Cyber Security Incident Response Team Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Reviewed Date – 05/10/2024

1. Purpose

Establish policy for the appropriate functions and duties of the District's Cyber Security Incident Response Team.

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. 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 responsible for application identity and role definition on behalf of the District, and/or any entity who receives any enterprise services from OCTO. In addition, this policy applies to any provider or third-party entity with access to District information, systems, networks, and applications.

4. Policy

DC agencies must adopt the framework provided in this policy when responding to cybersecurity incidents to ensure that they safeguard the information systems and information technology contained on the internal District of Columbia Wide Area Network (DC Government system). 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. Identification of Incidents

4.1.1. All users of the DC Government system must refer cybersecurity-related suspicious activities or concerns (security events) to the OCTOHelps or the Security Operations Center (SOC) for the appropriate security review and handling through the following:

- Contact the SOC by phone at +1-202-724-2447
- Contact the SOC by email at *soc@dc.gov*
- Contact the OCTOHelps at +1-202-671-1566

4.1.2. After the security incident is reported to OCTO, or after it is discovered by OCTO's internal monitoring, OCTO will take the following actions:

- Log and track the reported incidents; and

- Take steps to investigate, escalate, remediate, refer, otherwise address the incident.

4.1.3. Agency Chief Information Officers (CIO) and/or Agency Information Security Officers (ISO) must participate in all CSIRT security incident-related communications regarding his or her DC Agency until CSIRT remediates or stabilizes the security incident.

4.2. Cyber Security Incident Response Team (CSIRT) and Coordinator

4.2.1. CSIRT Coordinator: OCTO will have a dedicated CSIRT coordinator that is responsible for all communication regarding security incidents. The CSIRT coordinator is responsible for resolving and reporting security incidents and assembling a CSIRT team. The Chief Technology Officer (CTO) or his or her designee must designate an OCTO employee to serve as the CSIRT coordinator.

4.2.2. CSIRT Team: The CSIRT coordinator must identify and recruit Agency CIOs, Agency ISOs, and associated stakeholders to form the CSIRT. The membership of the CSIRT depends upon the severity level of an incident.

4.3. Security Incident Classification Matrix

OCTO has established a Security Incident Assessment Classification Matrix (Matrix) to guide CSIRT's response to each security incident. The Matrix establishes a class of security incidents and specific procedures for responding to each class of security incident. The description of each class of security incidents identifies the OCTO personnel and DC Agency personnel which must be contacted and engaged to resolve the security incident. Lastly, the Matrix contains escalation procedures that identify contact persons within OCTO and, if applicable DC Agencies, to respond to each level of escalation and must be included within the Incident Response Plan.

4.4. Documentation and Communication of Incidents

OCTO will ensure that incidents are appropriately logged and archived. The CSIRT Coordinator will be responsible for communicating the incident to appropriate personnel and provide updates and instruction for the duration of the incident.

4.5. Subordinate Procedures

The Chief Information Security Officer (CISO) must maintain standard procedures to respond to and investigate each security incident. They must also ensure the custody of any evidence obtained during the investigation. The Incident classification matrix governs the application of these procedures.

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*.