VULNERABILITY MANAGEMENT POLICY

*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

1.3.2 Applicability to External Parties 3

1.3.3 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Vulnerability Management Process 4

2.2 Threat Identification 4

2.3 System Configurations 4

2.4 Anti-Malware / Change Detection Capability 4

2.5 Patch Management 4

2.6 Information System Asset Logging & Monitoring 5

2.7 Privileged Access Logging & Monitoring 5

2.8 Security Testing 5

2.9 Application Change Limitation 5

2.10 Detection of Unauthorised Systems 6

3. Policy Compliance & Enforcement 7

3.1 Compliance Measures 7

3.2 Enforcement 7

4. Exception Process / Glossary 8

4.1 Exception Process 8

4.2 Glossary / Acronyms 8

5. Document Management 9

5.1 Document Revision Log 9

5.2 Document Ownership 9

5.3 Document Coordinator 9

5.4 Document Approvers 9

5.5 Document Distribution 9

# Introduction

## Document Definition

This document is a Policy.

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

## Objective

The objective of this Policy is to provide information security requirements to effect appropriate vulnerability policies related to the security of all XXXX’s Information Technology assets.

## Scope

### Applicability to Employees

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

### Applicability to External Parties

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

### Applicability to Assets

This Policy 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*
* *XXXX-POL-ALL-008 - Business Continuity Management Policy*
* *XXXX-POL-ALL-012 - Incident Response Policy*
* *XXXX-POL-ALL-013 - Disaster Recovery Policy*
* *XXXX-PRC-ALL-002 - Change Control Procedure*
* *XXXX-PRC-ALL-007 - Log Review & Monitoring Procedure*
* *XXXX-PRC-ALL-011 - Rogue Device Detection Procedure*
* *XXXX-PRC-ALL-015 - Vulnerability Management Procedure*

# Policy Statements

## Vulnerability Management Process

A Vulnerability Management process must be established and include the following:

* defined roles and responsibilities for management;
* an approach to patching (e.g., what is to be patched);
* identification of vulnerabilities that are applicable to the organisation, including feeds from external trusted sources;
* assignment of an appropriate risk ranking (e.g. Information, Low, Medium, High, Critical);
* an assessment of the business impact of implementing patches (or for not);
* provisions that all patches are tested against known criteria;
* detailed deployment methods for patches (distribution tools);
* reports on the status of patch deployment across the organisation.

XXXX-PRC-ALL-015*- Vulnerability Management Procedure(s)* and *XXXX-STD-ALL-020 - Vulnerability Management Standards* refers.

## Threat Identification

Key personnel and/or functional teams will subscribe to trusted external information security feeds relevant to their responsibilities and follow threat notification procedures detailed in *XXXX-PRC-ALL-015 - Vulnerability Management Procedure* and *XXXX-STD-ALL-020 - Vulnerability Management Standards*.

## System Configurations

System owners will amend their corresponding configuration standard in accordance with XXXX-PRC-ALL-014 *- Vulnerability Management Procedure* to ensure compliance with currently accepted best security practices.

## Anti-Malware / Change Detection Capability

Where appropriate, anti-malware software capable of detecting and removing all known type of malicious software, must be implemented on servers and workstations across all XXXX environments in compliance with related security Standards.

The software must be purchased legally and used within the parameters of license agreement.

## Patch Management

Patches, hot fixes, and other technical or security updates that are identified as applicable through the *XXXX-PRC-ALL-014* *- Vulnerability Management Procedure* must be applied to all systems in accordance to results of the risk rank assignment and company goals. *XXXX-PRC-ALL-014 - Vulnerability Management Procedure* refers.

Compensating controls must be applied if patching cannot be completed within the specified timeframes.

Appropriate capacity monitoring and planning will be conducted to meet current and future needs of the organisation to ensure system availability and currency of patch levels.

Where possible, patching through automated means is preferred.

## Information System Asset Logging & Monitoring

Where available, all Information System Assets will log relevant events for subsequent collection and review.

Logging and monitoring mechanisms and processes will, when feasible, automate incident response alerts based on digression from a known-good baseline.

At a minimum, system log-files will be reviewed on a frequency determined in the *XXXX-STD-ALL- 009 Logging and Monitoring Standard* and the results reported through the XXXX-PRC-ALL-012 *- Incident Response Procedure* as appropriate.

## Privileged Access Logging & Monitoring

Where available, all Information System Assets will log privileged access (e.g. Administrator, or root access) events for subsequent collection and review.

Logging and monitoring mechanisms and processes will, when feasible, automate incident response alerts based on digression from a known-good baseline.

At a minimum, privileged access log-files will be reviewed on a frequency determined in *XXXX-STD-ALL- 009 Logging and Monitoring Standard* and the results reported through the XXXX-PRC-ALL-012 *- Incident Response Procedure* as appropriate.

## Security Testing

Full security testing which will include both vulnerability assessment and penetration testing and will be done by a qualified vendor on behalf of XXXX. The frequency will be determined in the XXXX-STD-ALL-020 *– Vulnerability Management Standard*.

## Application Change Limitation

As far as possible and practicable, vendor-supplied software packages should be used without modification. Where changes are deemed necessary, a full technical review will be performed in a test environment prior to release into production.

## Detection of Unauthorised Systems

Technology and processes will be put in place to detect the use of unauthorised ('rogue') assets. It is recommended that this detection be as automated and in near real-time as possible.

Detection scan frequency is determined in the XXXX-STD-ALL-020 *- Vulnerability Management Standard* and XXXX-PRC-ALL-011 *- Rogue Device Detection Procedure* refers.

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Observe the following processes to determine relative effectiveness for protecting the XXXX environment. Threat Identification   * Network Device Review * System Configurations * Anti-Malware * Patch Management * Logging & Monitoring * External Vulnerability Scanning * Internal Vulnerability Scanning * External Penetration Testing * Internal Penetration Testing | * Interview with system administrators * Event notifications * Incident Response reports |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. 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.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| XXXX | XXXX. |

# Document Management

## Document Revision Log

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

## Document Ownership

This Policy is owned by the YYYY.

## Document Coordinator

This Policy is coordinated by the YYYY.

## Document Approvers

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

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff