[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 | Abdullah | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc454539926)

[2. Reference documents 3](#_Toc454539927)

[3. Access control 3](#_Toc454539928)

[3.1. Introduction 3](#_Toc454539929)

[3.2. Access control rules for [organization name] 3](#_Toc454539930)

[3.2.1. User Profile A 3](#_Toc454539931)

[3.2.2. User Profile B 4](#_Toc454539932)

[3.3. Access control rules for cloud services 4](#_Toc454539933)

[3.3.1. Cloud Service’s Profile A 4](#_Toc454539934)

[3.3.2. Cloud Service’s Profile B 5](#_Toc454539935)

[3.4. [organization name]’s privilege management 6](#_Toc454539936)

[3.5. Cloud services privilege management 6](#_Toc454539937)

[3.6. Regular review of [organization name]’s access rights 7](#_Toc454539938)

[3.7. Regular review of cloud services access rights 7](#_Toc454539939)

[3.8. Change of status or termination of contract 8](#_Toc454539940)

[3.8.1. For [Organization name]’s employees and subcontractors 8](#_Toc454539941)

[3.8.2. For Customer’s users with cloud environment administrative privileges 8](#_Toc454539942)

[3.9. Technical implementation 8](#_Toc454539943)

[3.9.1. General information 8](#_Toc454539944)

[3.9.2. Technical implementation related to [organization name]’s assets 8](#_Toc454539945)

[3.9.3. Technical implementation related to customers’ cloud services environments 9](#_Toc454539946)

[3.10. User identification, authentication and authorization 10](#_Toc454539947)

[3.11. User password management 10](#_Toc454539948)

[4. Managing records kept on the basis of this document 11](#_Toc454539949)

[5. Validity and document management 11](#_Toc454539950)

# 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
* ISO/IEC 27017 standard, clauses 6.1.1, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.1, 9.4.2, and 9.4.3
* ISO/IEC 27018 standard, clauses 6.1.1, 9.1, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.2, A.9.2, A.10.8, A.10.9, and A.10.10
* 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 [organization name]’s individual documents and records, and the Customer’s Cloud Service Agreement defines rules for access to individual documents and records in the Customer’s Cloud Service environment.

## Access control rules for [organization name]

### 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]

## Access control rules for cloud services

According to the cloud service’s provisioning models adopted in the service agreements between the customers and [organization name], the following set of access rights must be applied to ensure the proper balance of operational, management, and security responsibilities in the cloud environment.

### Cloud Service’s Profile A

Cloud Service’s Profile A has the following access rights:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Name of service / platform / infrastructure provided*** | ***Customer’s rights*** | | ***[Organization name]’s rights*** | |
| ***Regular*** | ***Administrative*** | ***Regular*** | ***Administrative*** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

The following job titles and cloud service customers’ users have access rights according to Cloud Service’s Profile A:

|  |  |  |
| --- | --- | --- |
| ***Customers*** | Regular | [Customer’s lists of authorized users] |
| Administrative | [Customer’s lists of authorized users] |
| ***[Organization name]*** | Regular | * [job title 1] * [job title 2] |
| Administrative | * [job title 1] * [job title 2] |

### Cloud Service’s Profile B

Cloud Service’s Profile B has the following access rights:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name of service / platform / infrastructure provided** | **Customer’s rights** | | **[Organization name]’s rights** | |
| ***Regular*** | ***Administrative*** | ***Regular*** | ***Administrative*** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

The following job titles and cloud service customers’ users have access rights according to Cloud Service’s Profile B:

|  |  |  |
| --- | --- | --- |
| ***Customers*** | Regular | [Customer’s lists of authorized users] |
| Administrative | [Customer’s lists of authorized users] |
| ***[Organization name]*** | Regular | * [job title 1] * [job title 2] |
| Administrative | * [job title 1] * [job title 2] |

## [organization name]’s privilege management

Privileges in respect to the abovementioned user profiles for [organization name] (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.

## Cloud services privilege management

Privileges in respect to the cloud service’s profiles mentioned in section 3.3 (granting or removing access rights) are allocated by [organization name] in the following way:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Name of service / platform / infrastructure provided*** | ***Who is authorized for granting or removing access rights*** | | ***Form of authorization process*** | |
| ***For customer’s rights*** | ***For [organization name]’s rights*** | ***For customer’s rights*** | ***For [organization name]’s rights*** |
|  | [job title] | [job title] | [job title] | [job title] |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

When allocating privileges in a cloud computing environment, [organization name]’s person responsible must take into account the customer’s business and security requirements for access (defined in the Cloud Service Agreement), as well as the [organization name]’s own business and security requirements, in accordance with the Information Security Policy.

## Regular review of [organization name]’s 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].

## Regular review of cloud services access rights

[Organization name]’s personnel defined in section 3.4. as responsible for granting administrative access rights to its public cloud services, platforms, and infrastructure, including the facilities hosting [organization name]’s public cloud infrastructure must, at the following intervals, review whether the access rights granted are in line with those defined in section 3.3 of this policy:

|  |  |  |
| --- | --- | --- |
| ***Name of service / platform / infrastructure provided*** | ***Intervals for regular review*** | ***Responsible*** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

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

## Change of status or termination of contract

### For [Organization name]’s employees and subcontractors

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 public cloud service customers affected and 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.

### For Customer’s users with cloud environment administrative privileges

Upon Customer notification through [describe the forms of communication to be used] about changes of employment, or termination of employment, of users with administrative privileges on the cloud environment, [job title] must immediately inform the responsible persons who approved privileges (see section 3.3) for each cloud service’s profile used by that customer, so they can perform the proper adjustments in the access rights.

Upon change to the Customer Cloud Service Agreement, or upon expiration of the agreement, [job title] must immediately inform the responsible persons who approved privileges (see section 3.3) for each cloud service’s profile used by that customer, so they can perform the proper adjustments in the access rights.

## Technical implementation

### General information

Persons listed in the following tables 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.

### Technical implementation related to [organization name]’s assets

The technical implementation of the allocation, or removal, of access rights to [organization name]’s assets is carried out by the following persons:

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

### Technical implementation related to customers’ cloud services environments

The technical implementation of the allocation, or removal, of access rights to the customer’s cloud service environment is carried out by the following persons:

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

Where customer’s user management will be performed by the customer’s own staff, the technical implementation of the allocation, or removal, of access rights to user management functionalities is carried out by the following persons in [organization name]:

|  |  |  |
| --- | --- | --- |
| ***Name of system / network / service / physical area*** | ***User management functionality to be accessed by customer*** | ***Person responsible for implementation*** |
|  |  |  |
|  |  |  |
|  |  |  |

For the access of the customer’s staff to cloud service control functionalities, the person responsible for implementation must provide authentication techniques according to the identified risk levels.

For the user management functionalities, the person responsible for implementation must provide the [document name] by [describe which means are used to make the document available] to the cloud service customers’ staff, so they can know how to inform and handle access control incidents.

## User identification, authentication and authorization

When granting access to systems and services, the following rules must be complied with:

* users must have a distinct user ID
* cloud service customer’s administrative staff must make use of [describe the authentication method to be used by them] to have access to administrative capabilities of the cloud service. [job title] is responsible for the implementation of the [describe the authentication method to be used by them].

## User password management

When allocating and using [organization name]’s own 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

The allocation and use of cloud service customers’ user passwords must be in compliance with at least these minimal requirements:

* [List here all password allocation and usage rules that all cloud service customers must follow]

Stricter rules defined by cloud service customers are described in [specify the documents]. [job title] must inform cloud service customers’ users about the rules for password management.

# 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 5 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 5 years |
| [Records of password management rules defined by customers] | [[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 5 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
* number of incidents related to unauthorized access to Personally Identifiable Information (PII) in cloud services

Previous versions of this policy must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

[job title]

[name]

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

[signature]