MTN POSITION STATEMENT

Information Security

The issue

Information is a critical asset for MTN and must be protected from a wide range of threats that could affect confidentiality, integrity or availability. Failure to safeguard information assets can lead to business disruption, financial loss, reputational damage, legal exposure and weakened operational resilience. Effective information security supports business continuity, protects resources, enables resilience and acts as a business enabler across MTN's operations.

Linking the issue to our strategy

MTN's approach to information security is guided by globally defined standards, including the NIST Cyber Security Framework and ISO/IEC 27001:2013, as well as critical security controls, which support alignment between information security controls and MTN's business objectives, strategy and operational requirements.

The Group Information Security Policy defines responsibilities, governance structures and organisational coordination required across MTN's business units and operating companies. Protecting information assets, managing information security risks, maintaining appropriate levels of user awareness and ensuring compliance with local laws, regulatory requirements, contractual obligations and licence conditions are integral to MTN's resilience, continuity planning and long-term sustainability.

Scope

This position statement applies to all users and third parties accessing MTN information, devices, applications, processing facilities, equipment and networks, including directors, officers, employees and representatives (permanent, temporary or contract). It also applies to MTN information that is generated, accessed, processed, stored or destroyed on or off MTN premises.

MTN expects intermediaries, agents, contractors, suppliers and business partners to uphold the same information security standards. The MTN Supplier Code of Conduct outlines the minimum information security requirements applicable to suppliers of products or services.

Our commitments

Direct operations

MTN commits to:

- Implementing information security policies, procedures, guidelines and standards aligned with business objectives and applicable best practices.
- Applying a risk-based approach to information security management, proportionate to the sensitivity and criticality of information assets
- Maintaining an organisation-wide Information Security Management System (ISMS) based on a business risk approach to establish, implement, operate, monitor, review and improve information security.
- Defining and maintaining clear roles, responsibilities and authority for consistent information security implementation across the organisation.
- Identifying, classifying and protecting information assets according to confidentiality, integrity, availability, sensitivity and value, with clearly defined asset ownership.
- Ensuring physical and environmental protection of information assets, campuses and information processing facilities against unauthorised access, misuse, damage or theft.

- Implementing controls to prevent unauthorised access, misuse, system failure or data compromise across information systems, applications, equipment and network devices.
- Restricting access to information and information processing facilities based on business requirements, job responsibilities and the principle of least privilege.
- Integrating information security requirements into the acquisition, development, testing, maintenance and operation of systems, products and services.
- Implementing information security incident management processes to enable early detection, reporting, response, investigation and mitigation of security incidents.
- Embedding information security requirements within business continuity and resilience management to support recovery from anticipated or unanticipated disruptions.

Value chain

MTN commits to:

- Requiring intermediaries, agents, contractors, suppliers and business partners comply with MTN's information security requirements.
- Ensuring third-party relationships are governed by formal agreements that include confidentiality, data protection and information security obligations and that third-party access to MTN information is limited, monitored and reviewed.
- Applying communications security controls to manage risks associated with network services, including communication between MTN operating companies, third parties and online transactions.

Systems change

MTN commits to:

- Upholding the core information security principles of confidentiality, integrity and availability across all systems and operations.
- Maintaining security governance structures that support consistent implementation, monitoring and continuous assessment of information security controls.
- Applying information security controls throughout the system and technology lifecycle, including design, development, testing and operational environments.
- Ensuring compliance with applicable laws, regulations, statutory and contractual requirements when designing, operating and managing information systems.

Accountability

- The MTN Board, through the Group Audit Committee, oversees the Group's actions and performance regarding information security.
- The Executive Committee is responsible for implementing information security policy and addressing information security risks, supported by the Group information security function.
- Accountability for information security is assigned across functional heads and operating companies, with management responsible for maintaining compliance within their areas of responsibility.
- MTN is committed to transparency and disclosure regarding information security performance, in line with applicable legal and regulatory requirements.
- Information security policies are made available to employees and relevant third parties, and translated where required.
- Regular awareness initiatives and training are provided to ensure users understand their information security responsibilities.
- MTN recognises that information security threats continue to evolve and requires controls to remain appropriate to changing risks.
- MTN continuously reviews, monitors and improves information security approach, recognising the evolving nature of technology, threats, regulation and business operations.