IT or Departmental IT, in direct guidance and association with the County information system owner, shall:

a. Provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

b. Provide that the information system implements transaction recovery for systems that are transaction-based.

VI. Exceptions

See ITAM-0600, IT Security Program

VII. Non-Compliance

See ITAM-0600, IT Security Program

VIII. References and Sources

1. Applicable Rules, Laws, and Regulations:
   a. National Institute of Standards and Technology (NIST) Special Publications (SP):

      i. NIST SP 800-53a – Contingency Planning (CP)

      ii. NIST SP 800-16

      iii. NIST SP 800-34

      iv. NIST SP 800-50

      v. NIST SP 800-84

   b. NIST Federal Information Processing Standards (FIPS) 199

   c. State of California State Administrative Manual (SAM) 5300 et seq.

   d. Statewide Information Management Manual (SIMM) et seq.

2. Related Policies:

3. Referenced Documents:

4. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	CISO/Policy Committee	08/25/2021