**<Your Company Logo>**

**Log Management Policy**

# ***Version Control Table***

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Updated |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

|  |  |
| --- | --- |
| **Date of Next Revision** | **<date>** |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarize the change and not a substitute for reading the full text.

# ***Table of Contents***

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_77h423ppzf4j)

[**Table of Contents 5**](#_nfredm5g5fwd)

[**Purpose 6**](#_31776hgm8qpl)

[**Scope 6**](#_tpmk4ks5sbmm)

[**Responsibilities 6**](#_jymydov2gbme)

[**Policy 7**](#_jhj76rxbza7i)

[Event logging 7](#_a4ixjy7vham4)

[Administrator and operator logs 7](#_fbo2i9c8qtjs)

[Log retention period and storage 8](#_53r1l4vaclfc)

[Protection of log information 8](#_kp0a4pfuvqoy)

[Clock synchronization 8](#_6c33z6j14mho)

[**Disciplinary actions 8**](#_oo4pebgvtuk2)

[**Change, Review, and Update 8**](#_6cu0cv3y3y7n)

[**Responsibility 8**](#_fxvzxllev4xj)

[**Reference 8**](#_abyh665p4kb0)

[**Related Documents 8**](#_ukche8hbs94u)

# 

# Purpose

The purpose of this policy is to address the regulatory requirements for auditing, logging, and monitoring activities.

# Scope

This policy applies to all employees, users, and third parties who access or use <Company> information assets, regardless of physical location.

IT resources include all company-owned, licensed, leased, or managed hardware and software and use the <Company> network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

# Responsibilities

**ISMS Manager:**

1. Manage logging and monitoring process.
2. Create documentation.

**SOC Analyst:**

1. Analyze and proceed with alerts, events, and vulnerabilities mentioned in security systems;
2. Prepare a report on critical information security incidents;
3. Escalate true positive events to the Incident Management team.

**Incident Management Team:**

1. Respond to the security incidents in time.

**Security Engineer:**

1. Set up security configurations on the network equipment;
2. Connect log sources with <SIEM>, and confirm the existence of alerts;
3. Continuously improve the security system.

**Asset Manager:**

1. Install all necessary logging software on all company laptops and periodically review if it is in place.

# Policy

## Event logging

* Logging and monitoring are enabled on all systems and devices which are listed as log source. Access to information systems and data, as well as significant system events, must be logged.
* Employees must not be assigned to be the only reviewers of their activity.
* The information in logs includes:
  + event source,
  + event ID;
  + event body;
  + event timestamp;
  + event body with enough fields to understand the action, for example:
    - source and target users
    - source and destination IPs
    - file owner, path, and content hash
    - process execution parameters
* All logs across the <Company> system and resources are gathered in SIEM for log correlation, further analysis, and reactions.
* All logged sources are described in this spreadsheet.
* When using the outsourced cloud environment (AWS), logs must be kept on cloud environment access and use, resource allocation, and utilization. These logs are sent to SIEM.
* DNS query logging must be enabled to detect requests to the known malicious domains.
* The availability of critical resources has to be monitored too.
* During remote working and connecting to the office network, all VPN activity inside the corporate environment must be gathered and monitored.

## Administrator and operator logs

These actions, including, but not limited to, taken by accounts with root or administrative privileges, must be logged:

* System administrator commands.
* Log-in attempts (successful and unsuccessful).
* System log-offs.
* Account lockouts.
* System configuration changes.
* System errors and corrective actions taken.

## Log retention period and storage

All audit logs must be retained for the defined time. The retention time for log storage is 90 days, but logs are also deleted when there are 512 gigabytes for the particular index (log source).

## Protection of log information

Logs must be read-only by authorized people. The logs are stored in our SIEM on-premise.

## Clock synchronization

All information systems synchronize their clocks by implementing Network Time Protocol (NTP) or a similar capability. All information systems must synchronize with the same primary time source.

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how severe an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* ISO 27001 Annex A.12.4.1 Event Logging
* ISO 27001 Annex A.12.4.2 Protection of Log Information
* ISO 27001 Annex A.12.4.3 Administrator & Operator Logs
* ISO 27001 Annex A.12.4.4 Clock Synchronisation

# Related Documents

* <Company> Log Sources