P2112 - HITRUST - Audit Logging & Monitoring

Contents

Purpose:

The purpose of the Audit Logging and Monitoring policy is to provide and establish Executive level explicit direction for all individuals and entities to follow comprehensive procedures for the recording, retention, and analysis of audit logs and monitoring activities within the organization, in alignment with HITRUST CSF requirements.

The Organization is responsible for overseeing the development, implementation, and maintenance of the Information Security Program and associated components.

Scope:

This policy applies to all implemented information systems and supporting infrastructure used to support and protect sensitive data (PHI). This applies to systems whether managed centrally or in a distributed fashion, and to all individuals and entities who intend to access information systems and data. Within this document, the phrase "information systems and data" includes all technology resources and systems, transactions, applications, platforms, networks, databases, and other information systems within Integrity's technological environment.

Statement:

Auditable Events

The organization determines which of the following auditable events require auditing on a continuous basis in response to specific situations:

- user log-on and log-off (successful or unsuccessful);
- configuration changes;
- application alerts and error messages;
- all system administration activities;
- modification of privileges and access;
- account creation, modification, or deletion;
- concurrent log on from different workstations; and
- override of access control mechanisms.

Reference: 12148.06i1Organizational.1

Audit Logging

Audit records include

- a unique user ID,
- unique data subject ID (if applicable),

- function performed, and
- date/time the event was performed.

Reference: 1203.09aa1System.2

Retention policies for audit logs are specified by the organization and the audit logs are retained accordingly.

Reference: 1239.09aa1System.4

Audit Log Review

The organization specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.

Reference: 12101.09ab1System.2

Audit Log Access

Access to audit trails / logs is safeguarded from unauthorized access and use.

Reference: 1223.09ac1System.1

Administrative Logs

The organization validates that proper logging is enabled in order to audit administrator activities.

The organization validates system administrator logs and operator logs are reviewed on a regular basis.

Reference: 1270.09ad1System.12

Error Logging

Faults reported by users or by system programs related to problems with information processing or communications systems are logged.

Error logging is enabled if this system function is available.

Reference: 1272.09ae1System.13

Clock Synchronization

The organization uses at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Reference: 1295.09af1System.2

This Audit Logging & Monitoring Policy is supported by the following procedures:

- *12 – HITRUST – Audit Logging & Monitoring Procedure*

The Organization - Integrity, LLC and applicable Business Units.

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

The Integrity Security Governance Committee will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Integrity Security Governance Committee in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A contractor found to have violated this policy may be subject to an immediate termination of the right to access Integrity's systems and may also include the termination of Integrity's engagement with the contractor's employer.

Policy References:

Related Procedure References:

Related Regulatory Information:

P2112 - HITRUST - Audit Logging & Monitoring		
Document Author	**Name:** **Title:** **Email:**	Sumit Dhawan Manager Cybersecurity Compliance Sumit.Dhawan@integrity.com
Document Owner	**Name:** **Title:** **Email:** **Approved Date:**	Matt Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 2/24/2026
Legal Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Duncan McQueen Assistant General Counsel Duncan.McQueen@integrity.com 3/16/2026
Executive Management Approval	**Name:** **Title:** **Email:** **Approved Date:**	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 3/30/2026

Last Published Date: 3/30/2026

Document Version Number 2.0