medical ACCESS

INFORMATION SECURITY POLICY

Medical Access specializes in cost-effective, reliable, and sustainable healthcare supply chain management solutions for Africa. We provide supply chain management services for medical, pharmaceutical, health and other commodities.

We are committed to implementing and maintaining compliance with ISO 27001:2013, and delivering long term and sustainable value to our stakeholders through secure information practices and continually improving the existing systems through audits and technological advancements to ensure confidentiality, integrity, and availability of information. It is our priority to have all our employees and stakeholders commit to the information security requirements in all their operations.

The provisions of this document are consistent with MA’s IT policy.

OBJECTIVES:

It is our goal to manage the Security of Information and Information assets in our custody to ensure that our services and products are always available as and when required.

By deploying an Information Security Management System (ISMS), We aim at ensuring that known risks are controlled to acceptable levels, while emerging risks are handled in an effective and consistent manner for customer satisfaction, maximum return on investment and guaranteed business continuity.

WE PURPOSE TO: -

- Continually improve a certified information security management system according to ISO 27001
- Ensure that our employees and other stakeholders are aware of and adhere to our information security policies; legal, customer as well as regulatory requirements.
- Ensure that all assets are classified in terms of their criticality and sensitivity and are protected in accordance with their classification for guaranteed confidentiality, integrity, and availability of information.
- Protect our stakeholders, information, intellectual property, assets, activities and facilities against misuse, loss, damage, disruption, interference, espionage, or unauthorised disclosure. We strive to retain the confidence of those who entrust sensitive information to us.
- Define and clearly communicate all Information Security roles and responsibilities for continued compliance.
- Set strategic objectives with the aim of continually improving the Information Security Management System.
- Maintain consistent approach to risk management that lays out risk acceptable criteria and tolerable levels that is well suited to the company's business, legal and customer regulatory requirements.

RESPONSIBILITIES: -

- It is the direct responsibility of management to maintain and offer advice and guidance for implementation of this policy.
- All MA Heads of Department are responsible for implementing and enforcing this Information Security policy within their functional units.
- Each member of staff is required to adhere to this policy and all other formulated and disseminated Information Security policies.
- Each contracted provider, stakeholders and partners are required to adhere to this policy and all other formulated and disseminated Information Security policies in as far as stipulated in contractual, memoranda and/or partnership documents.

APPROVED BY: **SOWEDI MUYINGO** **SIGN:** **DATE:** **31 MARCH 2021**