Information System Audit Controls Policy

Policy Number: **Approved By:**	**OCTO – 4002.0 (Supersedes Information System Audit Controls Policy Number: OCTO0004)**	**Creation Date:**	July 30, 2010
		Approval Date:	April 7, 2011
Effective Date:	March 29, 2011	**Revised Date:**	March 29, 2011

1. **Scope/Applicability:** This policy applies to all DC Agency Information Security Officers.
2. **Authority:** DC Official Code § 1-1402 et seq.
3. **Purpose:** This policy requires that each DC Agency integrate auditable controls into Agency information systems to enable logging of user access and other related system security events.
4. **Policy:** Each DC Agency Information Security Officer (ISO) must ensure that the following auditable controls are implemented for each Agency information system:
   - 4.1. **Underlying requirements:** All systems that handle confidential information, except network connections, or make access control (authentication and authorization) decisions shall record and retain audit-log information sufficient to answer the following questions:
     - 4.1.1. What activity was performed?
     - 4.1.2. Who or what performed the activity, including where or on what system the activity was performed from (subject)?
     - 4.1.3. On what was the activity performed (object)?
     - 4.1.4. When was the activity performed?
     - 4.1.5. With what tool(s) was the activity performed?
     - 4.1.6. What was the outcome status (such as success vs. failure) or result of the activity?
   - 4.2. **Auditable System and User Security Events:** The ISO must ensure that the Agency's information system audit controls are capable of recording at least the following user and system security events to an audit log:
     - 4.2.1. All successful and unsuccessful user logons.
     - 4.2.2. All unsuccessful access attempts.
     - 4.2.3. All successful accesses when required by applicable regulations, OCTO policy, or Agency requirements.
     - 4.2.4. All successful and unsuccessful access-attempts to both audit logs and audit log backups.
     - 4.2.5. All actions taken and update commands issued by Security Administrators, Network Administrators, and System Administrators with privileges such as Root, RACF Special, RACF Auditor, RACF Operations, and Unix Superuser.
   - 4.3. **Content of Security Event Records:** The ISO must ensure that each security event record contains at a minimum the following information in order to establish what events occurred and who or what caused the events:
     - 4.3.1. Type of security event, such as a user logon/logoff, password change, dataset access, etc.
     - 4.3.2. Date and time security event occurred.
     - 4.3.3. User ID associated with the security event.
     - 4.3.4. Network, system, or application where the security event occurred.
     - 4.3.5. Program or command used to initiate the security event.
     - 4.3.6. Target of security event such as dataset accessed, transaction executed, User ID created/deleted, etc.

4.3.7. Success or failure of security event such as a successful logon, invalid password, access violation, transaction failure, etc.

4.4. **Review of Security Event Records.** The ISO must designate an individual(s) who must daily review security event records to prevent and detect security incidents and minimize their impact.

4.5. **Protection of Audit Logs.**

4.5.1. The ISO must ensure that the confidentiality, integrity, and availability of audit logs and audit log backups are protected from the date of creation and at least until the log retention expires in accordance with policy statement "4.6 Retention of Audit Logs" of this policy.

4.5.2. The ISO must ensure that access to audit logs is granted on a business "Need-to-Know" and "Minimum Necessary" access basis to accomplish the intended purpose of the use, disclosure, or request. *For example, update access to an audit log should not be granted when the user only needs read access to run an audit report.*

4.6. **Retention of Audit Logs.** The ISO must ensure that audit logs are retained for at least one year from the date of creation or as required by applicable regulation, whichever is longer.

5. **Procedures:** Each DC Agency ISO must implement information system audit controls and procedures in accordance with this policy.

6. **Sanctions:** Non-compliance with the provisions of this policy may result in referral of the responsible individual for disciplinary action up to and including termination of employment, in accordance with District Personnel Manual Chapter 16.

7. **Exemptions:** None

8. **Policy Maintenance:** The Office of the Chief Technology Officer must review and update this policy at least annually to ensure technological currency and compliance with applicable law.

9. **Policy Enforcement:** The Office of the Chief Technology Officer is responsible for the enforcement of this policy.

10. **Supporting Regulations and Policies:**
    10.1. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA).
    10.2. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.

11. **Reference Documents:**
    11.1. 42 U.S.C. § 1320d-5.
    11.2. NIST Special Publication 800-30, *"Risk Management Guide for Information Technology Systems".*
    11.3. NIST Special Publication 800-53 Revision 3, *"Recommended Security Controls for Federal Information Systems and Organizations".*
    11.4. NIST Special Publication 800-66 Revision 1, *"An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule".*
    11.5. NIST Special Publication 800-92, *"Guide to Computer Security Log Management".*

12. **Definitions:** Definitions for OCTO policies can also be found in the Glossary Section of the OCTO website.

Audit	To record independently and later examine system activity (e.g., logins and logouts, file accesses, security violations.) This is a fundamental security principle.
Availability	The property requiring that information system components, data or information will be accessible and available to authorized parties when needed. This is a fundamental security principle.

Confidentiality	The property ensuring that information assets are accessible only for reading by authorized parties. This is a fundamental security principle.
Information System	An integrated set of components (e.g. hardware, software, processes) for collecting, storing, processing, and communicating information.
Integrity	The property ensuring that only authorized parties are able to modify data or information disclosed in an electronic document. This is a fundamental security principle.

13. **Policy Acceptance:**

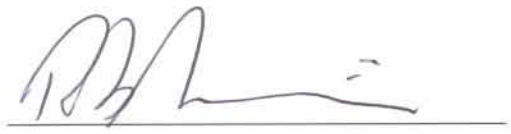
Information System Audit Controls Policy

Effective March 29, 2011

4/7/11

Rob Mancini
Chief Technology Officer
Government of the District of Columbia

Date



4/7/11

Rob Mancini
Interim Chief Security Officer
Government of the District of Columbia

Date