\*\* 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 3](#_Toc496549705)

[2. Reference documents 3](#_Toc496549706)

[3. Basic Security Rules 3](#_Toc496549707)

[3.1. Definitions 3](#_Toc496549708)

[3.2. Acceptable use 3](#_Toc496549709)

[3.3. Responsibility for assets 3](#_Toc496549710)

[3.4. Prohibited activities 3](#_Toc496549711)

[3.5. Taking assets off-site 4](#_Toc496549712)

[3.6. Return of assets upon termination of contract 4](#_Toc496549713)

[3.7. Backup procedure 4](#_Toc496549714)

[3.8. Antivirus protection 4](#_Toc496549715)

[3.9. Authorizations for information system use 4](#_Toc496549716)

[3.10. User account responsibilities 4](#_Toc496549717)

[3.11. Password responsibilities 4](#_Toc496549718)

[3.12. Internet use 5](#_Toc496549719)

[3.13. E-mail and other message exchange methods 5](#_Toc496549720)

[3.14. Copyright 6](#_Toc496549721)

[4. Managing records kept on the basis of this document 6](#_Toc496549722)

[5. Validity and document management 7](#_Toc496549723)

# 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].

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

# Reference documents

* ISO/IEC 27001 standard
* [Information Classification Policy]
* [Security Procedures for the IT Department]

# Basic Security Rules

## 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

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

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