MTN POSITION STATEMENTS

Information security

Introduction

Information is an asset and consequently needs to be suitably protected. Information security protects information assets from a wide range of threats to ensure business continuity and resilience, minimise business damage and maximise return on investments.

Purpose

The minimum requirements for managing information security and the roles and responsibilities. The requirements for information security policies, procedures, guidelines, and standards to be aligned with business objectives and applicable best practices. User awareness requirements to ensure that awareness is prioritised.

MTN's approach

The following globally defined standards guide MTN:

- NIST Cyber Security Framework.
- ISO/IEC 27001:2013.

MTN's key principles on information security

The following control objectives drive information security:

- Confidentiality, which relates to the protection of sensitive information from unauthorised access.
- Integrity, which relates to the accuracy and completeness of information and the validity of information in accordance with business values and expectations.
- Availability relates to information being available at the right time for the business process. It also deals with the safeguarding of necessary resources and associated capabilities.

MTN's policies governing information security

Our governance approach to information security is enshrined in the MTN Group Information Security Policy, which other policies, standards, and guidelines support.

Information security organisation

The Group Information Security Policy (GISP) defines appropriate responsibilities, authority, and relationships to consistently implement and manage information security in MTN. The information security organisation has representation from all business and relevant supporting functional units to ensure structured co-ordination of information security-related activities.

Asset management

The asset management statements specify the importance of information/information assets, including identification of the asset owner, asset classification and determining confidentiality, integrity, and availability ratings of the assets.

Human resources security

Information assets should be physically protected from unauthorised access, misuse, damage, and theft. The MTN campus and information processing facilities should be protected from physical and environmental threats.

Physical security

Information assets should be physically protected from unauthorised access, misuse, damage and theft. The MTN campus and information processing facilities should be adequately protected from physical and environmental threats.

Operations security

The operations security statements establish appropriate controls that must be implemented to prevent unauthorised access, misuse or failure of the information systems and equipment and to ensure confidentiality, integrity and availability of information processed by or stored in the information systems, applications, equipment, and network devices.

Communications security

The communications security statements cater to the implications associated with using network services, including communication between MTN OPCOs, third parties and on-line transactions.

Access control

The Access Control statements define the controls that must be implemented and maintained to protect information assets against unauthorised logical access that poses a substantial risk to the organisation.

Access to information/information assets, information processing facilities, systems, applications equipment, and network devices should be restricted per the valid business requirements, user's job responsibility and information security requirements. Formal procedures should be in place to control the allocation of access rights.

Information system acquisition, development and maintenance

The information systems acquisition, development, and maintenance statements define the security requirements that must be identified and integrated during the development and maintenance of applications, software, products and/or services.

Information security incident management

The information security incident management statements provide direction on the development and implementation of information security incident management procedures for information systems, applications, equipment and network devices, improving user security awareness, early detection and mitigation of security incidents and suggesting the actions that can be taken to reduce the risk due to security incidents.

Business continuity and resilience management

A business continuity and resilience management process should be implemented to minimise the impact on the organisation and recovery from loss of information/information assets, systems, applications equipment, and network devices resulting from anticipated (e.g. a

labour strike or hurricane) or unanticipated events (natural disasters such as earthquake, accidents, blackouts and equipment failures), to an acceptable level. This process should identify the critical business processes and integrate business continuity's information security management requirements with other requirements relating to operations, staffing, materials, transport and facilities.

Compliance

The compliance statements provide direction towards designing and implementing appropriate controls to meet MTN's local laws, regulations, and statutory and contractual requirements. The design, operation, use and management of information systems should be subjected to local laws, regulations, statutory and contractual security requirements.

Roles and responsibilities

Our Board, through the Group Audit Committee, oversees the Group's actions and performance regarding information security.

The Group's Executive Committee is responsible for policy implementation and for identifying, addressing, and remedying information security risks, driven by the Group Information Security function, in line with the MTN's policy.

Applicability and transparent reporting

Our information security policy applies to all our directors, officers, employees, and representatives of the Company whether permanent, temporary or on contract.

We expect our intermediaries, agents, contractors, suppliers, and business partners to uphold the same standards.

Our Supplier Code of Conduct outlines the minimum standards, including information security, that each supplier of products or services must comply with.

We are committed to transparency and disclosure regarding information security at MTN.

Communication and training

MTN's information security policy is shared with all employees of MTN's operating entities, subsidiaries and partners. The policy is translated into local languages as required. Detailed training is provided to employees and partners based on an annual basis.