[organization logo]

[organization name]

**ACCEPTABLE USE 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](#_Toc415650319)

[2. Reference documents 3](#_Toc415650320)

[3. Acceptable use of information assets 3](#_Toc415650321)

[3.1. Definitions 3](#_Toc415650322)

[3.2. Acceptable use 3](#_Toc415650323)

[3.3. Responsibility for assets 3](#_Toc415650324)

[3.4. Prohibited activities 3](#_Toc415650325)

[3.5. Taking assets off-site 4](#_Toc415650326)

[3.6. Return of assets upon termination of contract 4](#_Toc415650327)

[3.7. Backup procedure 4](#_Toc415650328)

[3.8. Antivirus protection 4](#_Toc415650329)

[3.9. Authorizations for information system use 4](#_Toc415650330)

[3.10. User account responsibilities 4](#_Toc415650331)

[3.11. Password responsibilities 5](#_Toc415650332)

[3.12. Clear desk and clear screen policy 5](#_Toc415650333)

[3.12.1. Clear desk policy 5](#_Toc415650334)

[3.12.2. Clear screen policy 6](#_Toc415650335)

[3.12.3. Protection of shared facilities and equipment 6](#_Toc415650336)

[3.13. Internet use 6](#_Toc415650337)

[3.14. E-mail and other message exchange methods 6](#_Toc415650338)

[3.15. Copyright 7](#_Toc415650339)

[3.16. Mobile computing 7](#_Toc415650340)

[3.16.1. Introduction 7](#_Toc415650341)

[3.16.2. Basic rules 7](#_Toc415650342)

[3.17. Teleworking 8](#_Toc415650343)

[3.18. Monitoring the use of information and communication systems 8](#_Toc415650344)

[3.19. Incidents 9](#_Toc415650345)

[4. Managing records kept on the basis of this document 9](#_Toc415650346)

[5. Validity and document management 10](#_Toc415650347)

# Purpose, scope and users

The purpose of this document is to define clear rules for the use of the information system and other information assets in [organization name].

This document is applied to the entire scope of the Information Security Management System (ISMS), i.e. to all information systems and other information assets used within the ISMS scope.

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.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
* Information Security Policy
* [Information Classification Policy]
* [Incident Management Procedure]
* [Inventory of Assets]
* [Operating Procedures for Information and Communication Technology]
* [Information Transfer Policy]

# Acceptable use of information assets

## Definitions

Information system – includes all servers and clients, network infrastructure, system and application software, data, and other computer subsystems and components which are owned or used by the organization or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

Information assets – in the context of this Policy, the term *information assets* is applied to information systems and other information/equipment including paper documents, mobile phones, portable computers, data storage media, etc.

## Acceptable use

Information assets may be used only for business needs with the purpose of executing organization-related tasks.

## Responsibility for assets

Each information asset has an owner designated in the Inventory of Assets. The asset owner is responsible for the confidentiality, integrity and availability of information in the asset in question.

## Prohibited activities

It is prohibited to use information assets in a manner that unnecessarily takes up capacity, weakens the performance of the information system or poses a security threat. It is also prohibited:

* to download image or video files which do not have a business purpose, send e-mail chain letters, play games, etc.
* to install software on a local computer without explicit permission by [job title]
* to use Java applications, Active X controls and other mobile code, except when authorized by [job title]
* to use cryptographic tools (encryption) on a local computer, except in the cases specified in the Information Classification Policy
* to download program code from external media
* to install or use peripheral devices such as modems, memory cards or other devices for storing and reading data (e.g. USB flash drives) without explicit permission by [job title]; use in accordance with the Information Classification Policy is allowed

## Taking assets off-site

Equipment, information or software, regardless of its form or storage medium, may not be taken off-site without prior written permission by [job title].

As long as said assets are outside the organization, they have to be controlled by the person who was granted permission for their removal.

## Return of assets upon termination of contract

Upon termination of an employment contract or other contract on the basis of which various equipment, software or information in electronic or paper form is used, the user must return all such information assets to [job title].

## Backup procedure

The user must [specify backup procedure method] all sensitive information stored on his/her computer at least once a day.

## Antivirus protection

[name of antivirus software] must be installed on each computer with activated automatic updates.

## Authorizations for information system use

Users of the information system may only access those information system assets for which they have been explicitly authorized by the asset owner.

Users may use the information system only for purposes for which they have been authorized, i.e. for which they have been granted access rights.

Users must not take part in activities which may be used to bypass information system security controls.

## User account responsibilities

The user must not, directly or indirectly, allow another person to use his/her access rights, i.e. username, and must not use another person’s username and/or password. The use of group user names is forbidden.

The owner of the user account is its user, who is responsible for its use, and all transactions performed through this user account.

## Password responsibilities

Users must apply good security practices when selecting and using passwords:

* passwords must not be disclosed to other persons, including management and system administrators
* passwords must not be written down, unless a secure method has been approved by [job title]
* user-generated passwords must not be distributed through any channel (using oral, written or electronic distribution, etc.)
* passwords must be changed if there are indications that the passwords or the system may have been compromised – in that case a security incident must be reported
* strong passwords must be selected, in the following way:
  + using at least twelve characters
  + using at least one numeric character
  + using at least one uppercase and at least one lowercase alphabetic character
  + using at least one special character
  + a password must not be a dictionary word, dialectal or jargon word from any language, or any of these words written backwards
  + passwords must not be based on personal data (e.g. date of birth, address, name of family member, etc.)
  + the last three passwords must not be re-used
* passwords must be changed every 3 months
* password must be changed at first log-on to a system
* passwords must not be stored in an automated log-on system (e.g. macro or browser)
* passwords used for private purposes must not be used for business purposes

## Clear desk and clear screen policy

All information classified as "Internal use," "Restricted" and "Confidential" as specified in the Information Classification Policy are regarded as sensitive in this item.

### Clear desk policy

If the authorized person is not at his/her workplace, all paper documents, as well as data storage media labeled as sensitive, must be removed from the desk or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorized access.

Such documents and media must be stored in a secure manner in accordance with the Information Classification Policy.

### Clear screen policy

If the authorized person is not at his/her workplace, all sensitive information must be removed from the screen, and access must be denied to all systems for which the person has authorization.

In the case of short absence (up to 30 minutes), the clear screen policy is implemented by logging out of all systems or locking the screen with a password. If the person is absent for a longer period of time (over 30 minutes), the clear screen policy is implemented by logging out of all systems and turning off the workstation.

### Protection of shared facilities and equipment

Documents containing sensitive information must immediately be removed from printers, fax and copy machines.

Facilities for dispatch and reception of mail [specify facilities and their location] are protected by [specify the manner of protection when the authorized person is absent – e.g. locking the facility, etc.].

Shared fax machines [specify machines and their location] are protected by [specify the manner of protection when the authorized person is absent – e.g. locking the facility, etc.].

Unauthorized use of printers, photocopiers, scanners and other shared equipment for copying [specify machines and their location] is prevented by [specify how – e.g. by locking the facility, use of PIN numbers, access cards, etc.].

## Internet use

Internet may be accessed only through the organization's local network with appropriate infrastructure and firewall protection. Direct Internet access through modems, mobile Internet, wireless network or other devices for direct Internet access is forbidden.

[job title] may block access to some Internet pages for individual users, groups of users or all employees at the organization. If access to some web pages is blocked, the user may submit a written request to [job title] for authorization to access such pages. The user must not try to bypass such restriction autonomously.

The user must regard information received through unverified websites as unreliable. Such information may be used for business purposes only after its authenticity and correctness have been verified.

The user is responsible for all possible consequences arising from unauthorized or inappropriate use of Internet services or content.

## E-mail and other message exchange methods

Message exchange methods other than electronic mail also include download of files from the Internet, transfer of data via [provide names of specialized communication systems], telephones, fax machines, sending SMS text messages, portable media, and forums and social networks.

In accordance with [Operating Procedures for Information and Communication Technology / Information Transfer Policy], as well as [Information Classification Policy], [job title] determines the communication channel that may be used for each type of data, as well as possible restrictions on who is allowed to use communication channels, i.e. defines which activities are forbidden.

Users may only send messages containing true information. It is forbidden to send materials with disturbing, unpleasant, sexually explicit, rude, slanderous or any other unacceptable or illegal content. Users must not send spam messages to persons with whom no business relationship has been established or to persons who did not require such information.

Should a user receive a spam e-mail, he/she must inform [job title].

If sending a message with a confidentiality label, the user must protect it as specified in the Information Classification Policy.

The user must save each message containing data significant for the organization's business using the method specified by [job title].

Each e-mail message must contain a disclaimer, except messages sent through communication systems determined by [job title]. Should a user post a message on a message exchange system (social networks, forums, etc.), he/she must unambiguously state that it does not represent the organization's viewpoint.

## Copyright

Users must not make unauthorized copies of software owned by the organization, except in cases permitted by law, by the owner or [job title].

Users must not copy software or other original materials from other sources, and are liable for all consequences that could arise under the intellectual property law.

## 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.

### Basic rules

Special care should be taken when mobile computing equipment is placed in cars or other forms of transportation, 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 [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 [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 line with the Clear Desk and Clear Screen 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 equipment and data in the case of termination of employment
* minimum level of configuration of the facility where teleworking activities will be performed
* permitted and forbidden type of activities

## Monitoring the use of information and communication systems

All data which is created, stored, sent or received through the information system or other organization's communication systems, including various applications, e-mail, Internet, fax, etc., whether it is personal or not, is considered the ownership of [organization name].

Users agree that authorized persons from the organization may access all such data, and that access by such persons will not be considered a violation of the users' privacy.

The organization may use specialized tools for the purpose of identifying and blocking forbidden methods of communication and filtering forbidden content.

## Incidents

Each employee, supplier or third person who is in contact with data and/or systems of [organization name] must report any system weakness, incident or event pointing to a possible incident as specified in the Incident Management Procedure.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [Authorizations for software installation, use of Java applications and Active X controls, use of cryptographic tools, download of program code from external media, installing peripheral devices] – electronic form | [intranet folder] | [job title] | Records cannot be edited; only [job title] has the right to store such records | Records are stored for a period of 3 years |
| [Authorization for taking assets off-site] – electronic form | [intranet folder] | [job title] | Records cannot be edited; only [job title] has the right to store such records | Records are stored for a period of 3 years |
| [Authorization for access to selected Internet pages] – electronic form | [intranet folder] | [job title] | Records cannot be edited; only [job title] has the right to store such records | Records are stored for a period of 3 years |
| [Decision on how each data type may be exchanged] – electronic form | [intranet folder] | [job title] | Records cannot be edited; only [job title] has the right to store such records | Records are stored for a period of 3 years |
| [Decision on how messages containing business-relevant data should be stored] – electronic form | [intranet folder] | [job title] | Records cannot be edited; only [job title] has the right to store such records | Records are stored for a period of 3 years |
| [Authorization for teleworking] – electronic form | [intranet folder] | [job title] | Records cannot be edited; only [job title] has the right to store such records | Records are stored for a period of 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 need to be considered:

* number of incidents related to unacceptable or unauthorized use of information assets
* number of incidents related to inappropriate employee training or awareness programs regarding acceptable use of information assets

[job title]

[name]

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

[signature]