CORPORATE INFORMATION SECURITY POLICY	Interswitch	PCIDSS 12.1, 12.1.1, 12.1.2, 12.1.3, 12.2.a - 12.3.10. b, 12.4.a, 12.4.b, 12.5 – 12.5.5, 12.6.a -12.6.2. ISO/IEC 27001:2013 5.1, 6.2, 7.3, A.15. ISO/IEC 20000:2018 8.7.3.1

Date Created	09-Oct-08
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
Version Number	7.0
Document Reference	ISW/IMS/POL/CISP/07/23

Document Control and Information

Approval List

	Job Title	Date
Prepared by	Information Engineer Security	07-Feb-2023
Checked by	Chief Information Security Officer	16-Feb-2023
Approved by	EVP Risk & Information Security	25-Mar-2023
Approved by	Board of Directors	28-Mar-2023

Revision History

Version	Date	Author	Summary of Change	Approved by	Approved Date
Version1.0	09-Oct-2008	Information Security Engineer	First Draft	Divisional CEO	28-Oct-2008
Version1.1	21-May-2009	Information Security Engineer	To specify PCI DSS requirements	Divisional CEO	30-May-2009
Version1.2	03-Oct-2012	Information Security Engineer	Reviewed	Head, Information Security	19-Oct-2012
Version 2.0	11-Mar-2013	Information Security Engineer	Reviewed for PCI DSS compliance	Head, Information Security	23-Mar-2013
Version2.1	13-June-2014	Information Security Engineer	Reviewed for PCI DSS	Head, Information Security	28-Jun-2014
Version2.2	29-Sept-2014	Information Security Engineer	Inclusion of Prohibition of wireless access to cardholder data environment	Head, Information Security	11-Sep-2014

Version3.0	30-Mar-2015	Head, Information Security	Inclusion of Information Security objectives, methods for communicating awareness, additional responsibilities,	Head, Information Security	14-Mar-2015
Version 3.1	26-Jun-2015	Head, Information Security	Included Commitment to Continual improvement and upgraded to ISMS format	Group Managing Director	18-Sept-2015
Version 3.2	10-May-2016	Head, Information Security	Change of department details Annual review	Group Managing Director	8-Jun-2016
Version 3.2	10-May-2017	Head, Information Security	Inclusion of extra accompany policy	Chief Information Officer	19-June-2017
Version 3.2	03-May-2018	Head, Information Security	Reviewed for correctness	Chief Information Officer	07-May-2018
Version 4.0	04-Feb-2019	Head, Infrastructure Services	Updated Policy statement and ISMS Objectives	Chief Information Officer	29-Mar-2019
Version 4.1	13-March-2020	Head, Information Security	Yearly review	Chief Risk Officer	13-Mar-2020

Version 4.2	30- April 2020	Head, Information Security	Interswitch will report suspected or actual data security breach to its business partners (such as Card Schemes – Discover, Visa, etc.) and relevant regulatory agencies via email or other channels, in line with contractual and regulatory requirements. In the event where Personally Identifiable Information is affected, the data subjects and relevant Stakeholders will be notified in accordance with the Data Protection Policies.	Chief Risk Officer	04-May-2020
5.0	30- April-2021	Head, Information Security	Yearly Review	Chief Risk Officer	11-May-2021
6.0	30- April-2022	Head, Information Security	Yearly Review	Chief Risk Officer	04-May-2022
7.0	07-Feb-2023	Chief Information Security Officer	Yearly Review	EVP Risk & Information Security Board of Directors	25-Mar-2023

Distribution List

Department	Version	Date
All 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 corporate information security policy is the apex policy for Interswitch Information Security Management System (ISMS). It details out the objectives for maintaining and improving the ISMS and defines how Information Security will be set up, managed, measured and reported within Interswitch.

Specifically, the policy defines:

i. Information Security requirements and objectives
ii. Information security roles and responsibilities
iii. Acceptable usage
iv. Risk assessment
v. Information security incident reporting.
vi. Commitment to continual improvement of the ISMS

2.0 Introduction

Interswitch Limited is committed to protecting the security and privacy of information, regardless of media type in accordance with applicable laws and regulations. Information is critical and an asset for Interswitch.

3.0 Policy Statement

Interswitch Limited is committed to protecting the security and privacy of information, regardless of media type in accordance with applicable laws and regulations. Information is critical and an asset for Interswitch.

The objective of information security is to reduce the risk to Interswitch by protecting information, information systems and communications that deliver information, from failures of integrity, confidentiality, and availability, whether information is in storage, processing, or transmission. Information Security is seen as an enabler to achieve Interswitch's business strategy and objectives.

4.0 Scope

This Policy fulfils PCI DSS Requirement 12.1, 12.1.1, 12.1.2, 12.1.3, 12.3.1, 12.3.2, 12.3.4, 12.3.7, 12.3.10, 12.4, 12.5, 12.5.1, 12.6, 12.6.1a & b, 12.6.2, ISO/IEC 27001:2013 requirements: 5.1, 5.2, 6.2, 7.3, A.15 and ISO/IEC 2000:2018 requirements: 8.7.3.

This policy encompasses all Interswitch Limited's employees, consultants, contractors, and vendors conducting business with Interswitch Limited, hereinafter described as "personnel" or "authorized users". The policy applies to all information in physical and electronic format (including cloud if applicable) held by or entrusted to Interswitch throughout the information lifecycle, which includes creation, transfer, collection, storage, distribution, archiving and disposal.

Security controls shall be used regardless of:

i. The media on which information is stored (including but not limited to hard copies, hard drives, cd's, severs, databases, handheld devices, transparencies, email systems, flash drives, external drives etc.).
ii. The system that processes the information (including, but not limited to workstations, laptops, handheld devices, PDAs, servers, email systems, databases, etc.).
iii. The method by which information is transferred (including but not limited to wireless, electronically, telephone, cd's, flash drives, external disks, or other removable media, etc.)

4.1 Scope of the ISMS

To the certification within Interswitch, the Scope, Boundaries & Interfaces and Exclusions to the ISMS have been defined in the Organizational Context, Requirements and Scope.

The Management of Interswitch group is committed to ensuring:

i. All Interswitch's information security policy, standards, guidelines, and practices shall be coordinated through the Information Security team under the Risk Management Group and shall be consistent with the enterprise-wide approach in developing, implementing, and managing information systems security.
ii. All Interswitch Staff shall undergo information security awareness which will be propagated using different methods at regular intervals to enhance competence and awareness across board.
iii. That Interswitch complies to all legal and other applicable requirements to which the company subscribes to including Payment Card Industry Data Security and ISO 27001 Standard.
iv. That ISMS objectives are set, and adequate resources are provided to achieve them.

Interswitch Management acknowledges the need for continual improvement and has introduced various methods to ensure that effectiveness and continual improvement of the processes are achieved.

Interswitch Management shall ensure that the review of the Information Security Policy and related documents is performed at least on an annual basis or when significant changes occur to ensure suitability, adequacy, and effectiveness of the ISMS framework.

All Interswitch personnel are expected to comply with the Acceptable Use policy in the use of information created, stored, transmitted, or disposed of in the course of their job duties, regardless of the medium in which that information is maintained.

5.0 Information Security Requirements

A clear definition of the requirements for information security will be agreed and maintained with the business so that all ISMS activity is focused on the fulfilment of those requirements. Statutory, compliance, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements regarding the security of new or changed systems or services will be captured as part of the design stage of each project. It is a fundamental principle of Interswitch Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents

6.0 Information Security Objectives

Based on the ISMS requirements, the following objectives are set for information security:

S/N	Organization Strategy	ISMS Objectives
1	Maximize Shareholder Value by achieving Board approved EBITDA target for the Group..	□ (ISMS 01) Minimize impacts on stakeholders by protecting all (at least 80%) critical resources through a coordinated approach of management and recovery.
2	Grow All Round Market Share to ~60% by Delivering Best Value to our customers.	□ (ISMS 02) Minimize loss of revenue by ensuring 99.9% optimal uptime of critical services and product delivery.

3	Institutionalize Processes that drive Operational and Tactical excellence (yielding cost savings of ~NGN500 million).	• (ISMS 03) Maintain a robust Information Security plan that ensures 99% confidentiality, integrity, and availability of the critical assets. • (ISMS 04) 100% adherence to regulatory and legal requirements that pertain to Information security
4	A motivated & result-oriented workforce dedicated to doing the right thing, on time, every time (seen in staff engagement results of ≥ 90%).	1. (ISMS 05) Improve skill capability annually by 80% for all staff through ISMS awareness and other training enabling consistent and excellent delivery of products and services.

The success of the ISMS will be judged on its ability to meet these overall objectives.

The information security objectives are based on the clear understanding of the business objectives as defined in the Organizational Context, Requirement and Scope and the details of how they will be achieved is captured in the ISMS Metrics.

7.0 Information Security Roles and Responsibilities

Within the field of information security, there are several management roles that correspond to the areas defined within the set scope. In Interswitch, these roles are filled by an individual in each area.

Full details of the responsibilities associated with each of the roles and how they are allocated within Interswitch are given in a separate document **ISMS Roles & Responsibilities.** It is the responsibility of Human Resources to ensure that staff understand the roles they are fulfilling and that they have appropriate skills and competence to do so.

Top Management Leadership and Commitment

Commitment to information security extends to senior levels of the organisation and will be demonstrated through this ISMS Policy and the provision of appropriate resources to provide and develop the ISMS and associated controls.

Top management will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that quality objectives are being met and quality issues are identified through the audit programme and management reviews. Management Review can take several forms including departmental and other management meetings. We are committed to continual improvement through regular management review"

8.0 Information Systems and Communications Environment

Interswitch's information systems (wired and/or wireless) which include: mobile devices, operating systems, databases, applications, Internet, telecommunications, and electronic are for authorized users only. Authorized users shall have an identification code; user ID and password. Authorized users shall also have an access card assigned to them, which will be used to physically access different areas in the office. This is outlined in greater detail in the Physical Security Policy. Sharing of user IDs, access cards and passwords is strictly prohibited. User IDs may be revoked or disabled to protect the information systems at any time.

All authorized users are required to follow the requirements defined in the Acceptable Use of Systems Policy.

9.0 Education and Awareness

This policy shall be made available to all Interswitch employees through sharepoint. All new Interswitch personnel will be made aware of the importance of information security and their responsibilities during the induction program. All Interswitch personnel will receive sufficient information to meet their security responsibilities and obligations upon hire and at least annually. In addition, they will have access to necessary information regarding security efforts and news.

The Information Security Unit, in conjunction with other appropriate business/operational units, shall disseminate educational information to Interswitch personnel regarding information security issues.

10.0 Acceptable Usage

Interswitch employees and contractor will follow acceptable usage policies for employee facing technologies. Such as:

i. Authorisation by form of approval from Management/team leads will be required to use all devices at Interswitch.
ii. All users will only gain access to devices using authentication in form of username and password or other authentication items such as tokens.
iii. All devices at Interswitch will be recorded on a list, which will include the personnel authorised to use the devices.
iv. All devices will be labelled with the contact information of the owner, and purpose of the device.
v. When accessing cardholder data remotely storage of cardholder data onto local hard drives, floppy disks, or other external media is not allowed. User will not be allowed to cut and-paste or use print functions and other technologies such as imaging technology to duplicate cardholder data during remote access.

vi. If an incident occurs, the incident response plan and procedure shall be followed by all Interswitch employees. Infrastructure and Information security will handle all incidents, including appropriate units when needed.
vii. All functionalities allowed/configured on the infrastructure shall be justified to the business and approved.
viii. The use of wireless is prohibited from accessing the cardholder data environment directly.

11.0 Risk Assessment

The Risk Management department will perform an annual information security risk assessments to identify information security risk to ISMS and SMS by considering critical assets, threats, and vulnerabilities, loss of confidentiality, integrity and availability of information system and the information resource based on the Risk Management Framework, to identify information security risk by considering the potential threats to information, the information system and the information resource, and the likelihood of each threat occurring. Potential threats include the loss of the information or systems due to accident or malicious intent, loss of availability such as the system being unavailable for a period, and unknown changes to the information or system so the information is no longer reliable.

These risks will be weighed against the value of the system by evaluating the ensuing cost if each threat were to occur. Costs should be interpreted broadly to include money, resources, time, and loss of reputation among others. Information Security controls will be selected based on the level of risk assessed for each information system and according to the risk treatment plan.

Risk treatment (accepting, transferring, avoiding, and mitigating) will be based on value and following best practice of maintaining and achieving Interswitch Information Security objectives. It is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

The information security unit will also ensure that regular log reviews are conducted weekly. Review frequency shall be commensurate with the risks associated.

The Information security unit shall carryout regular log reviews for all system components. Documented security policies and procedures need to require daily review of security logs, including follow-up to exceptions.
The Information Security Risk Management Methodology outlines how the information security risk assessment is conducted.

12.0 Incident Reporting

12.1 General Security Breaches

It is the responsibility of all Interswitch personnel to be aware of an actual or suspected information security breach, as defined below, to report it immediately to their respective team leads and the Information Security team for review. A “security breach” means an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of information maintained by Interswitch and covered under this policy. This includes physical security as well as computer or information systems security breaches that involve information assets.

In the case of an information system security breach, the security Incident response procedure will be followed. The Head of Information Security and Data Protection Officer shall be notified immediately. The Information Security team will investigate of the actual or suspected breach as well as review internal procedures and controls. The Information security engineer will ensure that the incident is logged and will notify and coordinate with the impacted department or business unit, as necessary and appropriate, to remediate the breach, recover information if possible, prevent further breach and conduct a forensic investigation. In the event where Personally Identifiable Information is affected, the data subjects and relevant Stakeholders will be notified in accordance with the Data Protection Policies.

A final report of the findings will be forwarded to the Chief Risk Officer. The Head of Information Security, in consultation with the CRO, shall make recommendations to the appropriate senior manager for review and implementation and assist in implementation of such recommendations, as appropriate. Impacted departments or business units are required to implement the corrective action agreed to by the senior manager to improve departmental controls over information security.

Departments or units will not conduct their own investigation without first consulting with the Security Administrator.

Interswitch will report suspected or actual data security breach to its business partners (such as Card Schemes – Discover, Visa, etc.) and relevant regulatory agencies via email or other channels, in line with contractual and regulatory requirements.

13.0 Compliance

All Interswitch personnel shall comply with this policy, including all future information security policies and implementing procedures and amendments as appropriate. Compliance with the Interswitch's information security policies and procedures shall be monitored regularly in conjunction with the organization's monitoring of its information security program. The Information Security unit will conduct periodic internal assessments to ensure compliance with this policy.

Interswitch personnel who do not comply with the terms of the information security policy are subject to disciplinary action up to and including immediate termination of employment. Consultants and contractors will be subject to termination of their contractual agreement

14. Exemptions

Deviation from the minimum requirements of this policy shall be submitted to the Policy Owner and approved by the Risk Management Group. All exceptions to this policy shall be formally recorded, tracked, and approved by Interswitch management and communicated to relevant stakeholders. Any exceptions shall have a clear action plan and due date for the exception to be closed.

15. Commitment to Continual Improvement

Interswitch's policy regarding Continual Improvement is to:

i. Continually improve the effectiveness of the ISMS
ii. Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001:2013 standard.
iii. Achieve ISO/IEC 27001:2013 certification and maintain it on an on-going basis
iv. Increase the level of proactivity (and the stakeholder perception of proactivity) regarding information security
v. Make information security processes and controls more measurable to provide a sound basis for informed decisions
vi. Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data.

vii. Obtain ideas for improvement via regular meetings with stakeholders and document them in a Continual Improvement Plan.

viii. Review the Continual Improvement log at regular management meetings to prioritize and assess timescales and benefits.

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, incident reports, risk assessments and service reports. Once identified they will be added to the Continual Improvement log and evaluated by the responsible team.

16. References

The following documents should be read along with this policy:

i. Acceptable Use of Asset policy
ii. Information Classification policy
iii. Cyber Threat Intelligence Policy
iv. Handling Cryptographic Encrypted Data
v. Secure Software Development Standard
vi. Third party security standard
vii. Physical Security policy
viii. Application Security Checklist
ix. Information Security Roles and Responsibilities
x. Security Incident response procedure
xi. Information Security Risk Management Methodology
xii. Change Management Control Policy
xiii. Data Protection Policies [Privacy Policy, Vendor Data Privacy Policy, Event Attendants Privacy Policy, Job Applicants Privacy Policy]

Appendix 1.0

Terms	Definitions
Account	An account (user account) by which a user, system and/or service can access an IT system.
Business continuity management	The ongoing management and governance process to identify potential events and their impact on business processes and to maintain recovery plans to ensure continuity of services if these events occur.
Classification	The rating given to information assets based on value, sensitivity, criticality, legal, regulatory, risk and business requirements.
Customer	A customer (also known as a client) is the recipient of a service and/or product provided by the Organization.
Cybercrime	Cybercrime is any criminal activity using computers and the Internet.
Cryptography	Cryptography is the science concerned with the study of secret writing.

Cryptographic artefact	All applications, infrastructure, algorithms, certificates, keys, methodologies used for cryptographic operations.
Decryption	Reverse process of encryption.
Employees	Means full-time and non-full-time employees employed by the Organization.
Encryption	Encryption is the process of hiding information or making it secret. The process involves transforming information (“plaintext”) using an algorithm (“cipher”) to make it unreadable to anyone except those with special knowledge or the code (a “key”). The result of the process is encrypted information (“ciphertext”).
File-sharing	File-sharing is the sharing of information on a computer, mobile device or network. File-sharing of information can include everything from music and movies to business documents.
Information asset	This is a collective term for information and associated facilities. Includes data messages and Organization information in any form and the systems and applications associated with its creation, collection, capture, recording, processing, storage, transmission, display, disclosure, analysis and disposal.
Information owner	The individuals responsible for the security (that is, the confidentiality, integrity and availability) of the information they control.
Information security event	Identified occurrence of a system, service or network state indicating a possible breach of Information Security policy or failure of controls, or a previously unknown situation that may be security relevant.
Information security (IS) incident	An event that impacts on the confidentiality, integrity or availability of information, such as the unauthorised disclosure of sensitive information, loss or theft of computer equipment, network attacks, unauthorised access to Organization premises or improper use of email or Internet facilities.
IT system	The technology-based resources that are used to support business processes, which include: • Hardware (for example, computers, servers, storage and peripheral devices); and • Software (for example, applications installed on the hardware to access, process, store, transmit and/or retrieve data).

Information security risk	The potential that a given threat will exploit vulnerabilities of an information asset or Organization of information assets and thereby cause harm to the organisation
Information Security Management System (ISMS)	From ISO/IEC 27001, the definition of an ISMS is: “That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. Note: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources.”
Logical access	The ability to interact with IT systems through access control procedures such as identification, authentication, and authorisation, and being able to use the applications and information made available by these systems.
Management	Management refers to Senior Management roles.
Mobile device	Includes laptops, tablets, handhelds (PDA s, smart phones) and portable storage devices (flash drives and memory sticks) including cameras when this is part of the device functionality. It further extends to removable media such as CD, DVD, diskettes, and tapes.
Network	A collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.
Personal information	Means information relating to an identifiable, living, natural person and, where applicable, an identifiable, existing juristic person.
Privacy	The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
Privileged account	An account (user account) that has elevated privileges/functions.
Residual risk	The level of risk remaining after the risk treatment plan is implemented.
Risk	The potential that a given threat will exploit vulnerabilities of an information asset or Organization of information assets and thereby cause harm to the organisation.
Risk appetite	Risk appetite is the level of operational risk the Organization is willing to accept in the normal course of business in pursuit of its strategic and financial goals.
Risk tolerance	Risk tolerance is an assessment of the maximum risk the Organization is willing to sustain for short periods of time.

Risk treatment	The process of selecting and implementing measures to manage the risk.
Supporting utilities	Electricity, water, sewage, heating/ventilation and air-conditioning supplies.
Telecommute	Telecommuting refers to work undertaken at a location that reduces commuting time, inside the home or at some other remote workplace, which is facilitated through a broadband connection and computer or phone lines.
Third party / third parties	A legal entity (organization or person) that is not part of Organization that provides services or goods.
Threat	A category of possible “bad things” that can happen to an information asset. The use of the term “threat” means that the action has not yet occurred, but that the possibility of it occurring is within reason and experience (known as risk).
Vulnerability	The “windows of opportunity” that allow threats to become a reality and affect assets.