octo

OFFICE OF THE CHIEF TECHNOLOGY OFFICER

District of Columbia Government – Office of the Chief Technology Officer

Information System Audit and Monitoring Control Policy

Policy Number:	**OCTO – 4002.2**	**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 Agencies" or DC Agency".

2. **Authority:** DC Official Code § 1-1401 et seq.

3. **Purpose:** This policy establishes system audit, logging, and monitoring controls to prevent, detect, or minimize the impact of security incidents on servers and critical applications.

4. **Policy:** Each DC Agency must implement the following information technology (IT) system audit, logging, and monitoring controls for all systems maintained by the DC Agency:

4.1. **Auditable System and User Security Events:** Each DC Agency must implement automated audit trails and backups to log, at a minimum, the following information system and user events:

4.1.1. All valid and invalid network, system, and application user logins.
4.1.2. All actions taken by system users that are assigned system and security administration privileges, such as:

4.1.2.1. Root
4.1.2.2. RACF Special, Auditor, Operations
4.1.2.3. Unix Superuser
4.1.2.4. Network and Firewall Administrators

4.1.3. All valid and invalid accesses to system audit logs.

4.2. **Content of Security Event Records:** For each of the above audit events logged, each DC Agency must record, at a minimum, the following audit trail entries:

4.2.1. User identification
4.2.2. Origination of event
4.2.3. Date and time of event
4.2.4. Type of event
4.2.5. Success or failure of event
4.2.6. Name or identity of affected data, system component, or resource.

4.3. **Protection of Audit Logs.** Each DC Agency must implement the following audit log safeguards to ensure the DC Agency is able to detect when an audit log is altered or destroyed:

4.3.1. Implement security controls for system and backup audit logs to ensure that only authorized users have access to the audit logs.

4.3.2. Grant access to audit logs only to authorized workforce members on a business "need-to-know" access basis.

4.3.3. Implement audit controls to system and backup audit logs to record all valid and invalid access to the audit log.

4.4. **Review of Security Event Records.** Each DC Agency must regularly review system activity reports to prevent, detect, or minimize the impact of security incidents.

4.5. **Retention of Audit Logs.** Each DC Agency must retain audit log data for at least one year, or as required by applicable law, whichever is greater.

4.6. **Notification.** Each DC Agency must forward audit logs for all servers and critical applications on the DC Government network to the Office of the Chief Technology Officer (OCTO) for active monitoring. For assistance with forwarding audit logs, DC Agencies should contact Network Operations Center at noc-eng@dc.gov.

5. **Procedures:** Each DC Agency Chief Information Officer (CIO) or his or her designee must implement the technical and administrative audit, logging, and monitoring procedures described above in written or electronic form.

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. DC Agencies must actively participate in the audit of this policy when requested by 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:**

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, Public Law No. 93-579.

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

11. **Reference Documents:**

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

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

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

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

11.5. NIST SP 800-92, *"Guide to Computer Security Log Management"*, September 2006.

12. **Policy Review:**

Document History

Policy Number	**Action**	**Effective Date**	**Next Review Date**
OCTO – 4002.0	Published	3/29/2011	3/29/2012
OCTO – 4002.0	Reviewed	11/1/2012	11/1/2013
OCTO – 4002.0	Reviewed	8/1/2013	8/1/2014
OCTO – 4002.1	Published	6/3/2014	6/3/2015
OCTO – 4002.2	Published	4/22/2016	4/22/2017

13. **Policy Acceptance:**

Information System Audit and Monitoring Control Policy

Effective April 22, 2016

Archana Vemulapalli   4/22/16

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