IT SECURITY POLICY

Document Reference: POL-ITS-001 **Version:** 3.0 **Effective Date:** January 1, 2025 **Review Date:** July 1, 2025 **Classification:** Confidential

---

1. PURPOSE

This policy establishes the security requirements for the use of information technology resources to protect company data, systems, and infrastructure from unauthorized access, misuse, and cyber threats in compliance with Nigerian law.

2. LEGAL FRAMEWORK

This policy is established in accordance with: - **Cybercrimes (Prohibition, Prevention, etc.) Act 2015** - Primary cybersecurity legislation - **Nigeria Data Protection Act (NDPA) 2023** - Data security requirements - **Nigeria Data Protection Regulation (NDPR) 2019** - Technical safeguards - **Evidence Act 2011** - Electronic evidence provisions - **National Cybersecurity Policy 2021** - **Central Bank of Nigeria (CBN) Risk-Based Cybersecurity Framework** (if applicable) - **Nigerian Communications Commission (NCC) Guidelines**

2.1 Key Cybercrimes Act Provisions

Offence	Penalty
Unauthorized system access (Section 6)	Up to 3 years imprisonment or ₦7 million fine
System interference (Section 8)	Up to 3 years imprisonment or ₦7 million fine
Data interference (Section 9)	Up to 3 years imprisonment or ₦7 million fine
Identity theft (Section 22)	Up to 3 years imprisonment or ₦7 million fine
Cyber fraud (Section 14)	Up to 7 years imprisonment or ₦20 million fine
Corporate liability (Section 40)	Fine up to ₦10 million

3. SCOPE

This policy applies to: - All employees, contractors, and third parties - All company-owned IT equipment and systems - Personal devices used for work (BYOD) - All data created, stored, or transmitted - Cloud services and applications

4. PASSWORD REQUIREMENTS

3.1 Password Standards

Requirement	Minimum Standard
Length	12 characters
Complexity	Uppercase, lowercase, number, special character
Expiry	Every 90 days
History	Cannot reuse last 12 passwords
Lockout	After 5 failed attempts

3.2 Password Guidelines

- Never share passwords with anyone
- Do not write passwords down
- Use unique passwords for each system
- Consider using a password manager
- Change immediately if compromised

3.3 Multi-Factor Authentication (MFA)

Required for: - Email access - VPN connections - Cloud applications - Financial systems - Remote access

4. EMAIL AND INTERNET USAGE

4.1 Acceptable Use

- Business-related communications
- Limited personal use during breaks
- Professional and respectful content
- Compliance with company policies

4.2 Prohibited Activities

- Sending confidential data to personal email
- Opening suspicious attachments
- Clicking unknown links
- Subscribing to non-work newsletters
- Downloading unauthorized software
- Streaming non-work content
- Accessing inappropriate websites
- Gambling or gaming sites
- Peer-to-peer file sharing

4.3 Email Security

- Verify sender before opening attachments
- Report phishing attempts to IT
- Encrypt sensitive information
- Do not auto-forward to external addresses
- Be cautious of urgent requests for money/data

5. DEVICE SECURITY

5.1 Company Devices

- Keep operating systems updated
- Install only approved software
- Enable automatic security updates
- Use encrypted storage
- Report loss/theft within 1 hour

5.2 Mobile Devices

- Enable screen lock (minimum 6-digit PIN)
- Enable remote wipe capability
- Do not jailbreak/root devices
- Install mobile device management (MDM)
- Disable Bluetooth when not in use

5.3 Personal Devices (BYOD)

- Register with IT department
- Install required security software
- Allow remote wipe of company data
- Keep personal and work data separate
- Agree to BYOD policy

6. NETWORK SECURITY

6.1 Office Network

- Connect only authorized devices
- Do not share WiFi passwords externally
- Report suspicious network activity
- Do not connect personal routers/hotspots

6.2 Remote Access

- Use company VPN for all remote work
- Connect only from secure networks
- Avoid public WiFi without VPN
- Log off when not actively working
- Do not save passwords in browsers

6.3 WiFi Security

- Verify network authenticity before connecting
- Prefer cellular data over public WiFi
- Disable auto-connect to open networks
- Use VPN on all non-company networks

7. DATA PROTECTION

7.1 Data Classification

Level	Description	Handling
Public	Marketing materials	Open sharing
Internal	Company procedures	Internal only
Confidential	Client data, financials	Need-to-know, encrypted
Restricted	Trade secrets, PII	Highly restricted, encrypted

7.2 Data Handling

- Encrypt confidential data in transit and at rest
- Use secure file sharing (not personal cloud)
- Shred physical documents containing sensitive data
- Clear desk policy for confidential materials
- Lock screens when leaving workstation

7.3 Data Storage

- Save files to company-approved locations only
- Do not store company data on personal devices
- Use OneDrive/SharePoint for cloud storage
- Regular backup of local files to network

8. SOFTWARE AND APPLICATIONS

8.1 Approved Software

- Only install IT-approved software
- Request new software through IT Service Desk
- Keep all software updated
- Uninstall unauthorized applications

8.2 Prohibited Software

- Pirated or unlicensed software
- Peer-to-peer file sharing applications
- Cryptocurrency mining software
- Unauthorized remote access tools
- Personal cloud storage for work data

8.3 Cloud Services

- Use only approved cloud services
- Do not create unauthorized accounts
- Enable MFA where available
- Review sharing settings regularly

9. PHYSICAL SECURITY

9.1 Office Security

- Badge in/out of secure areas
- Challenge unknown visitors
- Do not hold doors for others
- Report tailgating incidents
- Secure laptops with cable locks

9.2 Equipment Protection

- Lock devices when unattended
- Store laptops securely overnight
- Do not leave devices in vehicles
- Use privacy screens for sensitive work
- Transport devices in padded bags

10. INCIDENT RESPONSE

10.1 What to Report

- Suspicious emails or calls
- Lost or stolen devices
- Unusual system behaviour
- Potential data breaches
- Security policy violations
- Malware infections

10.2 How to Report

- Email: security@company.com
- Phone: +234 XXX XXX XXXX (24/7)
- Ticket: IT Service Desk portal
- Emergency: Contact IT Manager directly

10.3 Response Timeline

- Critical incidents: Immediate response
- High priority: Within 4 hours
- Medium priority: Within 24 hours
- Low priority: Within 72 hours

11. SOCIAL ENGINEERING AWARENESS

11.1 Common Tactics

- Phishing emails (fake urgent requests)
- Vishing (phone scams)
- Pretexting (impersonation)
- Baiting (infected USB drives)
- Tailgating (physical access)

11.2 Prevention

- Verify unexpected requests through official channels
- Never provide passwords over phone/email
- Be suspicious of urgency and threats
- Confirm identity before sharing information
- Report suspicious approaches

12. REMOTE WORK SECURITY

12.1 Home Office Requirements

- Secure home WiFi with strong password
- Separate work and personal networks if possible
- Lock doors during video calls with sensitive content
- Position screens away from windows
- Secure physical documents

12.2 Public Spaces

- Never discuss confidential matters publicly
- Use privacy screens
- Do not leave devices unattended
- Avoid sensitive work in public
- Use mobile data instead of public WiFi

13. COMPLIANCE AND MONITORING

13.1 Monitoring

The Company reserves the right to monitor: - Email communications - Internet usage - Network traffic - System access logs - Device usage

13.2 Audits

- Regular security audits conducted
- Compliance checks performed
- Vulnerability assessments
- Penetration testing

15. VIOLATIONS AND CONSEQUENCES

15.1 Disciplinary Action

Violations may result in: - Verbal warning - Written warning - Removal of access privileges - Suspension without pay - Termination of employment

15.2 Criminal Prosecution

Under the **Cybercrimes Act 2015**, serious violations may result in: - Report to Nigeria Police Force Cybercrime Unit - Report to Economic and Financial Crimes Commission (EFCC) - Criminal prosecution with imprisonment up to 7 years - Fines up to ₦20 million for individuals - Corporate liability fines up to ₦10 million

15.3 Civil Liability

Employees may be held personally liable for: - Data breaches caused by negligence (NDPA 2023) - Unauthorized disclosure of company information - Damage caused to third parties

16. TRAINING REQUIREMENTS

Training	Audience	Frequency
Security Awareness	All staff	Annual
Phishing Simulation	All staff	Quarterly
Data Handling	Data handlers	Annual
Incident Response	IT team	Bi-annual

---

17. REGULATORY CONTACTS

- **Nigeria Police Force Cybercrime Unit:** cybercrime@npf.gov.ng
- **EFCC (Cyber Fraud):** www.efcc.gov.ng
- **NITDA (Data Protection):** www.nitda.gov.ng
- **Nigerian Communications Commission:** www.ncc.gov.ng
- **Computer Emergency Response Team (ngCERT):** www.cert.gov.ng

---

IT Security Manager: [Name] **Approved by:** Chief Technology Officer **Date:** December 15, 2024

Report security concerns immediately to security@company.com