\*\* FREE PREVIEW VERSION \*\*

[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** |
| 01/10/2013 | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc368214968)

[2. Reference documents 3](#_Toc368214969)

[3. Access control 3](#_Toc368214970)

[3.1. Introduction 3](#_Toc368214971)

[3.2. User Profile A 3](#_Toc368214972)

[3.3. User Profile B 4](#_Toc368214973)

[3.4. Privilege management 4](#_Toc368214974)

[3.5. Regular review of access rights 5](#_Toc368214976)

[3.6. Change of status or termination of contract 5](#_Toc368214977)

[3.7. Technical implementation 5](#_Toc368214978)

[3.8. User password management 6](#_Toc368214979)

[4. Managing records kept on the basis of this document 7](#_Toc368214980)

[5. Validity and document management 7](#_Toc368214981)

# 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 …

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: <http://www.iso27001standard.com/en/documentation/Access-Control-Policy>