Incident Response Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Review Date – 05/17/2024

1. Purpose

Establish requirements for effective and efficient identification, reporting, escalation, response to, and evaluation of whether any security compromises or other related incidents that occur within the District of Columbia Government (District) Information Systems have been resolved.

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 performing official functions on behalf of the District Government, and/or any 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/or 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. Incident Response Training

District agencies must:

4.1.1. Provide incident response training to information system users consistent with assigned roles and responsibilities.

4.1.2. Provide training before assuming an incident response role or responsibility, when required by information system changes, and annually thereafter for as long as that responsibility remains.

4.1.3. Provide additional or supplemental IR training when information system changes occur.

4.2. Incident Response Testing

District agencies must annually test the incident response capabilities for the information

system using organizational resources responsible for related plans to determine the incident response effectiveness and then document the results.

4.3. Incident Handling

District agencies:

4.3.1. Must implement an Incident Response Plan for handling security incidents that include preparation, detection, analysis, containment, eradication, recovery, and post-incident activity.

4.3.2. Coordinate incident handling activities with contingency planning activities.

4.3.3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

4.4. Incident Monitoring

District agencies must track and document information system-level security incidents.

4.5. Incident Reporting

District agencies must:

4.5.1. Require personnel to report suspected security events to the District Security Operations Center (SOC) immediately the event is discovered.

4.5.2. Report all identified Information Security Incidents to the Office of Information Security

- Contact the SOC by phone at +1-202-724-2447
- Contact the SOC by email at *soc@dc.gov*

4.6. Incident Response Assistance

District agencies must provide incident response support that offers advice and assistance to users of agency-managed information systems for the handling and reporting of security incidents.

4.7. Incident Response Record Retention

The District agency must retain all documents and data related to an incident according to the agency's data retention schedule as required by the Data and Records Retention Policy.

4.8. Incident Response Plan

The District must develop an incident response plan that:

4.8.1. Provides the organization with a roadmap for implementing its incident response capability.

4.8.2. Describes the structure and organization of the incident response capability.

4.8.3. Provides a high-level approach for how the incident response capability fits into the District processes.

4.8.4. Meets the unique requirements of the District, which relate to mission, size, structure, and functions.

4.8.5. Is tested at least once every 6 months.

4.8.6. Defines reportable incidents.

4.8.7. Provides metrics for measuring the incident response capability within the District.

4.8.8. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

4.8.9. Is reviewed and approved by the Chief Technology Officer who will in turn:

- Distribute copies of the incident response plan to all District agencies
- Review the incident response plan once every quarter
- Update the incident response plan to address system/organizational changes or problems encountered during implementation, execution, or testing of the plan
- Communicates incident response plan changes to all District agencies
- Protects the incident response plan from unauthorized disclosure and modification

5. Exemption

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) for approval.

6. Definitions

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