[Organization logo]

[Organization name]

PROCEDURES FOR WORKING IN SECURE AREAS

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 these articles:

- Physical security in ISO 27001: How to protect the secure areas https://advisera.com/27001academy/blog/2015/03/23/physical-security-in-iso-27001-how-to-protect-the-secure-areas/

- The most common physical and network controls when implementing ISO 27001 in a data center https://advisera.com/27001academy/blog/2019/02/26/the-most-common-physical-and-network-controls-when-implementing-iso-27001-in-a-data-center/

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.

Change history

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

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. RULES FOR SECURE AREAS 3

3.1. LIST OF SECURE AREAS 3
3.2. RIGHT OF ACCESS TO SECURE AREAS 3
3.3. ENTRY CONTROLS 3
3.4. CONTINUOUS MONITORING 3
3.5. ACCESS OF VISITORS 3
3.6. PROHIBITED ACTIVITIES 4
3.7. PERIODIC CHECKS 4

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. VALIDITY AND DOCUMENT MANAGEMENT 5

1. Purpose, scope and users

The purpose of this document is to define basic rules of behavior in the secure areas.

This document is applied to all secure areas in the Information Security Management System (ISMS).

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.7.4 and A.7.6
- Access Control Policy
- Inventory of Assets

Commented [27A5]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "09_Annex_A_Security_Controls".

Commented [27A6]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "09_Annex_A_Security_Controls".

3. Rules for secure areas

3.1. List of secure areas

This procedure is applicable to the following secure areas:

-

Commented [270017]: List all the facilities here – e.g., server room, archives, storage for special equipment, CEO's room, etc.

3.2. Right of access to secure areas

3.3. Entry controls

-

Commented [270018]: List all the controls – e.g., swipe card readers, CCTV cameras, etc.

3.4. Continuous monitoring

Commented [27A9]: Delete this paragraph if control A.7.4 is found inapplicable in your Statement of Applicability.

Commented [2700110]: E.g., Security officer, CISO, security guard, or similar.

access or suspicious behavior, through the following means:

Commented [2700111]: List all means used for monitoring secure areas. E.g.: guards, alarms, video monitoring, etc.

-

3.5. Access of visitors

Commented [2700112]: Include the name of your organization.

according to the Access Control Policy.

[redacted]
area.

[redacted]
by [job title].

Commented [2700113]: Write here the name of the application used for logging the access to secure areas.

If there is no such application, write the document name where this information is stored.

3.6. Prohibited activities

In secure areas it is not allowed to:

- [redacted]
- [redacted]
- [redacted] specifically authorized to do so;
- [redacted]
- [redacted]
- [redacted]
- use any kind of heating devices;
- [redacted]

3.7. Periodic checks

[redacted]

Commented [2700114]: E.g., more than six months

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
[Swipe card reader logs]	[name of the system]	[job title]	Only [job title] has access to the system	3 years
[Recordings from CCTV cameras]	[name of the system]	[job title]	Only [job title] has access to the system	3 years
[Name of visitor logs]	[job title]'s computer / [name of the application]	[job title]	Only [job title] has access to logs	3 years

Commented [2700115]: 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 [2700116]: Adapt this period according to your specific needs.

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 a year.

Commented [2700117]: This is only a recommendation; adjust frequency as appropriate.

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

- [illegible]

[job title]
[name]

[signature]

Commented [2700118]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.