SELCOM PAYTECH LTD

IT SECURITY POLICY

selcom

TABLE OF CONTENTS

1. INTRODUCTION

The Information Security Policy states the types and levels of security over the information technology resources and capabilities that must be established and operated for those items to be considered secure. The information can be gathered in one or more documents. Selcom aims to secure its data from unauthorized access and protect from any data loss or leakage during the course of data transmission or stored into data storage facilities.

1.1. Purpose

This Security Policy document is aimed to define the security requirements for the proper and secure use of the Information Technology services in Selcom. Its goal is to protect Selcom and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

1.2. Scope

This document applies to all the users in Selcom, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory for this constituency.

1.3. Document Control

This section of the Security Policy is aimed to check the life time of a specific version of the whole document. In case you separate into several policy documents, ensure there is a version history for each one of them. Policies must be reviewed and eventually updated periodically to keep up with changes in risks, technologies and regulations.

Version	Description	Request By	Prepared By	Reviewed By
v1.0	IT security Policy	Sameer Hirji	Mohammedjawaad Kassam	Sarah Mohamed
v1.1	IT security Policy	SCB/Deloitte	Mohammedjawaad Kassam	Sarah Mohamed
V1.2	IT Security Policy	Kyte Consultant	Mohammedjawaad Kassam - Additional Section of PCI Requirements	Sarah Mohamed
V1.3	IT Security Policy	BOT	Mohammedjawaad Kassam - IT classification and security management System Acquisition	Viola Urasa

1.4. Responsibilities

Staff/Persons involved

Roles	Responsibilities
CEO	• Accountable for all aspects of Selcom's information
IT Compliance Officer/HOD of Technology and Software development	• Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Help in disaster recovery plans.
Information Owners	• Help with the security requirements for their specific area. • Determine the privileges and access rights to the resources within their areas.
Technology and Software Team	• Implements and operates IT security processes. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users/Staff	• Meet Security Policies. • Report any attempted security breaches.

1.5. General Policy Definitions

1. Exceptions to the policies defined in any part of this document may only be authorized by the IT Compliance Officer. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.

2. Every time a policy exception is invoked, an entry must be entered a security log specifying the date and time, description, reason for the exception and how the risk was managed. This can only be done by IT Compliance Officer or Head of Technology and Software development

3. All the IT services should be used in compliance with the technical and security requirements of the company

4. Infractions of the policies in this document may lead to disciplinary actions. In some serious cases, they could even be led to prosecution because Information is critical aspect of the company.

5. Selcom has updated their internal processes by setting up Information Security document is created to make sure policies are implemented and no breach of data should occur.

6. Selcom has implemented such process in place due to the fact it believes in Information being vital part of the organization and how critical it is to secure the same.

7. The IT Security Policy document has referred to various aspects and Selcom has implemented best practices method.

2. IT Assets Policy

2.1.1. Selcom is committed to manage the lifecycle of its IT assets and everyone has a duty of care to protect IT assets at all time whether they are in use, storage, movement or in disposal.

2.1.2. IT assets shall be protected against physical or financial loss whether by theft, mishandling or accidental damage either through primary prevention (e.g. physical security)

2.1.3. Selcom is committed to legal compliance in all regards of use and handling of IT assets. All IT assets shall be traceable and auditable throughout the entire lifecycle. Information about all IT assets shall be held in a suitable electronic database that enables them to be tracked, managed and audited throughout the entire lifecycle.

2.1.4. Finance/Admin Department works closely along with IT department to maintain required information for all Electronic items.

2.1.5. This policy shall be reviewed and updated on a regular basis to ensure that it remains appropriate due to the consequences of any relevant changes to the law, Selcom policies or contractual obligations by IT Services Management Team

2.2. Purpose

IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in Selcom.And, to monitor usage of devices and lifetime of an asset.

2.3. Scope

This policy applies to all staff who hold IT equipment purchased by Selcom. *(Note: Financial Regulations stipulate that all IT equipment must be purchased through Technology and Software Development Team with limited exceptions.)*IT equipment is currently defined as:

- All desktop, laptop and server computers and associated infrastructure;
- All monitors, printers and scanners;
- All phones, mobile and smartphones and portable computing equipment;
- Lecture Theatre and General Teaching Space equipment (projectors, microphones, cameras etc.);
- Routers, firewalls, switches, access points and other network infrastructure;
- Software licenses;
- Any other IT peripheral costing $100 or more. As IT is by nature constantly changing, other items not listed here may still be required to be included in the asset management processes.

2.4. Policy Definitions

- IT assets must only be used about the business activities they are assigned and / or authorized.All the IT assets must be classified into one of the categories in Selcom’s security categories; according to the current business function they are assigned to.
- Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
- All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the assets.

- Active desktop and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced.
- Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.
- All personnel interacting with the IT assets must have the proper training. Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.
- Access to assets at Selcom location must be restricted and properly authorized, including those accessing remotely. Company's laptops, PDAs and other equipment used at external location must be periodically checked and maintained.
- The IT Technical Teams are the sole responsible for maintaining and upgrading configurations. None other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
- Special care must be taken for protecting laptops, PDAs and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields and falls.
- When travelling by plane, portable equipment like laptops and PDAs must remain in possession of the user as hand luggage.
- Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they were stolen. Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the IT Compliance Officer.
- Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of an Information Security Team member. Assets storing sensitive information must be completely erased in the presence of an Information Security Team member before disposing.

3. Access Control Policy

This section of the Security Policy lists policies for securing access control.

3.1. Purpose

The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure in Selcom.

3.2. Scope

This policy applies to all the users in Selcom, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

3.3. Policy Definitions

- Any system that handles valuable information must be protected with a password-based access control system.
- Any system that handles confidential information must be protected by a two factor - based access control system.
- Discretionary access control list must be in place to control the access to resources for different groups of users.
- Mandatory access controls should be in place to regulate access by process operating on behalf of users.
- Access to resources should be granted on a per-group basis rather than on a per-user basis.
- Access shall be granted under the principle of “less privilege”, i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their business functions.
- Whenever possible, access should be granted to centrally defined and centrally managed identities.
- Users should refrain from trying to tamper or evade the access control in order to gain greater access than they are assigned.
- Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.

4. PASSWORD CONTROL POLICY

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Selcom's entire network. As such, all Selcom employees (including contractors and vendors with access to [agency name] systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their Password.

4.1. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change

4.2. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Selcom's facility, has access to Selcom network.

4.3. Policy Definitions

- Any system that handles valuable information must be protected with a password-based access control system. Every user must have a separate, private identity for accessing IT network services.
- Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
- Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.
- Each regular user may use the same password for no more than 90 days and no less than 3 days. The same password may not be used again for at least one year.
- Password for some special identities will not expire. In those cases, password must be at least 15 characters long.
- Use of administrative credentials for non-administrative work is discouraged. IT administrators must have two set of credentials: one for administrative work and the other for common work.
- Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
- Whenever a password is deemed compromised, it must be changed immediately. For critical applications, digital certificates and multiple factor authentication using smart cards should be used whenever possible.
- Identities must be locked if password guessing is suspected on the account.

5. INTERNET USAGE POLICY

Our employee internet usage policy outlines our guidelines for using our company's internet connection, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks for our company's legality and reputation.

5.1. Purpose

The purpose of this policy is inducing strictness that Data cannot be shared over the Internet and Internet is a tool that should not be miss-used in any way. All staff should adhere to the policy document and maintain company's rules and regulations.

5.2. Scope

This policy applies to all the users in Selcom, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

5.3. Policy Definitions

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

- Limited access to Internet is permitted for all users. The use of Messenger service is permitted for business purposes.Access to pornographic sites, hacking sites, and other risky sites is strongly discouraged/denied.
- Downloading is a privilege assigned to some users. It can be requested as a service.
- Internet access is mainly for business purpose. –some limited personal navigation is permitted if in doing so there is no perceptible consumption of Selcom system resources and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
- Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back to back configuration is strongly recommended for firewalls.
- In accessing Internet, users must behave in a way compatible with the prestige of Selcom. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
- Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the IT Compliance Officer.
- Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

6. ANTIVIRUS POLICY

This section of the Security Policy lists policies for the implementation of anti-virus and other forms of protection.

6.1. Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Selcom in terms of lost data, lost staff productivity, and/or lost reputation. As a result, one of the goals of Selcom is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by Selcom employees to help achieve effective virus detection and prevention.

6.2. Scope

This policy applies to all computers that are connected to Selcom network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to Selcom network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

6.3. Policy Definitions

- All computers and devices with access to Selcom network must have an antivirus client installed, with real-time protection.
- All servers and workstations owned by Selcom or permanently in use in Selcom facilities must have an approved, centrally managed antivirus. That also includes travelling devices that regularly connects to Selcom network or that can be managed via secure channels through Internet.
- Selcom's computers permanently working in other Selcom's network may be exempted from the previous rule if required by the Security Policies of the other Selcom, provided those computers will be protected too.
- Traveling computers from Selcom that seldom connect to Selcom network may have installed an approved antivirus independently managed.
- All the installed antivirus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
- Visitors computers and all computers that connect to Selcom's network are required to stay "healthy", i.e. with a valid, updated antivirus installed.

7. INFORMATION CLASSIFICATION & SECURITY POLICY

This section of the Security Policy defines a framework for the classification and use of the information according to the importance and risk.

7.1. Purpose

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the company's "Selcom" Data is well controlled and no information is travelled or distributed outside without knowledge to the Board.

7.2. Scope

This policy applies to all the information created, owned or managed by Selcom, including those stored in electronic or magnetic forms and those printed in paper.

7.3. Information Classification

Classification owners must classify information under their control as follows:

- Public
- Internal
- Confidential

7.4. Classification Security requirements

All information categorised as internal or confidential must be controlled with at least the below security requirements

i. Audit trail
ii. Encryption
iii. Log review
iv. Monitoring
v. Secure disposal
vi. Non Disclosure Agreement (NDA)

7.5. Third Party Management

7.5.1. Identification of risks related to external parties

i. Application manager must ensure that the security of Selcom information and information system is not compromised by introducing third party's products or services
ii. Application administrators at Selcom should follow a formal external connectivity request for any third party access connectivity to servers and information systems on Selcom's internal network
iii. Selcom administrators must immediately notify the IT Compliance Manager when they receive notification from a third party of any unauthorised access to compromise information systems.

7.5.2. Third Party Administrators

Applications administrators are responsible in ensuring that a third party administrator in their application does not compromise information systems

7.5.3. License Management

Selcom must ensure that all applications and servers are controlled in an organised manner

7.6. Policy Definitions

- Information owners must ensure the security of their information and the systems that support it. Information Security Management is responsible for ensuring the confidentiality, integrity and availability of Selcom's assets, information, data and IT services.
- Any breach must be reported immediately to the IT Compliance Officer. If needed, the appropriate countermeasures must be activated to assess and control damages.

- Information in Selcom is classified according to its security impact. The current categories are: confidential, sensitive, shareable, public and private.
- Information defined as confidential has the highest level of security. Only a limited number of persons must have access to it. Management, access and responsibilities for confidential information must be handled with special procedures defined by Information Security Management.
- Information defined as sensitive must be handled by a greater number of persons. It is needed for the daily performing of jobs duties, but should not be shared outside of the scope needed for the performing of the related function.
- Information defined as shareable can be shared outside of the limits of Selcom, for those clients, Selcom, regulators, etc. who acquire or should get access to it.
- Information defined as public can be shared as public records, e.g. content published in the company's public Web Site.
- Information deemed as private belongs to individuals who are responsible for the maintenance and backup.
- Information is classified jointly by the IT Compliance Officer and the Information Owner.

8. Remote Access Policy

Policy which outlines and defines acceptable methods of **remotely** connecting to the internal network. It is essential in large organization where networks are geographically dispersed and extend into insecure network locations such as public networks or unmanaged home networks.

8.1. Purpose

The Remote Access Policy section defines the requirements for the secure remote access to Selcom's internal resources.

8.2. Scope

This policy applies to all Selcom employees, contractors, vendors and agents with a Selcom-owned or personally-owned computer or workstation used to connect to Selcom network. This policy applies to remote access connections used to do work on behalf of Selcom, including reading or sending email and viewing intranet web resources. This policy covers all technical implementations of remote access used to connect to Selcom networks.

8.3. Policy Definitions

- To gaining access to the internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user or partner can be requested only by the Manager responsible for the information and granted by Access Management.
- Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates.
- Remote access to confidential information should not be allowed. Exception to this rule may only be authorized in cases where is strictly needed.
- Users must not connect from public computers unless the access is for viewing public content.
- All hosts that are connected to Selcom internal networks via remote access technologies must use the most up to date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement

9. Outsourcing Policy

This section of the Security Policy lists policies for the outsourcing of IT services, functions and processes.

9.1. Purpose

The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions and processes. Selcom do not consider or depend on any 3rd Party Service.All core business function is handled by Selcom In-House Team. The reason of mentioning such policy is to cater for future purposes only.

9.2. Scope

This policy applies to Selcom; the services providers to whom IT services, functions or processes are been outsourced, and the outsourcing process itself.

9.3. Policy Definitions

- Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
- Whenever possible, a bidding process should be followed to select between several service providers.
- In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
- Audits should be planned to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If Selcom has not enough knowledge and resources, a specialized company should be hired to do the auditing.
- A service contract and defined service levels must be agreed between Selcom and the service provider.
- The service provider must get authorization from Selcom if it intends to hire a third party to support the outsourced service, function or process.

10. PCI Requirement Policy

10.1. NETWORK CONFIGURATION POLICY

- The network diagram must be kept current.
- The data flow diagram must be kept current.
- Limit inbound and outbound traffic to what is needed. Include deny all rules if possible.
- Company change management policies are to be followed and documented when:
  i. making changes to network connections
  ii. making firewall and/or router configuration changes

- A firewall must:
  iii. be present at each network connection
  iv. be present between any DMZ and internal zones
  v. be present where connections to WiFiexist
  vi. make sure that internal IPs are not disclosed
  vii. have its rules reviewed at least every 6 months

- Maintain an equipment inventory using the Equipment Matrix sheets. Details to include are:
  i. Make, model and serial number (in case of POS machines)
  ii. Physical / virtual (and what technology is used)
  iii. Location (physical or on which hypervisor / cloud)
  iv. A list of protocols and ports necessary for business use
  v. A list of insecure protocols – their business justification and how they are secured

- Mobile and/or employee-owned computers with direct access to internet and connect to the company's networkshould have a personal firewall installed, actively running and cannot be altered by the user.

- Wi-Fi keys are to be changed when

i. Wi-Fi device is first installed
ii. An employee with knowledge of the key leaves the company

- Strong encryption is used throughout the company
  i. HTTPS: no use of SSLv3 and early TLS is allowed
  ii. Wi-Fi: use industry best practice (eg: 802.11i)
  iii. Certificates / keys : minimum 2048 bit, yearly expiry

10.2. System Configuration Policy

- Maintain the System Configuration Standard for all components and include:
  i. A solution to all known security vulnerabilities
  ii. Reference to industry accepted hardening standards

- Update System Configuration Standard should new vulnerabilities be identified.

- Before releasing a new server:
  i. Apply the known configuration and all updates
  ii. Disable and/or remove vendor default accounts
  iii. Change default password/s, if any
  iv. Ensure one function per server
  v. Enable only necessary services, protocols, etc…
  vi. Implement additional security for services considered insecure
  vii. Remove all unnecessary functionality, scripts, drivers, features, etc…
  viii. Fill in an Equipment Matrix for the new server

10.3. System Acquisition

10.3.1. Security in Development and Support processes

i. Change Control Procedures

- Selcom management should ensure that all changes follow change management procedures
- Infrastructure managers are responsible for ensuring that all configuration changes to the system and network devices are implemented in accordance with the change management procedures.

ii. Technical Review of application changes
Infrastructure and application managers shall ensure that when operating systems are changed or upgraded, applications are reviewed and tested to ensure there is no adverse impact on organisational operations or security.

iii. Restriction of changes to softwares
Infrastructure and application managers are responsible for ensuring that all configuration changes to software packages are implemented in accordance with change management procedures.

iv. Control of technical vulnerabilities
Compliance manager must ensure that all systems and applications undergo vulnerability assessment periodically and when major changes are introduced and that issues are remediated within the established timeframe.

10.4. Back up and Restoration

Data backup and recovery process for each system must be documented and periodically reviewed.
The data recovery process must be regularly tested to verify correctness of the backup process ensuring that the backup arrangement meets the requirements of the business continuity plans.

10.5. Segregation of Networks

Separation of development, test and production environment

i. All development and test environment must be physically or logically segregated from production environment to reduce the risk of accidental changes or unauthorised access to production.

ii. Transfer of software to production environment shall be done in a defined and controlled manner following a documented procedure.

10.6. Anti-virus Malware Policy

- Evaluate and identify evolving malware threats as part of the ongoing Risk Assessment

- For all platforms commonly affected by virus / malware, run AV/malware software and ensure that:
  i. Is actively running
  ii. Detects and removes known virus and malware
  iii. regularly updates its AV / malware definitions
  iv. regularly performs a complete system scan
  v. retains logs as per Data Retention Policy

- For all platforms not commonly affected by virus / malware, AV/malware software has not been installed because:
  i. AV / malware exposure of the platform is limited
  ii. No active browsing is conducted from these servers
  iii. Incoming / outgoing traffic is strictly controlled by firewall rules
  iv. Administrative access to the servers is restricted and on a need to use basis
  v. File integrity checking, where applicable, performs a “similar” AV detection role

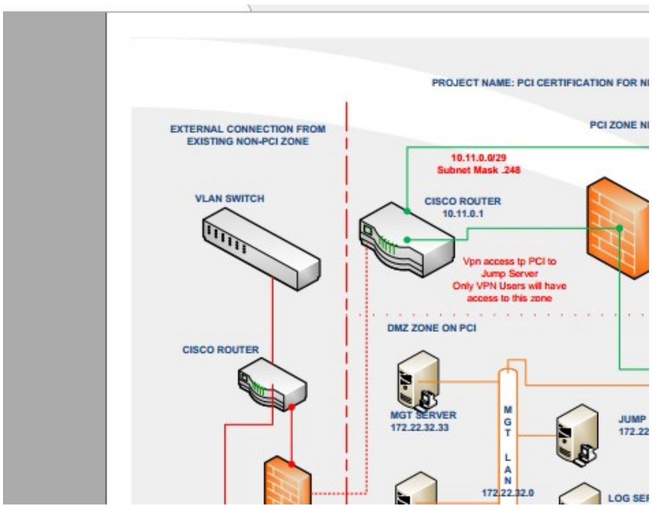
11. ANNEX

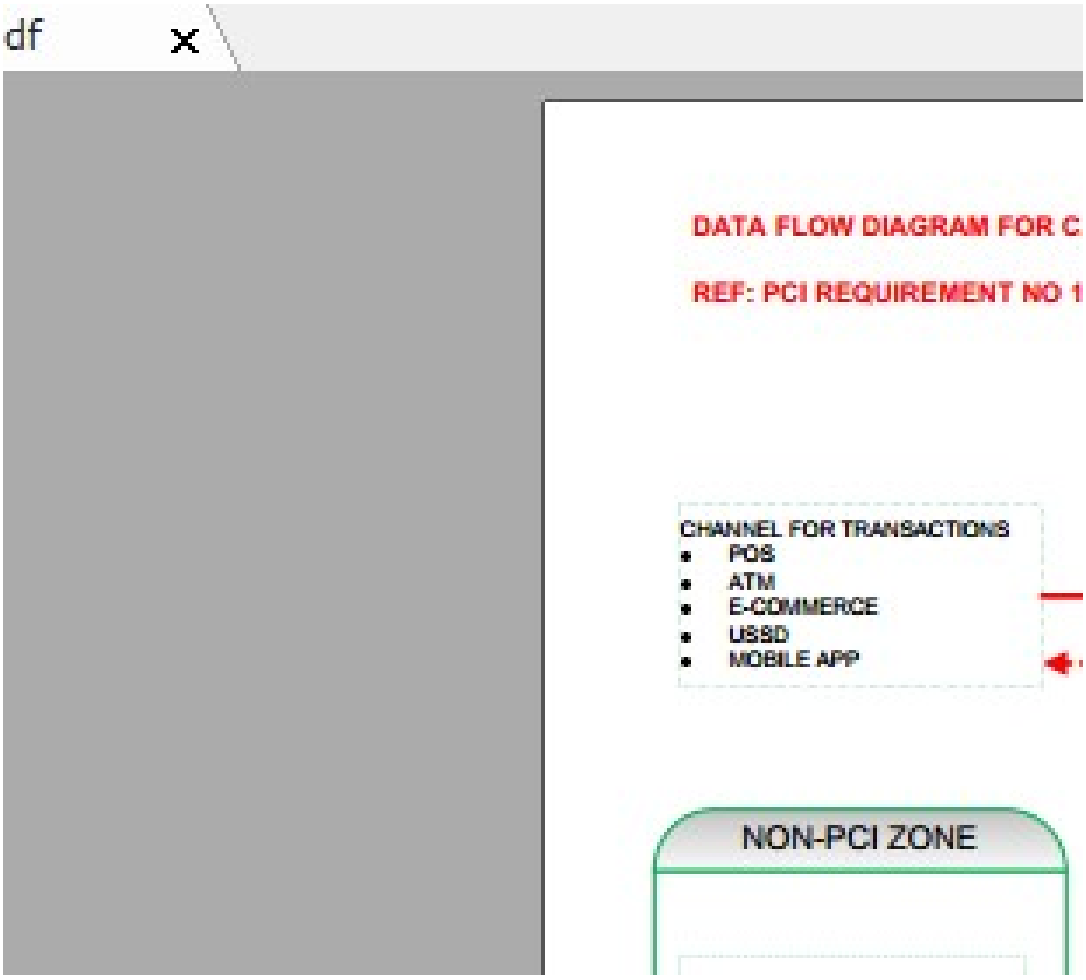
This section of the Security Policy provides the definitions of terms, acronyms, and abbreviations required to understand this document.

Term	Definition
Access Management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External Service Provider	An IT service provider that is part of a different Selcom from its customer.

Term	Definition
Identity	A unique name that is used to identify a user, person or role.
Information Security Policy	The policy that governs Selcom’s approach to information security management
Outsourcing	Using an external service provider to manage IT services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.

12. Appendix


PROJECT NAME: PCI CERTIFICATION FOR NI
EXTERNAL CONNECTION FROM EXISTING NON-PCI ZONE
PCI ZONE NI
10.11.0.0/29
Subnet Mask .248
VLAN SWITCH
CISCO ROUTER
10.11.0.1
Vpn access tp PCI to Jump Server
Only VPN Users will have access to this zone
DMZ ZONE ON PCI
CISCO ROUTER
MGT SERVER
172.22.32.33
MGT LAN
172.22.32.0
JUMP
172.22
LOG SEI


df
DATA FLOW DIAGRAM FOR C
REF: PCI REQUIREMENT NO 1
CHANNEL FOR TRANSACTIONS
• POS
• ATM
• E-COMMERCE
• USSD
• MOBILE APP
NON-PCI ZONE