SOFTWARE DEVELOPMENT LIFECYCLE

*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

2. Objectives 3

3. Scope 3

3.1.1 Applicability to Employees 3

3.1.2 Applicability to External Parties 3

3.1.3 Applicability to Assets 3

4. Software Development Life Cycle 3

5. Standard Compliance & Enforcement 9

5.1 Compliance Measures 9

6. Enforcement 9

7. Exception Process/ Glossary 9

7.1 Exception Process 9

8. Document Management 9

8.1 Document Revision Log 9

8.2 Document Ownership 10

8.3 Document Coordinator 10

8.4 Document Approvers 10

8.5 Document Distribution 10

A.1 Project Documentation Checklist Error! Bookmark not defined.

A.2 Requirements Specification Template Error! Bookmark not defined.

A.3 Functional & Technical Specification Template Error! Bookmark not defined.

A.4 Test Script Template Error! Bookmark not defined.

A.5 Change Request Template Error! Bookmark not defined.

# Introduction

XXXX at all points in time adopt the system development methodology which best fits to the overall cultures, standards and expectations of the XXXX and this methodology shall govern the process of developing, acquiring, implementing and maintaining computerized information systems and related technology.

# Objectives

To establish guidelines and procedures for application and software development in XXXX

# 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.

# Software Development Life Cycle

XXXX development methodology shall

* Be appropriate for the systems to be developed, acquired, implemented and maintained
* Provide standards covering test requirements, verification, documentation and retention for testing individual software units that interface with the XXXXing application as part of every information system development or modification project.
* Require that adequate mechanisms for audit trails are available or can be developed for the solution identified and selected. The mechanisms should provide the ability to protect sensitive data (e.g., user ID’s and passwords) against discovery and misuse.
* In the event of major changes to the XXXX’s existing information technology, management shall ensure that this system development methodology is observed, as in the case of the acquisition or development of new technology.
* Provide for an examination of the technological feasibility of each alternative for satisfying the business requirements established for the development of a proposed new or modified information system project.
* Provide that adequate user procedures manuals be prepared and refreshed as part of every information system development, implementation or modification project.
* Provide for the evaluation of the requirements and the specifications for an RFP (request for proposal) when dealing with a third-party service vendor.
* Provide, in each proposed information systems development, implementation and modification project, for an analysis of the costs and benefits associated with each alternative being considered for satisfying the established business requirements.
* The XXXX’s system development methodology shall provide that appropriate procedures and techniques, involving close liaison with system users, are applied to create the design specifications for each new information system development project and to verify the design specifications against the user requirements.
* Ensure that security is built into applications forming a business requirement for systems to be acquired.

##### PROCEDURE 1: Application Development Framework

* Project Definition:

o A project will be initiated by a project manager, sponsor or user by requesting for a service or product

o Each project shall be defined and documented in a project charter or notes

* Requirements Definition
* A requirements definition will be jointly undertaken by Users of the technology and the technology group.
  + - The User Requirements definition will be drawn up and documented and will form development details from the customer perspective; specific requirements desired, expected business benefits, value proposition, detailed functionality and reports and development details from an IT perspective documenting functional requirements, application architecture, presentation and project scope. Refer to the Appendix for a Requirements Specification template
    - There should be risk assessment and mitigation measures documented by Operational Risk Management/Information Security team in every Project Initiation Document.
    - The requirements specification document is signed off by the project manager, sponsor and a representative of IT.
    - The approved requirement specification document serves as the Project Initiation Document (PID). The PID will be circulated for sign off by the requesting unit.

This document will be referenced from the beginning to the end of the project and shall form the basis of development

* Feasibility Analysis
  + A feasibility analysis depending on the scope of the project will be performed from a technical and functional perspective.
  + This analysis will include a comparison of available options and a decision on if to custom build a solution or procure an off the shelf application. The functional/business feasibility analysis will include
    - * Total Cost Impact
      * Impact on existing Business Process and Process requirements
      * Required Standard Operating Procedures
      * Who is to have access to the application, and what infrastructure investment is required to deliver the solution to them.
      * Can the solution be easily extended to additional business units of external stakeholders
      * Training required for the application
      * Does a similar solution exist within the Enterprise and can it be customized for this need.
  + The Technical feasibility will include an analysis of:
    - * Hardware and software requirements
      * Development platform
      * Database platform
      * Connectivity between client and server
      * Software architecture (e.g. 2-tier (fat client) or n-tier (thin client with middleware) Client/Server, Web-based development
* Project Mandate
  + Each project requiring specific development (software programming) to meet a line function or staff function need will require the concurrence of the Head, IT
* Systems Design and Development
  + System design will be the responsibility of IT, but must be in line with pre-defined standards and methodologies.
  + The developers must understand the business environment and processes. Training should be provided if there is a knowledge gap

It is also important to asses existing processes and procedures that support the system in development to make sure that these are optimized.

* + At the end development, a test release plan should be produced in conjunction with the business.
  + A Technical Specification should be produced.
  + A training plan should be produced along with end user manuals and/or job cards where applicable. Refer to Appendix for complete project documentation checklist.
  + Control measures and procedures for the protection of programs and data shall be built in, tested and audited to ensure that data and programs cannot be changed (amended/updated) without authorization, destroyed or subjected to sabotage and/or espionage due to negligence or on purpose.
  + Collaboration should occur during the project between the developer and project stakeholders to reduce iterative cycle times and provide more insight into business needs and reduce the required learning curve on the side of the user.
  + Design changes should be implemented immediately, to manage the deviation and the magnitude/importance of the change.
  + All changes should be coded, tested and deployed immediately.
  + All Applications developed must go through the software quality assurance stage which must be satisfactorily tested to an acceptable level of risk (if fundamental system functionalities exist) by the testing team and approved by the Head of IT or his/her delegation before calling for UAT. Refer to Appendix A for Application code review form
  + Where a completed module can be deployed for demonstration purposes, it should be. This allows the users to interact with the application at the earliest possible opportunity.
  + When developing reports the users should be involved in the design of the reports, keep in mind that a group of users will only interact with the application via the reports. They should be self-explanatory and easy to use.
  + Except in those cases where the security features of the operating system are required as an additional measure, security for the application should be built into the application itself.
  + Facilities to update the application settings and data should be built into the application itself. All applications should be web based and centrally controlled and updated.
  + Application change control will be managed using IT change request forms to be filled in by the user, and counter-signed by the user’s line manager and coordinated through IT Department
* Commercial Off-The-Shelf Purchase (COTS)
  + COTS shall be considered to meet customer requirements after the options of in house development by the application development team or the option of contract application programming
  + In such a case IT management, will issue a tender for contract software development based on the standards set by the XXXX.
* Contract Application Programming
  + Contract Application Programming will only be considered once technology group cannot provide the application development service or are unable to deliver the service in the required time frame. And that there are no cost-effective COTS that will meet the customer needs
  + In such a case IT management, will issue a tender for contract software development based on the standards set by the XXXX.
* System / Program Testing
  + All emergency maintenance programs (e.g. backdoors) shall be removed before a system is installed. Systems shall be audited before installation and implementation.
  + System and program testing is undertaken by the application testing and quality assurance team in conjunction with selected officials of the user group.
  + No application / program / module will be released for production purposes until signed off by the Head, IT as error-free. The results of the test must be documented.
* Conversion Planning and Parallel Testing
  + Where applications / modules are to be converted, the user department and the development team will plan, agree on and document the conversion process.
  + Once conversion development is complete the development team will test the application using data copied from the live system. Where possible, parallel testing will be undertaken, but only where enough human resources exist to do so.
* Final Acceptance and Post Implementation Review
  + Following the successful deployment of an application or module, a post implementation review will be held one month after the successful deployment in order to finalize the project
  + **Step 1: Review the project performance**
* To start, we need to determine how the project performed against each of the targets defined during the Initiation phase. We should identify whether the project:
* Delivered the business benefits in the Business Case Requirement as contained in the Project Initiation Document (PID)
* Achieved the objectives specified in the Project Initiation Document (PID)
* Remained within the scope defined in the Project Initiation Document (PID)
* Produced the deliverables as contained in the Project Initiation Document (PID)
* Met the quality targets defined in the Quality Plan in the Project Initiation Document (PID)
* Completed within the planned project schedule

**Step 2: Review the project conformance**

Next, identify the extent to which the project has conformed to the following management processes initially defined:

* Time Management
* Cost Management
* Quality Management
* Change Management
* Risk Management
* Issue Management
* **Step 3: Identify project achievements**

Next, list the major achievements for the project and describe the positive effect that each achievement has had on the customer’s business.

* **Step 4: Identify project failures**

List any project failures and describe the effects they have had on the customer’s organization.

* **Step 5: Identify lessons learned**

Describe the lessons learned from undertaking this project and list any recommendations for similar projects in the future.

* All changes or alterations to the application will then be processed in line with the Change Management Policy.
* Systems Documentation.

# 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** |
| * Take a sample of software development projects and acquisitions to confirm if it follows this standard | * Check sample PID, Project risk reports, post implementation reviews. |

# 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*.

# 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

* IS department
* IT department

**Appendix A**

XXXX

Information Technology Department

**Vulnerability and Code check /review process**.

The essence of having a secure code check or reviews in any system before the codes are released into the production system is to avoid vulnerabilities. Code reviews are therefore, required to be carried out by another person other than the coder, and should consider vulnerabilities that are relevant to T24 and Info Basic.

This form should be completed during code checks or vulnerability checks.

**Reviewer:** **Reference ID: Date:**

|  |  |  |
| --- | --- | --- |
| S/NO | Description of Code areas checked | Yes/No/NA |
| 1 | Improper Restriction of Operations within the Bounds of a Memory Buffer |  |
| 2 | Improper Neutralization of Input During or if Web Page Generation is done within the codes i.e. ('Cross-site Scripting') |  |
| 3 | Improper Input Validation (unstructured routine) |  |
| 4 | Information Exposure |  |
| 5 | Out-of-bounds Read |  |
| 6 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |  |
| 7 | Use After Free |  |
| 8 | Integer Overflow or Wraparound |  |
| 9 | Cross-Site Request Forgery (CSRF) |  |
| 10 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |  |
| 11 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |  |
| 12 | Out-of-bounds Write (especially with Dimension) |  |
| 13 | Improper Authentication |  |
| 14 | NULL Pointer Dereference or Non initialization |  |
| 15 | Incorrect Permission Assignment for Critical Resource |  |
| 16 | Unrestricted Upload of File with Dangerous Type |  |
| 17 | Improper Restriction of XML External Entity Reference |  |
| 18 | Improper Control of Generation of Code ('Code Injection') |  |
| 19 | Any use of Hard-coded Credentials or Parameter variables |  |
| 20 | Uncontrolled Resource Consumption – File handler Routine calls |  |
| 21 | Missing Release of Resource after Effective Lifetime |  |
| 22 | Untrusted Search Path |  |
| 23 | Deserialization of Untrusted Data |  |
| 24 | Improper Privilege Management – Any assignment of Passwords |  |
| 25 | Improper Certificate Validation |  |
|  | Remarks: |  |

Code Developed By:

Code Reviewed By: