[Organization logo]

[Organization name]

ACCESS CONTROL POLICY

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

Commented [270011]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [270012]: To learn more about this topic, read this article:

How to handle access control according to ISO 27001
https://advisera.com/27001academy/blog/2015/07/27/how-to-handle-access-control-according-to-iso-27001/

Commented [270013]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

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 [organization name].

Commented [270014]: Include the name of your organization.

2. Reference documents

- ISO/IEC 27001 standard, clauses A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, and A.8.5
- Information Security Policy
- Statement of Applicability
- [Information Classification Policy]
- [Statement of Acceptance of the ISMS Documents]
- [List of Legal, Regulatory, Contractual and Other Requirements]

Commented [27A5]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "05_General_Policies".

Commented [27A6]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "07_Applicability_of_Controls".

Commented [270017]: If you don't have this List, then in these bullets list all the legislation and contracts that contain requirements for access control.

3. Access control

3.1. Introduction

[illegible]

Access to all physical areas in the organization is allowed, except to areas for which privilege must be [illegible]

[illegible]

Commented [270018]: To be deleted if the Information Classification Policy is not documented.

3.2. User Profile A

Commented [270019]: Adapt to the organization's standard naming system.

User profile A has the following access rights:

[illegible]	[illegible]

Commented [2700110]: May be specified on the level of the [illegible]

Commented [2700111]: Specify whether they include rights [illegible]

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

[illegible]

- [job title 1]
- [job title 2]

Commented [2700112]: [illegible]

3.3. User Profile B

Commented [2700113]: Additional user profiles may be listed in the manner described in this item.

[illegible]

[illegible]	[illegible]

Commented [2700114]: May be specified on the level of the entire system or for single modules.

Commented [2700115]: [illegible]

[illegible]

- [job title 1]
- [job title 2]

3.4. Privilege management

Commented [2700116]: Delete this item if control A.8.2 is marked as inapplicable in the Statement of Applicability.

[illegible] allocated in the following way:

Commented [2700117]: [illegible]

Commented [2700118]: By e-mail, written decision, orally, through the system, etc. Preferably, there should be a record in which can be traced who has given the authorization to whom.

[illegible]	[illegible]	[illegible]

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

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.

3.5. Regular review of access rights

Commented [2700119]: Delete this item if control A.5.18 is marked as inapplicable in the Statement of Applicability.

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:

Commented [2700120]: Adapt, if necessary.

[illegible]	[illegible]

Commented [2700121]: [illegible]

[illegible]

Commented [2700122]: A form, formal report, notes written by hand, etc. may be used.

3.6. Change of status or termination of contract

Commented [2700123]: Delete this item if control A.5.18 is marked as inapplicable in the Statement of Applicability.

Upon change of employment or termination of employment, [job title] must immediately inform the [illegible]

[illegible]

[illegible] section.

3.7. Technical implementation

[illegible] following persons:

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

[illegible]	[illegible]

Persons listed in this table may not grant or remove access rights freely, but only based on user [illegible]

3.8. Secure authentication

Commented [2700124]: Delete this section if control A.8.5 is found inapplicable in the Statement of Applicability.

[illegible] services.

3.9. User password management

Commented [2700125]: Delete this item if the Password Policy constitutes a separate document.

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

Commented [2700126]: Adapt these rules according to assessed risks.

Commented [2700127]: Separate rules may be set for administrator and user passwords.

- [illegible]
- [illegible]
- [illegible]
- the temporary password used for first system log-on must be unique and strong, as described above
- [illegible]
- [illegible]
- [illegible]
- the password management system must require the users to change their passwords every three months
- [illegible]
- [illegible]
- [illegible]
- the password must not be visible on the screen during log-on

Commented [2700128]: More details may be provided here.

Commented [27A29]: This is only recommendation; you can change the frequency according to your organization's practices.

Commented [2700130]: E.g. by sending an e-mail instructing the user to perform an action, etc.

Commented [2700131]: E.g., three previous passwords.

Commented [2700132]: E.g. by logging on to the system within a time interval, etc.

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

- [illegible]
- [illegible]
- [illegible]

4. 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

Commented [2700133]: Alter these records to match what you already have in your company. If you do not have similar records, you can create new ones in the format that suits you best.

Commented [2700134]: Adjust as appropriate.

Commented [2700135]: Adjust as appropriate.

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

5. 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.

Commented [2700136]: This is only a recommendation; adjust frequency as appropriate.

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

- [illegible]
- [illegible]
- [illegible]
- [illegible]

[job title]
[name]

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

____

[signature]

Commented [2700137]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.