[Organization logo]

[Organization name]

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

MOBILE DEVICE, TELEWORKING, AND WORK FROM HOME POLICY

Commented [2]: To learn more about this topic, please read this article:

How to Use ISO 27001 To Secure Data When Working Remotely
https://advisera.com/27001academy/blog/2021/10/27/how-to-use-iso-27001-to-secure-data-when-working-remotely/

Commented [270013]: There is no need to write a separate document for the Mobile Device, Teleworking and Work from Home Policy if the same rules are prescribed by the IT Security Policy.

Commented [270014]: 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 prevent unauthorized access to mobile devices both within and outside of the organization's premises.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all persons, data and equipment in the ISMS scope.

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.6.7, A.7.9, and A.8.1
- Information Security Policy
- [Information Classification Policy]
- [IT Security Policy]

Commented [27A6]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "05_General_Policies".

Commented [27A7]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "09_Annex_A_Security_Controls".

Commented [27A8]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "09_Annex_A_Security_Controls".

3. Mobile computing

3.1. Introduction

Mobile computing equipment includes all kinds of portable computers, mobile phones, smart phones, memory cards and other mobile equipment used for storage, processing, and transferring of data, no matter where such equipment is used.

The abovementioned equipment may be taken off-premises only after obtaining authorization in accordance with the IT Security Policy.

Commented [270019]: Delete this paragraph if control A.7.10 is excluded from the Statement of Applicability.

3.2. Basic rules

Special care should be taken when mobile computing equipment is placed in vehicles (including cars),

The person taking mobile computing equipment off-premises must follow these rules:

-
- cannot be read by unauthorized persons
- updates of patches and other system settings are
- protection against malicious code is installed and

Commented [2700110]: To be deleted if control A.7.9 is marked as inapplicable in the Statement of Applicability.

Commented [27A11]: E.g., weekly accessing of the

Commented [27A12]: E.g., by enforcing installation of the tool

- the person using mobile computing equipment off-premises is responsible for regular back-
- connecting to communication networks is performed
- [information] on portable computers must be encrypted
- protection of sensitive data must be implemented in accordance with the [Information Classification Policy]
-
-

[Job title] is responsible for training and raising awareness of persons who are using mobile

4. Teleworking & work from home

4.1. Introduction

include the use of mobile phones outside the organization's premises.

4.2. Additional rules for teleworking

of this document, and the rules defined below:

- the physical location where teleworking is performed must be protected by [specify how this
-
- prevention of unauthorized access by persons living or working at the location where the
- protection of the organization's intellectual property rights, either for software or other
-
- implemented in accordance with the [IT Security Policy]
- specific forbidden activities for employees performing teleworking are: [list here the

Commented [27A13]: E.g., by accessing the organization's

Commented [27A14]: E.g., by establishing a secure communication channel using VPN for encrypting data

Commented [27A15]: Specify the type of information stored

Commented [27A16]: E.g., through virtual disk encryption, volume encryption, or file/folder encryption

Commented [27A17]: If your organization does not have an

Commented [27A18]: If your organization does not have a

Commented [19]: To be deleted in case usage of employees' own devices is not allowed.

Commented [27A20]: You can use the following Security Awareness Training to train your employees: https://training.advisera.com/awareness-session/security-awareness-training/

Commented [21]: To learn more about this topic, please read this article:

How to Use ISO 27001 To Secure Data When Working Remotely https://advisera.com/27001academy/blog/2021/10/27/how-to-use-iso-27001-to-secure-data-when-working-remotely/

Commented [2700122]:

Commented [27A23]: Examples of elements to use are:

Commented [27A24]: E.g., uninterruptable power supply, alternative communication links, etc.

Commented [27A25]: In case the Clear Desk and Clear Screen Policy is implemented as part of the IT Security Policy, then change this reference to the "IT Security Policy."

Commented [27A26]: If your organization does not have an

Commented [27A27]: E.g., participating in meetings with the

Commented [2700128]: You can delete this text if there are no specific forbidden activities for employees.

- [redacted]

Commented [27A29]: E.g., changing configurations on network devices, etc.

Commented [27A30]: You can delete this text if there are no specific allowed activities for employees.

5. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
[Authorization for teleworking]	[specify, considering the form of authorization given]	[job title]	[specify, considering the form of authorization given]	Records are stored for a period of 3 years

Commented [2700131]: Adjust as appropriate.

Only [job title] can grant other employees access to the any of the abovementioned documents.

6. 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.

Commented [2700132]: This is only a recommendation; adjust frequency as appropriate.

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

- [redacted]
- [redacted]

[job title]
[name]

[signature]

Commented [2700133]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.