THE REPUBLIC OF RWANDA

THE OFFICE OF THE AUDITOR GENERAL

Third-Party Information Security Policy v2.3

September 18, 2023

Document Control

S. No.	Type of Information	Document Data
a.	Document Title	OAG Third-Party information Security Policy
b.	Date of Release	24th December 2021
c.	Document Number	OAG-ISMS-PO- Third-Party information Security Policy –v2.3
d.	Document Version No	2.3
e.	Document Owner	Office of the Auditor General
f.	Document Author(s)	Sentinel Africa Consulting Ltd, OAG ICT Team

Document Approvers

S. No.	Approver	Approver Designation	Signature	Approval Date
1.	Evergiste Bushayija	IT Director		24th December 2021
2.	Olive MULIGO	Secretary General		24th December 2021

Change Log

Version No.	Revision Date	Nature of Change	Date Approved
1.0	28th January 2019	First version	8/2/2019
2.0	03rd March 2020	Annual review(Extraction of the policy from OAG ISMS Policies document)	O3/03/2020
2.1	11th January 2021	Annual review (no change made)	11th January 2021
2.2	24th December 2021	Annual review (no change made)	24th December 2021
2.3	18th September 2023	Annual review (Minor formatting changes)	

Third-Party Information Security Policy.

1 THIRD PARTY INFORMATION SECURITY POLICY.

This policy sets out OAG's expectations in respect to information security when dealing with third parties. This Information Security Policy demonstrates OAG's commitment to safeguarding the confidentiality, integrity and availability of all its physical and operational information assets that are critical to the provision of its services.

1 Scope.

This policy governs all information that is created, transmitted, processed, stored or disposed during OAG's mandate, information assets and the systems used to create and maintain that information.

The scope of this policy applies to procurements and partnership agreements that involve IT solutions or provision of services which require access to/or the processing of confidential data for the delivery and/or support of OAG's services and organizational functions.

2 Definitions.

Information: Facts or processed data that relates to the OAG.

Information Security: This refers to the protection of critical assets to ensure their confidentiality, integrity and availability.

Risk: The probability that a threat, an unwanted event or action will adversely affect OAG's ability to achieve its organizational objectives.

Information Asset: A collection of information and facilities used to capture, record, transmit, process and display it.

3 Policy Statement.

Information security risks will be identified and maintained at an acceptable level to ensure procurement of services and solutions that are able to provide the level and quality of Information Security required.

Risks resulting from organizational, physical, environmental and emerging technological changes and the use of third parties will be assessed and appropriately managed.

Contracts with third parties shall define their information security responsibilities such as in Confidentiality Clauses within contracts.

During the duration of contracts with third parties OAG will manage the relationship to ensure information security is maintained.

OAG, as appropriate, will allow third parties access to its information/ information systems where a formal contract stating information security responsibilities exist.

Information security awareness will be made available to all third parties as appropriate.

All breaches of information security will be reported to and investigated by following the existing Incident Management Procedure.

Third party access to OAG's information/information systems for support and/or maintenance will be monitored and subject to periodic checks

4 Enforcement.

Violation of this policy may result in disciplinary action, which may include termination for permanent and temporary employees. Individuals may be subject to loss of OAG Information Resources access privileges, civil, and criminal prosecution. For third parties, violation of this policy may result in termination of contract.

5 Responsibility.

All employees, contractors, consultants, vendors, suppliers are responsible for knowing, understanding, and adhering to the OAG Third Party Information Security Policy.

6 Exceptions.

Where systems, procedures or processes are not able to meet the requirements of this policy and an appropriate justification exists, an exception should be raised for review and approval according to the Exceptions Procedure.