SOVEREIGN TRUST INSURANCE PLC

ICT SECURITY POLICY

This document describes the Information Security Policy of Sovereign Trust Insurance PLC.

17, ADETOKUNBO ADEMOLA STREET
VICTORIA ISLAND,
LAGOS, NIGERIA

1. INTRODUCTION

In today's world, organizations are becoming increasingly dependent upon information systems (IS) for strategic advantage, to enhance business operations, and facilitate management decision-making. The more the organizations are moving towards electronic business environment, the dependence on IS has led to a corresponding increase in the impact of IS security abuses. Thus, it is becoming increasingly difficult for organizations to maintain a satisfactory level of IS security (von Solms, 1997). The inadequate management concern for IS security is
worrisome given evidence that significant IS security abuse do occur (Zviran & Haga, 1999). Thus, the concept of IS security is responsible for the integrity and safety of system resources and activities

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 the Organization. Its goal is to protect the Organization and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.
Specifically, the purpose of this IT Security Policy is to establish a robust framework for managing information security risks, safeguarding Sovereign Trust Insurance Plc's (STI) information assets, and ensuring compliance with relevant laws, regulations, and industry standards. This policy outlines the principles, responsibilities, and standards for protecting all data, systems, and networks against unauthorized access, use, disclosure, disruption, modification, or destruction.

1.2 Scope: This policy applies to all the users in the Organization, 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.
Furthermore, this policy applies to all employees, contractors, consultants, temporary staff, and any third parties who have access to STI's information systems, data, and physical facilities, regardless of their location or the device used. It covers all information assets, including but not limited to:

- Customer data (personal, financial, health information)
- Company proprietary data (financial records, business strategies, intellectual property)
- Software applications and databases
- Hardware (servers, workstations, mobile devices, network equipment)
- Network infrastructure
- Cloud-based services and data
- Paper-based records containing sensitive information

1.3 Policy Statement: Sovereign Trust Insurance Plc is committed to protecting its information assets and maintaining the trust of its customers. Information security is an integral part of our operations and business strategy. We will implement and continuously improve an Information Security Management System (ISMS) in line with international standards, and adhere to all applicable Nigerian laws and regulations, including the Nigeria Data Protection Act (NDPA) 2023, and directives from the National Information Technology Development Agency (NITDA) and the National Insurance Commission (NAICOM).

1.4 History

Version	Description	From	To	Author
1.0	Initial version	04/02/2013	28/02/2017	ICT Department
2.0	Reviewed	01/03/2017	31/01/2023	ICT Department
3.0	Revised	01/02/2023		ICT Department

2. GOVERNANCE AND ROLES & RESPONSIBILITIES

2.1 Information Security Governance Structure:

- **Board of Directors:** Overall responsibility and oversight for information security strategy and risk management.
- **Executive Management (EXCO):** Approves policies, allocates resources, and champions information security initiatives.
- **Chief Information Officer (CIO):** Accountable for the development, implementation, maintenance, and continuous improvement of the ISMS. The CIO reports directly to the Board or EXCO.
- **IT Department:** Responsible for the technical implementation and operational management of security controls.
- **Risk Management Department:** Integrates IT security risk management into the overall enterprise risk management framework.
- **Internal Audit:** Provides independent assurance on the effectiveness of IT security controls and compliance.
- **All Employees:** Are responsible for understanding and adhering to this policy and reporting any suspected security incidents.
- **Information Security Committee (ISC):** Comprising representatives from IT, Risk, Legal, HR, and relevant business units, responsible for overseeing the ISMS, policy review, and strategic direction.

2.2 Roles and Responsibilities:

- **Chief Information Security Officer (CIO):**
  - Accountable for all aspects of the Organization's information security.
  - Responsible for the security of the IT infrastructure.
  - Develop and update IT security policies, standards, and procedures.
  - Plan against security threats, vulnerabilities, and risks.
  - Implement and maintain Security Policy documents.
  - Conduct regular risk assessments and manage identified risks.
  - Oversee security awareness training programs.
  - Ensure IT infrastructure supports Security Policies.
  - Manage security incidents and coordinate response efforts.
  - Help in disaster recovery plans.
  - Monitor compliance with internal policies and external regulations.
  - Report on the overall security posture to executive management.

- **Information Owners:**
  - Help with the security requirements for their specific area.
  - Determine the privileges and access rights to the resources within their areas.

- **IT Department / IT Security Team:**
    - Implements and operates IT security.
    - Implements the privileges and access rights to the resources.
    - Supports Security Policies.
    - Implement and maintain security technologies (firewalls, intrusion detection systems, antivirus, encryption).
    - Manage access controls, network security, and data backup/recovery.
    - Ensure timely patching and vulnerability management.
    - Provide technical support for security-related issues.

- **Human Resources:**
    - Ensure security awareness is part of employee onboarding and ongoing training.
    - Integrate security clauses into employment contracts.
    - Manage disciplinary actions for policy violations.

- **Legal Department:**
    - Ensure compliance with all relevant data protection and cybersecurity laws and regulations.
    - Review contracts with third-party vendors for security requirements.

- **Users:**
    - Meet Security Policies.
    - Report any attempted security breaches.

3. REGULATORY AND COMPLIANCE REQUIREMENTS

Sovereign Trust Insurance Plc shall comply with all applicable Nigerian laws, regulations, and industry guidelines, including but not limited to:

- **Nigeria Data Protection Act (NDPA) 2023:** Mandates the protection of personal data of Nigerian citizens. Key requirements include:
    - Lawful, fair, and transparent processing of personal data.
    - Purpose limitation for data collection.
    - Data minimization.
    - Accuracy of data.
    - Storage limitation.
    - Integrity and confidentiality (security).
    - Accountability.
    - Appointment of a Data Protection Officer (DPO) if processing significant personal data.
    - Conducting Data Protection Impact Assessments (DPIAs) for high-risk processing.
    - Implementing a data breach notification process.
    - Annual data protection audits for organizations processing over 2,000 data subjects.

- **Cybercrimes Act 2015:** Addresses various cybercrimes and mandates certain cybersecurity measures for critical national information infrastructure.

- **National Information Technology Development Agency (NITDA) Regulations:** NITDA issues guidelines and frameworks for IT governance and data protection in Nigeria, such as the Nigeria Data Protection Regulation (NDPR) 2019 (now largely superseded by NDPA 2023, but relevant interpretations may still apply) and other IT regulatory instruments.

- **National Insurance Commission (NAICOM) Directives:** NAICOM issues specific guidelines and circulars related to IT governance, cybersecurity, and data protection for the insurance industry in Nigeria. These will be strictly adhered to.

- **Central Bank of Nigeria (CBN) Regulations (where applicable):** While primarily for banks, some IT security guidelines from CBN (e.g., in areas of electronic payments, outsourcing) may serve as best practice references or be directly applicable if STI engages in specific financial services that fall under CBN's purview.

4. IT SECURITY STANDARDS AND CONTROLS

This section details the specific security standards and controls to be implemented across STI's IT environment, largely aligned with international best practices.

4.1 Information Security Management System (ISMS) - Based on International Principles:

- **Risk Assessment and Treatment:**
  - Conduct regular (at least annual) comprehensive information security risk assessments to identify, analyse, and evaluate risks to information assets, considering confidentiality, integrity, and availability impacts.
  - Implement appropriate risk treatment plans to mitigate identified risks, prioritizing those with the highest impact and likelihood, applying a recognized risk management methodology.
  - Maintain a risk register that document identified risks, their assessment, and treatment actions, including residual risks.
- **Information Security Objectives:**
  - Define clear, measurable, and time-bound information security objectives that align with business goals and risk appetite.
  - Monitor and review progress against these objectives regularly, reporting to management.
- **Continual Improvement:**
  - Establish a process for continuous monitoring, review, and improvement of the ISMS based on performance metrics, internal audits, management reviews, and external changes (e.g., new threats, technologies, regulations).

4.2 Organization of Information Security:

- **Internal Organization:**
  - Clearly define and document roles and responsibilities for information security at all levels.
  - Establish an Information Security Committee (ISC) comprising representatives from IT, Risk, Legal, HR, and relevant business units, responsible for overseeing the ISMS, policy review, and strategic direction.
  - Implement formal authorization processes for new information systems, major changes to existing ones, and new information processing activities.

- **Mobile Devices and Teleworking:**
    - Implement a robust Mobile Device Management (MDM) or Unified Endpoint Management (UEM) solution for all company-issued and approved personal devices (BYOD) accessing corporate resources.
    - Enforce strong authentication, data encryption, remote wipe capabilities, and application control on mobile devices.
    - Establish clear policies and guidelines for secure teleworking, covering acceptable use of personal devices, network access (VPN), data storage, and physical security of remote work environments.
    - Ensure secure configuration of home networks for teleworking staff.

4.3 Human Resource Security:

- **Prior to Employment:**
    - Conduct thorough background checks (e.g., identity verification, criminal records, professional references) for all new employees and contractors who will have access to sensitive information, in accordance with applicable laws.
    - Ensure all employees and contractors sign non-disclosure agreements (NDAs) and acknowledge understanding of their security responsibilities.

- **During Employment:**
    - Provide mandatory information security awareness training to all employees and contractors upon joining and annually thereafter, covering policy updates, current threats (e.g., phishing, social engineering), and best practices.
    - Ensure employees understand their roles and responsibilities regarding information security and data protection.
    - Implement a formal disciplinary procedure for security policy violations, clearly communicated and consistently applied.

- **Termination or Change of Employment:**
    - Implement a formal and documented process for revoking all access rights (physical and logical) and retrieving all company assets (laptops, mobile devices, ID cards) upon employee termination, resignation, or significant role change.
    - Conduct exit interviews that include a review of security responsibilities.

4.4 Asset Management:

- **Inventory of Assets:** Maintain an accurate and up-to-date inventory of all information assets, including hardware (desktops, laptops, printers and other equipment), software applications, databases, information (data types), and services. Asset owners shall be assigned.

- **Information Classification:**
    - Implement a formal information classification scheme based on sensitivity and criticality (e.g., Public, Internal, Confidential, Restricted/Highly Confidential). The current categories are confidential, sensitive, shareable, public and private. Information is classified jointly by the Information Security Officer and the Information Owner.
    - Establish clear handling, storage, retention, and access controls for each

classification level, applied consistently across all systems and media.

- **Media Handling:**
  - Establish documented procedures for the secure handling, storage, transportation, and disposal of all media (digital and physical) containing sensitive information.
  - Implement data destruction methods (e.g degaussing or secure wiping for digital media) that meet industry standards to prevent unauthorized recovery of data. 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.

4.5 Access Control:

- **User Access Management:**
  - Implement a "least privilege" and "need-to-know" principle, granting users only the minimum access necessary for their specific job functions.
  - Establish formal user registration, modification, and de-registration processes, including approvals.
  - Implement strong password policies (minimum length, complexity, history, no reuse) and enforce Multi-Factor Authentication (MFA) for all critical systems, remote access, and cloud services. Any system that handles confidential information must be protected by a two-factor-based access control system.
  - Conduct regular (at least quarterly for privileged accounts, bi-annually for others) reviews of user access rights to ensure they remain appropriate.

- **System and Application Access Control:**
  - Implement role-based access control (RBAC) where appropriate to streamline access management.
  - Log all successful and failed access attempts to critical systems and applications.
  - Ensure all users have unique user IDs; generic or shared accounts are prohibited, except under specific, approved, and auditable circumstances.
  - Access to resources should be granted on a per-group basis rather than on a per-user basis.
  - Whenever possible, access should be granted to centrally defined and centrally managed identities.

- **Privileged Access Management (PAM):**
  - Implement robust controls for privileged accounts (e.g., system administrators, database administrators, security officers).
  - Utilize a Privileged Access Management (PAM) solution to manage, monitor, and record privileged sessions, enforce just-in-time access, and automatically rotate privileged account passwords.
  - Segregate duties for administrative functions where feasible.

- **Access Control Enforcement:**
  - Users should refrain from trying to tamper or evade the access control 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.

4.6 Cryptography:

- **Encryption of Data at Rest:**
  - Encrypt all sensitive data stored on servers, databases (including backups), endpoints (laptops, mobile devices), and removable media.
  - Utilize industry-standard and strong encryption algorithms

- **Encryption of Data in Transit:**
  - Encrypt all data transmitted over public networks (e.g., VPNs for remote access, TLS/SSL for web applications).
  - Secure internal network traffic where appropriate, especially between sensitive zones.

4.7 Physical and Environmental Security:

- **Secure Areas:**
  - Implement robust physical access controls (e.g., access cards, biometric readers, locks) for data centers, server rooms, and other areas housing sensitive information assets.
  - Monitor entry and exit points with CCTV surveillance, with recordings retained for a defined period.
  - Maintain an access log for all entries into secure areas.
  - Active desktops and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced.
  - Access to assets is forbidden by non-authorized personnel.

- **Equipment Security:**
  - Secure all IT equipment (servers, networking devices, workstations) to prevent theft, unauthorized access, or tampering.
  - Implement controls to protect against power outages (UPS, generators), environmental hazards (e.g., fire detection/suppression, water leakage detection, temperature/humidity control), and unauthorized cabling.
  - 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.

- **Off-Premise Equipment:**
  - Implement policies and technical controls (e.g., full disk encryption, strong authentication, remote wipe) for laptops and other portable devices used outside the office.
  - Provide guidelines for secure use of company equipment in remote or public locations.
  - 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 are stolen.
- Losses, theft, damage, tampering or other incident related to assets that compromise security must be reported as soon as possible to the Information Security Officer.

4.8 Operations Security:

- **Operational Procedures and Responsibilities:**
  - Document and implement clear, detailed operational procedures for all IT systems and services, including system startup/shutdown, backup/restore, patch management, and incident response.
  - Segregate duties for critical operational tasks to prevent fraud and errors.

- **Protection from Malware:**
  - Deploy and maintain centralized anti-malware solutions (Endpoint Detection and Response - EDR) on all endpoints, servers, and email/web gateways.
  - Ensure regular, automated updates of anti-malware signatures and software. They must be monitored to ensure successful updating is taken place.
  - Implement proactive threat detection and prevention measures, including sandboxing and behavioural analysis.
  - Prohibit the use of unauthorized software or external media without prior scanning.
  - Visitor's computers and all computers that connect to the Organization's network are required to stay "healthy", i.e. with a valid, updated antivirus installed.

- **Backup and Recovery:**
  - Implement a comprehensive data backup strategy (e.g., 3-2-1 rule: 3 copies of data, on 2 different media, with 1 copy offsite).
  - Regularly test backup and recovery procedures (at least annually) to ensure data integrity.
  - Maintain offsite backups in a secure, environmentally controlled location with appropriate access controls.

- **Logging and Monitoring:**
  - Implement comprehensive logging for all critical systems, applications, and network devices, capturing security-relevant events (e.g., access attempts, configuration changes, system errors).
  - Centralize log management and use a Security Information and Event Management (SIEM) solution for real-time analysis, correlation, and alerting of security events.
  - Retain logs for a defined period (e.g., 1 year for operational analysis, 7 years for forensic and compliance purposes).
  - Regularly review logs for suspicious activities and indicators of compromise.

- **Control of Operational Software:**
  - Implement strict controls over the installation, modification, and use of all software, including system utilities and development tools.

- Maintain a centralized, version-controlled inventory of authorized software.
- Prohibit the use of unlicensed or unauthorized software.

- **Vulnerability Management:**
  - Conduct regular vulnerability scans (internal and external, at least quarterly) of all network devices, applications, and systems.
  - Perform periodic penetration testing (at least annually) by qualified independent third parties.
  - Establish a robust patch management program to ensure timely identification, testing, and application of security patches and updates to all systems and software.
  - Develop and implement formal remediation plans for identified vulnerabilities, prioritizing based on severity and risk.

4.9 Communications Security:

- **Network Security Management:**
  - Implement multi-layered network security controls, including firewalls, intrusion prevention/detection systems (IPS/IDS) at network perimeters and key internal segments. Back-to-back configuration is strongly recommended for firewalls.
  - Segment networks (VLANs) to isolate sensitive systems and data from less critical ones and limit the scope of potential breaches.
  - Implement secure configuration standards for all network devices (routers, switches, wireless access points).
  - Disable unnecessary ports and services.
  - Implement robust Wireless LAN security (e.g., WPA2 Enterprise or WPA3, strong authentication).
  - Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the Information Security Officer.

- **Information Transfer:**
  - Establish clear policies and procedures for the secure transfer of information both internally and externally.
  - Utilize secure protocols for data exchange (e.g., SFTP, HTTPS, secure email gateways, secure file transfer solutions).
  - Implement Data Loss Prevention (DLP) solutions to prevent unauthorized transmission of sensitive information.

- **Email Policy:**
  - All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the Organization.
  - Occasional use of personal email address on the Internet for personal purpose may be permitted if in doing so there is no perceptible consumption in the Organization system resources and the productivity of the work is not affected.
  - Use of the Organization resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the Organization business is strictly forbidden.
  - In no way may the email resources be used to reveal confidential or sensitive

information from the Organization outside the authorized recipients for this information.

- Using the email resources of the Organization for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.
- Use of the Organization email resources is maintained only to the extent and for the time is needed for performing the duties.
- When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts.
- Users must have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed appropriated.
- Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged.
- Only the Information Security Officer may approve the interception and disclosure of messages.
- Identities for accessing corporate email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the company's procedures for managing identities. Sharing of passwords is discouraged. Users should not impersonate another user.
- Outbound messages from corporate users should have approved signatures at the foot of the message.
- Attachments must be limited in size according to the specific procedures of the Organization. Whenever possible, restrictions should be automatically enforced.
- Whenever possible, the use of Digital Rights technologies is encouraged for the protection of contents.
- Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
- Security incidents must be reported and handled as soon as possible according to the Incident Management and Information Security processes. Users should not try to respond by themselves to security attacks.
- Corporate mailboxes content should be centrally stored in locations where the information can be backed up and managed according to company procedures. Purge, backup and restore must be managed according to the procedures set for the IT Continuity Management.

- **Internet Policy:**
  - 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.
  - 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

the Organization system resources, and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
    - In accessing Internet, users must behave in a way compatible with the prestige of the Organization.
    - Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
    - 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.

4.10 System Acquisition, Development, and Maintenance:

- **Security Requirements of Information Systems:**
    - Integrate security requirements into the entire System Development Life Cycle (SDLC), from initial design to deployment and retirement.
    - Conduct security reviews, threat modelling, and testing (e.g., static/dynamic code analysis, penetration testing, vulnerability assessments) at appropriate stages before deploying new systems or major changes.
- **Secure Development Policy:**
    - Establish and enforce secure coding guidelines and standards for all internal software development.
    - Ensure that third-party developed software adheres to STI's security requirements and industry best practices.
    - Provide secure coding training to developers.
- **Test Data:** Use anonymized, masked, or synthetic data for development and testing environments where possible, to prevent exposure of real sensitive data. Production data should only be used in non-production environments under strictly controlled and documented circumstances.

4.11 Supplier Relationships (Outsourcing Policy):

- **Information Security in Supplier Agreements:**
    - Include clear and comprehensive information security requirements, data protection clauses, and service level agreements (SLAs) in all contracts with third-party vendors and service providers (e.g., cloud providers, software vendors, IT support).
    - Require third parties to demonstrate adherence to STI's security standards and relevant regulations (e.g., NDPA compliance).
    - The service provider must get authorization from the Organization if it intends to hire a third party to support the outsourced service, function or process.

- **Supplier Service Delivery Management:**
    - Monitor and regularly review supplier compliance with agreed-upon security requirements through audits, reviews, and performance metrics.
    - 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 the Organization has not enough knowledge and resources, a specialized company should be hired to do the auditing.
    - Conduct due diligence and risk assessments on all new and existing critical

suppliers. 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.

4.12 Information Security Incident Management:

- **Responsibilities and Procedures:**
  - Establish a formal Information Security Incident Response Team (ISIRT) with clearly defined roles, responsibilities, and communication channels.
  - Develop and implement a comprehensive Incident Response Plan (IRP) that outlines procedures for identification, containment, eradication, recovery, post-incident analysis, and communication (internal and external, including regulatory notifications).
  - Ensure all employees know how to report suspected security incidents.

- **Learning from Incidents:**
  - Conduct post-incident reviews for all significant security incidents to identify root causes, lessons learned, and opportunities for improvement.
  - Implement corrective and preventive actions identified during post-incident analysis.
  - Maintain a detailed record of all security incidents, their resolution, and associated metrics.

4.13 Information Security Aspects of Business Continuity Management:

- **Information Security Continuity:**
  - Integrate information security requirements and considerations into the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
  - Ensure that critical information systems and data are recoverable within defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) to minimize disruption to critical business functions.
  - Regularly test BCP and DRP components involving IT systems to validate their effectiveness.
- **Redundancy:** Implement appropriate levels of redundancy for critical systems, network components, and data paths to minimize single points of failure and ensure high availability.

4.14 Compliance:

- **Compliance with Legal and Contractual Requirements:**
  - Identify, document, and maintain an up-to-date register of all applicable legal, statutory, regulatory, and contractual obligations related to information security and data protection (e.g., NDPA, NAICOM directives).
  - Regularly review compliance with these requirements through internal checks and external audits.

- **Information Security Reviews:**
  - Conduct independent internal audits of the ISMS at planned intervals (at least annually) to assess compliance with this policy, standards, and regulatory requirements.
  - Facilitate external audits by regulatory bodies or certification agencies.

- **Data Protection and Privacy:**
    - Adhere strictly to the principles of the Nigeria Data Protection Act (NDPA) 2023, ensuring that personal data is processed lawfully, fairly, and transparently.
    - Implement privacy-by-design and privacy-by-default principles in all data processing activities and system development.
    - Provide data subjects with clear, concise information about how their data is collected, used, stored, and protected, as per NDPA requirements.
    - Establish clear and accessible mechanisms for data subjects to exercise their rights (e.g., right to access, rectification, erasure, restriction of processing, data portability).
    - Appoint a Data Protection Officer (DPO) and ensure they have the necessary resources and independence to fulfill their responsibilities under the NDPA.

5. POLICY REVIEW AND ENFORCEMENT

5.1 Policy Review: This IT Security Policy shall be reviewed every 3years, or more frequently if there are significant changes to the threat landscape, business operations, organizational structure, or regulatory requirements. The CIO is responsible for initiating and coordinating this review, with approval from the Executive Management and Board of Directors.

5.2 Policy Enforcement and Disciplinary Action: Compliance with this policy is mandatory for all individuals falling within its scope. Any employee, contractor, or third party found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract, and potential legal action in accordance with applicable laws.

5.3 Exceptions: Any exceptions to this policy must be formally documented, justified with clear business rationale, undergo a thorough risk assessment, and receive explicit approval from the CIO and relevant executive management. In those cases, specific procedures may be put in place to handle request and authorization for exceptions. Every time a policy exception is invoked, an entry must be entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed. All approved exceptions will be reviewed periodically (at least annually) to ensure continued necessity and risk acceptability.

6. DEFINITIONS AND ABBREVIATIONS

- **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.
- **BCP:** Business Continuity Plan
- **CIO:** Chief Information Officer
- **CIA Triad:** Confidentiality, Integrity, and Availability (the three pillars of information security)
- **Confidentiality:** A security principle that requires that data should only be accessed by authorized people.
- **DLP:** Data Loss Prevention
- **DPO:** Data Protection Officer
- **DPIA:** Data Protection Impact Assessment
- **DRP:** Disaster Recovery Plan
- **EDR:** Endpoint Detection and Response
- **EXCO:** Executive Committee
- **External Service Provider:** An IT service provider that is part of a different organization from its customer.
- **Identity:** A unique name that is used to identify a user, person or role.
- **IPS/IDS:** Intrusion Prevention System/Intrusion Detection System
- **IRP:** Incident Response Plan
- **ISIRT:** Information Security Incident Response Team
- **ISMS:** Information Security Management System
- **MFA:** Multi-Factor Authentication
- **NAICOM:** National Insurance Commission
- **NDPA:** Nigeria Data Protection Act 2023
- **NDPR:** Nigeria Data Protection Regulation (2019)
- **NITDA:** National Information Technology Development Agency
- **NIST CSF:** National Institute of Standards and Technology Cybersecurity Framework
- **PAM:** Privileged Access Management
- **RBAC:** Role-Based Access Control
- **RPO:** Recovery Point Objective
- **RTO:** Recovery Time Objective
- **SDLC:** System Development Life Cycle
- **SFTP:** Secure File Transfer Protocol
- **SIEM:** Security Information and Event Management
- **STI:** Sovereign Trust Insurance Plc
- **TLS/SSL:** Transport Layer Security/Secure Sockets Layer
- **UEM:** Unified Endpoint Management
- **UPS:** Uninterruptible Power Supply
- **VPN:** Virtual Private Network
- **WPA2/WPA3:** Wi-Fi Protected Access (Security Protocols)