BYOD POLICY

CONTENTS

LIST OF ABBREVIATIONS (OR) SYMBOLS **3**

DEFINITION OF BYOD **4**

BY THIS POLICY **4**

APPLIES TO **4**

POLICY GUIDELINES **5**

Responsibilities 5

Security 5

Risks/liabilities/disclaimers 5

POLICY COMPLIANCE **6**

Compliance Measurement 6

Exceptions 6

Non-Compliance 6

RELATED STANDARDS, POLICIES AND PROCESSES **6**

REVISION HISTORY **6**

ZtotheZ
Address
Postcode City

https://company.com
name@companysite.fi

LIST OF ABBREVIATIONS (OR) SYMBOLS

BYOD	Bring your own device
PIN	Personal identification number

DEFINITION OF BYOD

{company} recognizes the benefits that can be achieved by allowing students/employees to use their own devices while working. Such devices include, but is not limited to, laptops, smart phones and tablets. It is committed to supporting staff in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing {company} provided services on BYOD. The use of such devices to create and process {company} information and data creates issues that need to be addressed, particularly in the area of information security.

BY THIS POLICY

This document provides policies, standards, and rules of behaviour for the use of personally-owned devices by {company} employees to access {company} resources and/or services.

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

All relevant {company} policies apply to all students, employees and other affiliates using BYOD. Following policies are directly relevant to adopting BYOD.

- Acceptable use policy
- Password policy

Responsibilities

- 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.
- Use his or her devices in an ethical manner at all times and adhere to {company}'s acceptable use policy.

Security

- 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.

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	