\*\* FREE PREVIEW VERSION \*\*

[Organization logo]

[Organization name]

**IT SECURITY POLICY**

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

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| dd.mm.yyyy | 0.1 | EUGDPRAcademy | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 4](#_Toc114516364)

[2. Reference documents 4](#_Toc114516365)

[3. Acceptable use of information assets 4](#_Toc114516366)

[3.1. Definitions 4](#_Toc114516367)

[3.2. Acceptable use 4](#_Toc114516368)

[3.3. Responsibility for assets 4](#_Toc114516369)

[3.4. Deletion of information 5](#_Toc114516370)

[3.5. Prohibited activities 5](#_Toc114516371)

[3.6. Taking assets off-site 5](#_Toc114516372)

[3.7. Return of assets upon termination of contract 5](#_Toc114516373)

[3.8. Backup procedure 5](#_Toc114516374)

[3.9. Antivirus/malware protection 5](#_Toc114516375)

[3.10. Authorizations for information system use 5](#_Toc114516376)

[3.11. User account responsibilities 6](#_Toc114516377)

[3.12. Password responsibilities 6](#_Toc114516378)

[3.13. Clear desk and clear screen policy 6](#_Toc114516379)

[3.13.1. Clear desk policy 7](#_Toc114516380)

[3.13.2. Clear screen policy 7](#_Toc114516381)

[3.13.3. Protection of shared facilities and equipment 7](#_Toc114516382)

[3.14. Internet use 7](#_Toc114516383)

[3.15. E-mail and other message exchange methods 8](#_Toc114516384)

[3.16. Copyright 8](#_Toc114516385)

[3.17. Mobile computing 8](#_Toc114516386)

[3.17.1. Introduction 9](#_Toc114516387)

[3.17.2. Basic rules 9](#_Toc114516388)

[3.18. Teleworking & work from home 9](#_Toc114516389)

[3.18.1. Introduction 9](#_Toc114516390)

[3.18.2. Additional rules for teleworking 10](#_Toc114516391)

[3.19. Monitoring the use of information and communication systems 10](#_Toc114516392)

[3.20. Incidents & data breaches 10](#_Toc114516393)

[4. Managing records kept on the basis of this document 10](#_Toc114516394)

[5. Validity and document management 11](#_Toc114516395)

# Purpose, scope and users

The purpose of this document is to define clear rules for the acceptable 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, and to all personal data processing activities.

Users of this document are all employees of [organization name].

# Reference documents

* ISO/IEC 27001 standard, clauses A.5.9, A.5.10, A.5.11, A.5.14, A.5.17, A.5.32, A.6.7, A.7.7, A.7.9, A.7.10, A.8.1, A.8.7, A.8.10, A.8.12, A.8.13, A.8.19, and A.8.23
* EU GDPR Article 32
* Information Security Policy
* [Information Classification Policy]
* [Data Breach Response and Notification Procedure]
* [Inventory of Assets]
* [Security Procedures for IT Department]

# 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 that are owned or used by the organization or that 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 the information on the asset in question.

## Deletion of information

When no longer required, the asset owner must delete sensitive information stored on his/her computer or mobile device.

## 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
* …

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

To download full version of this document click here: <https://advisera.com/eugdpracademy/documentation/it-security-policy/>