[organization logo]

[organization name]

**ACCESS CONTROL 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](#_Toc415650666)

[2. Reference documents 3](#_Toc415650667)

[3. Access control 3](#_Toc415650668)

[3.1. Introduction 3](#_Toc415650669)

[3.2. User Profile A 3](#_Toc415650670)

[3.3. User Profile B 4](#_Toc415650671)

[3.4. Privilege management 4](#_Toc415650672)

[3.5. Regular review of access rights 5](#_Toc415650673)

[3.6. Change of status or termination of contract 5](#_Toc415650674)

[3.7. Technical implementation 5](#_Toc415650675)

[3.8. User password management 6](#_Toc415650676)

[4. Managing records kept on the basis of this document 7](#_Toc415650677)

[5. Validity and document management 7](#_Toc415650678)

# Purpose, scope and users

The purpose of this document is to define rules for access to various systems, equipment, facilities and information, based on business and security requirements for access.

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

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

# Reference documents

* ISO/IEC 27001 standard, clauses A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3
* Information Security Policy
* Statement of Applicability
* [Information Classification Policy]
* [Statement of Acceptance of the ISMS Documents]
* [List of Legal, Regulatory, Contractual and Other Requirements]

# Access control

## Introduction

The basic principle is that access to all systems, networks, services and information is forbidden, unless expressly permitted to individual users or groups of users. There should be a user registration procedure for each system and service.

Access to all physical areas in the organization is allowed, except to areas for which privilege must be granted by the authorized person (item "Privilege management").

This Policy specifies rules for access to systems, services and facilities, while the [Information Classification Policy] defines rules for access to individual documents and records.

## User Profile A

User profile A has the following access rights:

|  |  |
| --- | --- |
| ***Name of system / network / service*** | ***User rights*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

The following job titles have access rights according to User Profile A:

* [job title 1]
* [job title 2]

## User Profile B

User Profile B has the following access rights:

|  |  |
| --- | --- |
| ***Name of system / network / service*** | ***User rights*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

The following job titles have access rights according to User Profile B:

* [job title 1]
* [job title 2]

## Privilege management

Privileges in respect to the abovementioned user profiles (granting or removing access rights) are allocated in the following way:

|  |  |  |
| --- | --- | --- |
| ***Name of system / network / service / physical area*** | ***Who is authorized for granting or removing access rights*** | ***Form of authorization process*** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

When allocating privileges the person responsible must take into account business and security requirements for access (defined in risk assessment), as well as the classification of information which is accessed with such access rights, in accordance with the Information Classification Policy.

## Regular review of access rights

Owners of each system and owners of facilities for which special access rights are required must, at the following intervals, review whether the access rights granted are in line with business and security requirements:

|  |  |
| --- | --- |
| ***Name of system / network / service / physical area*** | ***Intervals for regular review*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Each review should be recorded [specify how records are kept].

## Change of status or termination of contract

Upon change of employment or termination of employment, [job title] must immediately inform the responsible persons who approved privileges for the employee in question.

Upon change of contractual relations with external parties who have access to systems, services and facilities, or upon expiration of the contract, contract owner must immediately inform the responsible persons who approved privileges for the external parties in question.

The access rights for all the persons who have changed their employment status or contractual relationship must immediately be removed or changed by responsible persons as defined in the next section.

## Technical implementation

The technical implementation of the allocation or removal of access rights is carried out by the following persons:

|  |  |
| --- | --- |
| ***Name of system / network / service / physical area*** | ***Person responsible for implementation*** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Persons listed in this table may not grant or remove access rights freely, but only based on user profiles defined in this Policy, and requests by persons authorized for allocation of privileges.

## User password management

When allocating and using user passwords, the following rules must be complied with:

* by signing the Statement of Acceptance of ISMS Documents, users also accept the obligation to keep passwords confidential, as prescribed by this document
* each user may use only his/her own uniquely allocated username
* each user must have the option to choose his/her own password, where applicable
* the temporary password used for first system log-on must be unique and strong, as described above
* temporary passwords must be communicated to the user in a secure manner, and user's identity must be checked prior
* the password management system must require the user to change the temporary password at first log-on to the system
* the password management system must require the user to select strong passwords
* the password management system must require the users to change their passwords every three months
* if the user requests a new password, the password management system must determine the identity of the user by [specify how]
* the user has to confirm the receipt of the password by [specify how]
* the password must not be visible on the screen during log-on
* if a user enters an incorrect password three consecutive times, the system must block the user account in question
* passwords created by the software or hardware manufacturer must be changed during initial installation
* files containing passwords must be stored separately from the application's system data

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [Record of privilege allocation (in electronic form – e-mail message)] | [intranet folder] | [job title responsible for technical implementation] | Records cannot be edited; only [job title] has the right to store such records | Records are stored for a period of 3 years |
| [Records of regular review of access rights] | [[job title]'s computer / [job title]'s cabinet] | [job title] | Only [job title] has access rights to such records | Records are stored for a period of 3 years |

Only [job title] can grant other employees access to the any of the abovementioned documents.

# 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 every six months.

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

* number of incidents related to unauthorized access to information
* delayed change of access rights in case of change or termination of employment/contract
* number of systems not included in this document
* level of confusion regarding responsibilities for the implementation of this document

[job title]

[name]

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

[signature]