<Organization Name>

**<Procedure Title>**

|  |  |
| --- | --- |
| **Standard** | ISO/IEC 27001:2022 |
| **Version** | <Version No> |
| **Effective Date** | <Date> |
| **Reviewed Date** | <Date> |
| **Next Review Date** | <Date> |
| **Policy Owner** | <Title><Name>/ <Department> |
| **Approved by** | <Title><Name> |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

**Table of Contents**

[Purpose 1](#_Toc179822274)

[Scope 1](#_Toc179822275)

[Related Policies 1](#_Toc179822276)

[Roles and Responsibilities 2](#_Toc179822277)

[Procedure Steps 3](#_Toc179822278)

[Key Performance Indicators (KPIs) 5](#_Toc179822279)

[Compliance and Review 5](#_Toc179822280)

# Purpose

The purpose of this procedure is to ensure that <Organization Name> complies with the requirements of the ISO 27001:2022 standard by providing a systematic approach to <procedure's objective, e.g., managing access controls, incident handling, etc.>. It aims to mitigate risks associated with information security and ensure the security, integrity, and availability of the organization’s information assets.

# Scope

This procedure applies to all employees, contractors, and third parties that interact with the information systems and data within <Organization Name>. The procedure is relevant to <specific systems, departments, or operations covered>.

# Related Policies

This procedure is linked to the following policies.

1. <Policy 1 Title, e.g., *Information Security Policy*>
2. <Policy 2 Title, e.g., *Data Protection Policy*>

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Policy Owner | Responsible for developing, maintaining, and updating this procedure. |
| IT Department | Responsible for the technical implementation and monitoring the procedure. |
| HR Department | Ensures that employees are trained in the procedure and are aware of their roles and responsibilities. |
| Senior Management | Provides oversight and ensures resources are available for the effective implementation of this procedure. |
| Employees and Contractors | Responsible for following the procedure and reporting any security breaches or incidents immediately. |
| Third-Party Vendors | Must comply with [Organization Name]’s procedures as outlined in contracts and service-level agreements (SLAs). |
| Legal Department | Ensures compliance with legal and regulatory requirements associated with the procedure. |
| <Role> | <Responsibility> |

# Procedure Steps

**Step 1 - Initiating the Process**

|  |  |
| --- | --- |
| **Description** | <Describe the initial step, e.g., how access control requests are submitted, or how an incident is first reported.> |
| **Responsibility** | <Role responsible for this step.> |

**Step 2 - Verification or Review**

|  |  |
| --- | --- |
| **Description** | <Describe the review or verification process, such as verifying user identity or reviewing logs.> |
| **Responsibility** | <Role responsible for this step.> |

**Step 3 - Implementation/Action**

|  |  |
| --- | --- |
| **Description** | <Describe the implementation of actions, e.g., granting access, isolating a threat.> |
| **Responsibility** | <Role responsible for this step.> |

**Step 4 - Monitoring**

|  |  |
| --- | --- |
| **Description** | <Explain how the implemented actions will be monitored, such as monitoring access logs, network traffic, etc.> |
| **Responsibility** | <Role responsible for this step.> |

**Step 5 - Reporting**

|  |  |
| --- | --- |
| **Description** | <Describe how reports will be created, the frequency, and to whom they will be sent.> |
| **Responsibility** | <Role responsible for this step.> |

# Key Performance Indicators (KPIs)

The effectiveness of this procedure will be measured by the following KPIs.

* KPI 1 - *Number of incidents reported within X timeframe*
* KPI 2 - *Number of successful access control reviews completed*
* KPI 3 - *Compliance rate with this procedure during internal audits*

# Compliance and Review

This procedure must be reviewed annually or after any significant changes to the IT infrastructure, relevant regulations, or following a security incident. The review will ensure continued compliance with ISO 27001:2022 and organizational objectives.

**Appendices**

**Appendix A:** <Include any supplementary documentation, e.g., flowcharts, checklists, or forms>

**Appendix B:** <Other related supporting documentation>

***Note: This procedure document may be adjusted based on the organizational structure, resources, and any specific compliance needs related to ISO 27001:2022.***