[Insert Company Name Or Logo]	
Title: Cybersecurity Continuity of Operations Plan Testing Policy	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: To specify procedures for periodic testing and revision of contingency plans. Proper testing and revision will serve to continually refine recovery procedures and reduce the potential for failure and unauthorized access to sensitive and regulated data.

Scope: This policy applies to all employees and other members of the workforce (whether paid or volunteer) working in all facilities under the organization's ownership.

Definitions:

1. Disaster (Information System): An event that makes the continuation of normal information system (IS) functions impossible; an event which would render the information system unusable or inaccessible for a prolonged period of time (may be departmental or organization-wide).
2. Disaster Recovery Coordinator (DRC): Individual assigned the authority and responsibility for the implementation and coordination of IS disaster recovery operations.
3. Disaster Recovery Plan: The document that defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.
4. Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices; an adverse event whereby some aspect of computer security could be threatened; an IS Disaster would be considered a security incident.

Policy: In order to ensure that backup and emergency plans are effective when necessary [Insert Company name] requires periodic testing of all procedures and plans. Should any of the plans and policies not meet facility requirements, revisions will be made.

Procedure:

1. The Disaster Recovery Coordinator will implement all the testing for Emergency and Contingency plans. The DRC will work with the Security and Privacy officers to ensure that sensitive and regulated data remains confidential during this testing.
2. Two types of testing will be performed:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

    a. Announced:
        i. In an announced test, employees are instructed when testing will occur, what the objectives of the test are, and what the scenario will be for the test.
        ii. Announced testing is helpful for the initial test of procedures.
        iii. It gives teams the time to prepare for the test and allows them to practice their skills.
        iv. Once the team has had an opportunity to run through the procedures, practice, and coordinate their skills, unannounced testing may be used to test the completeness of the procedures and sharpen the team's abilities.
    b. Unannounced:
        i. Unannounced testing consists of testing without prior notification.
        ii. The use of unannounced testing is extremely helpful in preparing a team for emergency response because it focuses on the adequacy of in-place procedures and the readiness of the team.
        iii. Unannounced testing, combined with closely monitored restrictions, will help to create a simulated scenario that might exist in an actual contingency operation.
        iv. This more closely measures the teams' ability to function under the pressure and limitations of a disaster.
    c. Once it has been determined whether a test will be announced or unannounced, the actual objective(s) of the test must be determined.

3. A recommended schedule for testing is as follows:
    a. Desktop testing on a quarterly basis.
    b. One structured walk-through per year.
    c. One integrated business operations/information systems exercise per year.
    d. Data backups are stored off-site.
    e. Facility systems may have regular downtime, so this testing may not be required
    f. Facility disaster testing and response required every month (fire, flood, earthquake, etc.).
    g. Generator and backup testing semi-annually.
4. Address how documentation will be collected and maintained from the practice and drills.

VIOLATIONS: Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.