ABC GHANA Network Security Policy

Prepared by: GRC Team

Date: 29th August 2025

Field	Details
Policy Name	Network Security Policy
Policy ID	ABC-NSP-2025-V1.0
Company Name	ABC Ghana
Business Unit	Technology & Information Security
Functional Area	GRC
Effective Date	August 2025
Prepared By	GRC Team
Review/Revise	Jan 2026
Approved By	Chief Information Security Officer (CISO)

1. Acknowledgement

We would like to express my sincere gratitude to God Almighty for the successful completion of this document. Special thanks go to my dedicated team members for their collaboration and insights throughout the research and drafting process. We are deeply appreciative of our facilitator Dr. Noah Adjei-Darko, whose guidance and expertise were instrumental in shaping the direction of this work. We also want to extend our thanks to the institution Yesyoucan Cybersecure LLC. for providing the resources and academic environment necessary to undertake this project.

2. Introduction

Network security is a fundamental and critical component of ABC Ghana's operational framework. As a leading telecommunications provider in Africa, ABC's business model is fundamentally dependent on the integrity and continuity of its network infrastructure and the vast volumes of data it handles. The company's strategic vision, encapsulated in "Ambition 2025," focuses on building the largest and most valuable platform business in Africa through expansion into new digital services, FinTech solutions, and a "Network as a service" model. These emerging growth platforms are built upon a foundation of customer trust and a resilient network. A single, significant security breach could irreparably damage this trust, leading to customer churn and jeopardizing the company's long-term strategic goals. Therefore, network security is not merely a defensive measure but a core strategic enabler that ensures business continuity, protects brand reputation, and underpins the company's competitive advantage.

This Network Security Policy is designed to establish a definitive framework for safeguarding ABC's network and information assets. Its primary aim is to mitigate a wide range of cyber threats, from malicious external attacks to inadvertent internal errors. The policy outlines clear guidelines, procedures, and responsibilities to ensure a proactive and coordinated approach to security.

This policy serves as the cornerstone for ABC Ghana's security posture, working to safeguard the Confidentiality, Integrity, and Availability of all information and network assets.

The document is structured to provide a comprehensive and logical guide to network security management. It begins by defining the core purpose and scope of the policy, establishing who and what is covered. This is followed by a detailed set of policy statements, each addressing a specific domain of network security, from access control and data protection to incident response and vendor management. The report concludes by defining the operational aspects of the policy, including roles and responsibilities, enforcement mechanisms, and the crucial processes for continuous review and maintenance.

3. Purpose & Scope

The purpose of this Network Security Policy is to establish a comprehensive framework for protecting ABC Ghana's information assets from unauthorized access, use, disclosure, disruption, modification, or destruction. The policy is designed to protect the business from a broad spectrum of threats, including supply chain vulnerabilities, DDoS attacks, phishing, and insider threats.

The core objectives of this policy are aligned with the fundamental pillars of information security, ensuring:

- **Confidentiality:** The protection of sensitive information from unauthorized access, preventing its disclosure to individuals or systems that do not have the required permissions.
- **Integrity:** The preservation of information's accuracy and completeness, ensuring that data remains valid and reliable in accordance with business values.
- **Availability:** The guarantee that information and associated resources are accessible at the right time for business processes, ensuring uninterrupted service delivery to millions of customers.

The policy also serves to minimize business damage, maintain business continuity in the face of security incidents, and foster a culture of security awareness and accountability among all personnel.

Scope

This policy covers all ABC Ghana network infrastructure, systems, and data, including data centers, core switches/routers, transmission links, wireless networks, cloud services, and endpoints. It also applies to ABC mobile money platforms (e.g. Mobile Money) and any new telecom services. Related policies (e.g. Information Classification, Asset Management, Human Resources, Acceptable Use) provide detailed procedures that support these network controls.

To ensure clarity, the scope applies to both people and resources as outlined below:

CATEGORY	CATEGORY COVERED ENTITIES / ASSETS
People	Employees, Contractors, Consultants, Vendors, Temporary Staff
Systems	Servers, Databases, Applications, Cloud Platforms
Devices	Laptops, Desktops, Mobile Phones, Tablets
Data	Customer Data, Financial Records, Intellectual Property, Strategic Plans
Physical	Server Rooms, Data Centers, Communication Equipment

This policy covers:

- All ABC network devices, including routers, switches, and firewalls.
- All physical facilities, including data centers, critical infrastructure rooms (CIR), and offices.
- All servers, applications, databases, and other information processing assets, regardless of their location (on-premises or cloud-based).

- All mobile and fixed access networks, including 2G, 3G, 4G, and fiber networks.
- All corporate and employee-owned devices (BYOD) are used to access the ABC network or process company information.
- All information assets, whether in electronic, paper, or other physical forms.

4. Policy Statements

The Policy Statements form the core of ABC Ghana's Network Security Policy, setting out clear rules to safeguard information assets. They cover how data is classified and accessed, ensuring only authorized users with the least privilege and strong authentication can gain entry. They mandate strict data protection measures, compliance with legal and industry standards, and physical safeguards for critical facilities. The policy also provides structured procedures for incident response, outlines acceptable system use, and enforces security requirements for third-party vendors. Additionally, it establishes data retention timelines, mandates employee training, and ensures compliance through regular audits, altogether creating a robust framework to maintain confidentiality, integrity, and availability across ABC Ghana's network.

The following statements establish guidelines for managing, protecting, and using ABC Ghana's information assets.

4.1. Access Control

Access to ABC Ghana's network and information assets is strictly controlled to ensure that only authorized individuals and systems can access resources necessary for their designated roles. The policy is founded on the principle of least privilege, which states that a user should only have the minimum permission required to perform their assigned tasks.

4.2. Information Classification

All information assets at ABC Ghana must be classified into one of four levels of sensitivity. This classification determines the level of protection required for the data, including handling, storage, and transmission procedures. This approach ensures a consistent and risk-based security posture across the organization. The four classification levels are defined as follows:

Classification Level	Description	Examples
Public	Information intended for open use and public distribution. Its disclosure would cause no harm or risk to the organization.	Press releases, marketing materials, and publicly posted schedules.
Internal Use	Data is used exclusively within the organization. Unauthorized disclosure could result in minor damage or risk.	Internal memos, employee directories, and non-sensitive project reports.
Confidential	Sensitive data whose unauthorized access could cause significant damage to the organization's reputation or operations.	Financial records, customer lists, and strategic planning documents.
Highly Confidential / Restricted	The highest level of classification for data that, if disclosed, could lead to severe legal consequences, financial penalties, or significant damage.	Personally identifiable information (PII) such as customer names, addresses, credit card numbers, and medical records.

4.3. Access Control Principles

1. **Principle of Least Privilege**: Access to network resources will be granted on a need-to-know, need-to-do basis. All users, process, and program access will be limited to the minimum resources and privileges absolutely necessary to perform a legitimate function.
2. **Unique Credentials**: Every user, including employees, contractors, and vendors, must be assigned a unique login credential. The sharing or reuse of passwords

across multiple accounts is strictly prohibited.

3. **Multi-Factor Authentication (MFA)**: MFA is a mandatory requirement for access to all critical systems, including but not limited to, privileged accounts, administrative consoles, and remote access systems. MFA requires a user to provide at least two forms of verification (something they know, something they have, or something they are) to significantly reduce the risk of credential-based attacks like phishing and credential theft.

5. Data Protection

Data protection is a paramount concern for ABC Ghana, as the company handles vast amounts of customer, employee, and business data. The policy mandates strict security controls, including encryption, to protect this sensitive information. ABC is committed to adhering to all relevant national and international data protection laws.

Data Protection Requirement	**Description / Implementation**	**Compliance Standards**
Encrypt data at rest and in transit	All customer and business data stored on servers, databases, or mobile devices must be encrypted using AES-256 or higher. Data transmitted over networks must use secure protocols such as TLS 1.3 or VPNs.	ISO/IEC 27001 (Control A.10.1 – Cryptographic Controls), NIST SP 800-57 (Key Management Guidelines)
Protect customer personal data	Personally Identifiable Information (PII), mobile money records, and call	GDPR (Articles 5, 32), Ghana Data Protection Act, 2012 (Act 843)

	detail records (CDRs) must be collected, processed, and stored in line with legal data protection requirements.	
Limit data retention	Customer and business data must only be retained for the period required for business, legal, or regulatory purposes. Data exceeding the retention timeline must be securely deleted (digital wiping, shredding).	MTN Data Retention Policy, Act 843, ISO/IEC 27001 – A.18.1.3
Monitor and log access	All access to sensitive systems must be logged. Logs should capture who accessed what, when, and why, and must be reviewed regularly for anomalies.	ISO/IEC 27002 (Logging and Monitoring), NIST SP 800-92 (Guide to Computer Security Log Management)
Data minimization	Only collect and store the minimum amount of data needed for business operations. Avoid over-collection of customer data. GDPR	GDPR – Article 5(1c) (Data minimization principle)
Third-party data handling	Vendors and partners with access to MTN Ghana data	ISO/IEC 27036 (Information Security for

	must comply with MTN’s security requirements and undergo annual security reviews.	Supplier Relationships)

The company's security posture is built to satisfy not only the local legal requirements of Ghana's Data Protection Act but also the more stringent, extraterritorial obligations of GDPR. This layered approach is essential for a multinational corporation that processes data across different jurisdictions. By aligning with both standards, the policy guarantees a robust and consistent level of protection, which is crucial for maintaining customer trust and avoiding potential legal and financial repercussions.

6. Physical Security

Physical security measures are deployed to protect critical IT assets and facilities from unauthorized access, damage, and theft. The policy works to ensure the safety of tangible assets, which in turn safeguards the intangible data and networks they contain.

- **Restricted Access**: Access to secure areas, such as data centers and server rooms, is restricted to authorized personnel only. Access control systems (ACS) will be used to enforce entry restrictions, and all access attempts will be logged and monitored for suspicious activity.
- **Surveillance**: Video surveillance systems (VSS) will be deployed at all critical entry points and within secure facilities. The footage will be used for both deterrence and post-incident investigations.
- **Physical Hardening**: Critical facilities will employ physical hardening measures and barriers to deter unauthorized entry and intrusion. All server racks,

communication rooms, and backup storage must remain locked.

- **Protect-in-Depth**: Physical security controls will be integrated with logical network security controls to create a layered and comprehensive defense strategy, minimizing overlap and ensuring a coordinated response to threats.
- **Security Guards**: Trained personnel must provide round-the-clock physical protection.
- **Visitor Management**: Visitors must be escorted, recorded in access registers, and issued temporary badges.
- **Environmental Controls**: Fire suppression, UPS, backup generators, and climate control must be operational to prevent damage to assets.

7. Incident Response

Despite robust preventive measures, security incidents may occur. This policy mandates a clear, documented, and approved incident response (IR) plan to ensure that ABC Ghana can effectively identify, contain, and recover from security breaches.

Objectives

- Rapidly detect and contain security incidents.
- Minimize disruption to mobile and Internet services.
- Safeguard customer and company data.
- Ensure compliance with Ghana’s Cybersecurity Act, 2020 (Act 1038) and Data Protection Act, 2012 (Act 843).

7.1. Incident Classification

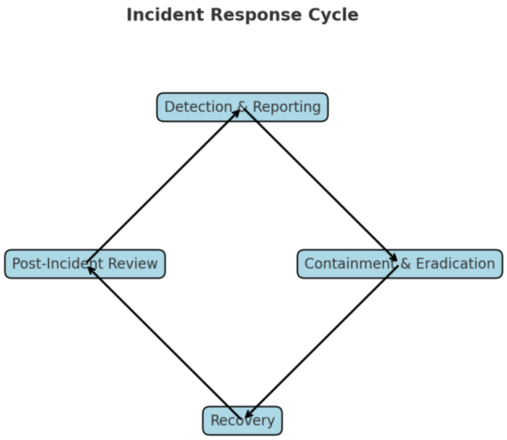
- Incidents will be classified by severity:
- Low: Spam, phishing attempts, failed logins.
- Medium: Malware infections, limited DoS.
- High: Data breach, insider misuse, major service outage.
- Critical: National-level impact, compromise of core telecom/ISP systems.

Roles & Responsibilities

- Incident Response Manager – Coordinates overall response, escalates to senior management.
- Technical Response Team – Conducts forensic analysis, containment, recovery.
- Communications Officer – Handles internal, customer, regulator, and media communication.
- Legal & Compliance Officer – Ensures reporting to National Cyber Security Centre (NCSC), Data Protection Commission (DPC), and law enforcement.

7.1. Incident Response Steps

The incident response plan follows a phased approach to ensure a coordinated and effective response. The steps are as follows:



- **Preparation**: This is the most crucial phase, involving the proactive development of the IR plan, training employees on their roles, and conducting regular mock drills to test the plan's effectiveness and identify weaknesses.
- **Identification**: This phase involves the timely detection and confirmation of a security event. The team must determine the nature of the breach, when it occurred, and its scope and impact on operations.
- **Containment**: Once identified, the primary goal is to limit the spread of the attack to prevent further damage. This may involve isolating compromised systems, quarantining malware, and changing credentials to prevent the attacker from

moving laterally within the network.

- **Eradication**: The root cause of the incident is identified and eliminated. All malicious software and artifacts are securely removed, and affected systems are patched and hardened to a trusted state.
- **Recovery**: This phase focuses on restoring affected systems and services to normal operations. Systems are restored from trusted backups and monitored closely to ensure the threat has been fully neutralized.
- **Lessons Learned**: A formal retrospective or "postmortem" meeting will be held after every significant incident. This process is designed to be blameless, with the goal of analyzing what worked well and what weaknesses were exploited. The findings will be used to improve security policies, procedures, and employee training to prevent similar incidents in the future. This approach fosters an environment where personnel are encouraged to report security weaknesses and errors without fear of reprisal, transforming them from a potential liability into a proactive layer of security defense.

7.2. Escalation Process

The policy includes a clear escalation process based on the severity of the incident. It defines the criteria for escalation, which stakeholders need to be notified (including senior management and legal teams), and the communication channels to be used. This structured approach prevents delays and ensures that critical events are addressed by the appropriate resources and management in a timely manner.

8. Acceptable Use

This section outlines the acceptable use of ABC Ghana's network, systems, and information technology resources. All employees, contractors, and third-party personnel are required to adhere to these guidelines. Violations will result in disciplinary action.

8.1. Prohibited Activities

The following table provides examples of activities that are strictly prohibited on ABC Ghana's network and IT resources.

Activity	Description	Consequence
Unauthorized Software Installation	Installing or running software on company devices that has not been approved and authorized by the IT Security Team.	Disciplinary action, up to and including termination.
Unauthorized Access	Attempting to access or circumvent security measures, or using unauthorized credentials to access systems, networks, or applications.	Disciplinary action, up to and including termination, and potential legal action.
Password Sharing	Sharing login credentials, including passwords, with any other individual.	Disciplinary action, up to and including termination.
Unauthorized Data Access	Accessing sensitive data that is not required for a user's specific job duties.	Disciplinary action, up to and including termination, and potential legal action.
Illegal Activities	Using ABC's network or resources to store, transmit, or view illegal content, or engaging in any activity that violates the law.	Immediate termination of employment and legal action.

Monitoring & Enforcement

- ABC Ghana may monitor network activity for compliance and security.
- Customers violating this AUP may face suspension or termination of services.
- Employees violating this AUP may face disciplinary action, termination, or legal prosecution.

9. Vendor Management

ABC Ghana recognizes that its security perimeter extends to all third-party vendors and partners that have access to its network and data assets. Supply chain vulnerabilities are a major threat to telecommunications providers, making a robust vendor management policy a critical component of the overall security strategy. This policy establishes a formal framework to manage the security risks associated with these external entities.

Data Retention and Disposal

This policy ensures that personal data is not retained for a period longer than is necessary to achieve the purpose for which it was collected, as mandated by Ghana's Data Protection Act, 2012. A clear retention schedule is defined, and secure disposal methods are implemented to mitigate the risk of data breaches and ensure compliance.

Due Diligence:

ABC Ghana must undertake an extensive security assessment of all third-party vendors that shall be engaged and granted access to the company's data and network infrastructure. Security assessment will, depending on the purpose of the vendor's engagement with ABC Ghana focus on:

- Security worthiness and relevant certification such as ISO 27001, SOC 2, ISO 9001/TL 9000, PCI-DSS and GSMA Mobile Money Certification depending on.
- Approval by relevant entities such as the NCA
- Compliance with the Data Protection Act 2012 (Act 843), Electronic Communications Act of Ghana, 2008 (Act 775), Payment Systems and Services Act, 2019 (Act 987), Cybersecurity Act, 2020 (Act 1038)
- Registration of business in accordance with the Companies Act, 2019 (Act 992)
- Compliance with the Ghana Investment Promotion Centre Act, 2013 (act 865) if the vendors are foreign entities operating in Ghana.

Contractual Agreements:

All third-party vendors must sign contracts with ABC Ghana before being granted access to the company's systems and infrastructure. Contract documents must include a security addendum which explicitly clarifies the following:

- Vendors responsibilities towards protecting the data and infrastructure they have access to.
- Data handling procedures
- Breach notifications protocols and communication channels
- Grant ABC Ghana the right to audit the vendor's security controls
- Specify audit timelines
- Define incident response procedures and communication

Access Control:

To control access, all vendors must:

- operate on the principle of least privilege
- have unique accounts
- have their accounts and access periodically reviewed
- be deprovisioned upon the termination/expiry of their contracts with ABC Ghana

Monitoring and Auditing:

Third-party vendors' access and activities will be continuously and regularly monitored and audited to ensure compliance with this policy, security standards and contractual obligations.

Data Retention & Disposal

This part defines ABC Ghana's policy of data retention, handling and disposal. This is to ensure legal; regulatory and security compliance of data are met while satisfying business needs.

Data Classification

ABC Ghana classifies data into different categories and the data under each category is marked with one of three indicators: High, Medium and Low. Data marked high is highly confidential and restricted while data marked medium is maybe accessible to ABC staff and some part of the general public. Data marked low is publicly available and accessible via platforms publicly made available by ABC Ghana such as its websites or that of its partners.

Category	**Data**	**Sensitivity**
Customer Data	PII, SIM registration, Momo details	High
Network & Technical Data	Call Data Records, device info	High
Location Data	Cell tower logs, GPS	High
Business & Corporate Data	Vendor contracts, employee HR	Medium
Regulatory Data	SIM database, lawful intercept	High
Cybersecurity Data	Logs, threat reports	High
Marketing & Analytics	Usage patterns, survey responses, Fraud awareness campaigns, SIM registration reminders	Low

Service Coverage Maps	Network coverage areas (2G, 3G, 4G, 5G), Fibre broadband	Low
Tariffs & Pricing Plans	Voice, data, SMS bundles	Low
Quality of Service Data	reports on call drop rates, network availability	Low
CSR Data	Public projects, sponsorships, and donations	Low

9.1. Data Retention

Data will be retained according to the Data Retention Schedule which specifies the retention timelines for each data type. The retention schedule will define the minimum and maximum retention periods in compliance with the relevant legal and regulatory frameworks such as the Data Protection Act 2012 (Act 843) and inline with business operational requirements.

9.2. Data Retention Timeline

The following table provides an overview of the data retention periods based on the type of data and its purpose.

Data Type	Retention Period	Rationale
Customer PII (Personal Data)	For the duration of the customer relationship plus a period required by law or contractual obligation.	To comply with the Data Protection Act, 2012, which prohibits excessive retention and requires a lawful purpose for data storage.

Data Type	Retention Period	Rationale
Financial Records	Minimum of 7 years, or as required by financial regulations.	To meet statutory and regulatory requirements for financial reporting and tax purposes.
Employee Records	For the duration of employment plus a period required by law (e.g., for legal claims, pensions).	To meet legal and business requirements, and to provide the employee with the right to access their records for a reasonable period.
Network Traffic Logs	Retained for a minimum of 90 days.	To facilitate security incident investigations and forensic analysis.

Data Disposal

After data has reached its maximum retention period, the data must be securely disposed of. One or more of the following disposal methods may be used depending on the data type and format.

- Overwriting/Wiping: writing random data over the original data multiple times.
- Cryptographic erasure: securely deleting the keys associated with encrypted data to ensure the data is impossible to access.
- Degaussing: using a powerful magnetic field to scramble data stored on magnetic media such as hard drives, making it permanently unrecoverable and unreadable.
- Shredding: using sharp blades of industrial machines to shred hard drives and other physical storage media into pieces, making stored data unrecoverable.
- Drilling: used to destroy physical storage material by drilling holes into them to make them unusable and rendering the data unreadable.
- Incineration: burning the storage media into ashes to completely destroy them and make them unusable.

- Vendor-managed secure deletion: closely working with third-party vendors to use their secure disposal methods to dispose of data hosted by third-party vendors.
- Implement data lifecycle policies: implement lifecycle policies such as automatic deleting of logs, backups and analytics.

10. Training and Awareness

The human element is a critical component of ABC's security posture. This policy mandates a robust and continuous security awareness and training program for all personnel. The program aims to educate employees on their individual roles in maintaining security and to foster a "security-first" culture throughout the organization.

- **Mandatory Training**: All employees, contractors, and third-party vendors must complete mandatory cybersecurity training upon hiring and at least annually thereafter.
- **Targeted Content**: Training content will be tailored to address specific, relevant threats, such as phishing, social engineering, and the dangers of insider threats.
- **Policy Reinforcement**: The training will explicitly cover the requirements of this Network Security Policy and other related security policies to ensure all personnel are aware of their responsibilities.
- **Ongoing Communication**: Regular security updates, alerts, and reminders will be communicated to all personnel to reinforce best practices and keep them informed of emerging threats.

11. Compliance and Audits

ABC Ghana must fully satisfy legal, regulatory and security requirements and collaborate with the relevant regulators in ensuring compliance with Ghana’s national laws, data protection and cybersecurity frameworks. In line with that, compliance with national regulatory frameworks and policies and collaboration with regulators must be a priority. Specifically, ABC Ghana must regularly review its compliance with:

- Data Protection Act 2012 (Act 843)

- Cybersecurity Act, 2020 (Act 1038)
- Payment Systems and Services Act, 2019 (Act 987)
- Electronic Communications Act of Ghana, 2008 (Act 775)
- Electronic Transactions Act 2008 (act 772)
- National Cybersecurity Policy and Strategy (NCPS)
- Directive for the Protection of Critical Information Infrastructure (CII)
- May maintain international compliance with ISO 2000, ISO 22301, ISO 27001 and TL 9000 among others

Regulators:

- National Communications Authority (NCA), the national regulator
- Cyber Security Authority (CSA
- Submit data protection compliance audits to the Data Protection Commission (DPC)
- Report incidents, breaches and attacks on the CSA
- Submit site approvals for cell towers, compliance with radiation/emissions standards to the Environmental Protection Agency (EPA)

To ensure the effectiveness and continued relevance of this policy, ABC Ghana will conduct regular security audits and assessments. These audits serve as a proactive measure to verify that the company's IT practices align with established frameworks and internal policies.

- **Regular Audits**: The IT Security Team will conduct regular internal audits of the network infrastructure, access controls, and security configurations to identify vulnerabilities and compliance gaps.
- **Vulnerability Assessments**: ABC will perform periodic vulnerability assessments and penetration tests to identify and remediate weaknesses in the network, applications, and systems.
- **Compliance with Standards**: Audits will verify adherence to relevant regulatory and industry standards, including the Ghana Data Protection Act and international

frameworks like ISO 27001 and NIST.

- **Employee Accountability**: Audit findings will be used to identify areas for improvement and will inform the training and awareness programs. All employees are accountable for ensuring their adherence to security protocols, and non-compliance will be addressed as per the enforcement section of this policy.

12. Roles and Responsibilities

This policy outlines the acceptable use of networks, determines who has access to data, and establishes measures for handling security breaches.

This involves an approach that integrates security technologies with procedural safeguards.

In conformity and understanding the organization’s risks and regulatory frameworks, the following roles and responsibilities have been outlined:

The effective implementation of this policy requires a clear definition of roles and responsibilities across the organization.

Role	Responsibility
Chief Information Security Officer (CISO)	Responsible for developing and implementing a comprehensive cybersecurity strategy that aligns with ABC Ghana's business objectives. The CISO provides executive leadership, manages overall security risk, and ensures the allocation of sufficient resources for security initiatives.
IT Security Team	Responsible for the day-to-day security operations, including monitoring, detection, and response to security incidents. The team manages the security infrastructure, conducts proactive threat assessments, and ensures that

Role	Responsibility
	systems are patched and configured securely.
Department Heads	Responsible for ensuring that employees within their functional area understand and comply with this policy. They must promote a security-conscious culture and support the IT Security Team in implementing security controls and responding to incidents.
All Employees	Responsible for adhering to all security policies and procedures. This includes using IT resources appropriately, protecting assigned credentials, completing mandatory training, and promptly reporting any suspected security incidents or weaknesses.

13. Enforcement

Adherence to this Network Security Policy is mandatory for all personnel. Failure to comply will result in disciplinary action. The severity of the action will be determined in conjunction with Human Resources and Legal departments, considering the nature of the violation, intent, and frequency.

1. **Warning from Management**: A verbal or written warning will be issued for minor policy violations.
2. **Revocation of Privileges**: Access to certain network resources or systems may be temporarily or permanently revoked. This may be used for repeated minor offenses or more serious violations that do not warrant immediate termination.
3. **Suspension without Pay**: For serious policy violations that could put the company at significant risk, an employee may be suspended for a limited time without pay.
4. **Termination of Employment**: Gross or repeated violations, especially those that result in significant damage or legal risk to the company, will lead to immediate

termination of employment.

5. **Legal Action**: In cases of malicious intent, data theft, or illegal activity, ABC Ghana may pursue legal action against the individual in addition to termination of employment.

14. Review and Maintenance

This policy is a living document that must be continuously reviewed and updated to remain effective. It is essential for the policy to adapt to evolving threats, new technologies, and changes in the business landscape.

- **Annual Review**: The CISO will lead a formal review of this policy on an annual basis. This review will assess the policy's effectiveness, alignment with business goals, and compliance with all relevant laws and standards.
- **Ad-hoc Review**: An ad-hoc review will be conducted following any major security incident or significant changes to ABC's network architecture, business model, or regulatory obligations.
- **Approval**: Any revisions or modifications to this policy must be formally approved by the CISO and other relevant senior management.

15. Related Policies

This Network Security Policy is supported by, and should be read in conjunction with, the following related policies:

- Acceptable Use Policy.
- Incident Response Policy.
- Data Classification Policy.
- Vendor Management Policy.
- Password Management Policy.

16. Approval

This Network Security Policy has been reviewed and formally approved by ABC Ghana’s executive management. Its provisions are mandatory for all employees, contractors, vendors, and third parties who interact with ABC Ghana’s network infrastructure and information assets.

The approval affirms ABC Ghana’s commitment to safeguarding the confidentiality, integrity, and availability of its information systems in alignment with business objectives and legal requirements.

Signature: Dr. Noah Darko-Adjei,
CISO: ABC GH,
DATE: 30th August 2025.

17. Conclusion

This Network Security Policy is more than a set of rules; it is a strategic document that formalizes ABC Ghana's commitment to protecting its most critical assets. By establishing clear standards for access control, data protection, and incident response, the policy ensures that ABC's network remains resilient and trustworthy. The policy's emphasis on continuous training, regular audits, and the shared responsibility of all personnel is designed to cultivate a security-first culture that proactively mitigates risks. Adherence to this policy is not only a matter of compliance but is crucial for protecting the brand's reputation, maintaining customer loyalty, and enabling ABC's continued growth as a leader in the telecommunications and digital services sector.

18. Glossary of Terms

Term	Definition
Access Control	A security technique that regulates who or what can view or use resources in a computing environment. Ensures only authorized users gain access.
Acceptable Use Policy (AUP)	A set of rules applied by an organization that restricts the ways in which a network, website, or system may be used.
Authentication	The process of verifying the identity of a user or system, often through passwords, biometrics, or tokens.
Availability	One of the three core principles of information security (CIA triad), is ensuring that information and resources are accessible when needed by authorized users.
CIA Triad	A foundational model of information security consisting of Confidentiality, Integrity, and Availability.
Confidentiality	Ensuring that sensitive information is accessed only by authorized individuals.
Data Classification	The process of organizing data into categories (e.g., Public, Internal, Confidential, Highly Confidential) based on sensitivity and impact if compromised.

Data Encryption	A method of converting information into a code to prevent unauthorized access. Used for both data at rest and in transit.
Data Retention	Policies and practices that govern how long data is stored before being securely disposed of.
Disposal (Secure Data Disposal)	The permanent removal of data using secure methods such as shredding (physical) or data wiping (digital).
Encryption Standards	Official guidelines (e.g., AES-256) that define how data should be encrypted to ensure protection.
Enforcement	The disciplinary measures applied when policy violations occur (e.g., warning, suspension, termination).
Firewall	A network security device that monitors and filters incoming and outgoing network traffic based on predetermined rules.
Incident Response (IR)	The structured approach is taken by an organization to detect, respond to, and recover from security incidents.
Information Security Policy	A set of rules and guidelines that govern how an organization protects its information assets.
Integrity	The assurance that data remains accurate, complete, and unaltered except by authorized individuals.
ISO/IEC 27001	An international standard for managing information security.
ISO/IEC 27035	An international standard specifically for incident management and response.
Least Privilege Principle	A security principle where users are granted the minimum level of access — or

	permissions — needed to perform their job functions.
Malware	Malicious software is designed to damage, disrupt, or gain unauthorized access to systems.
Multi-Factor Authentication (MFA)	A security process that requires users to provide two or more verification factors to access systems.
Network Security	The practice of protecting a computer network from intruders, misuse, or unauthorized access.
NIST SP 800-53	A U.S. government standard providing security and privacy controls for federal information systems.
Phishing	A form of cyberattack where attackers impersonate trusted entities to steal sensitive information.
Physical Security	Security measures are designed to prevent unauthorized physical access to facilities, such as CCTV, locks, and guards.
Policy Enforcement	The implementation of disciplinary actions to ensure compliance with security rules.
Review & Maintenance	The process of regularly evaluating policies to ensure they remain up-to-date and effective.
Risk Management	The process of identifying, assessing, and controlling threats to an organization’s assets.
Roles & Responsibilities Matrix	A chart or table that assigns specific duties and accountability to individuals or teams.
Scope	Defines who the policy applies to (employees, contractors, vendors) and

	what assets are covered (servers, networks, data centers, etc.).
Security Audit	A systematic evaluation of an organization’s information system to ensure compliance with security standards and policies.
Third-Party Vendor	An external company providing services to ABC Ghana that must also comply with security requirements.
Training & Awareness	Programs that ensure employees understand security risks, policies, and best practices.
Vendor Management	The process of ensuring that third-party vendors follow the organization’s security requirements.
Vulnerability	A weakness in a system, network, or process that can be exploited by a threat actor.

19. Appendix

The appendix serves as a repository for any supplemental diagrams, technical guides, or other supporting documentation. This may include detailed technical standards for encryption, network architecture diagrams, or specific procedures for data destruction. This section provides a flexible space for detailed information that is not essential to the policy's primary narrative but is crucial for its implementation.

20. References

- Exabeam, Inc. (2023). *What Is a Network Security Policy? 9 Key Components and How to Make Them Work*. Retrieved from https://www.exabeam.com/explainers/network-security/network-security-policy-9-key-components-and-how-to-make-them-work/.

- Ghana Parliament. (2012). *Data Protection Act, 2012 (Act 843)*. Retrieved from https://en.wikipedia.org/wiki/Data_Protection_Act,_2012.
- International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 Information Security Management*. Retrieved from https://www.iso.org/standard/84511.html.
- National Institute of Standards and Technology (NIST). (2018). *NIST Cybersecurity Framework (CSF)*. Retrieved from https://www.nist.gov/cyberframework.
- New York Institute of Technology (NYIT). (2024). *IT Vendor Management Policy*. Retrieved from https://site.nyit.edu/policies/it_vendor_management_policy.
- SecurityMetrics. (2023). *6 Phases of an Incident Response Plan*. Retrieved from https://www.securitymetrics.com/blog/6-phases-incident-response-plan.

- 1. Information Security | ABC Group, https://group.ABC.com/wp-content/uploads/2020/09/ABC-Position-on-Information-Security-1.pdf 2. Strategy – ABC Group, https://group.ABC.com/who-we-are/strategy/ 3. Telecommunications Data Compliance - Ground Labs, https://www.groundlabs.com/industry/telecommunications/ 4. Network Security Policy: 9 Key Components & How to Make Them Work | Exabeam, https://www.exabeam.com/explainers/network-security/network-security-policy-9-key-components-and-how-to-make-them-work/ 5. Cybersecurity in the Telecom Industry: Challenges and Career Opportunities | Coursera, https://www.coursera.org/articles/cyber-security-in-telecom-industry 6. Data Classification Levels Explained: Enhance Data Security, https://dataclassification.fortra.com/blog/data-classification-levels-explained-enhance-data-security 7. Network Security Policy: Complete Guide & Examples - Rippling, https://www.rippling.com/blog/network-security-policy 8. The Importance of Stakeholder Communication in Cybersecurity Excellence, https://www.cyberriskinsight.com/operations/importance-stakeholder-communication-cybersecurity-excellence/ 9. data center physical security guidelines - Open Compute Project, https://www.opencompute.org/documents/open-for-comment-ocp-physical-security-white-paper-1-pdf 10. Mastering MFA Requirements: Compliance, Risks, and Best Practices - RSA Security, https://www.rsa.com/pt/resources/blog/multi-factor-authentication/mastering-mfa-requirements-compliance-risks-and-best-practices/ 11. Data Security Policies: Why They Matter and What They Contain - Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/data-security-policy 12. The Principle of Least Privilege: Best Practices and Benefits - Cohesity, https://www.cohesity.com/blogs/the-principle-of-least-privilege-best-practices-and-benefits/ 13. What Is Least Privilege & Why Do You Need It? - BeyondTrust, https://www.beyondtrust.com/blog/entry/what-is-least-privilege 14. IT Vendor Management Policy | Policies | NYIT, https://site.nyit.edu/policies/it_vendor_management_policy 15. Appendix | Examples of Reportable Acceptable Use Violations - UMN Policy Library, https://policy.umn.edu/it/itresources-appd 16. Cybersecurity Fundamentals: Why MFA Needs to Be So Robust | American Public University, https://www.apu.apus.edu/area-of-study/security-and-global-studies/resources/cybersecurity-fundamentals-why-mfa-needs-to-be-so-robust/ 17. Information Security and Acceptable Use - Oakland Community College, https://www.oaklandcc.edu/policies/information-technologies-policies/information-security-acceptable-use 18. 6 Phases in the Incident Response Plan - Security Metrics, https://www.securitymetrics.com/blog/6-phases-incident-response-plan 19. Incident Response Plan (IRP) Basics - CISA, https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf 20. A Practical Approach to Incident Management Escalation - Blog - Exigence, https://blog.exigence.io/a-practical-approach-to-incident-management-escalation 21. How to build an escalation policy for effective incident management - xMatters, https://www.xmatters.com/blog/how-to-build-an-escalation-policy-for-effective-incident-management 22. Data Protection Act, 2012 - Wikipedia, https://en.wikipedia.org/wiki/Data_Protection_Act,_2012 23. Creating a Data Retention Policy: Examples, Best Practices & Template -

Secureframe, https://secureframe.com/blog/data-retention-policy 24. Security Awareness Training Requirements - TeachPrivacy, https://teachprivacy.com/security-awareness-training-requirements/ 25. Network Security Plan: Develop & Implement In 8 Steps - PurpleSec, https://purplesec.us/learn/network-security-plan/ 26. IT Compliance Audit - A Comprehensive Guide in 2025 - Zluri, https://www.zluri.com/blog/it-compliance-audit 27. Network Security Audit | Audit Checklist & Best Practices - Darktrace, https://www.darktrace.com/cyber-ai-glossary/how-to-conduct-a-network-security-audit 28. Ideas for Security Policy Sanctions - Information Shield, https://informationshield.com/2009/02/17/ideas-for-security-policy-sanctions/ 29. ISO 27001 Annex A 6.4 Disciplinary Process - High Table, https://hightable.io/iso-27001-annex-a-6-4-disciplinary-process/ 30. 10 Must Have IT Security Policies for Every Organization, https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/ 31. ISO 27001 vs. NIST Cybersecurity Framework | Blog | OneTrust, https://www.onetrust.com/blog/iso-27001-vs-nist-cybersecurity-framework/