Policy Exception Procedure

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Procedure Statements 4

2.1 Roles and Responsibilities 4

2.2 Exception Process 4

2.3 Exception Procedure 4

3. Procedure Compliance & Enforcement 6

3.1 Compliance Measures 6

3.2 Enforcement 6

4. Glossary / Acronyms 7

4.1 Glossary / Acronyms 7

5. Document Management 8

5.1 Document Revision Log 8

5.2 Document Ownership 8

5.3 Document Coordinator 8

5.4 Document Approvers 8

5.5 Distribution 8

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Objective

All information technology resources connected to XXXX network are expected to comply with information security policies and standards, which are designed to establish the controls necessary to protect the XXXX’s information assets. A control deficiency in one business process or IT resource can jeopardize other processes or resources. This is because erroneous data may be inherited, privacy compromised, or a conduit for an intrusion into XXXX systems may be created. However, there may be a case where compliance cannot be achieved for a variety of reasons. In such cases, an exception must be documented and approved using this procedure.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Procedure Statements

## Roles and Responsibilities

* Security Committee/Executive Management – To review and approve the policy on a periodic basis
* Line Manager/HOD – this is the manager who is directly responsible for raising the exception to security committee/Executive Management.
* Document Coordinator – This is the staff responsible for research, developing, and reviewing documentation drafts
* Users – To raise policy exception uses and breach of policies to line managers/HOD.
* ISO – Carries out annual reviews of approved exceptions and advise security committee/Executive Management on next actions. Also communicates approved exception to relevant parties and ensure compensating controls are carried out.

## Exception Process

An exception MAY be granted by XXXX Security Committee/Executive Management for non-compliance with a policy/standard resulting from:

* Implementation of a solution with equivalent or superior protection.
* Scheduled retirement of a legacy system within 12 months.
* Inability to implement the policy/standard due to some limitation, or for valid operational issues. Exceptions are granted for a specific period.
* Exceptions are reviewed on a case-by-case basis, and their approval is not automatic.
* Unless otherwise specified, exceptions will be valid for a maximum of one year, but can be renewed after new representation to Security Committee/Executive Management

## Exception Procedure

* The exception must be raised on the helpdesk portal ([https://XXXXhelpdesk.sdpondemand.manageengine.com/home](https://zbukhelpdesk.sdpondemand.manageengine.com/home)) or a mail sent to the Document Coordinator, initiated by the applicable staff. The Exception Request must include:

1. Description of the non-compliance.
2. Describe the exception request (i.e. which policy or standard in the XXXX policies cannot be met).
3. Outline why the XXXX policies and standards cannot be complied with. Include any resource implications, system limitations, business needs, etc. Please note any benefits to XXXX associated with accepting this risk.
4. List any associated hardware or software products relevant to the exception request.
5. If the exception request is granted, describe any compensating controls to minimise any additional risks caused by not meeting the specific policy or standard referenced above exception request (i.e. which policy or standard in the XXXX policies cannot be met).
6. Anticipated length of non-compliance (1-year maximum). New exception process have to be followed if non compliance persists in subsequent periods
7. Proposed assessment of risk associated with non-compliance.
8. Proposed plan for managing the risk associated with non-compliance.
9. Proposed metrics for evaluating the success of risk management (if risk is significant).
10. Proposed review date to evaluate progress toward compliance.

* The staff send the completed exception request on the helpdesk portal to the Document Coordinator who reviews and in turn send the request to the Security Committee/Executive Management
* The Security Committee/Executive Management will hold a meeting to gather any necessary background information, determine if other administrative officials need to be consulted, and make a recommendation to approve or deny the request.
* The Security Committee/Executive Management will contact the requester if additional information is required.
* The Security Committee/Executive Management will approve or deny the request for an exception and through the Document Coordinator notify the requester and manager in writing as to the basis for the approval or an explanation of the denial.
* If approval is contingent upon meeting specific requirements not documented in the request form, the requester must sign and submit an updated request form to the Security Committee/Executive Management
* Departments may appeal a denial by submitting additional information or requesting a meeting with Security Committee/Executive Management to discuss the decision. After that, all decisions will be considered final.
* All requests, approvals and denials for exception will be documented and retained by the Security Committee/Executive Management secretariat

If the non-compliance is due to a superior solution, an exception will normally be granted until the published standard or procedure can be revised to include the new solution. An exception request must still be submitted.

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with this Procedure. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| ISO | Information Security Officer |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

* The distribution is to all staff