Approved by order No 183 of 18 October 2024 of the Director for Administration

In force from: 18.10.2024

Logging Policy

Table of Contents

1 General information

The Logging Policy of Tallinn University of Technology (hereinafter referred to as "the university") has been prepared in accordance with the requirements of the ISO 27001:2022 standard and the university's Information Security Policy. The purpose of the Logging Policy is to ensure that logs are generated, stored and analysed to support the fundamental principles and objectives of the university's information security, thereby protecting IT assets and data while ensuring their availability, integrity and confidentiality (and enabling the collection of legal evidence from logs when required).

2 Definitions

"**Logs**" means automatically or manually generated records of actions within a system or application that contain information about operations, events, changes, security incidents and other circumstances.

"**Logging**" means the process of recording actions, events and changes.

"**Log aggregation**" means consolidating logs from multiple sources into one central hub, allowing for more comprehensive analysis and monitoring.

"**Anomaly detection**" means the process of identifying deviations from normal behaviour that may indicate a potential security threat.

3 Scope of application

The Logging Policy applies to all information systems and IT assets used by the university, including those managed by third parties. The Policy governs the generation, storage and analysis of logs, including exceptional cases, failures, and other critical events. The Policy applies to all components of the information system and persons associated with them, i.e. the university staff, students and third parties. The persons responsible for logging shall ensure that logs are generated, stored, and analysed accurately and securely.

4 Principles

All information systems and IT assets must generate logs in accordance with established requirements and security standards. Logs must be securely stored and kept confidential for a period long enough to help with the investigation and resolution of potential security incidents. Access to logs must be restricted to authorised users who have a legitimate need to know. Logs must be analysed regularly to detect potential security incidents, data breaches and anomalous behaviour. Logs must be protected from unauthorised modification and deletion. The logging configuration must be documented and reviewed regularly to ensure that it is relevant and effective. The log retention period and regulatory requirements for each information system or IT asset are specified in the JIRA Assets module.

The university collects logs from various information and data systems that record the operations, usage, and changes to these systems. Logs must be monitored regularly, and users are prohibited from modifying logs, i.e. access to logs should be read only.

Logging and monitoring tools must comply with the university's information security standards and be updated regularly.

By consolidating logs from information systems and IT assets into a centralised repository, log aggregation enhances the ability to detect more complex security incidents.

The persons responsible for collecting, storing, and analysing logs must be aware of their responsibilities, and their actions must be documented.

5 Objectives

The objective of storing and managing logs is to ensure the transparency and auditability of actions performed within systems and applications, facilitating quick detection of and response to security incidents and use of the logs for other purposes, such as analysis and service continuity.

Log administrators are responsible for contributing to regulatory compliance and audits by supplying the necessary log data. Logs are also used to evaluate and enhance the effectiveness of security measures, thereby supporting proactive security management.

6 Log management

6.1 Log data

Each event log must contain at least the following data:

- user ID;
- name of the information system or IT asset;
- system activities, i.e. including clearly identifiable automated processes;
- authentication and logon/logoff events: if authentication is performed through a third-party identity management service provider, the event logging is performed and managed in the relevant service logs. These events are not saved in the application's logs;
- date, time and relevant details of the events.
    - The following standard shall be used: UTC time in ISO8601 format YYYY-MM-DDTHH:mm:ss.SSSZ;
- input values (e.g. file names, query objects, authentication method);
- device identification information, system identifier and location;
- the event or action log type or category (e.g. user identification, administration and type details);
- network addresses and protocols;
- correlation ID: to track an event chain;
- session ID: when session-based monitoring is applied.

6.2 Log events

The following events must be logged, unless it is technically impossible and approved as an exception:

- successful and failed login attempts, incl. failed authentication attempts, and brute-force attacks;
- successful and failed attempts to access data and other resources;
- if an application has an administrator interface or other tools for modifying a system configuration, all successful and failed configuration change attempts must be logged. If a configuration change occurs outside the application (e.g., at the server or infrastructure level), the change must be recorded in system administration or infrastructure logs;
- warnings and error messages generated by the information system or IT assets;
- data export and import operations;
- use of privileges;
- files accessed and the type of access, including the deletion of critical data files;
- alerts generated by the access control system;
- enabling and disabling security systems, e.g. antivirus software and intrusion detection systems;
- creation, modification, or deletion of identities, including changes in roles;
- transactions performed by users within applications. These include technical users (applications) performing automated operations.
- log receipt time in the management and processing system;
- use of log management and processing programs and applications.

6.3 Protection of log data

Users, including those with privileged access, must not have the right to delete or disable their activity logs, unless it is not technically feasible to impose such restrictions. All log data shall be stored and protected against unauthorised access, and access rights to log data shall be documented in accordance with the IT Asset Access Control Policy.

Log information must be protected from unauthorized modification, whereas:

- when logs are sent for log aggregation, all log data must be encrypted using protocols such as TLS;
- changes to the saved message types should not be allowed;
- it should be ensured that log files cannot be edited or deleted;

- it is essential to prevent the failure to record events or the overwriting of previously recorded events when the log files storage is full;
- all logging settings and procedures must be subject to version control and updated in line with changes in systems and regulations.

The following methods can be used to protect logs:

- cryptographic hashing;
- saving to a read-only file;
- saving to a public transparency file.

The availability and integrity of the logs must be ensured even in the event of data loss or system failure. Backup log files must be secured using the same security measures as those applied to original log files.

Logs that must be retained for an extended period should be archived in compliance with data and/or regulatory requirements. The retention periods for the logs are defined for each specific information system or IT asset.

If an organization must send system or application logs to a third party in order to detect errors, any sensitive information should be removed from the logs using data masking techniques if possible. Usernames, IP addresses, hostnames, organization names, and any other unnecessary information should be removed prior to sending logs to a third party.

6.4 Log analysis

Log analysis entails examining and interpreting information security events to identify unusual activity or anomalous behaviour that may indicate potential compromise. The Information Security Division of the Information Technology Services analyses the university's log data. The Information Security Division uses automated tools designed to detect and alert anomalies and potential security incidents.

The results of log analysis must be documented and regularly reviewed to assess and enhance the effectiveness of logging. The results of log analysis are incorporated into the information security risk management process, so that identified risks and vulnerabilities can be effectively evaluated and managed.

7 Supervision

The Information Security Manager shall coordinate the implementation, monitoring, and regular review of the Logging Policy. The Information Security Manager conducts regular exercises and tests to validate the effectiveness of logging systems and policies.

Regular monitoring and audits shall be organised by the Information Security Manager to ensure compliance with the requirements of the Logging Policy.

If any non-compliance is detected, corrective measures are taken and documented.

8 Documentation and review

All logging settings and procedures shall be clearly documented and available to authorised persons. The Logging Policy shall be reviewed and updated at least once a year to ensure its relevance and effectiveness.

9 Implementation

All university employees and third parties are responsible for implementing and complying with the Logging Policy to ensure the security of the university's information systems and data.

The Policy must be available to all persons concerned, who should be provided with an overview of the Policy along with necessary training.

The Policy shall be reviewed and updated at least once a year or as necessary to ensure it aligns with the changing regulatory requirements and technological advancements.