Insert Company Logo

Access Control Policy

Document Control

Document Number:	ISMS-POL-003
Version Number:	1
Review Date:	Insert date
Next Review:	Insert date
Authorised by:	Insert Job Title and Department

Version History

Version	Date	Author	Brief Description of Changes
First version	Insert Effective Date	Insert author	Describe changes that were made to document in order to qualify changing the version.

1. 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 Insert Company Name.

2. Reference documents

- ISO 27001:2013 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
- Password Policy
- Statement of Applicability
- List of Legal, Regulatory, Contractual and Other Requirements

3. Access control

3.1 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.

3.2 Privilege management

Privileges in respect to the below mentioned areas (granting or removing access rights) are allocated in the following way:

Complete the table below:

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.

3.3 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:

Complete the table below:

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

3.4 Change of status or termination of contract

Upon change of employment or termination of employment, Security Officers 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 privilege management section above.

4. Managing records kept on the basis of this document

Complete the table below:

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Record of privilege allocation (in electronic form – e-mail message)				
Records of regular review of access rights				

Only Security Officers can grant other employees' access to the any of the above-mentioned documents.

5. Validity and document management

This document is valid as of Insert Date.

The owner of this document is Insert position of authority 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