OFFICE OF THE CHIEF TECHNOLOGY OFFICER

District of Columbia Government – Office of the Chief Technology Officer

Responsible Disclosure Policy

Policy Number:	**OCTO – 6052.1**	**Creation Date:**	**10/20/17**
CIS Top 20:	3, 4, 6, 11, 12, 13, 14, 18, 20	Approval Date:	
NIST Control Family:	AC, AU, CM, CP, MA, PL	Revised Date:	

1. **Applicability.** This policy applies to:

   1.1. Executive Branch agencies, organizations, and personnel that fall under the direct authority of the Mayor of the District of Columbia.

   1.2. Any agency or organization that does not fall under the authority of the Mayor (City Council, Independent Agencies, D.C. Charter Schools, and others) shall adopt this policy and manage the maintenance of their government-owned IT equipment in accordance with OCTO policies, directives and standards.

2. **Authority.**

   2.1. DC Official Code § 1-1401 *et seq.*, provides 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.

3. **Overview.** The District of Columbia government (the "District" or "District government") is responsible for ensuring the confidentiality, integrity, and availability of its data and constituent's data processed, transmitted, or stored on the District's systems. The District government has a legal obligation and fiduciary responsibility to properly maintain government equipment. Effective implementation of this policy will facilitate functional longevity of District government IT assets and maximize use of government funds.

4. **Purpose.** The purpose of this policy is to establish general guidance and expectations for responsible vulnerability reporting in the District. The District is responsible for protecting information from unauthorized disclosure and providing safe mechanisms for Agencies to report vulnerabilities they discover for appropriate remediation.

5. **Scope.** This policy applies to:

   5.1. District assets – All servers, workstations, laptops, tablets, smartphones, network -- used to conduct official District government business or interact with internal networks and business systems, whether owned or leased by the District Government, the employee, or a third party.

   5.2. District workforce - Employees, contractors, consultants, temporary staff, interns, volunteers, and other personnel performing official information technology (IT) system administration and management functions at, or on behalf of the District Government, and general users of government IT.

5.3. External parties – District business partners, vendors, suppliers, outsource service providers, and other third-party entities that provide technical operations support to District IT systems.

6. **Policy.** The District Workforce, Residents, and External parties play an integral role in protecting the public's information, including financial and personal information, from unwarranted disclosure. District Workforce, Residents, and External parties should have a method to report vulnerabilities they discover. This policy covers the types of research allowed, guidelines for publicly disclosing vulnerabilities and instructions for reporting to OCTO through a centralized system.

6.1. Authorized testing or research. All testing or research into the District IT systems shall be coordinated through the District Agency and OCTO.

6.2. Unauthorized testing or research. Testing or research not specifically authorized by OCTO and the specific District Agency on the part of the District Workforce, Residents, and External parties is disallowed and may result in privacy violations, degradation of user experience, disruption to production systems and destruction or manipulation of data.

6.3. Coordinated Disclosure. OCTO is committed to patching vulnerabilities as outlined in the District Patch Management and Vulnerability Management Policies.

District Workforce and External parties who discover a vulnerability shall report the vulnerability following the process outlined in this document. They shall refrain from sharing the reporter's personally identifiable information ("PII") and other sensitive or confidential information with others.

District residents and visitors to the District's information technology systems, who discover a vulnerability, are encouraged to report the vulnerability following the process outlined in this document. They should refrain from sharing their PII and other sensitive or confidential information with others

By default, the District does not share vulnerabilities or mitigation efforts outside of the District, and we will never publish information about you or our communications with you without your permission. In some cases, we may also have some sensitive information that should be redacted. Pease check with us before self-disclosing your information.

6.4. Vulnerability reporting. When vulnerabilities are discovered, District Agencies and workforce should follow normal reporting processes. Residents and External parties may use one of the following methods to report:

6.4.1. Signal App account (202) 445-1726

6.4.2. WhatsApp account (202) 445-1726

6.4.3. Perrio App account ciso_dc

6.4.4. Disclosure email: responsibledisclosure@dc.gov

6.5. Upon receipt of a vulnerability report, the OCTO Chief Information Security Officer ("CISO") will acknowledge receipt of the report. The OCTO CISO and Security Operations Center ("SOC") Manager will contact the affected District Agency Chief Information Officer ("CIO") to begin remediation efforts. District Residents, visitors and External parties shall have no expectation of further communication of remediation efforts.

6.6. Policy Maintenance. OCTO is responsible for the maintenance, administration, and publication of this policy. OCTO will annually review this policy and update as needed to ensure the policy's technical relevance and regulatory compliance.

7. References.

7.1. DC Official Code § 1-1401, *et seq.*

7.2. National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)

7.3. NIST Special Publication (SP) 800-37 – Guide for Applying the Risk Management Framework (RMF)

7.4. NIST Special Publication (SP) 800-40 v2 – Creating a Patch and Vulnerability Management Program

7.5. NIST Special Publication (SP) 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

8. Effective Date(s). This policy shall be effective upon the date the CTO signs the document, and will remain in effect until superseded or cancelled in writing.

9. Revision History.

Date of Change	Responsible Entity	Summary of Changes
October 2017	OCTO / GRC	New Policy

10. Policy Acceptance.

Archana Vemulapalli 11/28/17

Archana Vemulapalli
Chief Technology Officer
Government of the District of Columbia

Date