

Logging and Monitoring Policy

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This policy supports the SOC 2 common criteria CC7.1 and CC7.2 by establishing requirements for logging, monitoring, and alerting.

This policy applies to all [In-scope systems] and production infrastructure.

2. Logging

- Centralized logging: All system, application, and audit logs are collected in [Logging system].
- Log content: Logs include timestamp, user, action, and source/destination.
- Log retention: Logs are retained for at least [Log retention period].

3. Events that are always logged

- Sign-ins to the identity provider, the cloud console and production systems, successful and failed.
- Changes to accounts, roles and permissions.
- Administrative actions in the cloud account and in the application admin tools.
- Production deployments and infrastructure changes.
- Staff access to customer data.
- Errors and security events from the application and its hosts.

4. Protecting logs

Logs are stored where the people whose actions they record cannot change or delete them. Access to logs is limited to named roles, and system clocks are synchronized so events can be put in order.

5. Monitoring and alerting

- Availability monitoring: System availability and performance are monitored to meet [Uptime commitment].
- Security alerting: Alerts are configured for security events (for example failed logins, malware detection) and routed to the appropriate on-call personnel.
- Review: The [Security owner role] reviews alert activity and alert rules at least monthly and records the review. Logs are available for investigation of any incident.

6. Alerts

Event	Who is alerted	Expected response
Repeated failed sign-ins to an administrator account	On-call engineer	Same day
Use of the cloud root or owner account	[Security owner role]	Within 1 hour
Multi-factor authentication disabled for any user	[Security owner role]	Same day
A new administrator or a change to administrator roles	[Security owner role]	Same day
Storage made public or a security group opened to the internet	On-call engineer	Within 1 hour
Malware detected on a Company device	[IT owner role]	Within 1 hour
Availability below [Uptime commitment]	On-call engineer	Immediately

7. Roles and responsibilities

Role	Held by	Responsibility
Policy approver	[Policy approver role]	Approves this policy, each new version, and any risk the Company accepts instead of meeting it.
Policy owner	[Security owner role]	Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year.
On-call engineer	A named rota	Responds to alerts and opens an incident record where one is needed.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

8. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Log retention settings	Configuration of log retention period.	[Logging system]
Alert configuration	Screenshot of key security alert rules.	[Monitoring tool]
Uptime report	Monthly availability metrics.	[Documentation system]
Monthly review records	The date, the reviewer and any action taken on alerts.	[Evidence storage location]

9. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

10. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

11. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Documentation system]	Where policies and procedures are published, for example the company wiki.
[In-scope systems]	The product, cloud accounts and tools inside the audit boundary.
[Logging system]	Where logs are collected and searched.
[Log retention period]	How long logs are kept, for example one year.

Field	What to enter
[Uptime commitment]	The availability you promise customers, if any, for example 99.9 percent.
[Monitoring tool]	The system that raises alerts.
[Evidence retention period]	How long audit evidence is kept, for example three years.
[IT owner role]	The role that runs company devices and accounts, for example IT lead.
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/logging-and-monitoring-policy (CC BY 4.0).