System Administration

System administration is a core function in digitalization implementation, it involves a range of activities from installation, server support or computer systems as well as service outage response and other related problems.

This section focuses on user management, general system management utilities, and password policies. Mechanisms by which data stored on every government institution’s owned computing system and utilized by government employees is defined.

- User collaboration and email service
- Password Policy
- Email Accounts
- System access and authorization

User collaboration and email service

- All Public institutions are obliged to encourage and make sure that all employees own official work emails and to collaborate online using official and well tested channels such as for video conferencing or document handling and transfer.
- All employees shall collaborate with each other using the official work email internally wit hin the
  institution and shall also use the same work email while collaborating with other public ins titutions or other institutions.
- An employee shall be assisted to set up their email by the system administrators and such email shall be suspended when the employee leaves their current employment from the institution.
- All public servants shall also be obliged to avoid using collaborative social media channels other than the officially provided channels for work related communication.
- Where such online collaboration is essential, but the official channel cannot support it, counsel
  shall be sought from the institution leadership and RISA shall be engaged to assess risks i nvolved and advise accordingly.

Password Policy

The following are minimum requirements to create as well as protecting password:

- The length of a password is 10 characters and shall comprise at least 2 lowercase, 2 uppercase, numbers, and special characters such as ! @ # $ {} : ” > ? <;
- Password shall not use part of your login name; and password shall not have part of numbers easily remembered such as birthdays, phone numbers, etc.
- Password shall not be “remembered” if the “Remember Password” feature in the application program such as Internet Explorer, Google Chrome, Safari and Mozilla Firefox are used.
- For more details refer to the Directives on Cybersecurity for Network and Information Systems for all public institutions in its section 12 page 8 and Minimum Cyber Security Standards for Public Institutions published on the National Cyber Security Authority website.

Email Accounts

- All employees shall use corporate emails for any official communication.
- Email accounts belonging to government institutions shall have a domain with a suffix of .gov.rw for example abc.xyz@risa.gov.rw.
- The e-mail account format shall be FirstName.LastName@institution.gov.rw
- Administrative visitors to the institution, academic and professional interns, consultants and experts shall be assigned temporary email accounts to facilitate operations and communications and those emails shall be closed immediately after the user's assignment is completed.
- Requests shall be made to the IT department and the temporary account created shall not be linked to the personal account (i.e., Gmail, yahoo mail, etc.)

System access and authorization

- All corporate computers shall be joined to the Active Directory-Domain Controller for proper management and access to institutional resources.
- **Connection to the local area network (LAN):** End-user/Personal computers that have been out of office shall be automatically updated with the latest antivirus.
- **Computers:** users shall terminate active sessions or log out of their computers when moving away from the workstation unless they lock the computer and re-enter the password as required.
- **Computer rooms and storage facilities**: shall always be locked when unattended. Failure to apply necessary protection for equipment shall constitute neglect and the user may be held liable for any loss.
- All users shall be responsible for the safety and custodianship of the end-user devices (laptops, tablets and Smartphones) in the office and outside the office.
- **Standardization of hardware and software:** IT administrators shall standardize computer software and hardware for users based on but not limited to job function, division, and the least privilege principle.
- **Printers and scanners operation:** users shall be required to share printers on the network based on physical proximity and division for resources optimization where applicable. IT administrators shall ensure that all management interfaces of printers are protected by a password to prevent unauthorized use or configuration.
- Individuals shall take care of efficient management of printing resources by only printing when a paper copy is necessary. Sensitive or classified printed documents shall immediately be removed from the printer after printing to prevent unwanted information disclosures. Only authorized maintenance personnel shall carry out printer repairs.
- **Remote administration and security:** This is the ability to manage and monitor systems, servers and network devices from a location other than their physical presence. While remote administration offers convenience and flexibility, it also presents security for security. Therefore, IT Personnel shall be cautious when providing remote support as well as accessing Office resources while at home.
- **License Activations:** Government institutions shall ensure that computers and Servers are installed and activated with genuine Operating systems and license keys.