

SELCOM PAYTECH LTD

Communication and Operations Management Policy





Table of Contents

1.	Policy Statement	3
2.	Purpose	3
3.	Scope.....	3
4.	Definition.....	3
5.	Risks.....	3
6.	Applying the Policy.....	3
6.1.	Operational Procedures and Responsibilities	3
6.1.1.	Documented Operating Procedures.....	3
6.1.2.	Change Management Procedures	3
6.1.3.	Separation of Development, Test and Operational Facilities	4
6.2.	System Planning and Acceptance	4
6.2.1.	Capacity Planning	4
6.2.2.	System Acceptance	4
6.3.	Protection against Malicious and Mobile Code	4
6.3.1.	Patching	5
6.3.2.	Controls against Malicious and Mobile Code	5
6.3.3.	Examples of Malicious and Mobile Code.....	5
6.4.	Backups	5
6.4.1.	Information Backup	5
6.4.2.	Information Restore	5
6.5.	Storage Media Handling	5
6.5.1.	Management of Removable Media	5
6.5.2.	Disposal of Storage Media	6
6.5.3.	Security of System Documentation.....	6
6.6.	Monitoring.....	6
6.6.1.	Audit Logging for Restricted Data Services.....	6
6.6.2.	Administrator and Operator Logs	6
6.6.3.	Clock Synchronisation	6
6.7.	Network Management	7
6.7.1.	Network Controls	7
6.7.2.	Wireless Networks	7
6.8.	Systems Development and Maintenance	7
6.8.1.	Protection of System Test Data	7
6.9.	Annual Health Check	7
7.	Policy Compliance	7
8.	Policy Governance.....	8
9.	Review and Revision	8
10.	References	8
11.	Key Messages.....	8
12.	Appendix 1	8



1. Policy Statement

Selcom will ensure the protection of the IT service (including any information systems and information processing equipment used by the Selcom) against malware and malicious and mobile code. Only authorized changes will be made to the Selcom IT service (including any information systems and information processing equipment). Information leakage will be prevented by secure controls such implementing Firewalls and DLP policy over transmitting information.

2. Purpose

This policy specifies Selcom's mandatory minimum security standards for the management of:

- IT operations
- Systems development
- Change
- Day to day operations
- Operational procedures

This policy covers the key areas in day to day operations management of the Selcom's IT services. The need to implement such policy is to make sure company data is not mis-used neither stolen. Communication of the data is maintained in correct and secured format. Any changes to data or systems are recorded and can be tracked.

3. Scope

This policy applies to all Selcom Committees, Departments, Partners, Employees of the Selcom, contractual third parties and agents of the Selcom with access IT facilities and equipment when required and appropriate permission is given. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

4. Definition

This policy is applied whenever users access Selcom's IT facilities and equipment, and especially when managing, developing, configuring or maintaining IT facilities and equipment.

5. Risks

Selcom recognizes that there are risks associated with users accessing and handling information to conduct official Selcom business.

This policy aims to mitigate the following risks:

- Lack of incident management
- Data loss due un-secured transmission
- Use of external devices to transmit data
- Not using encryption technique
- Poor coding of the application which leads to hacking or application breakthrough

Non-compliance with this policy could have a significant effect on the efficient operation of the Selcom and may result in financial loss and an inability to provide necessary services to our customers.

6. Applying the Policy

6.1. Operational Procedures and Responsibilities


6.1.1. Documented Operating Procedures

Operating procedures are used in all day to day maintenance of Selcom IT systems and infrastructure to ensure the highest possible service from these assets. These operating procedures must be followed to achieve departmental activities.

6.1.2. Change Management Procedures

Changes or upgrade to the Selcom's operational systems must be controlled with a formally documented change control procedure. The change control procedure should include references as follows:

- i. Filling a Change Request from

- 
- ii. Stakeholders approval:
 - ❖ Project Owner (business development team)
 - ❖ IT team
 - ❖ Chief of Operations
 - ❖ Internal Controls & Risk
 - ❖ Executive director/Board
 - ❖ Where regulatory approval is required submit request application with BOT or relevant authority.

All significant changes to the main infrastructure (e.g. Network, Directories) need to be assessed for their impact on information security as part of the standard risk assessment.

6.1.3. Separation of Development, Test and Operational Facilities

The development and test environment is separate from the live operational environment to reduce the risk of accidental changes or unauthorized access. The environments must be segregated by the most appropriate controls including, but not limited to, the following

- Running on separate computers, domains, instances and networks.
- Different usernames and passwords.
- Duties of those able to access and test operational systems.

6.2. System Planning and Acceptance

6.2.1. Capacity Planning

All Selcom IT infrastructure components or facilities are covered by capacity planning and replacement strategies to ensure that increased power and data storage requirements can be addressed and fulfilled in a timely manner.

Key IT infrastructure components include, but are not restricted to, the following:

- File servers.
- Domain servers.
- E-mail servers.
- Web servers.
- Printers.
- Networks.
- Environmental controls including air conditioning.

6.2.2. System Acceptance

All departments must inform of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems. All new products must be purchased through CEO or Technology and Software Development Department. New information systems, product upgrades, patches and fixes must all undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve management authorization.

3rd party applications must also be monitored for service packs and patches.

Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment that duplicates the operational system.

6.3. Protection against Malicious and Mobile Code

Appropriate steps are taken to protect all Selcom IT systems, infrastructure and information against malicious code. Effective and up-to-date anti-virus software is run on all servers and PCs. Selcom staff are responsible for ensuring that they do not introduce malicious code into Selcom IT systems

Where a virus is detected on a Selcom system, the individual must raise an alert to Technology and Software Department via email or print out that will enable IT Staff to immediately fix the matter



6.3.1. Patching

All servers must have appropriate critical security patches applied as soon as they become available. All other patches must be applied as appropriate. Patches must be applied to all software on the Selcom network where appropriate. There must be a full record of which patches have been applied and when. (*refer to Selcom Vulnerability and Patch Management Controls*)

6.3.2. Controls against Malicious and Mobile Code

To prevent malicious and mobile code, appropriate access controls (e.g. administration / user rights) shall be put in place to prevent installation of software by all users.

Requests for software installation shall only be accepted where there is a clear technical verification.

Anti-malware software will be installed on appropriate points on the network and on hosts.

6.3.3. Examples of Malicious and Mobile Code

Mobile code represents newer technologies often found in web pages and emails, and includes, but is not limited to:

- ActiveX
- Java
- JavaScript
- VBScript
- Macros
- HTTPS
- HTML

6.4. Backups

6.4.1. Information Backup

Regular backups of essential business information istobe taken to ensure that the Selcom can recover from a disaster, media failure or error. An appropriate backup cycle must be used and fully documented. Any 3rd parties that store Selcom information must also be required to ensure that the information is backed up.

REFER TO BCP DOCUMENT

Full back up documentation, including a complete record of what has been backed up along with the recovery procedure, must be stored at an off-site location in addition to the copy at the main site and be readily accessible. The remote location must be sufficiently remote to avoid being affected by any disaster that takes place at the main site.

6.4.2. Information Restore

Full documentation of the recovery procedure must be created and stored. Regular restores of information from back up media must be tested to ensure the reliability of the backup media and restore process and this should comply with the agreed change management process.

Retention schedules are defined in Selcom *BCP AND DR PLAN DOCUMENT*

6.5. Storage Media Handling


Storage media includes, but is not restricted, to the following [amend list as appropriate]:

- Computer Hard Drives (both internal and external).
- CDs.
- DVDs.
- Optical Disks
- Digital Cameras.
- Backup Cassettes.

6.5.1. Management of Removable Media

Removable computer media (e.g. tapes, disks, cassettes and printed reports) must be protected to prevent damage, theft or unauthorized access.

Documented procedures must be kept for backup tapes that are removed on a regular rotation from Selcom offices. Media stores must be kept in a secure



environment. Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

6.5.2. Disposal of Storage Media

Storage media that is no longer required must be disposed of safely and securely to avoid data leakage. (*refer to Selcom Document Destruction and Retention Policy*) Any previous contents of any reusable storage media that are to be removed from the Selcom must be erased. This must be a thorough removal of all data from the storage media to avoid the potential of data leakage.

6.5.3. Security of System Documentation

System documentation must be protected from unauthorized access. This includes bespoke documentation that has been created by Technology and Software Department or any other departmental IT staff.

This does not include generic manuals that have been supplied with software). Examples of the documentation to be protected include, but are not restricted to, descriptions of:

- In-House Applications software Manual
- Documented Processes for specific department or all departments
- Documented Procedures and related diagrams and forms
- Data structures.
- Authorization details.

Effective version control should be applied to all documentation and documentation storage.

6.6. Monitoring

6.6.1. Audit Logging for Restricted Data Services

Audit logs must be kept for a minimum of six months which record exceptions and other security related events. As a log must contain the following information

- System identity.
- User ID.
- Successful/Unsuccessful login.
- Successful/Unsuccessful logoff.
- Unauthorized application access.
- Changes to system configurations.
- Use of privileged accounts (e.g. account management, policy changes, device configuration).

Access to the logs must be protected from unauthorized access that could result in recorded information being altered or deleted. System administrators must be prevented from erasing or deactivating logs of their own activity.

Where appropriate, classified data should be stored separately from non-classified data

6.6.2. Administrator and Operator Logs

Operational staff and system administrators must maintain a log of their activities.

The logs should include

- Back-up timings and details of backup
- System event start and finish times and who was involved.
- System errors (what, date, time) and corrective action taken.

The logs should be checked regularly to ensure that the correct procedures are being followed.

6.6.3. Clock Synchronisation

All computer clocks must be synchronized to the standard System time source to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation. All server to updated and sync using NTP protocol connected to AD or ntp.pool which has accurate time zone



6.7. Network Management

6.7.1. Network Controls

Connections to the Selcom network infrastructure are made in a controlled manner. Network management is critical to the provision of Selcom services and must apply the following controls:

- Operational responsibility for networks should, where possible be separate from computer operations activities.
- There must be clear responsibilities and procedures for the management of remote equipment and users *Refer to Remote Access Policy*
- Where appropriate, controls must be put in place to protect data passing over the network (e.g. encryption).

The network architecture is documented and stored with configuration settings of all the hardware and software components that make up the network. All components of the network should be recorded in an asset register.

All hosts must be security hardened to an appropriate level. Operating systems will have their network services reviewed, and those services that are not required will be disabled.

As per Deloitte Audit; SCB is require to Use of 256 bit AES encryption standard.

6.7.2. Wireless Networks

Wireless networks must apply controls to protect data passing over the network and prevent unauthorized access. Encryption must be used on the network to prevent information being intercepted. WPA2 should be applied as a minimum. Selcom uses WIFI setup for internal use only which is encrypted in terms of WIFI Signals using WPA2

6.8. Systems Development and Maintenance

6.8.1. Protection of System Test Data

If personal information is used during the development and test phase of preparing application software it must be protected and controlled and where possible depersonalized. If operational data is used controls must be used including, but not limited to, the following:

- An authorization processes.
- Removal of all operational data from the test system after use.
- Full audit trail of related activities.
- Any personal or confidential information must be protected as if it were live data.

6.9. Annual Health Check

An annual health check of all Selcom IT infrastructure systems and facilities must be undertaken by Technology and Software Department along with Compliance Unit, the tasks should be run under IT Compliance Officer every 12 months. This health check must include, but is not restricted to, the following:

- A full penetration tests.
- A network summary that will identify all IP addressable devices.
- Network analysis, including exploitable switches and gateways.
- Vulnerability analysis, including patch levels, poor passwords and services used.
- A summary report with recommendations for improvement.

7. Policy Compliance

If any user is found to have breached this policy, they may be subject to disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

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 AND HEAD OF TECHNOLOGY AND SOFTWARE DEVELOPMENT DEPT
Accountable	IT COMPLIANCE OFFICER
Consulted	3 RD PARTY (LAWYER), BUSINESS OPERATIONS AND TECH/SOFTWARE DEPT.
Informed	All Selcom Employees, All Temporary Staff and All Contractors

9. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy was implemented effective from 1st July 2017. Policy review will be undertaken by *IT Compliance Officer and other Management Staff*.

10. References

The following Selcom policy documents are directly relevant to this policy, and are referenced within this document [amend list as appropriate]:

- Remote Access Policy.
- DR Policy
- IT Security Policy

11. Key Messages

- Changes to the Selcom's operating systems must be follow the Selcom's formal change control procedure.
- Appropriate access controls shall be put in place to prevent user installation of software and to protect against malicious and mobile code.
- Regular backups of essential business information will be taken to ensure that the Selcom can recover from a disaster, media failure or error.
- Storage media must be handled, protected and disposed of with care.
- Audit logs for RESTRICTED data and services must be kept for a minimum of six months.
- Connections to the Selcom network are made in a controlled manner.
- An annual health check must be made of all Selcom IT infrastructure systems.

12. Appendix 1

Change Request Form

Project Name	<i>Name of the new/updated project</i>
Project Owner	<i>Who requested for change/upgrade</i>
Date Requested	



Change Description	<i>Detailed explanation on the project</i>
Reason for Change	<i>Justification for the change</i>
Impact	<i>Value addition, Cost impact, operational impact, systems affected, etc</i>
Proposed Action	<i>Reason for accepting or rejecting the change</i>
Projected Cost and time	
Expected Completion date	

Approvals

Name	Role	Signature	Date

13. 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 <i>- Document Control and Version Control Added</i> <i>- Use of 256 bit AES encryption standard,- This has to be updated by SCB as link provided by SCB Tanzania</i> Section 6.7.1 Network	Sarah Mohammed



			<i>Control</i>	
15-01--2020	V1.1	Kytes Consultant	Mohammedjawaad Kassam <i>Review of Policy document and Update Policy No. 6.6.3 for NTP protocol</i>	Sarah Mohammed
30-06-2022	V1.2	Sameer Hirji	Mohammedjawaad Kassam- Change management proceducers Updated Change request form	Viola Urasa/Sarah Mohammed