\*\* 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 3](#_Toc496551051)

[2. Reference documents 3](#_Toc496551052)

[3. Security Procedures 3](#_Toc496551053)

[3.1. Change management 3](#_Toc496551054)

[3.2. Backup 3](#_Toc496551055)

[3.2.1. Backup procedure 3](#_Toc496551056)

[3.2.2. Testing backup copies 4](#_Toc496551057)

[3.3. Network security management 4](#_Toc496551058)

[3.4. Network services 4](#_Toc496551059)

[3.5. System monitoring 4](#_Toc496551060)

[4. Managing records kept on the basis of this document 5](#_Toc496551061)

[5. Validity and document management 5](#_Toc496551062)

# Purpose, scope and users

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

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

# Reference documents

* ISO/IEC 27001 standard
* IT Security Policy
* [Mobile Device and Teleworking Policy]
* [Information Classification Policy]

# Security Procedures

## 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. [job title] is responsible for checking that the change has been implemented in accordance with the requirement
5. [job title] is responsible for testing and verifying the system's stability – the system must not be put into production before thorough testing has been conducted
6. implementation of changes must be reported to the following persons: [list all necessary job titles]

Change records are kept [provide the name of the form, or describe a different method for recording changes].

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

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