Policy and Procedure 9-3
Audit and Accountability Program for Information Security

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	11/6/2023
Effective Date:	July 21, 2023		
Codes/Mandates:	Code of Virginia: §2.2-2007		
References:	Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00, ITRM Standard SEC501: Information Security Standard		
Forms:	N/A		

CONTENTS

PURPOSE

To establish policy and procedures for the administration of the agency's information security audit and accountability program.

POLICY

The Virginia Department of Forestry is committed to the implementation of an effective information security audit and accountability program to address the risks associated or resulting from inadequate event logging and transaction monitoring. This policy applies to all information technology resources owned or operated by agency staff. Any electronic file not specifically identified as the property of other parties that is transmitted or stored on agency information technology resources shall be considered agency property.

DEFINITIONS

"Agency" and **"DOF"** means the Virginia Department of Forestry.

"Agency information technology resource" and **"AITR"** means the agency employee who is designated by the state forester to be responsible for compliance with the policies, standards and guidelines established by the chief information officer for the Commonwealth, as required by Code of Virginia §2.2-2014(B). The director of information technology and helpdesk analyst currently serves in this role.

"Agency staff" means all Virginia Department of Forestry classified, restricted and wage personnel, consultants, contract personnel and other non-employees, such as volunteers or interns.

"Commonwealth" means the Commonwealth of Virginia.

"Electronic files" means media content (other than computer programs or system files) that are intended to be used in either an electronic form or as printed output. This includes, but is not limited to, email, documents, spreadsheets, images, photographs, presentations and GIS files.

"Information security officer" and **"ISO"** means the agency employee who is designated by the state forester to develop and manage the agency's information security program, as required in the Commonwealth's Information Security Standard, SEC501. The director of information technology currently serves in this role.

"Information technology resources" means any device or equipment that can be used to access and/or store electronic information including, but not limited to, laptops, desktops, tablets, mobile phones, thumb drives, external hard drives and networked printers.

"System owner" means the agency manager or supervisor who is responsible for the operation and oversight of any given agency business system.

"DOF business systems" means all automated applications used by DOF to meet the agency's business objectives.

"DOF sensitive business systems" means all DOF business systems that handle data having a high or moderate sensitivity with respect to confidentiality, integrity and availability.

PROCEDURES

Auditable Events

The information security officer (ISO) shall:

- Determine based on a risk assessment, as well as mission and business needs, that an information system must be capable of auditing the following events: authentication event, authenticated individual, access time, source of access, duration of access and actions executed.
- Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.
- Provide a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.
- Review and update the list of auditable events at least annually with the appropriate system owner.

Content of Audit Records

All DOF business systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event and the identity of any user/subject associated with the event. In addition, all DOF sensitive business systems may include additional organization-defined requirements in the audit records required to

centrally manage the content of audit records generated by all web servers, database servers, messaging servers, file servers, print servers, middleware servers, DNS servers, routers, firewalls, IDS/IPS and VoIP servers.

Audit Storage Capacity

- All DOF business systems must allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.
- DOF sensitive business systems must off-load audit records at least once every 30-days onto a different system or media than the system being audited.

Response to Audit Processing Failure

All DOF business systems must alert the system owner, the director of information systems and the ISO in the event of an audit processing failure. (Note: the director of information systems serves in the role of ISO). In the event of an audit processing failure, DOF business systems must configure the audit log to stop generating audit records or overwrite the oldest audit records. DOF sensitive business systems must provide real-time alerts when recording of authentication attempts or escalation of privilege events occur.

DOF sensitive business systems must provide an alert in real time to appropriate personnel including system owner, authorizing executive, director of information systems, ISO and AITR when the following events occur: recording of authentication attempts or escalation of privilege. (Note: the director of information technology serves in the role of ISO).

Audit Review, Analysis and Reporting

All DOF business systems must review and analyze information asset records at least every 30 days for indications of inappropriate or unusual activity, and report findings to system owner, director of information systems and ISO. (Note: the director of information technology serves in the role of ISO). In addition, DOF business systems must adjust the level of audit review, analysis and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations or the Commonwealth based on law enforcement information, intelligence information or other credible sources of information.

DOF sensitive business systems must:

- Integrate audit review, analysis and reporting processes to support organizational processes for investigations and response to suspicious activities.
- Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
- Centralize the review and analysis of audit records from multiple components within the system.
- Integrate analysis of audit records with analysis of vulnerability scanning information, performance data and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.
- Correlate the audit review with physical monitoring to enhance the ability to identify suspicious behavior or supporting evidence of such behavior.
- Defines permitted actions for each system process, role and user associated with the review, analysis and reporting of audit information.
- Correlate information from non-technical sources, such as human resources records, documenting policy violations.
- Adjusts the level of audit review, analysis and reporting when there is a change in risk based on information.

Time Stamps

All DOF business systems must use internal system clocks to generate time stamps for audit records to facilitate logging and monitoring.

DOF sensitive business systems must compare the internal information system clock every five minutes with a stratum two clock or better and synchronize the internal clocks to the authoritative time source when the time difference is greater than two seconds.

Protection of Audit Information

All DOF business systems must protect audit information and audit tools from unauthorized access, modification and deletion. DOF sensitive business systems must:

- Back-up audit records at least once every 24 hours to a different system or media than the system being audited.
- Authorize access to management of audit functionality to only a limited subset of privileged users.

Audit Record Retention

All DOF business systems must retain audit records for one year or until the next information security audit to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Audit Generation

DOF business systems:

- Provide audit record generation capability for the auditable events defined in **Auditable Events** section at operating system, services and application levels.
- Allow authorized personnel to select which auditable events are to be audited by specific components of the system.
- Generate audit records for the events and content defined in **Content of Audit Records**.

Monitoring for Information Disclosure

DOF monitors open-source information and/or information sites (website, open FTP) monthly for evidence of unauthorized disclosure of organizational information.

AUTHORITY

This policy and procedure is issued by the Virginia state forester.

INTERPRETATION

The chief of administration and the director of information technology are responsible for the interpretation of this policy and procedure.

APPROVAL

I certify that this policy and procedure is approved and ready for publication.

Parik Patel	DocuSigned by: Parik Patel 3448F7C5358F457...	10/18/2023
Director of Information Technology Name (Print)	Director of Information Technology Signature	
Amanda Davis	DocuSigned by: amanda davis C2CCAD60F85A4A6...	11/6/2023
Chief of Administration Name (Print)	Chief of Administration Signature	