**IT Security Audit, Monitoring and Logging Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the IT Security Audit, Monitoring and Logging Policy. This policy and procedure establishes the minimum requirements for the IT Security Audit, Monitoring and Logging Policy.

This policy is intended to meet the control requirements outlined in SEC502, and SEC501, Section 8.3 Audit and Accountability Family, Controls AU-1 through AU-11.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems classified as sensitive.

# ACRONYMS

CIO: Chief Information Officer

ISO: Information Security Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

SEC502: Information Security Audit Standard 502

SIEM: Security Information and Event Management

SOC: Security Operations Center

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The IT Security Audit, Monitoring and Logging Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the audit and accountability requirements as stipulated by the COV ITRM Security Standard SEC501, the COV ITRM Security Audit Standard SEC502, and security audit best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all sensitive IT systems.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Roles** | Internal Audit Director | Data Owner | System Owner | System Admin | Information Security Officer |
| **Tasks** |   |   |   |   |   |
| Responsible for the it security audits of “YOUR AGENCY NAME” systems | R | A |   |   | I |
| Oversight of software and infrastructure monitoring and logging  |  |  |  A | R | R |
| Audit correct events |   | A |  | R | I |
| Document rationale for audited events |   |  A/R |   |   | C |
| Content of audit records |   |  A |   |  R | I |
| Audit storage capacity |  |  | A | R | I |
| Alert on audit processing failures |  |  | A | R | I |
| Review and analyze system audit records |  | A |  | R | I |
| Generate timestamps |  | A |  | R | I |
| Protect audit information |  | A |  | R | I |
| Retain audit records |  | A |  | R | I |

# STATEMENT OF POLICY

In accordance with SEC502 and SEC501, AU-1 through AU-11, “YOUR AGENCY NAME” will conduct IT Security Audits for all systems classified as sensitive. Each system will be audited for security controls once every three years at a minimum to assess whether IT security controls implemented to mitigate risks are adequate and effective. “YOUR AGENCY NAME”’s Internal Audit Director is responsible for the IT Security audits of “YOUR AGENCY NAME” systems. The ISO or designee shall be responsible for oversight of comprehensive monitoring and logging for “YOUR AGENCY NAME” IT software applications and infrastructure and shall verify that IT Security Audits are performed by independent parties who are not associated with the processes or procedures of the system.

1. **AUDITABLE EVENTS**
2. All “YOUR AGENCY NAME” IT systems must, at minimum, be capable of and configured to:
	1. Produce audit logs with the necessary event information, and
	2. Have the ability to off load audit log data to a log aggregation server.
3. The Data Owner determines, based on a risk assessment and mission/business needs, that the IT system is auditing the following events:
	1. Authentication attempts,
	2. Authenticated individual,
	3. Access time,
	4. Source of access,
	5. Duration of access, and
	6. Actions executed.
4. Network devices such as routers, switches, hubs, firewalls, and other devices that facilitate the transfer of packets from one point to another must be configured to log security data as well as errors. Applications, including web services and database services, residing on servers that utilize cached or separate authentication capabilities must also maintain logs of all security, application and event related information. Events should be logged in real time, to the fullest extent possible, stored locally and sent to the central log analysis server as the event is recorded. Network devices must also be configured to transmit recorded events to the central log analysis server as the event is recorded by the network device.
5. End-user workstations, including but not limited to desktop and laptops, must also maintain logs of security related events. These devices must also forward the security event information to the central log analysis server as the event occurs.
6. The Data Owner will coordinate the security audit function with other “YOUR AGENCY NAME” entities that require audit related information to provide mutual support and to help guide the selection of auditable events.
7. The Data Owner will coordinate with the ISO to document the rationale for which auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

**B. CONTENT OF AUDIT RECORDS**

1. The System Administrator will configure the system such that the audit records contain sufficient information to, at a minimum:
	1. Establish what type of event occurred (i.e., event id),
	2. When (date and time) the event occurred (i.e., time stamp),
	3. Where the event occurred (i.e., destination IP address),
	4. The source of the event (i.e., source IP address),
	5. The outcome (success or failure) of the event,
	6. The identity of any user/subject associated with the event (i.e., user id/process id), and
	7. File names involved and access control or flow control rules invoked.
2. The System Administrator will configure the system to log additional data, commensurate with sensitivity and risk as determined by ISO and/or data owner or system owner.
3. “YOUR AGENCY NAME” will centrally manage the content of audit records generated by all servers providing application support to the agency, including but not limited to database servers, messaging servers, file servers, print servers, middleware servers, and DNS servers.
4. “YOUR AGENCY NAME” will centrally manage the content of audit records generated by all network devices providing connectivity to the agency, including but not limited to routers, firewalls, IDS/IPS, and VoIP servers.

**C. AUDIT STORAGE CAPACITY**

1. The System Administrator will ensure audit storage capacity is allocated in accordance with system configuration such that capacity is not exceeded.

**D. RESPONSE TO AUDIT PROCESSING FAILURES**

1. System Administrators will configure systems to alert the System Owner in the event of an audit failure.
2. All systems classified as sensitive will be configured by System Administrators to provide real-time alerts when the following audit failure events occur:
	1. Recording of authentication attempts, and/or
	2. Escalation of privileges.
3. These events will be considered a potential security event and be responded to as outlined in the “YOUR AGENCY NAME” Security Incident Response Policy.

**E. AUDIT REVIEW, ANALYSIS, AND REPORTING**

* + - * 1. The System Administrator will review and analyze information system audit records at least every 30 days for indications of inappropriate or unusual activity, and report findings to the Data Owner.
				2. The System Administrator will adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to “YOUR AGENCY NAME”’s operations, assets, individuals, other agencies, or the Commonwealth based on law enforcement information, intelligence information, or other credible sources of information.
				3. If the system is classified as sensitive, audit review, analysis and reporting processes must be integrated to support organizational processes for investigation and response to suspicious activities. This integrated approach correlates records across different repositories to gain agency-wide situational awareness. Further integration of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information should be used to enhance the ability to identify inappropriate or unusual activity.
				4. The security operations staff is responsible for monitoring of the infrastructure and log files on a continuous basis and documenting the activity. The security operations staff must analyze SIEM information and maintain regular contact with the SOC, and security research and coordination organizations, such as [US CERT](http://www.us-cert.gov).

**F. TIME STAMPS**

1. The system must be configured to generate time stamps to include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.
2. Whenever possible, all systems should utilize Network Time Protocol (NTP) time synchronization

**G. PROTECTION OF AUDIT INFORMATION**

1. Audit records, audit settings, and audit reports must be protected from unauthorized access, modification, and deletion.
2. Access to audit information must be restricted to System Owner and those authorized to perform IT Security Audits and/or investigate security incidents. Audit information must not be accessible by end-users of the resource or any other non-system/system administrator.

1. Regular backup and archival processes must be in place for audit files in order to protect historical log data and collect new log data processed by the server.
2. The central log analysis server must be heavily protected as it will contain sensitive data pertaining to all “YOUR AGENCY NAME” systems. To provide this protection, the central log analysis server must be located on a dedicated network segment and not on the DMZ or the internal network. The central log analysis server will forward alerts about anomalous events to the security operations staff for review and action.
3. Audit records must be backed up at least once every twenty-four hours to a different system or media than the system being audited.

**H. AUDIT RECORD RETENTION**

1. “YOUR AGENCY NAME” will retain audit records consistent with the agency’s records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO” ““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

 [ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

[ITRM Information Security Audit Standard (SEC502)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History |
| --- |
| Version | Date | Change Summary  |
| 1 | 07/01/2014 | This policy replaces the “YOUR AGENCY NAME” CSRM IT Security Audit Policy Procedure and the “YOUR AGENCY NAME” CSRM Monitoring and Logging Policy Procedure |
| 2 | 11/18/2021 | Formatting changes |