Policy Name:	Audit and Accountability Policy				
Revision #:	0.9	**Effective:**	January 1, 2024	**Page**	1 of 1

1.0 PURPOSE

This policy describes how the organization creates and maintains system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

2.0 SCOPE

This policy applies to all electronic records in the organization's data storage systems that contain sensitive information.

3.0 POLICY

- Logs of critical systems such as file storage, email, system logins, and firewalls are automatically created and maintained. The organization follows manufacturer recommendations on which event types are to be included in system logs, such as on servers, workstations, cloud services, and firewalls.
- The actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
- Audited events include those that indicate a possible auditing system failure.
- Logs are reviewed periodically to check for unusual activity.
- Logs use a common time stamp and can be correlated to assist in incident investigation.
- Logs collect information such as user ID, IP address, location, date, time, and activity. Logs can be queried on demand for audit review, analysis, and reporting.
- Systems that maintain logs are synchronized to a common time source.
- Logs are only accessible to authorized personnel and are protected from unauthorized access, modification, and deletion.

4.0 RELEVANT NIST CONTROLS

Control	Control Description	Document Section
NIST 800-171 3.3	Audit and Accountability	Entire Document

5.0 REVISION HISTORY

Date	Name	Changes Made	Revision #
12/25/2022	Frank Schipani	Initial draft created	0.9
10/9/2023	Frank Schipani	Annual review	0.9
12/30/2023	Audit Committee	Approved Policies	