Office of the Chief Technology Officer

Office of the Chief Technology Officer

Office Hours
Monday to Friday, 8:30 am to 5:30 pm

Connect With Us
200 I Street, SE, Washington, DC 20003
Phone: (202) 727-2277
Fax: (202) 727-6857
TTY: 711
Email: octo@dc.gov

Ask the Chief Technology Officer
Agency Performance

Contingency Planning Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Revised Date – 02/23/2023

1. Purpose

Specify the requirements for the development and maintenance of a plan for the District of Columbia Government (District") to contain and recover from any emergencies, disasters, and other occurrences (for example 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.us/dc/council/code/sections/1-1402.html*.

3. Applicability

This policy applies to all District workforce members performing official functions on behalf of the District, and/or any District agency/District/entity who receive enterprise services from OCTO. In addition, this policy applies to any provider and third-party entity with access to District information, systems, 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.

The District's agencies must develop and review or update annually and after change to the policy, a procedure in support of this policy wi0th the following requirements.

4.1. Contingency Plan

All the District agencies must:

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

- Identifies essential missions, business functions, and contingency requirements.
- Provides recovery objectives, restoration priorities, and metrics.
- Addresses contingency roles and responsibilities for assigned individuals and provides contact information.
- Addresses the maintenance of essential missions and business-critical functions during an information system disruption, compromise, or failure.
- Addresses the full restoration of information systems without the deterioration of security safeguards.
- Is reviewed and approved by Senior Management, ISOs, and ISCP (information system contingency plan) Coordinators.

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 handling activities.

4.1.4. Review the contingency plan on an annual basis.

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

4.1.6. Communicate contingency plan changes to Senior Management, ISOs, ISSOs, and ISCP Coordinators.

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

4.2. Contingency Training

All the 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 required by information system changes.

4.2.3. Annually or frequently as needed thereafter.

4.3. Contingency Plan Testing

All the 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 do the following:

4.3.1. Test the contingency plan for the information system annually using test methodologies like 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 the 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, and 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, and 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 the 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 is based on risk assessment.

5. Exemptions

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

6. Definitions

The definition of the terms used in this document can be found in the *Policy Definitions* website.


BEST OF THE
WEB
2014 WINNER


BEST OF THE
WEB
2013 FINALIST