[organization logo]

[organization name]

**BRING YOUR OWN DEVICE (BYOD) POLICY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415649520)

[2. Reference documents 3](#_Toc415649521)

[3. Security rules for using BYOD 3](#_Toc415649522)

[3.1. Company policy 3](#_Toc415649523)

[3.2. Who is allowed to use BYOD, and for what 3](#_Toc415649524)

[3.3. Which devices are allowed 3](#_Toc415649525)

[3.4. Acceptable use 3](#_Toc415649526)

[3.5. Special rights 4](#_Toc415649527)

[3.6. Reimbursement 4](#_Toc415649528)

[3.7. Security breaches 5](#_Toc415649529)

[3.8. Training and awareness 5](#_Toc415649530)

[4. Managing records kept on the basis of this document 5](#_Toc415649531)

[5. Validity and document management 5](#_Toc415649532)

# Purpose, scope and users

The purpose of this document is to define how [organization name] will retain control over its information while such information is being accessed through devices that are not owned by the organization.

This document is applied to all personally owned devices that have the ability to store, transfer or process any sensitive information from the Information Security Management System (ISMS) scope. Those devices include laptops, smart phones, tablets, USB memory sticks, digital cameras, etc. Such devices will be referred to as BYOD in this Policy.

Users of this document are all employees of [organization name].

# Reference documents

* ISO/IEC 27001 standard, clauses A.6.2.1, A.6.2.2, A.13.2.1

# Security rules for using BYOD

The rules in this Policy apply to all BYOD, whether they are used for work or for private use, or whether they are used within or outside of the organization's premises.

## Company policy

[organization name] supports widespread use of BYOD for work use – i.e. using such devices for performing work for the company.

The company data that is stored, transferred or processed on BYOD remains under the company’s ownership, and the company retains the right to control such data even though it is not the owner of the device.

## Who is allowed to use BYOD, and for what

[job title] will create a List of job titles and/or persons who are allowed to use BYOD, together with the applications and databases they are allowed to access with their own devices.

[job title] will create a List of BYOD-prohibited applications.

## Which devices are allowed

[job title] will create a List of acceptable devices which can be used as BYOD, together with mandatory settings for each device.

## Acceptable use

For each BYOD, the following are mandatory:

* [describe how the backup of company information must be made]
* [describe which security software must be installed – e.g. anti-virus software, intrusion prevention, mobile device management software, etc.]
* [describe the method of encryption that is to be used and for what]
* [describe the method of authentication that is to be used]
* [describe the secure method of connection to the company network]
* when using BYOD outside of the company premises, it must not be left unattended and, if possible, should be physically locked away
* when using BYOD in public places, the owner must take care that data cannot be read by unauthorized persons
* patches and updates must be installed regularly
* classified information must be additionally protected according to the [Information Classification Policy]
* notify [job title] before BYOD is being disposed of, sold, or handed to a third party for servicing

It is not allowed to do the following with BYOD:

* allow access to anyone else except the employee who is the owner of the device
* install applications that are listed in List of BYOD-prohibited applications
* store illegal materials on the device
* install unlicensed software
* connect via Bluetooth to any kind of device
* connect to unknown Wi-Fi networks
* locally store passwords, except when using the following applications: [list allowed applications where passwords can be stored]
* locally store the following information: [list sensitive information]
* transfer company data to other devices which are not allowed

## Special rights

[organization name] has the right to view, edit, and delete all company data that is stored, transferred or processed on BYOD.

[job title] is authorized to configure any BYOD according to this Policy and monitor its use via [specify the name of mobile device management software].

[organization name] has the right to perform full deletion of all data on BYOD if it considers that necessary for the protection of the company data, without the consent of the device owner.

## Reimbursement

[organization name] will not pay the employees (the owners of BYOD) any fee for using the device for work purposes.

[organization name] will pay for the following:

* Any new software that needs to be installed for company use
* Telecommunication costs (data and telephone charges): [define percentage] of the owner's monthly bills

## Security breaches

All security breaches related to BYOD must be reported immediately to [job title]. Further, all weaknesses that have not yet become incidents must be reported through the same channels within 1 business day.

## Training and awareness

[job title] is in charge of training new and existing employees on appropriate use of BYOD, as well as raising awareness about the most common threats.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [List of allowed users for BYOD and what they can access] | [company intranet] | [job title] | Only [job title] can edit and publish new version of the List | List that is no longer valid must be archived for 3 years |
| [List of acceptable BYOD devices and their settings] | [company intranet] | [job title] | Only [job title] can edit and publish new version of the List | List that is no longer valid must be archived for 3 years |
| [List of prohibited BYOD applications] | [company intranet] | [job title] | Only [job title] can edit and publish new version of the List | List that is no longer valid must be archived for 3 years |

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year. [job title] will review List of allowed users, List of acceptable devices, and List of prohibited applications every 3 months.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

* number of incidents related to use of BYOD
* number of employees using BYOD without authorization

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]