OFFICE OF THE CHIEF TECHNOLOGY OFFICER

District of Columbia Government – Office of the Chief Technology Officer

IT Risk Management Policy

Policy Number:	**OCTO – 1050.2**	**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 Government (DC) agencies.
2. **Authority:** DC Official Code § 1-1401 et seq.
3. **Purpose:** The purpose of this policy is to ensure that DC agencies reduce the risks and vulnerabilities of their information technology (IT) systems to a reasonable level through regular risk assessment, risk management, and monitoring..
4. **Policy:** Each DC agency shall identify, assess and mitigate risks to a reasonable level for all agency IT systems. Risk identification, assessment, and mitigation must address agency IT systems themselves, the environments in which they are housed, and the workforce members who use them.

   4.1. Each agency must conduct and document a risk assessment after every change to all critical applications and information systems.

   4.2. Each agency must conduct and document a risk assessment annually or after every major change to its IT infrastructure/environment in order to identify new risks and vulnerabilities.

   4.3. Each agency must review existing and proposed future systems, applications, and equipment in order to ensure compliance with applicable District and federal laws and regulations.
5. **Procedures:** Agency procedures to implement this policy must include at least the following components:

   5.1.1. Risk assessment/analysis;

   5.1.2. Risk management; and

   5.1.3. Monitoring and maintenance of the effectiveness of risk management measures.
6. **Policy Maintenance:** The Office of the Chief Technology Officer (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.
7. **Policy Enforcement:** OCTO is responsible for the enforcement of this policy. Agencies must actively participate in the audit of this policy when requested by the OCTO.
8. **Exemptions:** None.

10. **Supporting Laws and Regulations:**

    10.1. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA).

    10.2. Privacy Act of 1974, 5 U.S.C. § 552a, P.L. 93-579.

    10.3. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.

11. **Reference Documents:**

    11.1. ISO/IEC 27002, *"Information technology - Security techniques - Code of practice for information security management"*, June 2005.

    11.2. NIST IR 7298 Revision 2, "*Glossary of Key Information Security Terms"*, May 2013.

    11.3. NIST SP 800-30 Revision 1, *"Guide for Conducting Risk Assessments"*, September 2012.

    11.4. NIST SP 800-53 Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"*, April 2013.

    11.5. NIST SP 800-66 Revision 1, *"An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule"*, October 2008.

12. **Policy Review:**

Document History

Policy Number	Action	Effective Date	Next Review Date
OCTO – 1050.0	Published	4/26/2010	4/26/2011
OCTO – 1050.0	Reviewed	6/1/2011	6/1/2012
OCTO – 1050.0	Reviewed	11/1/2012	11/1/2013
OCTO – 1050.0	Reviewed	11/7/2013	11/7/2014
OCTO – 1050.1	Published	11/7/2014	11/7/2015
OCTO – 1050.2	Published	4/22/2016	4/22/2017

13. **Policy Acceptance:**

IT Risk Management Policy

Effective April 22, 2016

Archana Vemulapalli 4/22/16

Archana Vemulapalli
Chief Technology Officer
Government of the District of Columbia

Date