*VULNERABILITY MANAGEMENT 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. Security Committee.

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

3. Process for Patching and Updating Network Devices 5

4. Process for Patching and Updating Servers, Databases and Operating Systems 6

5. Process for Anti Malware Update and Review 7

6. Process for Vulnerability Scanning, Intrusion Detection and Remediation 7

7. Procedure Emergency Patch Deployment 7

8. Procedure Compliance & Enforcement 9

8.1 Compliance Measures 9

8.2 Enforcement 9

1. Glossary / Acronyms 10

1.1 Glossary / Acronyms 10

2. Document Management 11

2.1 Document Revision Log 11

2.2 Document Ownership 11

2.3 Document Coordinator 11

2.4 Document Approvers 11

2.5 Distribution 11

# 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 provide a step by step process to achieve the standards set by the XXXX for vulnerability management.

## 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 in relation to vulnerability management

### Applicability to Assets

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

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-STD-ALL-020 - Vulnerability Management Standard*

# Procedure Statements

This process describes the activities and steps involved in handling patches, updates and anti-malware of all IT Assets such as Operating Systems, Servers, Databases, Routers, Switches, computer systems etc to ensure optimal service uptime and they are adequately protected.

Vulnerabilities will be treated in line with vulnerability ratings on XXXX-STD-ALL-020 - Vulnerability Management Standard

# Process for Patching and Updating Network Devices

| **ACTIVITY (Monthly)** | **TASKS** | **RESPONSIBILITY** |
| --- | --- | --- |
| * 1. Prepare Asset Update/Maintenance Plan | * + 1. Log on to the device monitoring tool using username and password.     2. Generate device schedule report.     3. Review report for the following; * Operating System Version. * Device health status. * Device utilization and capacity   + 1. Identify devices that require new updates, configurations or patch deployments based on information from the OEM.     2. Test the updates and patches on a test environment if applicable. No test will be done on production environment.     3. For workstations, the test sample should include at least a PC from each department. In the absence of test servers, non-critical servers could be used.     4. Ensure the patches are tested for 1 week, and confirmed safe without adverse system impact, before rollout to production systems.     5. Develop Update/Maintenance plan for execution.     6. Send Update/Maintenance Plan to Head IT for approval | System Admin, Network and Comms. Officer |
| * 1. Approve Asset Update Plan | * + 1. Receive Asset Update plan from Network Officer/System Admin.     2. Review plan to ensure patches/updates will not be deployed during production hours except for an emergency.     3. If ok, approve plan for execution, else return to network officer for amendments | Head IT |
| * 1. Execute Asset Update Plan | * + 1. Log on to the Terminal Configuration Manager with username and password.     2. Connect remotely to each device identified.     3. Push identified upgrade, configuration or patch to the device.     4. Confirm update has been successfully completed.     5. If successful, proceed to 3.3.6 else, roll back to previous device configuration and repeat steps 3.3.1 to 3.3.4     6. Terminate remote connection with device.     7. Log out of Terminal Configuration Manager | Network Comms Officer/IT Representative/System Admin |

# Process for Patching and Updating Servers, Databases and Operating Systems

| ACTIVITY (Monthly) | TASKS | RESPONSIBILITY |
| --- | --- | --- |
| * 1. sPrepare System Update Plan | * + 1. Log on to the OEM site/Patch Manager or schedule a monthly alert from the OEM/Patch Manager to download the relevant patches and updates.     2. Review the requirements of the patches and updates and ensure it aligns with the internal systems: * Operating System Version * Device utilization and capacity * Server type * Database specifications   + 1. Test the updates and patches on a test environment if applicable. No test will be done on production environment.     2. For workstations, the test sample should include at least a PC from each department. In the absence of test servers, non-critical servers could be used.     3. Ensure the patches are tested for 1 week, and confirmed safe without adverse system impact, before rollout to production systems.     4. Develop system update plan for execution.     5. Send system update plan to Head IT for approval | System Admin |
| * 1. Approve System Update Plan | * + 1. Receive system update plan from System Admin     2. Review plan to ensure patches/updates are not released during production hours except during emergency.     3. If ok, approve plan for execution, else return to system admin for amendments | Head IT |
| * 1. Execute System Update Plan | * + 1. Push identified upgrade, configuration or patch to the identified system.     2. Confirm update has been successfully completed.     3. If successful, proceed to 4.3.4 else, roll back to previous device configuration and repeat steps 4.3.1 to 4.3.2.     4. Log on to server and rectify any potential errors and confirms system status is okay | System Admin |

# Process for Anti Malware Update and Review

| **ACTIVITY (Daily)** | **TASKS** | **RESPONSIBILITY** |
| --- | --- | --- |
| * 1. Prepare and Execute Anti Malware Update Plan | * + 1. Receive the update and patch notice from antimalware system on the helpdesk alert system.     2. Log on as administrator to antimalware system to apply the received patch and update.     3. Confirm update have been successfully completed.     4. Log out of antimalware system | System Admin |
| * 1. Review Anti malware Operations | * + 1. Confirm the required updates and patches have been done.     2. Confirm antimalware system is sending regular updates to all systems | Head IT |

# Process for Vulnerability Scanning, Intrusion Detection and Remediation

| **ACTIVITY** | **TASKS** | **RESPONSIBILITY** |
| --- | --- | --- |
| * 1. Perform Scans and Assessment | * + 1. Internal vulnerability scan is done monthly, and results reported to the security committee.     2. A vulnerability assessment and penetration testing (VAPT) is done annually.     3. Intrusion detection has been set up to be automatically running to detect disruptive behaviour | SOC team, external provider |
| * 1. Remediation Activities | * + 1. Receives reports and alerts from Netitude, Redscan.     2. Assigns remediation activities to system owners and system admin.     3. Inform Security Committee of assessment results and remediation plans.     4. Ensure remediation activities is done within timeline specified in XXXX-STD-ALL-020 - Vulnerability Management Standard | Head IT /ISO |
| * 1. Monitoring Activities | * + 1. Prepare list of outstanding vulnerabilities for presentation at every security committee meeting | Head IT/ISO |

# Procedure Emergency Patch Deployment

| ACTIVITY | TASKS | RESPONSIBILITY |
| --- | --- | --- |
| * 1. Identify emergency patch requirement | * + 1. Identify issue/vulnerability component that requires emergency patch.     2. Log on to the OEM site/Patch Manager download the relevant patches and updates.     3. Review the requirements of the patches and updates and ensure it aligns with the internal systems: * Operating System Version * Device utilization and capacity * Server type * Database specifications   + 1. Develop emergency update plan for execution including communication to users where a restart of systems are required.     2. Send update plan to Head IT for approval | System Admin |
| * 1. Approve System Update Plan | * + 1. Receive system update plan from System Admin.     2. Review plan to ensure it will not impact services during production periods.     3. If services will be impacted escalate to Security Committee on the details of downtime expected and obtain approval.     4. If ok, approve plan for execution, else return to system admin for amendments | Head IT |
| * 1. Execute System Update Plan | * + 1. Push identified upgrade, configuration or patch to the identified system.     2. Confirm update has been successfully completed.     3. If unsuccessful, roll back to previous device configuration and repeat steps 7.3.1 onwards.     4. Log on to server and rectify any potential errors and confirms system status is okay. | System Admin |

# 8. Procedure Compliance & Enforcement

## 8.1 Compliance Measures

Not applicable.

## 8.2 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

|  |  |
| --- | --- |
| SOC | Security Operations Centre |
| OEM | Original Equipment Manufacturer |

# 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*
* *Information Security*