



Cyber Security Incident Response Team Policy

Policy Number:	OCTO – 2020.0	Creation Date:	4/22/2016
		Approval Date:	4/22/2016
Effective Date:	4/22/2016	Revised Date:	

1. **Scope/Applicability:** This policy applies to all District of Columbia (DC) Government agencies (“DC Agency” or “DC Agencies”).
2. **Authority:** DC Official Code § 1-1401 et seq.
3. **Purpose:** The Office of the Chief Technology Officer (OCTO) Cyber Security Incident Response Team (CSIRT) Policy (“Policy”) establishes the methodology for DC Agencies to use to identify, track, and respond to network and computer-based information security incidents. DC Agencies’ adherence to this Policy ensures that DC Agencies are properly coordinating, remediating, investigating and reporting DC Government cyber security related events. This policy governs CSIRT activities related to cyber security incidents discovered by OCTO or DC Agencies’ personnel and users.
4. **Policy:** DC Agencies must adopt the following framework when responding to cyber security 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):

4.1. Identification of Incidents

- 4.1.1. All users of the DC Government system must refer cyber security related suspicious activities or concerns (“security incident”) to OCTO for security incident handling.
- 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:
 - i. Log and the track reported incidents; and
 - ii. 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 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 DC Agency CIOs, DC 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 must establish a “Security Incident Assessment Classification Matrix” (“Matrix”) to guide CSIRT’s



District of Columbia Government – Office of the Chief Technology Officer

response to each security incident. The Matrix must establish a class of security incidents and specific procedures for responding to each class of security incident. The description of each class of security incidents must also identify the OCTO personnel and DC Agency personnel that must be contacted and engaged to resolve the security incident. The Matrix must establish escalation procedures that identify contact persons within OCTO and, if applicable DC Agencies, to respond to each level of escalation.

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 maintaining contact, for the purpose of update and instruction, for the duration of the incident.

4.5. Subordinate procedures

The OCTO Chief Information Security Officer (CISO) or IT Security Director must maintain standard procedures to respond to and investigate each security incident. He or she must also secure the custody of any evidence obtained during the investigation. The Incident classification matrix will govern the application of these procedures.

5. **Policy Maintenance:** OCTO is responsible for the maintenance, administration, and publication of this policy. OCTO must annually review this policy and update as needed to ensure the policy's technical relevance and regulatory compliance.
6. **Policy Enforcement:** OCTO is responsible for the enforcement of this policy. DC Agencies must actively participate in the audit of this policy when requested by the OCTO.
7. **Exemptions:** None.
8. **Sanctions:** If OCTO discovers non-compliance with this policy, OCTO will:
 - 8.1. Advise the DC Agency CIO of the non-compliance and assist the DC Agency CIO in developing a corrective action plan and a reasonable timeframe for its implementation.
 - 8.2. If the DC Agency CIO does not implement the corrective action plan within the stated timeframe, OCTO will escalate the matter to the DC Agency Director for immediate action and resolution.
 - 8.3. If the DC Agency Director does not resolve the policy non-compliance within his/her DC Agency, OCTO will refer the matter to the DC City Administrator for immediate action and resolution.
9. **Supporting Laws and Regulations:**
 - 9.1. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA).
 - 9.2. Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579.
 - 9.3. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.
10. **Reference Documents:**
 - 10.1. IRS Special Publication 1075 Revision 10-2014, "Tax Information Security Guidelines for Federal, State and Local Agencies" October 2014.
 - 10.2. ISO/IEC 27002:2013, "*Information technology - Security techniques - Code of practice for information security management*"
 - 10.3. NIST IR 7298 Revision 2, "*Glossary of Key Information Security Terms*", May 2013.
 - 10.4. NIST SP 800-30 Revision 1, "*Guide for Conducting Risk Assessments*", September 2012.



District of Columbia Government – Office of the Chief Technology Officer

- 10.6. NIST SP 800-61 Revision 2, “*Computer Security Incident Handling Guide*”, August 2012.
- 10.7. NIST SP 800-66 Revision 1, “*An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*”, October 2008.
- 10.8. NIST SP 800-83 Revision 1, “*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*”, July August 2013.
- 10.9. NIST SP 800-86, “*Guide to Integrating Forensic Techniques into Incident Response*”, August 2006.



District of Columbia Government – Office of the Chief Technology Officer

11. Policy Review:

Document History

Policy Number	Action	Effective Date	Next Review Date
OCTO – 2020.0	Published	4/22/2016	4/22/2017



12. Policy Acceptance:

Cyber Security Incident Response Team Policy

Effective April 22, 2016

Archana Vemulapalli

**Archana Vemulapalli
Chief Technology Officer
Government of the District of Columbia**

4/22/16

Date