\*\* FREE PREVIEW VERSION \*\*

[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** |
| 01/10/2013 | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc368677598)

[2. Reference documents 3](#_Toc368677599)

[3. Acceptable use of information assets 3](#_Toc368677600)

[3.1. Definitions 3](#_Toc368677601)

[3.2. Acceptable use 3](#_Toc368677602)

[3.3. Responsibility for assets 3](#_Toc368677603)

[3.4. Prohibited activities 3](#_Toc368677604)

[3.5. Taking assets off-site 4](#_Toc368677605)

[3.6. Return of assets upon termination of contract 4](#_Toc368677606)

[3.7. Backup procedure 4](#_Toc368677607)

[3.8. Antivirus protection 4](#_Toc368677608)

[3.9. Authorizations for information system use 4](#_Toc368677609)

[3.10. User account responsibilities 4](#_Toc368677610)

[3.11. Password responsibilities 5](#_Toc368677611)

[3.12. Clear desk and clear screen policy 5](#_Toc368677612)

[3.12.1. Clear desk policy 5](#_Toc368677613)

[3.12.2. Clear screen policy 6](#_Toc368677614)

[3.12.3. Protection of shared facilities and equipment 6](#_Toc368677615)

[3.13. Internet use 6](#_Toc368677616)

[3.14. E-mail and other message exchange methods 6](#_Toc368677617)

[3.15. Copyright 7](#_Toc368677618)

[3.16. Mobile computing 7](#_Toc368677619)

[3.16.1. Introduction 7](#_Toc368677620)

[3.16.2. Basic rules 7](#_Toc368677621)

[3.17. Teleworking 8](#_Toc368677622)

[3.18. Monitoring the use of information and communication systems 8](#_Toc368677623)

[3.19. Incidents 9](#_Toc368677624)

[4. Managing records kept on the basis of this document 9](#_Toc368677625)

[5. Validity and document management 10](#_Toc368677626)

# 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

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: <http://www.iso27001standard.com/en/documentation/Acceptable-Use-of-Assets-Policy>