\*\* FREE PREVIEW VERSION \*\*

[Organization logo]

[Organization name]

**SECURITY PROCEDURES FOR IT DEPARTMENT**

|  |  |
| --- | --- |
| 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](#_Toc114520057)

[2. Reference documents 4](#_Toc114520058)

[3. Operating Procedures for Information and Communication Technology 4](#_Toc114520059)

[3.1. Change management 4](#_Toc114520060)

[3.2. Configuration management 5](#_Toc114520061)

[3.3. Capacity management 5](#_Toc114520062)

[3.4. Antivirus protection 5](#_Toc114520063)

[3.5. Backup 5](#_Toc114520064)

[3.5.1. Backup procedure 5](#_Toc114520065)

[3.5.2. Testing backup copies 5](#_Toc114520066)

[3.6. Network security management 5](#_Toc114520067)

[3.7. Network services 6](#_Toc114520068)

[3.8. Data deletion 6](#_Toc114520069)

[3.9. Disposal and destruction of equipment and media 6](#_Toc114520070)

[3.9.1. Equipment 7](#_Toc114520071)

[3.9.2. Mobile storage media 7](#_Toc114520072)

[3.9.3. Paper media 7](#_Toc114520073)

[3.9.4. Erasure and destruction records; commission for the destruction of data 7](#_Toc114520074)

[3.10. Information transfer 7](#_Toc114520075)

[3.10.1. Electronic communication channels 7](#_Toc114520076)

[3.10.2. Relations with external parties 7](#_Toc114520077)

[3.11. Handling the source code 8](#_Toc114520078)

[3.12. Use of utility programs 8](#_Toc114520079)

[3.13. System monitoring 8](#_Toc114520080)

[3.14. External threat monitoring 9](#_Toc114520081)

[4. Managing records kept on the basis of this document 9](#_Toc114520082)

[5. Validity and document management 10](#_Toc114520083)

# Purpose, scope and users

The purpose of this document is to ensure correct and secure functioning of information and communication technology.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all the information and communication technology, as well as to related documentation within the scope, and to all personal data processing activities.

Users of this document are employees of [organizational unit for information and communication technology].

# Reference documents

* ISO/IEC 27001 standard, clauses A.5.7, A.5.14, A.5.37, A.7.10, A.7.14, A.8.4, A.8.6, A.8.7, A.8.8, A.8.9, A.8.10, A.8.12, A.8.13, A.8.15, A.8.16, A.8.17, A.8.18, A.8.20, A.8.21, A.8.22, A.8.23, A.8.31, and A.8.32
* EU GDPR Article 32
* Information Security Policy
* [Disaster Recovery Plan]
* [Mobile Device, Teleworking and Work from Home Policy]
* [Information Classification Policy]
* [Inventory of Assets]
* [Supplier Security Policy]
* [Secure Development Policy]
* [Access Control Policy]

# Operating Procedures for Information and Communication Technology

## Change management

Each change to operational or production systems must be made in the following way:

1. change may be proposed by [specify job functions]
2. change must be authorized by [job title], who must assess its justification for business and potential negative security impacts
3. changes must be implemented by [job title]
4. …

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

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