[organization logo]

[organization name]

**MOBILE DEVICE AND TELEWORKING 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](#_Toc415649624)

[2. Reference documents 3](#_Toc415649625)

[3. Mobile computing 3](#_Toc415649626)

[3.1. Introduction 3](#_Toc415649627)

[3.2. Basic rules 3](#_Toc415649628)

[4. Teleworking 4](#_Toc415649629)

[5. Managing records kept on the basis of this document 4](#_Toc415649630)

[6. Validity and document management 5](#_Toc415649631)

# 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].

# Reference documents

* ISO/IEC 27001 standard, clauses A.6.2 and A.11.2.6
* Information Security Policy
* [Information Classification Policy]
* [Acceptable Use Policy]

# Mobile computing

## 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.

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

## Basic rules

Special care should be taken when mobile computing equipment is placed in vehicles (including cars), public spaces, hotel rooms, meeting places, conference centers, and other unprotected areas outside the organization's premises.

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

* mobile computing equipment carrying important, sensitive or critical information must not be left unattended and, if possible, should be physically locked away, or special locks should be used to secure the equipment
* when using mobile computing equipment in public places, the user must take care that data cannot be read by unauthorized persons
* updates of patches and other system settings are performed by [specify how this is technically implemented, or make reference to a document defining the process]
* protection against malicious code is installed and updated [specify how this is technically implemented, or make reference to a document defining this process]
* the person using mobile computing equipment off-premises is responsible for regular back-ups of data [specify how this is technically implemented, or make reference to a document defining the process]
* connecting to communication networks and data exchange must reflect the sensitivity of data and is performed by [specify how this is technically implemented, or make reference to a document defining the process]
* information on portable computers must be encrypted [specify whether this is mandatory for the entire hard disk or only for sensitive files, etc.]
* protection of sensitive data must be implemented in accordance with the [Information Classification Policy]
* in case mobile computing equipment is left unattended, rules for unattended user equipment must be applied in accordance with the [Acceptable Use Policy]

[job title] is responsible for training and raising awareness of persons who are using mobile computing equipment outside the organization's premises.

# Teleworking

Teleworking means that information and communication equipment is used to enable employees to perform their work outside the organization. Teleworking does not include the use of mobile phones outside the organization's premises.

Teleworking must be authorized by [job title] by [specify the authorization method].

[job title] is responsible for preparing plans and procedures to ensure the following:

* protection of mobile computing equipment as specified in the previous section
* prevention of unauthorized access by persons living or working on the location where the teleworking activity is performed
* appropriate configuration of the local network used for connecting to the Internet
* protection of the organization's intellectual property rights, either for software or other materials that may be protected by intellectual property rights
* process for return of data and equipment in the case of termination of employment
* minimum level of configuration of the facility where teleworking activities will be performed
* permitted and forbidden types of activities

# 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 |
| [Plans and procedures for teleworking] | [company intranet] | [job title] | [only (job title) can publish and edit the internal rules] | 3 years |

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

# 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.

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

* number of incidents related to taking mobile computing equipment outside the organization's premises without authorization
* number of incidents related to unauthorized access to mobile computing equipment outside the organization's premises

[job title]

[name]

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

[signature]