MTN position statement

Information Security

Introduction

Information Security is fundamental to MTN's daily operations and success. MTN has instituted an organisation wide information security programme to address the security needs across the Group. This programme has been instituted using a formal ISMS based on global leading industry practices and standards such as ISO/ IEC 27001:2013, the Critical Security Controls (CSC) and the NIST Cyber Security Framework. Establishing the ISMS at MTN is a strategic objective and encompasses people, process, and technology elements in MTN.

Information security is driven by the following control objectives:

- Confidentiality, which relates to the protection of sensitive information from unauthorised access.
- Integrity, which relates to the accuracy and completeness of information, as well as to the validity of information in accordance with business values and expectations.
- Availability, which 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.

Key principles

- The Compliance Policy provides direction towards design and implementation of appropriate controls to meet local laws, regulations, statutory and contractual requirements at MTN. The design, operation, use and management of information systems shall be subjected to local laws, regulations, statutory and contractual security requirements.

- The Asset Management Policy specifies the importance of information/information assets including identification of the asset owner, asset classification and determining confidentiality, integrity and availability ratings of the assets.

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

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

- The Operations Security Policy establishes appropriate controls that need to be implemented to prevent unauthorised access, misuse or failure of the information systems and equipment and to ensure confidentiality, integrity and availability of information that is processed by or stored in the information systems, applications, equipment and network devices.

- The Communications Security Policy caters to the implications associated with using network services including communication between MTN OPCOs, third parties and on-line transactions among others.

Our Access Control Policy

- The Access Control Policy defines the controls that need to be implemented and maintained to protect information assets against unauthorised logical access that poses substantial risk to the organisation.
- Access to information /information assets, information processing facilities, systems, applications equipment and network devices shall be restricted as per the valid business requirements, user's job responsibility and information security requirements. Formal procedures shall be in place to control the allocation of access rights.

Our Information System Acquisition, Development and Maintenance Policy

- The Information Systems Acquisition, Development and Maintenance Policy defines the security requirements that need to be identified and integrated during the development and maintenance of applications, software, products and/or services.

Our Information Security Incident Management Policy

- The Information Security Incident Management Policy provides directions to develop and implement the 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.

Our Business Continuity Management Process

- A business continuity management process shall be implemented to minimize 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 shall identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to aspects such as operations, staffing, materials, transport and facilities.

Applicability

The scope of the information security encompasses all MTN facilities, Group and OPCO functions, information assets, employees, contractors and third parties. It is applicable to the following:

- All information including, but not limited to; customer information, MTN employee and company related information generated, processed and stored by various functional units at MTN to perform its activities and delivery of services.
- All information assets that process information at MTN. Information assets may include, but are not limited to; hardware assets, software assets, services assets, people assets and paper assets.
- All employees, contractors and third-party personnel of MTN accessing MTN information processing facilities. MTN information processing facilities include, but are not limited to; MTN campus, facilities, offices, work areas, secure areas, critical infrastructure rooms (CIR) and telecommunications rooms.

Roles and Responsibilities

- The 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 a structured co- ordination of information security related activities.
- The responsibilities towards information security are prescribed below:
    - All employees, contractors and third-party personnel shall comply with the Group Information Security Policy (GISP) and associated procedures, standards and guidelines.
    - All personnel, contractors and third- party personnel involved with storing and processing of information at MTN have a responsibility for reporting information and cyber related security incidents and any identified weaknesses.
    - All personnel, contractors and third- party personnel involved with storing and processing of information at MTN shall be responsible for supporting and actively participating where necessary, in all steps taken to mitigate information security risks.

Comments and concerns

Any comments or concerns can be logged through our in-country customer help lines and via email to cybersecurity@mtn.com.