VULNERABILITY MANAGEMENT STANDARD

*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 4

1.1 Document Definition 4

1.2 Objective 4

1.3 Scope 4

1.3.1 Applicability to employees 4

1.3.1 Applicability to External Parties 4

1.3.2 Applicability to Assets 4

1.4 Related Documents / References 4

2. Standard Statements 5

2.1 Threat Intelligence Feeds 5

2.2 System Configurations 5

2.3 Anti-Malware 5

2.3.1 Anti-Malware Coverage 5

2.3.2 Users responsibility 5

2.3.3 Anti-Malware Capability 6

2.3.4 Anti-Malware Scanning 6

2.3.5 Anti-Malware Updates 6

2.3.6 Anti-Malware Installations 6

2.3.7 Anti-Malware Infection 6

2.3.8 Anti-Malware Logging 6

2.4 Vulnerability Management 7

2.5 Patch Management 8

2.6 Remediation and Priorities 8

2.7 File Change Detection 9

2.8 Detection of Unauthorised Systems 9

2.9 Mobile Devices Vulnerabilities 9

2.10 Technical Review Post-Installation 10

3. Standard Compliance & Enforcement 11

3.1 Compliance Measures 11

3.2 Enforcement 11

4. Exception Process / Glossary 12

4.1 Exception Process 12

4.2 Glossary / Acronyms 12

5. Document Management 13

5.1 Document Revision Log 13

5.2 Document Ownership 13

5.3 Document Coordinator 13

5.4 Document Approvers 13

5.5 Document Distribution 13

# Introduction

## Document Definition

This document is a Standard.

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

## Objective

The objective of this standard is to provide global information security requirements for the implementation of vulnerability management processes.

## Scope

### Applicability to employees

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

### Applicability to External Parties

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

### Applicability to Assets

This Standard 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-012 - Incident Response Policy*
* *XXXX-PRC-ALL-006 - Incident Response Procedure*
* *XXXX-PRC-ALL-015 - Vulnerability Management Procedure*

# Standard Statements

## Threat Intelligence Feeds

XXXX is operating a managed SOC where threat intelligence and alerts are analysed, contained and sent to XXXX

## System Configurations

System owners will amend their corresponding configuration Standard(s) in accordance with the relevant XXXX*-PRC-ALL-015 - Vulnerability Management Procedure* at least annually to ensure compliance with currently accepted best security practices.

## Anti-Malware

### Anti-Malware Coverage

* The approved enterprise anti-virus solution for windows operating systems clients and servers in the XXXX is Sophos; hence only this solution shall run on systems on the network. The use of other antivirus solutions is PROHIBITED unless approved by Head, IT.
* Appropriate anti-malware technology should be placed on all systems commonly affected by this attack vector. Lack of anti-malware should be justified and approved by Head IT

### Users responsibility

* Any activity with the intention to create and/or distribute malicious programs into the XXXX’s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited in accordance with the XXXX-POL-ALL-003 - Acceptable Use Policy - End User Agreement.
* Users must not disable or in any other way reconfigure antivirus software running on systems in such a way as to impair its normal functionality
* Laptop users who operate their laptops on and off the network must regularly connect to the network to ensure that the anti-virus software virus definitions remain up-to-date. Failure to do so could result in unnecessary virus outbreaks.
* Installation/use of unauthorized software on the network is strictly prohibited. Unauthorized use, in addition to breaching copyright requirements, could introduce malicious software into the network.
* If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report such incident to the IT Department/Information Security immediately by e-mailing xxxx@xxxx.com Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
* Users must not accept and/or open email attachments, macros and other executable files from unknown, untrustworthy or suspicious sources.
* Users are advised to avoid direct disk sharing with read/write access. Users must always scan any removable media for viruses before using it.

### Anti-Malware Capability

Anti-malware should be capable of at least detecting all current form of threat; i.e. worms, viruses, trojans etc.

Anti-Malware capable of quarantining and/or automatic eradication are preferred.

### Anti-Malware Scanning

* Virus-infected computers must be removed from the network until they are verified as virus-free.
* All software to be deployed/ installed on the XXXX’s information system must be reviewed and confirmed to be virus free before deployment. This requirement applies to in-house and off-the-shelf software, maintenance/customization releases (internally or externally developed), updates and patches, etc.
* IT is responsible for ensuring that anti-virus software is updated at regular intervals, and computers are verified as virus-free.
* Anti-Malware software must perform thorough system scanning on boot/reboot, at least monthly, and in real-time for non-executables.

### Anti-Malware Updates

* The antivirus database must be set to automatically update.
* Where applicable, Anti-Malware software and definitions must be configured to look for updates from respective vendors monthly, and in accordance with vulnerability management procedures.

### Anti-Malware Installations

Where relevant, Anti-Malware mechanisms must be running at all times and be unalterable by regular users unless otherwise approved.

### Anti-Malware Infection

Any suspected malware infections must trigger an alert. Alerts must be followed by an appropriate and effective response in accordance with the *XXXX-POL-ALL-012 - Incident Response Policy*.

### Anti-Malware Logging

All anti-malware systems must have logging enabled, and logs must be retained for a period of one (1) year

## Vulnerability Management

* The XXXX shall engage an external vendor to carry out at least annually Vulnerability Assessments and Penetration Testing on information system assets of the XXXX.  Reports of these assessments must be documented and approved by Head, IT/Information Security Officer.
* Only approved vulnerability scanning tools shall be used on the XXXX’s information systems. The Head, IT/ Information Security shall be solely responsible for the approval of vulnerability scanning tools to be used in the XXXX. If there is a need to use other scanning tools, such tools must have documented justifications and require the approval of the Head, IT/Information Security.
* Installation/use of unauthorized software on the network is strictly prohibited.
* Only Information Security and IT personnel have the approval to conduct vulnerability scans on the XXXX’s information systems. Any other staff seeking to conduct scans on the systems must obtain an approval from the Head, IT/Information Security Officer.
* The scope of the activities that will be involved in test include but not limited to:
* Network infrastructure (wired & wireless)
* Operating Systems
* Web Applications;
* Extranet;
* Perimeter Security Devices; and
* Applications
* Penetration testing and vulnerability assessment will follow the Open Web Application Security Project (OWASP) criteria for testing. Listed below are the OWASP Top 10 Web Application Security Risks:
* Injection
* Broken Authentication and session management
* Cross-site scripting (XSS)
* Insecure direct object references
* Security misconfiguration
* Sensitive data exposure
* Missing function level access control
* Cross-site request forgery (CSRF)
* Using components with known vulnerabilities
* Invalidated redirects and forwards
* The report of this exercise shall be a documentation of all findings, gaps in security measures and suggested countermeasures. The report shall serve as a means of remediation and improvement on the XXXX’s security defenses.
* Vulnerability assessment reports may contain sensitive XXXX information, as such; all reports must be treated as restricted. Also, a non-disclosure agreement must be signed with an external party before commencement of vulnerability scanning activities.
* All new information systems deployed in the XXXX – applications (in-house and off the shelf), network infrastructure (wired and wireless), etc. – must be scanned for vulnerabilities and all identified vulnerabilities remediated prior to migration to operational (live) environment. In the same vein, all major changes to the XXXX’s information system shall undergo vulnerability scanning and all identified vulnerabilities remediated prior to migration to the operational environment.
* Critical Information systems and networks will be regularly scanned and monitored to detect disruptive behaviour and alerts sent to Information Security officer/IT for responsive action.
* As part of their job function, the IT/Information Security Officer shall periodically visit security website such as SANS.org, CERT.org and CISecurity.org to keep abreast of evolving trends in information security especially as it affects information systems deployed in the XXXX.

## Patch Management

Patches, hot fixes, and other technical or security updates that are identified as applicable through the *XXXX-PRC-ALL-015 - Vulnerability Management Procedure* must be applied to all systems primarily in accordance to results of the Vulnerability Management process.

* XXXX will update and apply security patches to critical IT systems within 30 days of patch release to address information security vulnerabilities.
* Regular patching procedures are defined and follow a designated process.  Emergency patches will be applied when necessary, requiring the approval of the Head IT.
* XXXX will implement a process to keep up to date with current security vulnerabilities and associated patches.
* In addition, the IT/Information Security department will check vendor sites and communications for patches and updates to critical software systems on a monthly basis.

## Remediation and Priorities

* At the conclusion of each vulnerability and penetration testing assessment, a remediation plan/report shall be prepared and sent to the Head, IT by the Information Security Officer. The report shall summarize the following:
  + List of Vulnerabilities: All discovered vulnerabilities, the severity, and the affected information systems.
  + Remediation Steps: Each of the vulnerabilities listed shall have detailed information on how the vulnerability shall be remediated or eliminated with completion timelines.
  + The Head IT will regularly update the Information Security Officer on the progress of the remediation activities
* Head IT shall produce a documented update of the vulnerability remediation efforts at every Security Committee meeting. The vulnerability assessment report may also contain vulnerabilities discovered by other teams.
* Vulnerabilities discovered on information systems on the XXXX’s network shall be remediated and /or mitigated based on the schedule in the table below:

|  |  |  |  |
| --- | --- | --- | --- |
| S/N | VULNERABILITY RATING | DESCRIPTION | REMEDIATION INTERVAL |
| 1 | Critical | These are vulnerabilities through which an attacker could gain access to the system at the administrator level or could possibly access sensitive information stored on the system. | Vulnerabilities shall be fully addressed within 30 calendar days of been published by the vendor/discovered. |
| 2 | High | These vulnerabilities may allow an intruder to gain access to specific information stored on the host, including security settings. They can also allow intruders gain access to information that may be used to compromise the host in the future. | Vulnerabilities classified as high shall be addressed within 45 calendar days of been published by the vendor/discovered |
| 3 | Medium | Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. | Medium level vulnerabilities shall be addressed within 60 calendar days of been published by the vendor/discovered |
| 4 | Low | These vulnerabilities do not pose an immediate threat to the XXXX’s systems. They are mostly weaknesses that may allow an intruder access to information that may be used in the future to compromise the host | Low level vulnerabilities shall be addressed within 180 calendar days of been published by the vendor/discovered |

## File Change Detection

If required, file system comparisons should be performed with alerts fed into the *XXXX-PRC-ALL-006 - Incident Response Procedure* for appropriate action.

## Detection of Unauthorised Systems

Discovery processes will be conducted in accordance with *XXXX-PRC-ALL-011- Rogue Detection Procedure*

## Mobile Devices Vulnerabilities

All users must take appropriate secure measures under the XXXX’s acceptable use Policy including but not limited to:

* Ensuring that the mobile device is password protected using the features of the device and that a “strong password,” as defined in the XXXX-STD-ALL-013 - Authentication Standard, is required to access the XXXX’s network and information
* Ensuring that the mobile device locks itself with a password or PIN if the device is idle for one minute
* Ensuring that the mobile device locks itself and must be re-opened by another password or PIN after three failed login attempts
* Not using rooted (Android) or jailbroken (iOS) devices to access the XXXX’s information and network
* Not sharing the mobile devices with friends, relatives
* Not storing or transmit illicit material or proprietary information belonging to another organisation
* Using their BYOD devices to access only the information authorized to access under the XXXX XXXX-STD-ALL-013 - Authentication Standard
* Maintaining the mobile device themselves ensuring it is regularly patched and upgraded with the latest original equipment manufacturer software.
* Ensuring the basic security level of the mobile device is configured, this may include but not limited to blocking malicious sites from opening on the device, blocking malicious apps, activating the security features available on the device.
* Encryption of the XXXX’s data on the mobile device must be enabled
* Reporting lost, misplaced or stolen mobile devices to the IT department within 24 hours
* Report any security breach immediately to Information Security Team in accordance with the Information Security Policy
* Authorized users are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices
* The XXXX has the right, at any time, to monitor and preserve any communications that uses its networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.
* No user may knowingly disable any network software or system identified as a monitoring tool.
* From time to time, the XXXX may require that you install or update XXXX-approved device management software on your own device.
* It is your responsibility to familiarise yourself with the device sufficiently to keep data secure.

## Technical Review Post-Installation

A technical review of application and system integrity will be performed following operating system patches to ensure that vulnerabilities have not been introduced.

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. 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** |
| Check samples of vulnerability and penetration test assessment for remediation of vulnerabilities | * Check vulnerability remediation reports to see the update on resolution |
| Check latest patches from OEM sites | * Confirm the last patch applied on systems is the latest from OEM |
| Check for regular antivirus updates on systems | * Take a sample of systems and check if they are been regularly updated with antivirus |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards 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 Standard 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

|  |  |
| --- | --- |
| SOC | Security Operations Centre |

# Document Management

## Document Revision Log

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

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

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

## Document Distribution

Distribution is to all staff