



ISO 27001 Documentation kit – Information Security Management System

Level 1 – Context, Manual, Objectives, Plans & Policies	
Context	
1.	Information Security Management System Context, Requirements and Scope
Manual	
1.	ISMS Manual
Objectives	
1.	ISMS Roles, Responsibilities and Authorities
2.	Information Security Objectives and Plan
Plans	
1.	Risk Treatment Plan
2.	Internal Audit Plan
3.	Incident Response Plan Ransomware
4.	Incident Response Plan Denial of Service
5.	Incident Response Plan Data Breach
6.	ICT Continuity Plan
7.	ICT Continuity Test Plan
8.	Information Systems Audit Plan
9.	Capacity Plan
Policies	
1.	Information Security Policy
2.	Social Media Policy
3.	HR Security Policy
4.	Information Security Whistleblowing Policy
5.	Threat Intelligence Policy
6.	Asset Management Policy
7.	Acceptable Use Policy
8.	Internet Access Policy
9.	Electronic Messaging Policy
10.	Online Collaboration Policy
11.	Access Control Policy
12.	Information Security Policy for Supplier Relationships
13.	Cloud Services Policy
14.	IP and Copyright Compliance Policy

15.	Records Retention and Protection Policy
16.	Privacy and Personal Data Protection Policy
17.	Remote Working Policy
18.	Physical Security Policy
19.	CCTV Policy
20.	Clear Desk and Clear Screen Policy
21.	Mobile Device Policy
22.	
23.	Dynamic Access Control Policy
24.	Anti-Malware Policy
25.	Technical Vulnerability Management Policy
26.	Configuration Management Policy
27.	Information Deletion Policy
28.	Data Masking Policy
29.	Data Leakage Prevention Policy
30.	Backup Policy
31.	Availability Management Policy
32.	Logging and Monitoring Policy
33.	Monitoring Policy
34.	Software Policy
35.	Network Security Policy
36.	Web Filtering Policy
37.	Cryptographic Policy
38.	Secure Development Policy
39.	Secure Coding Policy
Level 2 - Procedures & Processes	
Procedures	
1.	Information Security Competence Development Procedure
2.	Control of Documented Information Procedure
3.	Internal Audit Procedure
4.	Management Review Procedure
5.	Management of Nonconformity Procedure
6.	Asset Handling Procedure
7.	Managing Lost or Stolen Devices Procedure

8.	Information Classification Procedure
9.	Information Labelling Procedure
10.	Information Transfer Procedure
11.	Supplier Due Diligence Assessment Procedure
12.	Information Security Event Assessment Procedure
13.	Information Security Incident Response Procedure
14.	ICT Continuity Incident Response Procedure
15.	Legal, Regulatory and Contractual Requirements Procedure
16.	Personal Data Breach Notification Procedure
17.	Employee Screening Procedure
18.	Information Security Event Reporting Procedure
19.	Data Centre Access Procedure
20.	Working in Secure Areas Procedure
21.	Taking Assets Offsite Procedure
22.	Management of Removable Media Procedure
23.	Physical Media Transfer Procedure
24.	Disposal of Media Procedure
25.	Technical Vulnerability Assessment Procedure
Processes	
1.	Risk Assessment and Treatment Process
2.	ISMS Change Process
3.	Monitoring, Measurement, Analysis and Evaluation Process
4.	Threat Intelligence Process
5.	User Access Management Process
6.	Supplier Information Security Evaluation Process
7.	Cloud Services Process
8.	Business Impact Analysis Process
9.	Employee Disciplinary Process
10.	Configuration Management Process
11.	Data Masking Process
12.	Change Management Process
Level 3 – SOPs	
1.	Group Internal and E-mail Usage
2.	Software Configuration Management

3.	Handling of Virus Attacks
4.	Personal Security
5.	Warehouse Security
Level 4 – Formats, Templates & Presentations	
Formats	
1.	ISMS Assessment Evidence
2.	ISO 27001 Project Progress Report
3.	Meeting Minutes Template
4.	Asset-Based Risk Assessment and Treatment Tool
5.	Statement of Applicability
6.	Scenario-Based Risk Assessment and Treatment Tool
7.	Opportunity Assessment Tool
8.	Competence Development Questionnaire
9.	Internal Audit Programme
10.	Internal Audit Action Plan
11.	Management Review Meeting Agenda
12.	Nonconformity and Corrective Action Log
13.	ISMS Regular Activity Schedule
14.	Segregation of Duties Worksheet
15.	New Starter Checklist
16.	Supplier Due Diligence Assessment
17.	Supplier Evaluation Questionnaire
18.	Cloud Services Questionnaire
19.	Incident Lessons Learned Report
20.	Business Impact Analysis Tool
21.	Personal Data Breach Notification Form
22.	Breach Notification Letter to Data Subjects
23.	Employee Screening Checklist
24.	Employee Termination and Change of Employment Checklist
25.	Leavers Letter
26.	Equipment Maintenance Schedule
27.	Requirements Specification
28.	Acceptance Testing Checklist
Templates	

1.	Annex A Control Attributes
2.	Executive Support Letter
3.	Risk Assessment Report
4.	ISMS Change Log
5.	Information Security Communication Programme
6.	ISMS Documentation Log
7.	Information Security Competence Development Report
8.	Internal Audit Report
9.	Segregation of Duties Guidelines
10.	Authorities Contacts
11.	Specialist Interest Group Contacts
12.	Threat Intelligence Report
13.	Information Security Guidelines for Project Management
14.	Information Asset Inventory
15.	Information Transfer Agreement
16.	Supplier Information Security Agreement
17.	Supplier Evaluation Covering Letter
18.	Cloud Service Specifications
19.	Business Impact Analysis Report
20.	ICT Continuity Exercising and Testing Schedule
21.	ICT Continuity Test Report
22.	Legal, Regulatory and Contractual Requirements
23.	Information Security Summary Card
24.	Guidelines for Inclusion in Employment Contracts
25.	Schedule of Confidentiality Agreements
26.	Non-Disclosure Agreement
27.	Physical Security Design Standards
28.	Configuration Standard Template
29.	Privileged Utility Program Register
30.	Network Services Agreement
31.	Principles for Engineering Secure Systems
32.	Secure Development Environment Guidelines
Presentations	
1.	Introduction to ISO 27001 Presentation

2.	ISO 27001 Awareness Training Presentation
Guidelines for Implementation Methodology	
1.	Guidelines for ISO 27001 Implementation
2.	ISO 27001 All-In-One Toolkit User Guide
3.	ISO/IEC 27001 Toolkit Index
4.	ISMS Project Initiation Document
5.	ISO/IEC 27001 Project Plan
6.	ISO 27001 Certification Readiness Checklist
7.	ISO 27001 Gap Analysis Checklist
Audit Checklist	
1.	ISO 27001 Internal Audit Checklist

Contents

1	Introduction.....	5
2	Asset Handling Procedure	6
2.1	Level 0: Public (or Unclassified).....	6
2.1.1	Secure Processing	6
2.1.2	Storage.....	6
2.1.3	Transmission	6
2.1.4	Declassification.....	6
2.1.5	Destruction	7
2.1.6	Chain of Custody.....	7
2.1.7	Logging of Security-Related Events.....	7
2.2	Level 1: Protected.....	7
2.2.1	Secure Processing	7
2.2.2	Storage	7
2.2.3	Transmission	8
2.2.4	Declassification.....	8
2.2.5	Destruction	8
2.2.6	Chain of Custody.....	8
2.2.7	Logging of Security-Related Events.....	8
2.3	Level 2: Restricted	8
2.3.1	Secure Processing	9
2.3.2	Storage.....	9
2.3.3	Transmission	9
2.3.4	Declassification.....	9
2.3.5	Destruction	9
2.3.6	Chain of Custody.....	9
2.3.7	Logging of Security-Related Events.....	10
2.4	Level 3: Confidential	10
2.4.1	Secure Processing	10
2.4.2	Storage.....	10
2.4.3	Transmission	10
2.4.4	Declassification.....	11
2.4.5	Destruction	11
2.4.6	Chain of Custody.....	11
2.4.7	Logging of Security-Related Events.....	11
3	Conclusion.....	12

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Introduction

The goal of this document is to lay forth the exact controls that must be utilised when dealing with classified information. Please check the Information Classification Procedure for further information on the criteria for classifying information assets.

There should be no disclosure of classified information to any person or organization via the following insecure methods, but not limited to:

- Paper based methods
- Email
- Telephone
- Fax
- Verbally

2 Asset Handling Procedure

There must be handling controls in place for every security classification level to ensure that the information assets are always appropriately protected.

2.1 Level 0: Public (or Unclassified)

Information in this classification is in the public domain or is freely available from an organization.

2.1.1 Secure Processing

enerally, there is no need to place specific controls on how such information is processed, though items like stationery and their electronic equivalents should not be freely available.

2.1.2 Storage

Information of Level 0 is often kept in open areas which are accessible to the public. There should be controls on large quantities of such information such as leaflets, where theft or misuse is still possible.

2.1.3 Transmission

Information that is considered Level 0 may be sent in the clear over unencrypted connections or distributed in hard copy without restriction.

Contents

1 Introduction..... 4

2 Data Centre Access Procedure5

2.1 Data Centre Access Principles 5

2.2 Requesting Access to the Data Centre 5

2.3 Visitor Guidelines..... 6

2.4 Equipment Deliveries 6

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Introduction

Specifically, this document provides an overview of how customers, third parties, visitors, and others should request access and behave within the Organization Name data centre.

Organization Name and its customers require a secure data centre to prevent a loss of confidentiality, integrity, or availability of their physical and information assets. However, such areas only remain secure if the people accessing them follow the protocol designed for their use. The document provides guidance to ensure the security of an area while still allowing business activities to proceed without disruption.

2 Data Centre Access Procedure

2.1 Data Centre Access Principles

There are several principles that govern access to data centers at Organization Name:

- The data center should be accessible only to authorized staff of Organization Name;
- There should be specific authorizations for all access;
- Visitors to secure areas must be supervised at all times by Organization Name employees;
- Visitor registration and dispersion are required at the data center;
- Visitor identification badges must always be worn by all visitors.

2.2 Requesting Access to the Data Centre

If you would like access to a Organization Name data centre, please contact access@domain.com or call +x (xxx) xxx-xxxx.

2.3 Visitor Guidelines

There may be certain rules that customers, third parties, and other visitors to Organization Name data centers have to follow:

- It is not allowed to bring food or drinks into the data center;
- Smoking is not permitted anywhere on site;
- Every health and safety policy of Organization Name must be followed at all times;
- Access can only be granted to the racks and servers listed in the access request;

Contents

1	Introduction.....	4
2	Business Requirements of Access Control	5
3	User Access Management.....	6
3.1	User Registration and Deregistration.....	6
3.2	User Access Provisioning	7
3.3	Removal or Adjustment of Access Rights.....	7
3.4	Management of Privileged Access Rights	7
3.5	User Authentication for External Connections	8
3.6	Supplier Remote Access to the Organization Network.....	8
3.7	Review of User Access Rights.....	8
3.8	User Authentication and Password Policy.....	9
4	User Responsibilities	11
5	System and Application Access Control	12

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Introduction

Controlling access to our information assets is a critical component of an information security defence in depth strategy. A comprehensive set of physical and logical controls is required for us to effectively protect the confidential, accurate, and reliable nature of classified information.

These specifications may be influenced by factors such as:

- The level of security assigned to information stored and processed by a specific system or service;
- Various laws and regulations may apply, e.g., the Data Protection Act, Sarbanes Oxley;
- Organizations and systems operate within a legal framework;
- Third-party contractual obligations;
- There are threats, vulnerabilities and risks involved;

2 Business Requirements of Access Control

It is necessary to develop the business requirements for access control as part of gathering requirements for new or significantly altered systems and services. They must then be incorporated into the design.

These are:

- **Defence in Depth:** Rather than relying on a single control, security must be based on the combined action of several controls.
- **Least Privilege:** It would be best to assume that access is not needed rather than assume that it is.
- **Need to Know:** It is only necessary to have access to the information needed to perform a role, and nothing more.
- **Need to Use:** Depending on their role, users will be able to access only the physical and logical resources that they require.

3 User Access Management

In order to ensure authorized user access and prevent unauthorized access, formal user access control procedures must be documented, implemented, and maintained. Ideally, they should cover the entire user access life cycle, from the initial registration of new users to the final de- registration of users who no longer require access.

Contents

1 Purpose 4

2 Scope 4

3 Responsibility 4

4 Tasks Descriptions..... 4

 4.1 Configuration Identification 4

5 References 11

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Purpose

A project's lifecycle includes the planning, implementation, and evaluation stages regarding all software configurable items. This document provides guidelines for Software Configuration Management activities to ensure the integrity of all software configurable items throughout the lifecycle.

2 Scope

This procedure includes the following activities:

- Finding and classifying software configurable items;
- Manage changes and revisions to configurable items in a systematic manner;
- Keeping track of the status of all configurable items and establishing control over them.

3 Responsibility

As part of the project execution and delivery process, the Software Head/Programmer is responsible for overall Configuration Management. It must be approved and audited any modification(s) made to the SCI (Software Configuration Item). It is their responsibility to ensure that this procedure is followed.

4 Tasks Descriptions

4.1 Configuration Identification

This procedure generally identifies configurable items in accordance with the information given in the items list below. Project managers are responsible for identifying and documenting any specific changes for any given project.

4.2 Configuration Control

Whenever changes are made, they are saved in the most recent folder, and the configuration is managed properly. If a customer requests proper version control after delivery, it is handled on a case-by-case basis by the director.

4.3 Change Request

- Problems – are fixes to CM controlled products (e.g., Discrepancy reports, corrective action reports).

INTERNAL AUDIT SCHEDULE					
Audit No:			Date:		
Auzdit Scope:					
Audit Criteria:					
Audit Objectives:					
Date	Time		Department / Function to be Audited	Auditee(s)	Auditor(s)
	From	To			
Prepared By:			Reviewed By:		Approved By:
Internal Auditor			Lead Auditor		Head of Information Security