Periodic Security Operations 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 Procedure 4

1. Perform Scans and Assessment 4

1.1 Internal vulnerability scan is done monthly 4

1.2 A vulnerability assessment and penetration testing (VAPT) is done every quarter 4

2. Remediation Activities 4

2.1 Receives reports from Netitude, Reliance ACSN. 4

2.2 Assigns remediation activities to system owners and system admin 4

2.3 Inform Security Committee of assessment results and remediation plans. 4

2.4 Ensure remediation activities is done within timeline specified in XXXX-STD-ALL-020 - Vulnerability Management Standard 4

3. Monitoring Activities 4

3.1 Prepare list of outstanding vulnerabilities every 6 months 4

3.2 Send list to Head of IT and Security Committee 4

4. Procedure Compliance & Enforcement 5

4.1 Compliance Measures 5

4.2 Enforcement 5

5. Glossary / Acronyms 6

5.1 Glossary / Acronyms 6

6. Document Management 7

6.1 Document Revision Log 7

6.2 Document Ownership 7

6.3 Document Coordinator 7

6.4 Document Approvers 7

6.5 Distribution 7

# 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

The objective of this procedure is to ensure all identified vulnerabilities and penetration test recommendation are implemented on the appropriate systems and networks

## 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 – To monitor remediation progress on external vulnerability assessment and penetration testing (VAPT)
* Data/process Owner – this is the staff member who is responsible for the data/process that needs to be remediated
* Head IT – To receive the VAPT report and assign activities to data/process owner to remediate the vulnerabilities.
* ISO – Monitors the level of resolution of VAPT remediation and prepare bi-annual report for security committee.

## Exception Procedure

The following outlines activities to be performed on Periodic Security Operations Procedure

| **ACTIVITY** | **TASKS** | **RESPONSIBILITY** |
| --- | --- | --- |
| Perform Scans and Assessment | Internal vulnerability scan is done monthlyA vulnerability assessment and penetration testing (VAPT) is done every quarter | YYYY |
| Remediation Activities | Receives reports from testing companyAssigns remediation activities to system owners and system adminInform Security Committee of assessment results and remediation plans.Ensure remediation activities is done within timeline specified in XXXX-STD-ALL-020 - Vulnerability Management Standard | Head IT |
| Monitoring Activities | Prepare list of outstanding vulnerabilities every 6 monthsSend list to Head of IT and Security Committee | ISO |

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures 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

* *IT*
* *ISO*