INFORMATION SECURITY POLICY

CONTENTS

LIST OF ABBREVIATIONS (OR) SYMBOLS 3

DEFINITION OF INFORMATION SECURITY POLICY 4

BY THIS POLICY 4

APPLIES TO 4

POLICY GUIDELINES 5

Security Goals 5

Security strategy 6

Risks/liabilities/disclaimers 6

ROLES AND RESPONSIBILITIES 6

Security Goals 8

Security strategy 8

Risks/liabilities/disclaimers 8

RISK MANAGEMENT 9

REFERENCE TO RELEVANT LEGISLATION 9

SECURITY AWARENESS AND TRAINING 10

RELATED STANDARDS, POLICIES, PROCESSES AND GUIDELINES 10

POLICY COMPLIANCE 11

Compliance Measurement 11

Exceptions 11

Non-Compliance 11

RELATED STANDARDS, POLICIES AND PROCESSES 11

REVISION HISTORY 11

LIST OF ABBREVIATIONS (OR) SYMBOLS

BYOD	Bring Your Own Device
CEO	Chief Executive Officer
IEC	International Electro Technical Commission
ISO	International Organization for Standardization
ISM	Information Security Manager
IT	Information Technology
PIN	Personal Identification Number

DEFINITION OF INFORMATION SECURITY POLICY

This information security policy is the basic framework for information security at {company}. Based on the continuous monitoring and reporting {company} Management reviews the information security policy at least annually as part of the overall security management.

BY THIS POLICY

The purpose of this policy is to provide requirements and specific recommendations for the protection of {company} information technology resources and the information stored on those resources. Information security measures are intended to protect information assets and preserve the privacy of {company}'s employees, students, sponsors, suppliers and other associated entities.

APPLIES TO

This document applies to all the users in {company}, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory. This policy documents the industry best practices with which {company} will align its security activities.

POLICY GUIDELINES

{company}'s information security program will be based upon best practices recommended in the "Code of Practice for Information Security Controls" published by the ISO/IEC 27002:2013, appropriately tailored to the specific circumstances of {company}.

The CEO shall ensure that the information security policy, as well as guidelines and standards, are utilized and acted upon.

The CEO shall ensure that availability of sufficient training and information material for all users, to enable the users to protect {company}'s data and information systems.

The information security policy shall be reviewed and updated annually or when necessary, in accordance with principles described in ISO/IEC 27001.

All important changes to {company}'s activities, and other external changes related to the threat level, should result in a revision of the policy and the guidelines relevant to the information security.

Security Goals

- Illegal activities are strictly prohibited.
- Students and employees using BYOD shall:
- Set up passwords according to the Password policy.
- Encrypt important documents as necessary.
- Not hold any sensitive or confidential information that belongs to {company} or its customers.
- Delete all essential information belonging to {company} once it is no longer required.
- Report any security breach immediately to Information security manager.
- Always use his or her devices in an ethical manner and adhere to {company}'s acceptable use policy.

Security strategy

- The device must lock itself with a password or PIN if it's idle for five minutes.
- Students and employees' access to company data is limited based on user profiles defined by System administrators and automatically enforced.

Risks/liabilities/disclaimers

The employee or student assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

ROLES AND RESPONSIBILITIES

{company}'s information security program will be based upon best practices recommended in the "Code of Practice for Information Security Controls" published by the ISO/IEC 27002:2013, appropriately tailored to the specific circumstances of {company}.

The administration has the overall responsibility for managing {company}'s values in an effective and satisfactory manner according to current laws, requirements and contracts.

The CEO has the overall responsibility for information security at {company}, including information security regarding personnel and IT security.

Roles	**Responsibilities**
Owner of the security policy	• The CEO is the owner of the security policy. The CEO delegates the responsibility for security-related documentation to the ISM. All policy changes shall be approved and signed by the CEO.

Information Security Manager	• Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents.
System Owners	• Help with the security requirements for their specific area. • Determine the privileges and access rights to the resources within their areas.
System Administrators	• Implements and operates IT security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users	• Meet Security Policies. • Report any attempted security breaches.

The CEO shall ensure that the information security policy, as well as guidelines and standards, are utilized and acted upon.

The CEO shall ensure that availability of sufficient training and information material for all users, to enable the users to protect {company}'s data and information systems.

The information security policy shall be reviewed and updated annually or when necessary, in accordance with principles described in ISO/IEC 27001.

All important changes to {company}'s activities, and other external changes related to the threat level, should result in a revision of the policy and the guidelines relevant to the information security.

Security Goals

- Illegal activities are strictly prohibited.
- Students and employees using BYOD shall:
- Set up passwords according to the Password policy.
- Encrypt important documents as necessary.
- Not hold any sensitive or confidential information that belongs to {company} or its customers.
- Delete all essential information belonging to {company} once it is no longer required.
- Report any security breach immediately to Information security manager.
- Always use his or her devices in an ethical manner and adhere to {company}'s acceptable use policy.

Security strategy

- The device must lock itself with a password or PIN if it's idle for five minutes.
- Students and employees' access to company data is limited based on user profiles defined by System administrators and automatically enforced.

Risks/liabilities/disclaimers

The employee or student assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

RISK MANAGEMENT

- {company}'s approach to security should be based on risk assessments.
- Companies should continuously assess the risk and evaluate the need for protective measures. Measures shall be evaluated based on efficiency, cost and practical feasibility.
- An overall risk assessment of the information systems should be performed annually.
- Risk assessments shall find, quantify and prioritize the risks according to relevant criteria for acceptable risks.
- Risk assessments are to be conducted when implementing changes affecting information security. Recognized methods of assessing risks should be employed, such as ISO/IEC 27005.
- The ISM handles ensuring that the risk management processes are coordinated by the policy.
- The system owners handle ensuring that risk assessments within their area of responsibility are implemented by the policy.
- Risk management is to be conducted according to criteria approved by the management at {company}.
- Risk assessments shall be approved by the management and/or the system owners.
- If a risk assessment reveals unacceptable risks, measures should be implemented to reduce the risk to an acceptable level.

REFERENCE TO RELEVANT LEGISLATION

{company} has an obligation to abide by all Finnish legislation and relevant legislation of the European Community. The relevant acts, which apply in Finnish law to Information Systems Security, include but are not limited to:

- Personal Data Act (523/1999)
- Act on the Protection of Privacy in Working Life (759/2004)

SECURITY AWARENESS AND TRAINING

Information security awareness training shall be included in the staff instruction process.

An ongoing awareness program shall be set up and kept ensuring that staff awareness is refreshed and updated, as necessary.

RELATED STANDARDS, POLICIES, PROCESSES AND GUIDELINES

The Information Security Policy is developed as a pinnacle document which has further policies, standards and guides which enforce and support the policy. Staff, students and any third parties authorized to access {company} network to use the systems and facilities must familiarize themselves with the policies and work following them. The supporting policies are grouped into 3 areas: Technical Security, Operational Security and Security Management.

Technical Security:

- Password Policy
- Information Security Policy (partly)
- BYOD Policy (partly)

Operational Security:

- Acceptable Use Policy
- Clean Desk Policy
- BYOD Policy (partly)
- Data Protection Policy (partly)

Security Management:

- Information Security Policy.
- Data Protection Policy (partly).

POLICY COMPLIANCE

Compliance Measurement

{company} will not monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both
- Prevent access to a particular system
- Take all necessary and appropriate steps to retrieve information owned by {company}

Exceptions

Any exception to the policy shall be approved by the information security manager in advance.

Non-Compliance

Students and employees found to have violated this policy may be subject to disciplinary action.

RELATED STANDARDS, POLICIES AND PROCESSES

- Acceptable use policy
- Password policy
- Password construction guidelines

REVISION HISTORY

Version	Description	Date	Author	Approved By
1.0	Initial version	14/04/2025	ZtotheZ	