



**Deputy Governor**

## **BNR INFORMATION SECURITY POLICY**

The BNR Management has established a documented information security policy based on the requirements of ISO/IEC 27001:2013 Standard, which is appropriate to the purpose of the Bank. This policy includes below information security objectives in order to protect the Confidentiality, Integrity and Availability of Information Assets from all threats, whether internal or external, deliberate or accidental in relation to the processing, transmitting and storing of sensitive Bank information:

- Establishing and implementing risk based information security controls;
- Periodically reviewing and updating operational procedures of all business functions;
- Complying with statutory & regulatory requirements and contractual security obligations;
- Spreading security awareness amongst staff, interns, service providers, third party contractors and end users of BNR information systems;
- Managing security incidents effectively through an Incident management framework;
- Developing Business Continuity Plans that addresses information security continuity; and
- Continually improving the Information Security Management System (ISMS) through regular reviews of measurable security objectives.

The BNR Management is committed to satisfy applicable requirements related to information security; and to the continual improvement of the information security management system.

This policy must be communicated to external interested parties (defined under Sec 4.2 of the ISMS Manual) through publishing on BNR website, communicated through SharePoint, or during contract signing and make the ISMS policy signed along with the Non-Disclosure Agreement (NDA).

Any changes to this ISMS policy must be communicated to internal parties and external parties.

Done in Kigali on 7 December 2023

**Soraya M. HAKUZIYAREMYE**

**Deputy Governor and Chairperson of the IT Steering Committee**