Report Title: Policy Details
Run Date and Time: 2026-02-06 18:49:17 Pacific Standard Time
Run by: System Administrator
Table name: sn_compliance_policy

Policy

Name:

Security Logging and Monitoring Policy

Type:	Policy	State:	Retired
Owning group:	IT Securities	Valid from:	2026-02-06 17:25:00
Owner:	Gabrielle Parker	Valid to:	2026-02-13 17:25:08
Compliance score (%):	0	Approval method:	Select approvers
Parent:	NIST CSF v2.0 - Identity Management, Authentication, and Access Control (PR.AA)	Approval rule:	
		Approvers:	Abel Tuter, Abraham Lincoln
		Reviewers:	Alejandra Prenatt
Policy categories:		Contributors:	

Description:

This policy defines the requirements for security logging, monitoring, and review of system and network activities to detect, investigate, and respond to potential security incidents in alignment with ISO/IEC 27001 requirements.

Policy text:

The organization shall implement centralized security logging and monitoring controls to ensure the timely detection, analysis, and response to security events that may impact the confidentiality, integrity, or availability of information assets.
Security logs shall be generated, collected, and retained for systems, applications, and network devices in accordance with defined retention requirements. Logged events shall include, at a minimum, authentication activities, privileged access, security alerts, system errors, and other relevant events necessary to support incident detection and investigation.
A centralized monitoring solution, such as a Security Information and Event Management (SIEM) system, shall be used to correlate and analyze log data from multiple sources. Alerts shall be generated for suspicious or anomalous activities and reviewed by authorized personnel in a timely manner.
Access to security logs shall be restricted to authorized individuals to prevent unauthorized modification or disclosure. Logs shall be protected against tampering and reviewed periodically to ensure completeness and effectiveness.
Security logging and monitoring activities shall support incident response, audit requirements, and ongoing risk management. This policy shall be reviewed at least annually or upon significant changes to systems, regulatory requirements, or threat landscape.

Knowledge Base

Policy knowledge base:	Governance, Risk, and Compliance	Policy template:	Example Article Template
Published policy:	KB0010001 v1.0		

Acknowledgement Setup

Frequency:	Semi-annually	Allow users to decline policy:	true
First acknowledgement:	2026-03-13	Allow users to request exception:	true
Number of days to respond:	5		
Next acknowledgement:			
Audience:	All Employees and Contractors with Access to Information Systems		
Reference material URL:			

Exception Setup

Maximum exception duration (days): 5

Activity

Additional comments:

2026-02-06 17:42:10 - System (Additional comments)
Approved by Abel Tuter

2026-02-06 17:40:05 - Alejandra Prenatt (Additional comments)
I have reviewed the Security Logging and Monitoring Policy. Please approve this review.

2026-02-06 17:36:40 - Alejandra Prenatt (Additional comments)
Review of the Security Logging and Monitoring Policy has been completed.

The policy aligns with ISO/IEC 27001 requirements (A.12.4 – Logging and Monitoring) and clearly defines roles, responsibilities, logging requirements, retention, and monitoring procedures.

Evidence provided for centralized security logging, SIEM alerts, and policy adherence has been reviewed and is deemed sufficient to support control effectiveness.

No further action is required at this time.

2026-02-06 17:32:21 - System Administrator (Additional comments)
This evidence request has been submitted for review to validate the effectiveness of security logging and monitoring controls aligned with ISO/IEC 27001 requirements.

Please review the provided evidence for completeness, relevance, and adequacy in addressing the identified compliance issue. Feedback or additional evidence requests may be provided as needed.

Settings

Functional domain:

Related List Title: GRC document version List

Table name: sn_irm_shared_cmn_document_version

1 GRC document versions

Name	Approved on	Approvers	Attachment	Contributors	KB article	Owner	Reason for change	Record	Reviewers
Security Logging and Monitoring Policy	2026-02-06 17:42:13	Abel Tuter, Abraham Lincoln			KB0010001 v1.0	Gabrielle Parker		Policy: Security Logging and Monitoring Policy	Alejandra Prenatt

Related List Title: Approval List

Table name: sysapproval_approver

2 Approvals

State	Approver	Comments	Approval for	Created
Approved	Abraham Lincoln			2026-02-06 17:40:08
Approved	Abel Tuter			2026-02-06 17:40:08

Related List Title: Policy approvals List

Table name: sn_compliance_policy_approvals

None

Related List Title: Control List

Table name: sn_compliance_control

None

Related List Title: Evidence List

Table name: sn_grc_advanced_evidence_response

None

Related List Title: Evidence request List

Table name: sn_grc_advanced_evidence_request

1 Evidence requests

Number	State	Name	Request reason	Assigned to
EVR0002002	Closed	Security Logging and Monitoring Policy Evidence Request	Issues	Alejandra Prenatt