

SELCOM PAYTECH LTD
Application Development Policy





Contents

1. Overview
2. Purpose
3. Scope
4. Policy
 - A. General
 - B. Role based Access Controls
 - C. Three Tier Development Environments
 - D. Program Data Owners
 - E. Quality Assurance and production delivery
 - F. Secure Code Practices by Selcom
5. Audit Controls and Management
6. Policy compliance
7. Distribution
8. Policy Governance
9. Review and Revisions
10. References
11. Document Control
12. Appendix



1 Overview

Software development requires a consistent process for designing and implementing applications. Implementing consistent approach methodology, change management, security policies, testing procedures, delivery, and maintenance strategies is key to managing expectations and costs associated with custom application development.

2 Purpose

This policy describes the requirements for developing, implementing, acquiring, and managing a software development life cycle within Selcom. Application development methodologies ensure that software will be adequately documented and tested before it is used for critical business processes and storing of information and which is in line with Other policies at Selcom. Doing this requires a standardized set of activities and tasks that staff use to assure process and deliverable quality.

3 Scope


This policy applies to all Selcom staff that create, deploy, or support application and system utility software.

4 Policy

A. GENERAL

Regardless of the software development methodology used (waterfall or agile), all methodologies have similar activities associated with successful execution. HQ software development shall be responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC) for their organization. All software developed in-house which runs on production systems shall be developed according to the established processes and procedures of the Selcom SDLC. At a minimum, SDLC activities and tasks should address the following ten activity areas:

- Project Initiation/Definition
- Risk Assessment
- Functional User Requirements
- Technical and Architectural Systems Design
- System Programming or Customized Off the Shelf (COTS) Software Development/Acquisition
- Quality Assurance
- Documentation and Training
- Systems Testing and Acceptance
- Installation
- Maintenance



Selcom Software Development department shall have the flexibility to determine the means and details of methodology implementation with the provision that whatever development and delivery mechanism chosen addresses each of the major project elements listed above, is consistent, and is applied across the Selcom.

B. ROLE BASED ACCESS CONTROLS

All Custom off the Shelf (“COTS”) and custom application production systems must have a role-based access control system to restrict system access privileges to users. Systems shall have designated access control administrators who manage system wide privileges for user roles. Should the access control administrator also be a regular user of the system, they shall have two role-based accounts – one for administrative access and one for user-based access.

C. THREE TIER DEVELOPMENT ENVIRONMENTS

There shall be a separation between non-production and production application environments to reduce the risks of unauthorized access or changes and aid in supporting methodology execution. The three operational environments are as follows:

Development – The development environment is predominantly accessed by application programmers creating and testing new functionality, functional enhancements, and bug fixes. Developers have full control over this environment and it is not considered to be a “stable” code platform as active development is occurring within the logical instance. Once enhancements have been unit tested and certified for quality assurance, they are moved in a stable testing environment. The following policy and procedure apply to the development environment:

- Software development staff shall not be permitted to have access to production systems and related data unless they are triaging a production outage
- Development systems must not contain sensitive or confidential information and shall be populated with test or dummy data
- Access to program source code shall be restricted to authorized personnel and managed using enterprise configuration management and versioning software.




Test –

This environment more closely mimics the production environment. Quality assurance and user acceptance test personnel operate in this environment to test enhancements and bug fixes scheduled for release into production. The environment is continually refreshed with test data and new functionality until such point the release is deemed stable and ready for promotion into production.

The following policy and procedure apply to the test environment prior to applications being promoted to production:

- Application-program-based access paths other than the production access paths must be deleted or disabled
- Software debugging code must be removed
- Test User IDs and passwords must be removed
- All pre-production code shall be reviewed and certified prior to release to identify any potential coding vulnerability. The following procedures shall be followed:
 - Code changes shall be reviewed by individual's other than the originating code author and by individuals knowledgeable about code-review techniques and secure coding practices
 - Results of testing are reviewed and approved by the Compliance Unit and Software Development Team prior to release
 - The requirement for code reviews applies to all custom code (both internal and public facing), as part of the change management promotion process
 - Code reviews and use-case tests shall be conducted by knowledgeable internal personnel or third parties
 - Public facing web applications are also subject to additional controls to address on-going threats and vulnerabilities after implementation
 - Development and systems staff will move programs from development into production on a structured release schedule communicated to users and approved by Selcom management
 - Software developers shall not be permitted to move programs into the production environment directly unless expressly authorized by the CEO or Head of Software Development Department or their designee

Production –



This is the operational environment for the current release of the application. The production environment is subject to stringent change management processes and procedures to limit risk and functional downtime to systems.

This system architecture and infrastructure ensures that security and stability is rigorously maintained for the production system while development and test environments maximize software development productivity.

D. PROGRAM DATA OWNERS

All production systems must have designated program Data Owners and Data Custodians for critical information they process and act on. Program owners ultimately control the release of new software into production based on testing results. The following applies to program Data Owners:


- Acceptance signoff is required to promote pre-release test code into production
- Test results shall be reviewed and provide prior written approval prior to moving new software or software updates into production
- Data owners shall also review and approve data migrations or system integrations from one application system to another



E. QUALITY ASSURANCE AND PRODUCTION DELIVERY

Managing the quality of the delivery methodology is key to the success of application development execution. The following procedures shall be implemented related to software delivery:

- The development of all software shall be supervised and monitored by Selcom management and shall include security requirements, periodic independent security review of the environment, certified security training for software developers, and ad-hoc code reviews
- Applications shall be securely designed, coded, and maintained in accordance with industry accepted security standards and comply with applicable statutory, regulatory, legal and business requirements
- Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data
- Quality assurance procedures shall include systematic monitoring and evaluation of software developed, outsourced, or acquired by Selcom
- Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established and documented
- Tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security
- Test data shall be carefully selected, protected, and controlled
- Management shall have a clear oversight capacity in the quality testing process with the final product being certified as fit for its desired purpose
- Procedures shall control the risks related to production software and hardware changes that may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications. This includes the following:
 - Separate three-tiered operational environments shall exist with enforced accesses controls
 - Discrete separation of responsibilities shall exist between development, test, and production environments
 - Production data shall not be used for testing or development purposes
 - Processes shall exist for the removal of test data and accounts before production systems become active (where appropriate)
- Change control procedures shall exist for security patches and software modifications including:

- 
- Change Impact Documentation
 - Authorized Change Approvals
 - Pre-Release functional testing to verify that the change does not adversely impact system security
 - Roll-back procedures

F. Secure Code Practice by Selcom

- All source codes are encrypted once deployed at client end.
- Use of SSL for Traffic between systems
- HTTPS protocol for any payment channel and portals
- User of Certificate for Signing into Systems
- Password Checks such as complexity and wrong attempts to Coding systems
- Code Management for version controls
- Log Management for any changes done
- Change Management for any changes on system level or code level

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the Selcom internal application development and release methodology. Examples of appropriate controls and management include:

- Evidence of software development methodology process artifacts across multiple project implementations
- Demonstrated change management processes and procedures
- Evidence of physical three-tier delivery environments
- Well documented access control strategies for three-tier environment
- Historical evidence of sustained practice (email, logs, interviews)

6. Policy Compliance

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.



7. Distribution

This policy is to be distributed to all Selcom staff involved in custom COTS or internally developed custom applications.

8. Policy Governance

The following table identifies who within Selcom is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	CEO, Compliance Officer and Head of Technology and Software Department
Accountable	All HOD are accountable on their individual Staff access
Consulted	Internal Compliance and Technology and Software Department
Informed	All Staff Internal and External

9. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by Compliance Officer and Head of Technology and Software Department.

10. References

To other policy document

- Selcom IT Security Policy
- Selcom Physical Environmental Policy
- Selcom Privacy Policy
- Web Portal Technical Document
- Application Request Form
- Document Sign off

11. Document Control

Date	Version	Requester	Tech. Writer	Change/Review
21-06-2017	V1.0	Sameer Hirji	Mohammedjawaad Kassam	Sarah Mohamed
30--08-2017	V1.1	Deloitte/SCB	Mohammedjawaad Kassam.	Sarah Mohammed



			<i>Changes done to the document for Updating Appendix to the Document Section 12.</i> <i>Updating Document Control and Version details Section 11</i> <i>Updating Section 4 Point F for Secure Coding Practice by Selcom</i>	
15-01-2020	V1.1	Internal team	Annual Review Updated to Staff List Section 12	Sarah Mohamed

12. Appendix

Secure Code Development Team

Staff Name	Position
Rosario Arun	HOD - IT & Software Development Dept
Thomas Sambhala	Developer - IT & Software Development Dept
Makame Sheriff	Developer - IT & Software Development Dept
Mohammedjawaad Kassam	IT Compliance - IT & Software Development Dept