INFORMATION SECURITY POLICY

Policy Statement

The Management of OAG has established this Information Security Policy based on the organization purpose, values and the requirements of ISO/IEC 27001:2013 standard. The OAG is committed to maintaining the confidentiality, integrity and availability of information and information assets that support its mandate, whether internal or external, deliberate or accidental. This policy seeks to ensure that:

1. Information security risks will be maintained at an acceptable level
2. Risk resulting from organizational, physical, environmental and emerging technological changes and the use of 3rd parties will be assessed and appropriately managed
3. The confidentiality of auditee information will be assured. Sensitive information (however or wherever stored) will be protected against unauthorized access and the integrity of information will be maintained. Information will only be made available to authorized organization processes, employees, suppliers and other interested parties when required. The requirements of interested parties (including regulatory and legislative requirements) will be met
4. The protection of information will be considered, when business continuity plans for mission critical activities are produced, maintained, tested or invoked
5. Information security training and awareness will be made available to all employees, suppliers and other interested parties where appropriate
6. All breaches of information security, actual or suspected, will be reported to and investigated by the OAG Security Incident Response Team (SIRT)

To support this policy;

1. OAG shall establish an Information Security Management System (ISMS) which incorporates a systemic approach to information security risk management. The ISMS shall identify organization needs and those of interested parties regarding information security requirements (including contractual, statutory and any other relevant requirements) and create an effective operational security framework
2. Objectives shall be agreed on an annual basis, supported by a set of key performance indicators (KPIs). These measures shall be reported to the Management for review
3. OAG shall ensure continual improvement of the ISMS. The ISMS shall constantly be reviewed by management and the need for it shall be communicated to all employees
4. OAG shall fully comply with and certify to the ISO/IEC 27001 Standard for information security.

This Information Security Policy is reviewed at a regular Management Review Meetings every 1 year or when there is a major change within the organization.

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Information Security Policy
2.	Date of Release	8th February 2019
3.	Document Number	OAG-ISMS-PO-Information Security Policy-v1.0
4.	Document Version No	1.0
5.	Document Owner	Auditor General, Mr. Obadiah BIRARO
6.	Document Author(s)	Sentinel Africa Consulting Ltd

Document Approvers

Approver	Approver Designation	Signature	Approval Date
Mr. Obadiah BIRARO	Auditor General		8/2/2019

Change Log

Version No.	Revision Date	Nature of Change	Date Approved
1.0	8th February 2019	First Version	8th February 2019