SELCOM PAYTECH LTD.

Physical and Environmental Policy

Table of Contents

1. Introduction

Purpose

The purpose of this procedure is to facilitate the implementation of Environmental Protectioncontrol requirements for the Physical and Environmental control. This policy and procedure provide detailed information on Selcom's policy and procedure in regarding to environmentalusage of Selcom's Physical location.

Scope

These procedures cover all Selcom information and information systems to include those usedmanaged, or operated by a contractor, another agency, or other organization on behalf of Selcom.

These procedures apply to all Selcom employees and all other users of Selcominformation and information systems that support the operation and assets of Selcom

.

Record Summary

- Camera records
- Badge issued
- Access records
- Visitor log
- Media inventory
- Media destruction

2. Procedure

Use appropriate facility entry controls to limit and monitor physical access to system

Access to Selcom Office, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.

Reviews and approves the access list and authorization credentials quarterly.

A current list of personnel with authorized access to the facility or designated area withina facility where the information system resides must be kept

Those areas within the facility officially designated as publicly accessible are exempt fromthis requirement.

Authorization credentials (e.g., badges, identification cards, and smart cards) must be issued.

- The level of access provided to everyone must not exceed the level of access required to complete the individual's job responsibilities. The level of access must bereviewed and approved.
- Keys, badges, access cards, and combinations must be issued to only thosepersonnel who require access.

- Authorizations and requirements for access must be coordinated with facility andpersonnel security managers, as required or needed.

Access lists and authorization credentials must be reviewed and approved week ly toensure the following:

- Access must be limited to only authorized personnel.
- The level of access provided to everyone must be consistent with the individual's jobresponsibilities
- Access rights must be promptly removed for terminated and transferred personnel orfor personnel no longer requiring access to the facility where the information systemresides.

Coordination must occur with human resources for Selcom employees

Coordination must occur with contract and grant management personnel for contractors andgrantees.

Physical Access to Computer Facilities and other Selcom Locations

The buildings that house Selcom comply with the following, and any future facility used must complywith this list of requirements:

- The data centre is a physically separated from all other Company offices. The facility islocated on the 8th floor of Company's headquarters building.
- The data centre is protected with physical security measures that prevent unauthorized persons from gaining access. This is done using a card access system or Biometric device
- All critical or sensitive Company information handling activities must take place in areas thatare physically secured and protected against unauthorized access, interference, and damage.
- Visitors are not allowed to access Data Centre unless Selcom Authorized staff escorts thevisitor to the Server Room and a Log Sheet must be signed
- Within the controlled perimeters of the Selcom facility, Mobile phone should not be usedunless permitted by authorized personal
- Selcom communications centres, that effect operation of Company systems is constructed toprotect against fire, water damage, vandalism, and other threats known to occur, or that are likely to occur at the involved locations.
- A secured intermediate holding area must be used for computer supplies, equipment, andother deliveries. Delivery personnel must not be able to directly access rooms containingmulti-user computer facilities.
- There must be no signs indicating the location of computer or communications centrescontaining equipment.
- Fire-rated walls surrounding computer facilities must be non-combustible and resistant to firefor at least one hour. All openings to these walls (doors, ventilation ducts, etc.) should be self-closing and likewise rated at least one hour.
- Computer facility rooms must be equipped with riot doors, fire doors, and other doorsresistant to forcible entry.
- Computer facility rooms must be equipped with automatic door closing equipment and whichset off an alarm when they have been kept open beyond a certain period.
- The data centre is always manned by at least two SELCOM people.
- SELCOM employee and visitor identification badges must always be worn.
- Unsupervised working in the data centre is not allowed.
- Removal of any information, equipment or media from the data centre is restricted, unlessauthorized (i.e. backups).

Compliance Unit in conjunction with staff sets standards for the physical environment. This standard may include such items as:

- Activities that may obscure video surveillance
- Actions that disrupt the power supply
- Network access interruptions
- Or other activity that may potentially lead to an incident.

SELCOM has backup power supplies and systems with power rectification in place. There are redundant communication links from the data centre to the Internet and these pass-through routers configured to protect andalert against unauthorized access.

Cameras are installed to monitor sensitive areas. Audits for the same activity is conducted yearly basis. Store for at least three months, unless otherwise restricted by law.

SELCOM deploys cameras in various strategic points around the head office to monitor entry and exit points and sensitive areas where cardholder data is processed. Camera data is viewed periodically by facility security personnel and stored for 3 months.

Restrict physical access to publicly accessible network jacks. Network jacks atSelcom offices are disabled unless in use. No jack is in a publicly accessible area. The SELCOM facility does not have any publicly accessiblejacks.

Restrict physical access to wireless access points, gateways, and handheld devices. Wireless systems are not authorized at Selcom unless such wireless network devices are associated with Selcom devices

Develop procedures to help all personnel easily distinguish between employees and visitors.

- All Selcom employees and vendors must wear badges in offices. These badges clearlyidentify staff and contractors. Visitors are issued temporary badges that clearly identifythem as visitors.
- SELCOM uses similar systems to determine who is an employee and who is a visitor, inaddition, SELCOM badges do not grant access, and this is done through a separate badge system.
- “Employee” refers to full-time and part-time employees, temporary employees/ personnel,and consultants who are “resident” on the Company site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

Visitor procedures

All visitors to Selcom head office must report to reception and sign in, to receive a badge before access is granted. Visitors must be admitted to Selcom premises only forspecific authorized purposes.

Authorized before entering areas where cardholder data is processed or maintained. Visitors to the data centre are not permitted to access the computerfloor unless special permission and authorization has been received from Company and SELCOM staff.

Contractors, repair personnel, telephone personnel, emergency workers and other authorized non-Company or non-SELCOM workers, who are required to enter related areas (including the computer floor), to perform authorized work must be escorted to and from that place of work by SELCOM staff. Visitors to theCompany head office may enter the areas where cardholder data can be accessed, but only if escorted by a Company employee.

Badge process

The visitor badges are for identification only and grants no access to any area. Badgesmust always be worn . Visitors are required to surrender the badge before they leave.

Visitor log

All visitors to the Selcom head office must sign the visitor log and be escorted by Companyemployee while on site. The visitor log is retained forever.

Back-ups of data centre

SELCOM performs backups of all the systems at the data centre. System backup dumps are writtento Storage Devices such as QNAP.

Media security

Computers that store cardholder data are kept at the SELCOM facility and never removed. Printingor storing of cardholder data on any media without management permission is forbidden.

Media distribution

Selcom Do not allow any Data to be transmitted physically except authorized by Compliance Unit orCEO.

Management approval

Company does not approve any removal of media from the SELCOM facility unless authorized bymanagement.

Media storage

All media of all types is strictly controlled. There is an inventory of all media types held by IT in asecure area.

Media destruction

Media destruction takes place as follows:

Media type	Destruction method
Paper	Cross-cut shredded
CD or DVD	Cross-cut shredded
Hard disk	Re-written using approved purge software
Broken hard disk	Securely stored indefinitely

3. Data Center Policy

Procedures to identify/distinguish between onsite personnel and visitors

All Selcom Staff has badges/identity cards with Photo's printed to identify their ID against the physical photo. Visitors are provided with Badges as Visitors Pass and recorded in the Log Book.Data Center can only be accessed by Selcom Staff, Visitors cannot access the Physical Data center without Selcom Staff.

Only authorized staff can perform the identification process

We have ground staff at our data center where PCI Compliant devices and deployed, who canidentify the personnel entering the data center. The data center can be accessed via Key Lockand Access Control using Finger Print or PIN Pad password. This can be configured by only Administrator.

Identify personnel authorized to access sensitive areas – revoke authorization to and/orreturn keys from such personnel upon termination

As part of company HR Policy this will is managed under Administration and HR Department, asit applies to all staff.

A visitor log to maintain a physical audit trail of visitor activity to the facility where cardholder data is stored or transmitted. Retain this log for a minimum of three months,unless otherwise restricted by law.

A Log book is in place for every visit made within the Card Holder premises. This log book is alsoused for staff accessing the area.

Procedures for physically protecting cardholder data including all media

Cardholder Data is not physically transmitted outside the premises and will be backed up within the same Data center, for Disaster Recovery and Business Continuity plan, a Cloud storage willbe implemented such as AWS.

Location of where all backup media are stored (including annual location review)

Reviews are in place for all IT Assets including Non-PCI Zone.

Policy to control how media is distributed – including to individuals

4. Policy Compliance

If any user is found to have breached this policy, they may be subject to Selcom's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken toassist in the prosecution of the offender(s). The Policy of breaching is maintained by

HR/A

dmin Department.

5. Policy Governance

The following table identifies who within Selcom is Accountable, Responsible, Informed orConsulted 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 oramendment.
- 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

6. Reviews

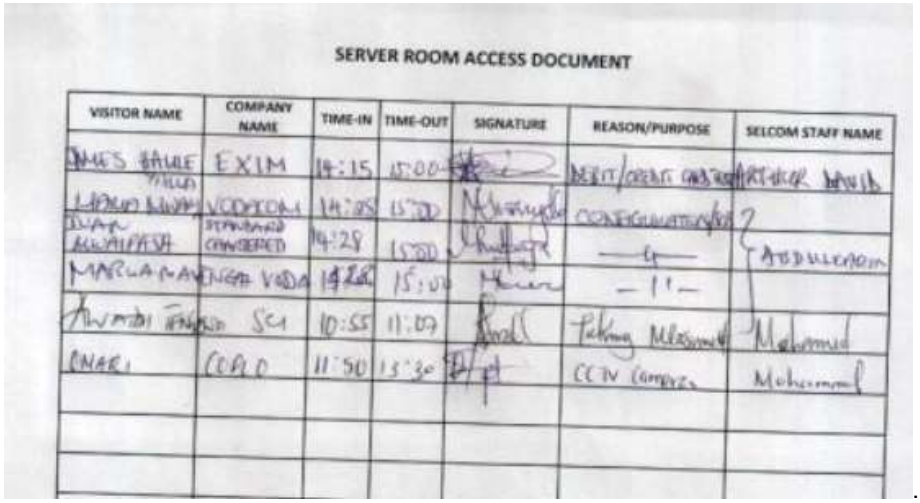
This policy will be reviewed as it is deemed appropriate, but no less frequently than every12 months. Policy review will be undertaken by Compliance Officer and Head ofTechnology and Software Department.

7. 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

8. Appendix

- Server Room Log Sheet Sample



SERVER ROOM ACCESS DOCUMENT

VISITOR NAME	COMPANY NAME	TIME-IN	TIME-OUT	SIGNATURE	REASON/PURPOSE	SELCOM STAFF NAME
[illegible]	EXIM	14:15	15:00	[signature]	[illegible]	[illegible]
[illegible]	[illegible]	14:05	15:00	[signature]	[illegible]	[illegible]
[illegible]	[illegible]	14:28	15:00	[signature]	— " —	[illegible]
[illegible]	[illegible]	[illegible]	15:00	[signature]	— " —	[illegible]
[illegible]	SCI	10:55	11:07	[signature]	Parking Measurement	Mohammed
[illegible]	COLO	11:50	13:30	[signature]	CCTV Camera	Mohammed

- Visitors Pass Sample