| Policy #: | Title: | Effective Date: |
|---|---|---|
| x.xx | Contingency Planning Policy | MM/DD/YYYY |

PURPOSE

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

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Contingency Planning (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST SP 800-84; NIST Federal Information Processing Standards (FIPS) 199

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. CONTINGENCY PLAN
   IT Department shall:

   a. Develop a contingency plan for the information system, 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 CISO (Chief Information Security Officer), the Business Continuity Manager 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
   IT Department shall:

   a. Provide contingency training to information system users 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
   IT, along with 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

IT, in direct guidance and association with the 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
   IT, in direct guidance and association with the 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 business objectives and availability requirements.

6. TELECOMMUNICATIONS SERVICES
   IT Department 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 national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

7. INFORMATION SYSTEM BACKUP
   IT, in direct guidance and association with the 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
   IT, in direct guidance and association with the 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.

COMPLIANCE

---

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to Information Technology (IT) resources, and other actions as well as both civil and criminal penalties.

## POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

## RESPONSIBLE DEPARTMENTS

Chief Information Office and Information System Owners

## DATE ISSUED/DATE REVIEWED

| | |
|---|---|
| Date Issued: | MM/DD/YYYY |
| Date Reviewed: | MM/DD/YYYY |