District of Columbia Government – Office of the Chief Technology Officer

Information System Change Control Policy

Policy Number:	**OCTO – 3010.2**	**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 agencies ("DC Agency" or "DC Agencies").
2. **Authority:** DC Official Code § 1-1401 et seq.
3. **Purpose:** This policy requires that each DC Agency implement an Information System Change Control process in order to protect the confidentiality, integrity, and availability of information systems.
4. **Policy:** Each DC Agency Chief Information Officer (CIO), must participate in the OCTO Information System Change Control process that includes at a minimum the following controls:

   a. **Policy:** Each DC Agency Chief Information Officer (CIO), must participate in the OCTO Information System Change Control process that includes at a minimum the following controls:

   b. **Change Advisory Board.** Each Agency CIO shall consult with the OCTO Change Advisory Board (CAB) in which each agency plans and coordinates all system changes within the DC Government enterprise with the OCTO CAB. The CAB must evaluate all information system and security configuration changes prior to implementation. The OCTO CAB must approve, disapprove, or modify a system change

   c. **Change Manager.** OCTO Change Manager is the member of the CAB who ensures the change request is following the standardized operating procedure. Has the ability to authorize the change. Ensures timely decision for change requests.

   d. **Change Owner/Initiator.** Each Agency CIO must designate a Change Owner or Initiator who must act as the liaison with the OCTO CAB, to track all agency system change requests, and report all CAB-approved system changes to the DC Chief Technology Officer through the CAB. The Change Owner/Initiator must be a District Government employee.

   e. **CAB Membership.** Representatives from each OCTO department and the change manager are the members of the Change Advisory Board. Each Agency CIO must ensure that the CAB meeting is joined by the IT technical and information security personnel and management officials who understand the impacts of information system changes in order to provide relevant and knowledgeable advice to the OCTO Change Manager.

   f. **Security Impact Analysis.** Each Agency must ensure that each proposed information system change or security configuration is analyzed for potential impacts on the confidentiality, integrity, and availability of the information system and the data contained therein prior to change approval and implementation.

   g. **Pre-Change Validation.** Each Agency Change Owner/Initiator must ensure that each proposed information system or security configuration change is documented, tested, and validated prior to change approval and implementation.

h. **System Access for Change Implementers.** Each Agency must ensure that only authorized change implementers are granted "Minimum Necessary" access to information system components in order to implement the CAB-approved system changes or upgrades.

i. **Post-Change Validation.** Each Agency Change Initiator/Owner must ensure that each system change outcome (successful or unsuccessful) is documented and that each change was implemented in accordance with the CAB-approved system change.

j. **Auditing of System Changes.** Each Agency in consultation with the Change Manager must conduct a monthly audit to detect and resolve unapproved system changes.

5. **Procedures:** Each DC Agency CIO in consultation with the Agency ISO must implement an Information System Change Management Procedure in written or electronic form in accordance with this policy.
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.
9. **Sanctions:** If OCTO discovers non-compliance with this policy, OCTO will:

   9.1 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.

   9.2 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.

   9.3 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.

10. **Supporting Laws and Regulations:**

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

    b. Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579.

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

11. **Reference Documents:**

    a. NIST FIPS 199, "*Standards for Security Categorization of Federal Information and Information Systems (moderate confidentiality impact)*", February 2004.

    b. NIST FIPS 200, "*Minimum Security Requirements for Federal Information and Information Systems*", March 2006.

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

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

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

f. 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 – 3010.0	Published	11/23/2010	11/23/2011
OCTO – 3010.0	Reviewed	10/7/2011	10/7/2012
OCTO – 3010.0	Reviewed	11/1/2012	11/1/2013
OCTO – 3010.0	Reviewed	11/7/2013	11/7/2014
OCTO – 3010.1	Published	11/7/2014	11/7/2015
OCTO – 3010.2	Published	4/22/2016	4/22/2017

13. **Policy Acceptance:**

Information System Change Control Policy

Effective April 22, 2016

Archana Vemulapalli 4/22/16

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