[organization logo]

[organization name]

**CLEAR DESK AND CLEAR SCREEN POLICY**

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

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415650909)

[2. Reference documents 3](#_Toc415650910)

[3. Clear desk and clear screen policy 3](#_Toc415650911)

[3.1. Workplace protection 3](#_Toc415650912)

[3.1.1. Clear desk policy 3](#_Toc415650913)

[3.1.2. Clear screen policy 3](#_Toc415650914)

[3.2. Protection of shared facilities and equipment 3](#_Toc415650915)

[4. Validity and document management 4](#_Toc415650916)

# Purpose, scope and users

The purpose of this document is to define rules to prevent unauthorized access to information in workplaces, as well as to shared facilities and equipment.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all workplaces, facilities and equipment located within the ISMS scope.

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

# Reference documents

* ISO/IEC 27001 standard, clauses A.11.2.8 and A.11.2.9
* Information Security Policy
* [Information Classification Policy]

# Clear desk and clear screen policy

All information classified as "Internal use," "Restricted" and "Confidential" as specified in the [Information Classification Policy] are regarded as sensitive in this Clear Desk and Clear Screen Policy.

## Workplace protection

### Clear desk policy

If the authorized person is not at his/her workplace, all paper documents, as well as data storage media labeled as sensitive, must be removed from the desk or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorized access.

Such documents and media must be stored in a secure manner in accordance with the [Information Classification Policy].

### Clear screen policy

If the authorized person is not at his/her workplace, all sensitive information must be removed from the screen, and access must be denied to all systems for which the person has authorization.

In the case of short absence (up to 30 minutes), the clear screen policy is implemented by logging out of all systems or locking the screen with a password. If the person is absent for a longer period of time (over 30 minutes), the clear screen policy is implemented by logging out of all systems and turning off the workstation.

## Protection of shared facilities and equipment

Documents containing sensitive information must immediately be removed from printers, fax and copy machines.

Facilities for dispatch and reception of mail [specify facilities and their location] are protected by [specify the manner of protection when the authorized person is absent – e.g. locking the facility, etc.].

Shared fax machines [specify machines and their location] are protected by [specify the manner of protection when the authorized person is absent – e.g. locking the facility, etc.].

Unauthorized use of printers, photocopiers, scanners and other shared equipment for copying [specify machines and their location] is prevented by [specify how – e.g. by locking the facility, use of PIN numbers, access cards, etc.].

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* number of incidents related to unauthorized access to information on desks, printers, photocopiers, fax machines, work stations, etc.

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]