**Log Management Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

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 summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_27bzi485wn03) **4**

[**Scope**](#_fvfpejodwg69) **4**

[**Policy**](#_l04o6nwkzpyx) **4**

[**Event Logging**](#_59r9kc7hbltd) **4**

[**Administrator logs**](#_iq1tkg4a269l) **4**

[**Log retention**](#_svg1w49lrqbo) **5**

[**Change, Review, and Update**](#_5rn1nok175xn) **5**

[**Disciplinary Action**](#_w6uxo3il3qvu) **5**

[**Responsibility**](#_jb29oi3s6k6i) **5**

[**Related Documents**](#_txxyldi18fn8) **5**

# 

# **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]’s* information assets, regardless of physical location. IT resources include all company-owned, licensed, leased, or managed hardware and software, regardless of the ownership of the computing device connected to the network.

# **Policy**

## **Event Logging**

* Employees can not review their activity.
* The information in logs minimally includes:
  + Event source;
  + Date;
  + User;
  + Timestamp;
  + Source address;
  + Destination address.
* The logs from the EDR solution have to be checked as well.
* While using AWS, logs must be kept on cloud environment access and use, resource allocation, and utilization.
* The availability of web resources has to be monitored too.
* DNS query logging has to be enabled to detect requests to the known malicious domains.

## **Administrator logs**

These actions, 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 are taken.

## **Log retention**

* The logs have to be stored for at least one month for a retrospective.

# **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. The IT Manager shall exclusively perform changes to this policy.

# **Disciplinary Action**

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

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed. However, all staff is responsible for following the Log Management Policy.

This policy shall be reviewed yearly or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Data Protection Policy