Contents

1. OBJECTIVE

The objectives of this Information Security Policy are the preservation of confidentiality, integrity, and availability of systems and information used by ISOQAR Africa Employees as well as our clients. These three principles compose the CIA (Confidentiality, Integrity, Availability) triad:

- Confidentiality involves the protection of assets from unauthorized entities.
- Integrity ensures the modification of assets is handled in a specified and authorized manner.
- Availability is a state of the system in which authorized users have continuous access to said assets.

Furthermore, this Policy assure and communicate the management direction and support for information security in accordance with the Protection of personal information Act (POPI) and General Data Protection Regulations (GDPR) regulation requirements.

2. SCOPE

This policy applies to ISOQAR Africa, its affiliated partners or subsidiaries, including data processing and process control systems, that are in possession of or using information and/or facilities owned by ISOQAR Africa.

This policy applies to all ISOQAR Africa staff and third parties that are directly or indirectly employed by ISOQAR Africa, subsidiaries or any entity conducting work on behalf of ISOQAR Africa that involves the use of information assets owned by ISOQAR Africa.

3. POLICY STATEMENT

3.1 INFORMATION SECURITY DEFINITION

The information asset's availability, integrity, confidentiality, and accountability are essential to maintain ISOQAR Africa's security compliance, and organization image. ISOQAR Africa acknowledges the importance of ensuring information security and is committed towards supporting the information security goals and its principles.

ISOQAR Africa Information Security Policy's ultimate goal is to ensure the following:

- Availability of information to authorized users, if and when required.
- Integrity of the information through the protection from unauthorized modification.
- Information is protected from unauthorized access.
- Confidentiality of information is maintained.
- Regulatory and legislative requirements are met.

All ISOQAR Africa staff, contractors and third parties should adhere to this information security policy.

3.2 INFORMATION SECURITY POLICY DOCUMENT

- Management understands their responsibilities toward sustaining the information security objectives within the ISOQAR Africa environment.
- Management acknowledges the importance of ensuring information security and committed towards supporting the information security goals and its principles.
- Management defines a well-structured information security framework to initiate control and maintain information security in accordance with ISOQAR Africa's business requirements.
- Management provides the direction and support for implementation of security requirements across ISOQAR Africa environment.
- ISOQAR Africa is committed to preserve the security of all the information assets owned and entrusted to us to ensure the information security and legal conformity of this information.
- ISOQAR Africa approach to information security management is based on international standards and globally accepted best practices to ensure:
    - Information is always available to all the individuals who have the proper and approved authorization to access this information.
    - Information is only changed and/or updated by authorized individuals who have the proper and approved authorization.
    - Information is only accessed by authorized individuals, who have the proper and approved access authorization.
    - All the confidential information is well protected with all the necessary controls.
    - All individuals who have been granted any form of access to information are fully accountable for the proper use of this information.
- All ISOQAR Africa staff and contractors should commit to strict adherence to information security policies and practices.
- ISOQAR Africa will disclose any client information to be disclosed to our head office in the UK.

3.3 REVIEW OF THE INFORMATION SECURITY POLICY

- Top Management review and update this information security policy on an annual basis.
- Top Management annually measure the effectiveness of the implemented controls to avoid security incidents and reduce resulting impacts, together with a process for benchmarking security maturity with other similar establishments. The below is considered:
  - Feedback and opinions of interested parties.
  - Reports and status of incidents reported.
  - Results of independent and management reviews.
  - Trends of threats and their vulnerabilities.
- Top Management ensure that this information security policy is well documented in line with relevant international standards, legal and regulatory requirements, and other compliance requirements.

4. POLICY ENFORCEMENT / COMPLIANCE

- Compliance with this policy is mandatory and ISOQAR Africa Management should ensure continuous compliance monitoring to all employees and contractors.
- Compliance with the statements of this policy is a matter of periodic review by Top Management. Any violation will result in disciplinary action in accordance with ISOQAR Africa internal processes.