[Organization logo]

[Organization name]

Commented [270011]: All fields in this document marked by square brackets [ ] must be filled in.

BRING YOUR OWN DEVICE (BYOD) POLICY

Commented [270012]: To learn more about this topic, please read this article:

What is a BYOD policy, and how can you easily write one using ISO 27001 controls?
https://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/

Commented [270013]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

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

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. 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.

Commented [270014]: Include the name of your 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].

Commented [270015]: Include the name of your organization.

2. Reference documents

- ISO/IEC 27001 standard, clauses A.5.14, A.6.7, and A.8.1

3. 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.

3.1. Company policy

[Organization name] supports widespread use of BYOD for work use – i.e. using such devices for

Commented [270016]: Include the name of your organization.

Commented [270017]: Alternatively, you can say something

and/or intellectual property even though it is not the owner of the device.

3.2. Who is allowed to use BYOD, and for what

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

3.3. Which devices are allowed

Commented [270018]: E.g. firewall, backup, screen locking, etc.

3.4. 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.]
- [illegible]
- [illegible]
- [illegible]
- when using BYOD outside of the company premises, it must not be left unattended and, if [illegible]
- [illegible] unauthorized persons
- [illegible]
- [illegible]
- [illegible] 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
- [illegible]
- [illegible]
- [illegible]
- connect via Bluetooth to any kind of device
- [illegible]
- [illegible]
- locally store the following information: [list sensitive information]
- [illegible]

3.5. Special rights

[Organization name] has the right to view, edit, and delete all company data that is stored, [illegible]

[illegible]

[illegible] necessary for the protection of the company data, without the consent of the device owner.

3.6. Reimbursement

[illegible]

[Organization name] will pay for the following:

Commented [270019]: E.g. passwords, pass codes, biometric readers, etc.

Commented [2700110]: E.g. VPN.

Commented [2700111]: To be deleted if this Policy does not exist.

Commented [2700112]: Include the name of your organization.

Commented [27A13]: Delete this if you do not use any mobile device management software.

Commented [2700114]: Include the name of your organization.

Commented [2700115]: [illegible]

Commented [2700116]: Include the name of your organization.

Commented [2700117]: [illegible]

Commented [2700118]: Include the name of your organization.

- [redacted]
- [redacted]

Commented [27A19]: [redacted]

3.7. Security breaches

All security breaches related to BYOD must be reported immediately to [job title]. Further, all [redacted]

Commented [2700120]: This is usually the Security Officer, or the Help Desk.

3.8. Training and awareness

[redacted] raising awareness about the most common threats.

Commented [2700121]: This training will help you raise the security awareness and track the knowledge of your employees: https://training.advisera.com/awareness-session/security-awareness-training/

4. 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

Commented [2700122]: Alter these records to match what you already have in your company. If you do not have similar records, you can create new ones in the format that suits you best.

Commented [2700123]: Modify as appropriate.

Commented [2700124]: Modify as appropriate.

Commented [2700125]: Modify as appropriate.

5. 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.

Commented [2700126]: This is only a recommendation; adjust frequency as appropriate.

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

- [illegible]
- [illegible]

[job title]
[name]

[signature]

Commented [2700127]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.