✓1. Purpose

This policy has been formulated with the purpose of ensuring compliance with applicable RRA statutes, regulations, and mandates regarding the management of information resources; establishing prudent and acceptable practices with regard to the use of RRA information resources; and educating individuals in the effective use of these information resources with respect to their responsibilities.

✓2. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at RRA herein referred to as Users.

It covers all devices owned by RRA and those personally owned devices, as long as they access RRA networks, data and systems. This includes but is not limited to desktops, laptops, smartphones and tablets.

✓3. Policy

Any access or use of RRA information assets shall adhere to this policy so as to minimize the risk of information security breaches and other possible adverse effects.

✓4. General Use and Ownership

RRA proprietary information stored in hardcopies, electronic and computing devices, remains the sole property of RRA. Staff members must ensure through legal or technical means that proprietary information is protected in accordance with the Information Classification Standard.

All staff have a responsibility to promptly report the theft, loss or unauthorized disclosure of RRA proprietary information in accordance with the Incident Management Policy. Staff members may access, use or share RRA proprietary information only to the extent that is authorized and necessary to fulfil their assigned duties.

Shared folders are created by IT for specific groupings or departments. The use of these shared folders will be guided by appropriate departmental and IT policies, and RRA's information security policy.

For security and network maintenance purposes, authorized individuals within RRA may monitor equipment, systems and network traffic at any time.

RRA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

RRA reserves the right to conduct software audit of all hardware once a year to ensure that software copyrights and license agreements are adhered to.

Where licensing states limited usage (i.e., number of computers or users etc.), then it is the responsibility of IT staff to ensure these terms are followed.

All software installation is to be carried out by IT staff. All employees must receive training on all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of the Commissioner of IT and Digital Transformation to ensure that the employee is properly trained before user login and password are provided on live system.