

Contingency Planning Policy

Approved Date – 02/22/2021

Published Date – 02/22/2021

Review Date – 03/29/2024

1. Purpose

Specify the requirements for the development and maintenance of effective plans for the District of Columbia Government (District) to contain and recover from any emergencies, disasters, and other occurrences (such as fire, vandalism, system failure, natural disaster, etc) that may affect the District information systems.

2. Authority

DC Official Code § 1-1401 et seq., provides the Office of the Chief Technology Officer (OCTO) with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District government. This document can be found at: <https://code.dccouncil.gov/us/dc/council/code/sections/1-1402>.

3. Applicability

This policy applies to all District workforce members (including contractors, vendors, consultants, temporary staff, interns, and volunteers) performing official functions on behalf of the District, and/or any District agency or entity (e.g. subordinate and independent agencies, Council of the District of Columbia, D.C. Charter Schools, etc.) who receive enterprise services from OCTO. In addition, this policy applies to any provider or third-party entity with access to District information, networks, and applications.

4. Policy

District agencies and departments must develop or adhere to a strategy which demonstrates compliance with this policy and its related standards. The following outlines the requirements for this policy. OCTO will review, update, and disseminate this policy annually at a minimum, to ensure accuracy, clarity, and completeness. The District's agencies must develop and review or update annually and after changes to the policy, a procedure in support of this policy with the following requirements.

4.1. Contingency Plan

All District agencies must:

4.1.1. Develop a contingency plan for the information system that:

- Identifies essential missions, business functions, and appropriate contingency requirements.
- Provides recovery objectives, restoration priorities, and metrics.
- Addresses contingency roles, responsibilities, and outlines the assigned individuals with contact information.

- Addresses the maintenance of essential missions and business-critical functions during an information system disruption, compromise, or failure.
- Addresses full information system restoration without deterioration of security safeguards originally implemented.
- Is reviewed by Agency ISOs and approved by senior management.

4.1.2. Distribute copies of the contingency plan to the ISO, senior management, and the appropriate teams (e.g., Network Operations, Security Operations) on an as-needed basis.

4.1.3. Coordinate contingency planning activities with incident response activities.

4.1.4. Review the contingency plan for the information system on an annual basis.

4.1.5. Update the contingency plan to address changes to the agency, information system, or environment of operation, as well as problems encountered during contingency plan implementation, execution, or testing.

4.1.6. Communicate contingency plan changes to senior management, ISSOs, and ISCP Coordinators.

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

4.2. Contingency Training

All District agencies must provide contingency training to information system users consistent with assigned roles and responsibilities:

4.2.1. Within 30 days of assuming a contingency role or responsibility.

4.2.2. When necessary due to information system changes.

4.2.3. Annually or as needed thereafter.

4.3. Contingency Plan Testing

All District agencies must coordinate contingency plan testing with District departments and groups responsible for related plans. A copy of the test report must be provided to District agencies.

Agencies must:

4.3.1. Test the contingency plan for the information system annually using test methodologies such as tabletop exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan.

4.3.2. Review the contingency plan test results.

4.3.3. Initiate corrective actions, if needed.

4.4. Information System Backup

All District agencies must:

- 4.4.1.** Conduct backups of user-level information contained in the information system on a daily (available for up to four (4) weeks), weekly, or monthly basis consistent with recovery time and recovery point objectives.
- 4.4.2.** Conduct backups of system-level information contained in the information system on a daily (available for up to four (4) weeks), weekly, or monthly basis consistent with recovery time and recovery point objectives.
- 4.4.3.** Conduct backups of information system documentation including security-related documentation on a monthly and annual basis, and/or when updates are required, consistent with recovery time and recovery point objectives.
- 4.4.4.** Protect the confidentiality, integrity, and availability of backup information at storage locations.

4.5. Information System Recovery and Reconstitution

All District agencies must provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure with specific timelines that are based on operational impact.

5. Exemptions

Exceptions to this policy shall be requested in writing to the Agency's CIO and the request will be escalated to the Chief Information Security Officer (CISO).

6. Definitions

The definition of the terms used in this document can be found on the [Policy Definitions website](#).