SYSTEM CONFIGURATION & MAINTENANCE 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

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 4

2. Policy Statements 5

2.1 Authorised Parties 5

2.2 Configuration Baseline 5

2.3 System Security Baseline 5

2.4 System Logging 5

2.5 Configuration Changes 6

2.6 Change Reversal 6

2.7 Testing Environment 6

2.8 Test Data and Developer Accounts 6

2.9 Security Reviews 6

2.10 Compliance Reviews 6

2.11 Application of Patches, Hot Fixes, and Updates 7

2.12 New Systems 7

2.13 Capacity Management 7

2.14 Network Time Synchronisation 7

2.15 Change Detection 7

2.16 Software Installation on Production Systems 7

2.17 Technical Review Post-Installation 8

3. Policy Compliance & Enforcement 9

3.1 Compliance Measures 9

3.2 Enforcement 10

4. Exception Process / Glossary 11

4.1 Exception Process 11

4.2 Glossary / Acronyms 11

5. Document Management 12

5.1 Document Revision Log 12

5.2 Document Ownership 12

5.3 Document Coordinator 12

5.4 Document Approvers 12

5.5 Document Distribution 12

# 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:

* Manage the configuration of Information Technology (IT) assets which includes hardware, software, and associated documentation;
* Ensure that vulnerability management processes have been implemented to administer patches, hot fixes, and other security updates to XXXX (XXXX) systems;
* Protect the network and systems from malicious software and code to ensure the integrity, availability and confidentiality of XXXX information and IT systems.

The scope of this policy includes all infrastructure devices, applications, software, and Software as a Service (SaaS)[[1]](#footnote-1)\*.

## 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 employees, 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-012 - Incident Response Policy*
* *XXXX-POL-ALL-014 - Vulnerability Management Policy*
* *XXXX-STD-ALL-016 - Logging and Monitoring Standard*
* *XXXX-STD-ALL-033 - Vulnerability Management Standard*
* *XXXX-STD-ALL-019 - Network Time Synch Standard*
* *XXXX-PRC-ALL-015 - Vulnerability Management Procedure*
* *XXXX-PRC-ALL-002 - Change Control Procedure*

# Policy Statements

## Authorised Parties

Computer systems must be installed, configured, maintained and removed by parties who are assigned formally to these tasks following agreed-upon procedures.

## Configuration Baseline

A configuration baseline must be created for all systems implemented. The baselines must be stored in a configuration management repository or equivalent. Configuration baselines will be based on industry accepted best practices and address at a minimum:

* Removal of vendor default(s) prior to promotion into production environments;
* Removal or disabling of unnecessary default accounts;
* Encryption of all non-console Administrative access;
* Business justification for all remaining services and ports available on each system;
* Business justification and management approval for all insecure service (if applicable);
* Business justification and management approval (where applicable) for all remaining system functionality;
* Updating of configuration standards based on output of vulnerability management processes (per *XXXX-PRC-ALL-015 - Vulnerability Management Procedure*);
* Verification of applied configuration standards prior to promotion in production environments;
* The necessity for a single ‘Primary Function’ (or security level).

## System Security Baseline

Configuration baselines must include a security configuration baseline as a component, or a security configuration baseline must exist separately and be applied to all systems.

Security baselines must take into account all applicable legislative, statutory, regulatory, and contractual requirements and set accordingly.

## System Logging

Systems must log relevant activity. Logs must be reviewed and retained in accordance with *XXXX-STD-ALL-016 - Logging & Monitoring Standard*.

If applicable, the review must be followed by an effective response as detailed in *XXXX-POL-ALL-012 - Incident Response Policy*.

## Configuration Changes

All changes to configurations must be made through the *XXXX-PRC-ALL-002 - Change Control Procedure* and include at a minimum:

* Documentation of impact;
* Change approval by authorised parties;
* Functionality and security testing;
* Updating of the configuration management repository if applicable.

## Change Reversal

Changes to system configurations or configuration baselines must include a back out or reversal (or equivalent, e.g. fix-forward) process.

## Testing Environment

Development/test environments must be separate from production environments with access control in place to enforce separation of both infrastructure and personnel responsibilities.

## Test Data and Developer Accounts

Data above INTERNAL classification must not be used in test environments, and all test data and developer accounts must be removed prior to promotion of code or applications into production.

Data used for testing systems will be stored and processed in a manner that ensures appropriate security controls and compliance with all applicable privacy requirements.

Production data used outside the production environment and used for testing is subject to the same production security and applicable privacy controls.

The use of production data outside of its production environment should be avoided to the greatest extent feasible, and, where not possible, all sensitive data should be redacted or otherwise obfuscated.

## Security Reviews

Security reviews must be conducted on configuration baselines periodically to ensure compliance with XXXX Information Security Policies and that vendor recommendations and industry good practices are considered.

## Compliance Reviews

A review of the configuration of implemented systems must be performed at least annually, or when significant changes to the security or functionality of a system are implemented, or if there is a significant change to the prevailing threat landscape.

## Application of Patches, Hot Fixes, and Updates

*XXXX-POL-ALL-014 - Vulnerability Management Policy* and *XXXX-STD-ALL-033 - Vulnerability Management Standard* refer.

## New Systems

The *XXXX-PRC-ALL-015 - Vulnerability Management Procedure* and relevant configuration standards must be applied to all new systems prior to implementation.

## Capacity Management

The following capacity requirements should be built into all systems from the design phase:

* disk usage and size;
* network traffic load;
* load balancing;
* necessary processing power; and
* necessary memory requirements.

## Network Time Synchronisation

The *XXXX-STD-ALL-019 - Network Time Synch Standard* must be applied to all new systems prior to implementation.

## Change Detection

A change detection mechanism (e.g. File Integrity Monitoring (FIM)) will be implemented on all systems processing data assets over classification of Internal Classification

Files to be monitored include, but are not restricted to:

* System executables;
* Application executables;
* Configuration and parameter files;
* Centrally stored, historical or archived, log and audit files;
* Additional critical files determined by IT/Information Security

## Software Installation on Production Systems

The installation of software packages on top of hardened operating systems shall follow documented Standards and Procedures to ensure that vulnerabilities have not been introduced.

## Technical Review Post-Installation

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

# 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** |
| For a selection of systems, evidence that personnel have been formally assigned installation, configuration, and maintenance tasks for the selected systems and that the personnel assigned are the personnel that have performed the related procedures | * Documented assignment of personnel to selected systems * Sign off of designated personnel in a procedure log or similar document |
| For a selection of systems, evidence of a baseline/standard configuration and the configuration repository | * A copy of the selected systems baselines (i.e., a router configuration and security baseline or a document that outlines all required settings) * A screenshot of the repository displaying the selected baselines |
| For a selection of systems, evidence that the configuration management baselines/standard include a security baseline or that a separate security baseline exists | * A copy of the selected systems baselines or a copy of separate security baselines for the systems selected * OR * A document outlining the security settings applied to acquired software or pre-configured systems |
| For a selection of configuration changes, evidence that the changes followed local change management procedure and that the changes were applied to the baseline repository | * A copy of the configuration management baselines before and after the change output from the repository * A copy of the local change management procedure |
| For a selection of configuration changes, evidence that a back out or reversal process was included in the change | * A copy of the procedures followed to complete the changes, including back out or reversal processes |
| For a selection of systems, evidence that the configuration was reviewed on an interval basis or when significant changes were made | * A copy of the reviews performed on the selected systems |
| For an established vulnerability management process, evidence that the process includes all of the minimum requirements specified by this policy | * A copy of the vulnerability management process document (i.e., the standard procedures performed on Windows servers to manage vulnerabilities.) |
| For a selection of patches, hot fixes, or other updates, evidence that the updates were applied in a timely manner | * A copy of the update/patch log including date and time stamps * Documentation regarding the date and time the patches/updates were approved for application to the system |
| For a selection of new systems implemented, evidence that the vulnerability management process was performed prior to the system’s implementation | * A copy of the procedures performed on the new systems selected dated prior to system implementation |

## 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

|  |  |
| --- | --- |
| Configuration Baseline | A document or system/device image detailing the exact configuration of a specific device type. |
| Configuration Management Repository | Typically, a database or other server containing all the configuration baselines and related information, such as revision logs, as well as an inventory of the systems base-lined (if available). |
| Hot Fix | A single, cumulative package that includes one or more files that are used to address a problem in a software product (i.e., a software bug). |
| Malware | Short for ‘malicious software’, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. e.g. viruses, spyware etc. |
| Patch | A small piece of software designed to fix problems with or update a computer program or its supporting data. |
| Security Baseline | Typically, a document or device configuration image that offers a "cookbook recipe" for a normal level of protection. |

# 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:

* IT
* Information Security

1. \* *Note: This policy makes no distinction between ‘applications’, ‘software’, and ‘SaaS’.* [↑](#footnote-ref-1)