Acceptable Use Policy

PCIDSSv3.2

4.2, 8.2, 8.5.10, 8.5.12, 8.5.13, 8.5.14, 8.5.15, 12.3.1, 12.3.2, 12.3.4, 12.3.8, 12.3.9, 12.3.10

ISO 27001:2013A8.1.3, A 8.3.1, A 11.2.8, A 11.2.9, A 12.6.2, A 13.2.2, A 18.2.2.

ISO 20000:2018

Date Created	08-Apr-2009
Document Author	Information Security Engineer
Document Owner	Chief Information Security Officer
Date Reviewed	07-Feb-2023
Document Classification	Internal
Next Review Date	07-Feb-2024
Document Version	7.0
Reference Number	ISW/ISMS/AUP/07/23

Document Control and Information Approval List

	Job Title	Date
Prepared by	Information Security Engineer	07-Feb-2023
Checked by	Chief Information Security Officer	07-Feb-2023
Approved by	EVP Risk & Information Security	25-Mar-2023

Revision History

Version	Date	Author	Summary of Change	Approved by	Approved Date
Version 1.0	08-Apr-2009	Information Security Engineer	First Draft	Divisional CEO	28-Apr-2009
Version 1.1	10-Mar-2009	Information Security Engineer	To meet PCIDSS requirement	Head, Information Security	19-Mar-2009
Version 1.2	09-Jun-2009	Information Security Engineer	Inclusion PAN encryption in email for PCIDSS	Head, Information Security	29-Jun-2009
Version 1.3	16-Aug-2009	Information Security Engineer	Chapter 4 sec 1 unique ID &password-Access control	Head, Information Security	27-Aug-2009
Version 1.4	19-Sep-2012	Information Security Engineer	Reviewed for completeness	Head, Information Security	30-Sep-2012
Version 2.0	16-Mar-2015	Information Security Engineer	Reviewed and inclusion of ISO 27001 implementation	Chief Information Officer Group Managing Director	04-Sep-2015
Version 2.1	7-Jun-2016	Head Information Security	Updated use of personal email and computers on the network.	Chief Information Officer Group Managing Director	15-Jun-2016
Version 2.2	12-Jun-2017	Head Information Security	Reviewed for correctness	Chief Information Officer	16-Jun-2017

Version 2.2	11-Jun-2018	Head Information Security	Reviewed for correctness	Chief Information Officer	15-Jun-2018
Version 3.0	01-Mar-2019	Head Information Security	Reviewed for correctness	Chief Information Officer	29- Mar- 2019
Version 4.0	09-Mar-2020	Head Information Security	Reviewed for correctness	Chief Risk Officer	29- Mar- 2020
Version 5.0	09-Feb-2021	Head Information Security	Reviewed for correctness	Chief Risk Officer	13- Feb- 2021
Version 6.0	05-Jan-2022	Head Information Security	Reviewed for correctness	Chief Risk Officer	04- Feb- 2022
Version 7.0	07-Feb-2023	Head Information Security	Review & Inclusion of ISMS audit corrections	EVP Risk & Information Security	25-Mar-2023

Distribution List

Department	Version	Date
Interswitch Employees	7.0	25-Mar-2023

Change Control

The contents of this document are subject to change control

Table of Contents

1.0 Summary

The acceptable use policy defines how all Interswitch's intellectual properties (tangible and non-tangible) are used solely to meet the organizations' objective. Efficient and appropriate use ensures that the organisation's IT resources, and Intellectual property are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others. Specifically, the policy details out the following:

i. The roles and responsibilities of all parties relating to this policy (Line managers, access controllers, Information security, Risk management and end users).
ii. Lists of prohibited activities
iii. List of mandatory activities
iv. Clear desk and screen
v. Information transfer
vi. Conditions of use of networking facilities
vii. Asset disposal guideline
viii. Teleworking or remote access
ix. Physical access

1.1 Objective

Interswitch's intentions for publishing an acceptable use policy are not to impose restrictions that are contrary to organization's established culture of openness, trust and integrity. Interswitch is committed to protecting its employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly. Interswitch acknowledges an obligation to ensure appropriate security for all Information, Intellectual property, equipment, and processes in its ownership and control. This obligation is shared, to varying degrees, by every member of the organisation.

2.0 Scope

This Policy fulfils PCIDSS Requirement 4.2, 8.2, .5.12, 8.5.13, 8.5.14, 8.5.15, 12.3.1, 12.3.2, 12.3.4, 12.3.8, 12.3.9, 12.3.10 and ISO/IEC 27001:2013 requirements A 8.1.3, A 8.3.2, A 11.2.8, A 11.2.9, A 12.6.2, A 13.2.2, A 18.2.2.

This policy encompasses all Interswitch employees, consultants, contractors, and vendors conducting business with Interswitch, hereinafter described as "personnel" or "authorized users". The policy applies to all intellectual properties of the organization (tangible and non- tangible).

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of Interswitch. These systems are to be used for business purposes in serving the interests of Interswitch, our clients and customers in the course of normal business operations. All electronic documents produced within the organisation remain the property of Interswitch.

3.0 Policy Statement

Interswitch is subject to the provisions of Nigerian laws, regulations, and governance requirements (including specifically requirements as pronounced from time to time by the Central Bank of Nigeria (CBN) and other regulatory bodies.

Interswitch's systems are critical for the operations of the Organization and the ability to service our customers. Interswitch's assets are intended for use for teaching, learning, research, and administration in support of the Organization's objectives. Although recognizing the increasing importance of these facilities to the activities of staff, the organization reserves the right to limit, restrict, or extend access to them. All members of staff using the assets shall be responsible for the appropriate use of the assets provided as specified by this policy and shall observe conditions and terms of usage as published by the Administrator of the system.

All electronic processing facilities provided by the organization, including e-mail, software, internet, and intranet, are business enablers and tools for productivity enhancement.

The Organization reserves the right to limit access to any or all of its electronic computing facilities to those users who have a legitimate business need and, at its discretion, to terminate the access of any user of its electronic computing facilities without notice.

This policy applies to all employees, non-permanent workers and consultants who directly or indirectly support or use the Organization's computing facilities. Contravention of this policy may lead to disciplinary action, including termination of employment.

4.0 Roles and Responsibilities

4.1 Line manager

i. Ensure that users are authorized to have access before they are granted access privileges
ii. Ensure that staff reporting to them understands the relevant policies and procedures and act in accordance with the stipulated requirements.
iii. Authorize the removal of any IT equipment, including mobile equipment, from organization premises.
iv. Act against staff whose actions deviate in any way from these policies and procedures and if required, take disciplinary action.
v. Ensure users enforce version control on documents created or updated.

4.2 Access Controllers

i. Ensure appropriate access rights is given to users and removed when not required (for example when a staff member has resigned or been transferred)
ii. Support Information security in review of access

4.3 Information Security

i. Reviews that only authorized users have access to systems
ii. Ensure periodic review of users access rights

iii. Conduct random software inventory audit on all Interswitch official laptop and desktop computers. The aim is to protect the company from exposure to liability arising from intellectual property right violation.
iv. Ensure that IT controls are properly applied to end-user computing and information.

4.4 Infrastructure Services Department

Ensure that the following are properly applied to end-user computing, namely spreadsheets and other applications used on workstation:

i. Access control including second factor authentication where necessary.
ii. Backup systems state, application, and files.
iii. Store all business-related information on the designated network file servers and not on the local drive. Lap top users must do so as soon as they have access to the designated file systems.
iv. Risk Management and Compliance group
v. Recommends permanent and temporary exceptions to this policy, for approval by the management of the organization.
vi. Manages disputes which may arise between businesses and risk due to non- compliance with this policy and relevant practices.

4.5 End Users

i. End Users entail all employees, contractors and vendors using Interswitch's intellectual properties.
ii. Users are co-responsible for the protection of information

As all electronic information including Personally Identifiable Information (PII), Card numbers or PANs, customer account numbers and other details are subject to the organization's policies on information security, end users:

i. are responsible for the availability, integrity and confidentiality of customer, employee or organization data held on their computers and all forms of storage media under their control
ii. should familiarize themselves with the content of this policy and the Corporate Information Security policy

4.5.2 Users are co-responsible for protection against malicious code

Ensure that the protective measures against malicious code (computer viruses), listed below, are implemented throughout the organization:

i. Anti-virus software provided by the Group Shared Technology (GST) department issued or supported by them. (All software received which is not issued by the GST should be regarded as possibly being infected).
ii. E-mail attachments with self-executing software programs such as files with .exe extensions (or any other file formats as may be communicated to users from time to time) may not be opened.

Users must immediately report malicious or potentially malicious codes to the Information Security unit and not use the machine until the relevant GST department gives its approval.

4.5.3 Users' responsibilities regarding access control

i. Protection of their tokens or passwords as they will be held accountable if these are disclosed to or made accessible to others. They shall not use other users' passwords
ii. Users must report any actual or suspected compromise of tokens or passwords to Information Security unit or Corporate Infrastructure unit.
iii. Safe keeping of issued access control cards and would be responsible for loss of the card

4.5.4 Users responsibility regarding equipment protection

i. Take all reasonable steps to ensure that equipment in their possession or under their control is always protected against theft, accidental or deliberate damage by others or by natural elements.
ii. Report lost, stolen or damaged IT equipment to Security Incident report module on share point.

4.5.5 Users' responsibilities regarding intellectual property and licences

i. Use only licensed software approved by the business unit or IT department as the use of illegal software can lead to disciplinary action
ii. Ensure that all use of software complies with the terms of the license, whether the usage is on hardware belonging to the organization or not
iii. Report any misuse of software within the organization to the Security incident module on share point.

4.5.6 Users' responsibilities when using e-mail, internet and intranet

i. Use the organization's communication system in a lawful, responsible and appropriate manner
ii. Ensure that all information from the intranet is for internal use only. The e-mail and intranet systems and all messages exchanged remain the property of the organization. The intranet is provided to the employees for viewing and retrieving information
iii. Be aware that the organization has the right to monitor, review, audit, intercept, access and delete all communication, including the content of all information or communications created, stored, transmitted, or received on or by its communication system in accordance with applicable local law.
iv. Be aware that internet use should be strictly for official purpose and doing otherwise will be breaching the policy.
v. Ensure that official email is used solely for official engagement and on no account should personal email be used for official purposes.

4.5.7 User Responsibilities when using the Organization's information

i. Ensure that the organization's information is used solely for official Interswitch engagement
ii. Ensure that the organization's information is used according to its classification
iii. Ensure that information is not disclosed unlawfully or in a way that contradicts the requirements of the Corporate Information Security Policy

5.0. Minimum requirements

5.1 Prohibited Activities

Computer users shall not:

i. Use, or attempt to use, any computer username and passwords which has not been allocated to the user personally or allow their computer username to be used by another person.
ii. Share their password or token with another person.
iii. Use or attempt to use any removable storage media to copy to or retrieve information from the workstations or servers.
iv. Access, or attempt to access, data/information which is not relevant to their current job
v. Bypass or attempt to bypass, or assist others to bypass security controls.
vi. Send unencrypted PANs via end-user messaging technologies, such as email, instant messaging and chat.
vii. Leave computer systems unattended and easily accessible to others.
viii. Use the organization's computer facilities for any form of unauthorized private or personal matters including the development of programs, the preparation of documents for an external organization (unless for legitimate business reasons) and gambling. They shall not use organization e-mail facilities or the Internet to access, download or distribute games, inappropriate graphics, picture files or illegal software
ix. Attach any unauthorized devices (for example modems) or mobile equipment to the organization's computing or communication infrastructure.
x. Store card holder information on local drives or network drives.
xi. Respond to chain mail or forward virus alerts on e-mail except when sending to Information Security unit for investigation or advice.
xii. Use email system for commercial purposes unless authorized by the organization.
xiii. Use the email system to send obscene, offensive or slanderous material
xiv. Use personal emails for official engagement
xv. Use personal computer/laptop to connect the organization’s network wither via VPN or directly without authorization/approval from Information security.
xvi. Steal electronic files or copying of electronic files not related to your normal business activities without management approval.
xvii. Use personal internet modems on the organization’s computer system to connect to the organization’s network without security VPN in place.
xviii. Browse the private files or accounts of others, except as provided by appropriate authority.
xix. Perform unofficial activities that may degrade the performance of information resources, such as playing online games or frivolously overload the email system (e.g. spamming and junk mail).
xx. Perform activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, and decrypt encrypted files, or compromise information security by any other means.
xxi. Write, copy, execute, or attempt to introduce any computer code e.g virus designed to self-replicate, damage, or otherwise hinder the performance of, or access to, any organization’s computer, network, or information.
xxii. Access the organization’s network via modem or other remote access service without the necessary security control (VPN).

xxiii. Promote or maintaining a personal or private business or using Organizations Service information resources for personal gain.
xxiv. Use the Organization's system to access an unauthorized wireless network connection.
xxv. Conduct fraudulent or illegal activities, including but not limited to:
gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any organization's computer.
xxvi. Conduct fundraising, lobbying, or participating in any partisan political activity except otherwise authorized.
xxvii. Stream offensive, pornographic or illegal content and/or video through the organization's network connection.
xxviii. Visit peer –to-peer or harmful sites, such as Kazaa, limewire or websites that contains sexually explicit, racist, or other potentially offensive material.
xxix. Visit social networking sites such as Facebook, twitter, Instagram and other similar web sites to divulge any information of the Organization information. Any divulge of Interswitch's information on social media site shall be explicitly approved by the Chief Marketing Officer and/or Divisional CEOs.
xxx. Engage in instant messaging such as using Yahoo, msn, Google and similar internet chat engines to divulge any sensitive or confidential information of the Organization.
xxxi. Run a virus scan on any executable file(s) received through the Internet.
xxxii. Download any program or software from the internet without authorization from GST.
xxxiii. Disclose their real names or usernames, addresses, or telephone numbers on unauthorized electronic bulletin boards, chat rooms, or other public forums reached by the Internet.
xxxiv. Unlawful or inappropriate use of e-mail. Unlawful activities include but not limited to are:
a. Fraudulent communications
b. Harassing, malicious, threatening, intimidating or abusive;
c. Sexually explicit, obscene or profane
d. Racist, hateful or encourages conduct that would constitute a criminal act or give rise to civil liability or unrest or breach of organization policies
xxxv. Defamatory, and that may affect the constitutional rights of any individual or organization or damage the reputation of the organization. This includes any communications that contain gender- specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

5.2 Mandatory Activities

Computer users must:

i. Comply with all relevant information asset protection standards, checklists and procedures
ii. Use organization authorized and licensed software only
iii. Maintain password confidentiality at all times
iv. Always follow instructions from the Infrastructure department to ensure that the latest patches and virus control files will be downloaded to desktop and laptop workstations
v. Use the organization's electronic communications facilities or e- mail in a lawful, responsible and appropriate manner in the best interests of the group, customers, business partners and other employees
vi. Clear all confidential printed documentation and assets from desks before leaving the office.
vii. Back up and store important records and programs on a regular schedule.

viii. Protect sensitive and confidential information where appropriate.
ix. Ensure all information generated (electronic or hard copy) are classified according to the Information classification policy

5.3 Clear Desk

i. Allocate time in your calendar daily to clear away your paperwork.
ii. Always clear your workspace before leaving for longer periods of time.
iii. If in doubt – keep it secure. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to keep it secured in a locked drawer or cabinet.
iv. Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office / room doors must be locked if left unattended.
v. At the end of each session, all sensitive information should be removed from the work place and stored in a locked area. This includes all employees' identifiable information, as well as business critical information such as salaries and contracts.
vi. Confidential sensitive or classified information, when printed, should be cleared from printers immediately.
vii. It is good practice to lock all office areas when they are not in use.
viii. Any visit, appointment or message books should be stored in a locked area when not in use.
ix. The reception desk can be particularly vulnerable to visitors. This area should be always kept as clear as possible.
x. Personal identifiable information should not be held on the desk within reach/sight of visitors.
xi. It is also worth noting that information left on desks is also more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.
xii. Ensure all disposed sensitive information are disposed securely (shredded or degaussed).

5.4 Clear Screen

i. Interswitch laptops and desktops should not be left logged on when unattended and should be password protected.
ii. Computer screens should be angled away from the view of unauthorized persons.
iii. The Windows Security Lock should be set to activate when there is no activity for a short pre-determined period not more than 5minutes.
iv. The Windows Security Lock should be password protected for reactivation.
v. Users should log off or lock their machines (by pressing the Windows key and L) when they leave their desk.

5.5 Information Transfer

There are occasions when Interswitch needs to share confidential information with other parties. This may be for a variety of purposes including software development, software testing, transactional activities, merger & acquisition projects and joint ventures. Under such circumstances, it is important that the method by which confidential information is transferred is understood and documented and that all parties involved are fully aware of the precautions that must be taken to ensure the

confidentiality, integrity and availability of the information. All transfer of information is aligned to the Information classification.

Specifically all letters and physical documents shall be received and collated at one single point of entry which is also the point of transfer of all information. Only couriers on the approved list will be used to transfer the information. Under no circumstances should other couriers be used.

The courier should only be contacted using the telephone number detailed on the approved list. The sender will check the courier's identification, give the package to the courier personally and obtain a signature for it. The dispatch documentation should then be placed in the transmission record file as evidence of traceability. A signature must be obtained at each point in the process where the information changes hands. Where available the package should be tracked electronically.

6.0 Conditions of Use of Networking facilities

The organization reserves the right to limit permanently or restrict any user's usage of the computing and networking facilities; to copy, remove, or otherwise alter any information or system that may undermine the authorized use of the computing and networking facilities; and to do so with or without notice to the user in order to protect the integrity of the computing and networking facilities against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.

i. The organization, through authorized individuals, reserves the right to periodically check and monitor the computing and networking facilities, and reserves any other rights necessary to protect them.
ii. All communication within should be done electronically except when requested in hardcopy by client.
iii. No other Laptop or Computer system is allowed to join the network except granted access by the Systems administrator.
iv. Explicit management approval is required to use all the technologies for other reasons apart from official use.
v. All technology used must be authenticated with user ID and password or other authentication item (for example, token).
vi. All external storage must be properly scanned automatically by the anti-virus on users systems.
vii. All information must be saved on the fileserver.
viii. All devices must be labelled, all labelled devices must have identified owners, contact information and purpose.
ix. Users should always Logon to the Domain with their Login name and password. Users should always utilize password facilities according to the password policy

7.0 Asset Disposal Guidelines

All assets are to be disposed according to the guideline for disposing asset in the Information classification. The following should be adhered to:

i. Sensitive information shall be destroyed/degaussed when disposing fixed disks, floppy disks, or flash drives that contain them.
ii. Shred all hard copies of confidential information that need to be disposed of.

8.0 Teleworking or Remote Access

Interswitch allows remote access connection however the following should be adhered to while connecting remotely:

i. After a period of 5 minutes of inactivity, all remote-access sessions to technologies must automatically disconnect.
ii. Remote-access technologies used by vendors will be activated only when needed by vendors, with immediate deactivation after use. Vendors remote access
iii. Copying, moving, or storing of cardholder data onto local hard drives, and removable electronic media when accessing such data via remote-access technologies is not allowed.
iv. For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. V. All remote access privileges shall be reviewed quarterly.
v. VI. Only Interswitch computers shall be used to connect remotely to the Interswitch network except approval is obtained from top management.

9.0 Physical Access

Interswitch's physical access including the data centres and offices is managed with physical access control. All personnel issued an access card shall adhere to the following:

i. Do not share, loan or give away your access card, as it is tied to your identity, and is your responsibility. If anyone engages in any fraudulent or suspicious activity with your access card, it is you who would be held responsible.
ii. Do not piggyback. Each staff must sign in with the access control terminal at the entry point of the building when gaining access.
iii. Access to staff and resumption can be monitored form the access logs.

10.0 Violations

Violations will be reviewed on a case-by-case basis.

i. If it is determined that a user has violated one or more of the above policy statements, that user will receive a reprimand from his or her supervisor and such user will be closely monitored henceforth.
ii. If a gross violation of the above policy statements occurs, management will take immediate action. Such action may result in severe reprimand as deemed fit by management.