SECURE APPLICATION DEVELOPMENT 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 employee 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Security Considerations 4

2.2 Industry Standards 4

2.3 Separate Development and Test Environments 4

2.4 Segregation of Duties 4

2.5 Use of Production Data 4

2.6 Test Data & Accounts 4

2.7 Risk Assessment and Control 5

2.8 Security Review 5

2.9 Security Testing (Development) 5

2.10 Security Testing (Acceptance) 5

2.11 Secure Coding Training 5

2.12 Application Patching 5

2.13 Development Access 5

2.14 Application Services Over Public Networks 6

2.15 Protection of Transactions 6

2.16 Open Source Applications and Software 6

2.17 Acquired Software 6

3. Policy Compliance & Enforcement 7

3.1 Compliance Measures 7

3.2 Enforcement 8

4. Exception Process / Glossary 9

4.1 Exception Process 9

4.2 Glossary / Acronyms 9

5. Document Management 10

5.1 Document Revision Log 10

5.2 Document Ownership 10

5.3 Document Coordinator 10

5.4 Document Approvers 10

5.5 Document Distribution 10

# 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 ensure all applications and systems are developed in a secure manner.

This policy covers all software developed internal to XXXX. (XXXX) and includes provisions regarding software procured from sources outside of XXXX’s internal development teams.

## Scope

### Applicability to employee

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-002 - Access Control Policy.*
* *XXXX-STD-ALL-036 - Secure Application Development Standards*

# Policy Statements

## Security Considerations

A documented systems development methodology must be developed and include Information Security considerations at each phase within the systems development lifecycle to ensure that systems are developed to comply with Information Security policies and standards, legal and regulatory requirements, and particular business requirements for security.

Security considerations must include all applicable legislative, statutory, regulatory, and contractual requirements and be implemented accordingly.

## Industry Standards

Software development processes will be based, where appropriate, on industry accepted best practices including, but not limited to:

* OWASP - Open Web Application Security Project
* SANS - SysAdmin, Audit, Network and Security

## Separate Development and Test Environments

Where feasible, production and test environments should be entirely separated by physical and / or logical access controls. Where this is not possible, detailed mitigating controls must be prepared and approved as a Policy Exception by the Security Committee. See *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Segregation of Duties

Where feasible, test personnel should not have access to the production environments. Where this is not possible, detailed mitigating controls must be prepared and approved as a Policy Exception by the Security Committee team. See *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Use of Production Data

Under no circumstances must raw production data above Data Classification level Internal be used in test environments. Production data may be sanitised for use in test if approved by the Security Committee.

## Test Data & Accounts

Under no circumstances may test data and / or test accounts by promoted into a production environment.

## Risk Assessment and Control

Applications must include appropriate controls to ensure the confidentiality, integrity and availability of application services and data. The definition of these controls must be based on a risk assessment performed by or under the direction of the Information Asset Owners and/or Data Owners in accordance with the *XXXX-POL-ALL-011 - Risk Management Policy*.

## Security Review

Before development work begins, system requirements and designs must be documented, verified to ensure that they comply with Information Security Policies and Standards, and are reviewed and approved by the Head of IT or designated party.

## Security Testing (Development)

Security testing will be conducted during the code development phase and all issues deemed HIGHRISK addressed prior to continuation of the development lifecycle.

## Security Testing (Acceptance)

All security-related issues deemed HIGH risk through the security review process must be tested and resolved prior to the system being promoted into the production environment.

All coding and testing processes will include reference to industry best practice standards and guidance against the most common security flaws (OWASP for example).

## Secure Coding Training

Training in secure coding techniques will be provided to all developers based on industry best practices. Training will include techniques specific to both the function of the application, and the classification of processed data.

## Application Patching

Patches, hot fixes, and other technical or security updates must be applied to both acquired software and internally developed applications.

## Development Access

As specified in the *XXXX-POL-ALL-009 - Access Control Policy*, controls must be applied in the development environment to protect against unauthorised access. Additionally, development personnel must not have access to the production environment unless authorised by the Security Committee and appropriate compensating controls (e.g., monitoring) and change management are implemented for the access.

## Application Services Over Public Networks

Where XXXX application exposes data of classification INTERNAL or higher over untrusted networks (particularly the Internet) the following security controls must be considered:

1. requirements for mutual authentication;
2. authorisation processes;
3. mutually agreed conditions of service;
4. requirements for confidentiality, integrity, proof of dispatch, receipt of key documents and non-repudiation;
5. levels of trust (integrity);
6. the protection requirements (confidentiality and integrity);
7. liability associated with any fraudulent transactions, and;
8. insurance requirements.

## Protection of Transactions

Information involved in application service transactions must be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, and unauthorised message duplication or replay.

## Open Source Applications and Software

Open source applications and/or software that are not obtained through the standard procurement process must have the licensing agreement reviewed and approved by the Legal department prior to deployment.

## Acquired Software

The acquisition of third party applications and/or software (including open source) must be reviewed by personnel that have the necessary skills to evaluate the security implications and approved by the person in charge of the system under development. Acquired software must also be tested for vulnerabilities and against the security and configuration baseline components that exist for internally developed applications.

# 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 the systems development methodology, evidence that the methodology includes considerations for information security policies, and legal and business requirements | * The systems development methodology (SDLC) or equivalent * Applicable project plan documentation based on the methodology utilised |
| For a selection of applications, evidence that security controls have been established based on a risk assessment | * Risk assessment documents from selected applications * Documented controls from selected applications * Steering or Security committee meeting minutes * Applicable project plan documentation based on the methodology utilised |
| For a selection of development work, evidence that the design and requirements have information security embedded and approved by the Security Committee or a designated party | * Project Management documentation related to the development work * Approval documentation dated prior to the start of development (forms, email, code review etc.) |
| For a selection of open source applications and/or software, evidence that the licensing agreement(s) were reviewed and approved by the Legal/Compliance Department prior to deployment. | * Documented review and approval of the selected software by Legal/Compliance |
| For a selection of third party software, evidence that the security implications were reviewed and approved | * Documented approval of the selected software * Review notes related to the selected software * Steering or Security committee meeting minutes * Applicable project plan documentation based on the methodology utilised * Vulnerability testing results * Security and Configuration baseline testing results |
| For a selection of systems promoted into production, evidence that security components were tested prior to production promotion | * Documented security testing results dated prior to system promotion * Work flow testing / tracking software output * Applicable project plan documentation based on the methodology utilised |
| For a selection of development environments, evidence that access controls are established to protect the environment from unauthorised access | * Documented access controls related to the selected environments * System configuration information |
| For a selection of applications, 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 the production environment, evidence that developers do not have access to production OR that mitigating controls are in place and operating effectively | * System configuration information (access lists) * Monitoring control documentation (review evidence, etc.) |

## 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. |
| 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). |
| 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. |
| OWASP | Open Web Application Security Project |
| SANS | SysAdmin, Audit, Network and Security |

# 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