

PRINCIPLES OF MONITORING THE IT ENVIRONMENT

Laurea University of Applied Sciences

Change log

Change Date	Effective Date	Key Changes	Change Author(s)
19.6.2025	1.9.2025	Minor changes to text	Graubner, Pettinen, Valjakka

Sisällys

1	Introduction	3
2	Objectives	3
3	Responsibilities and organization	3
4	Implementation methods	4

1 Introduction

This document defines the principles to be implemented in the monitoring of the data processing environment's communication at Laurea University of Applied Sciences (hereinafter referred to as Laurea). In this context, the data processing environment refers to the components of the communication network, the terminal devices connected to the communication network, information systems, and cloud services.

The definition of these principles takes into account the implementation of the basic level of information security as defined by the state administration.

Laws Related to the Monitoring of the Data Communication Environment:

- Act on the Protection of Privacy in Working Life (759/2004)
- Constitution of Finland (731/1999, Sections 10 and 12)
- Act on Electronic Communications Services (917/2014)
- EU General Data Protection Regulation (EU 2016/679)
- Data Protection Act (1050/2018)
- Act on Information Management in Public Administration (906/2019)

2 Objectives

The objective of Laurea's information security work is to protect important information and the operation of information systems, services, and networks at an adequate and appropriate level, and to prevent unauthorized use and destruction, or distortion of information. The aim is to create and maintain a reliable and secure environment where risks related to information are managed.

Monitoring the data processing environment is one part of achieving this goal defined in Laurea's information security policy. By monitoring the data processing environment, the aim is to ensure the service level, security, and cost-effectiveness of the environment, as well as the integrity, confidentiality, and availability of information.

3 Responsibilities and organization

Part of the monitoring of Laurea's data processing environment is outsourced to an external CSOC monitoring service provider. Both Laurea and the CSOC service provider conduct the monitoring of the data processing environment according to the principles outlined in this document. Each

monitoring party is responsible for the information security of the monitoring data they store. The responsibilities of the parties are agreed upon in the contract concluded with the service provider.

The individuals authorized for maintenance and monitoring at Laurea and the service provider have been specifically named. They must adhere to the principles of monitoring outlined in this document, the rules for using IT services, good information management practices, and the laws related to network communication monitoring. Administrators must treat monitoring data as confidential information and must not disclose it or its existence to anyone who does not need the information to perform their job duties. Information is only shared among the named administrators. In unclear cases, Laurea's Chief Information Officer (CIO) makes the decision regarding access to monitoring data.

The Chief Information Officer has the right to change the individuals authorized to access monitoring data at Laurea.

The implementation of the principles of monitoring the data processing environment is supervised together with the service providers delivering network and monitoring services, within a service monitoring group established for this purpose.

Any deviations are reported to Laurea's information security and data protection steering group.

4 Implementation methods

The administrators of Laurea's data processing environment monitor network activity, as well as the events and log data of systems and terminal devices. This monitoring does not target individual users but is carried out using automated monitoring systems. These systems generate notifications and alerts that can prompt targeted inspections.

A more detailed inspection can be conducted, for example, if:

- A device exhibits behavior typical of malware.
- The activity of a user account suggests it has been compromised.
- A device or user is connecting to malicious websites.

The administrator of the data processing environment may contact the owner of a device or user account exhibiting abnormal behavior. Network and/or service usage can be temporarily blocked if there is a justified suspicion that such a block is necessary to ensure the security of systems and/or information.

In all cases, the administrator of the machine, service, or network must promptly inform the Chief Information Officer (CIO), the information security specialist, and the affected user about the block. If the action is taken by the information security specialist, they will also inform the relevant administrator of the machine, service, or network as needed.

Laurea's users are trained to report observed deficiencies, problems, and suspicions primarily to Laurea's IT services Service Desk and through security notifications.

The content of this document is communicated to Laurea's staff, especially administrators and service providers. Service providers are responsible for communicating this information within their own organizations.