Cyber Security

- Security Policy and Procedures
- Minimizing the exposure of systems to External Networks
- Access Control
- Implement network segmentation
- Institution awareness and Training
- Audit and Accountability
- Configuration Management
- Identity Management and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Risk Assessment
- System and Communications Protection
- System and Information Integrity
- Personally identifiable information (PII) Processing and Transparency
- Contingency Planning
- Supply Chain Risk Management
- Passwords Protection

Security Policy and Procedures

The public institution shall as a minimum have a documented Information Security Policy (ISP) based on information security requirements defined in this document and applicable legal, statutory and regulatory requirements.

Information security and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and interested parties, and reviewed at planned intervals and if significant changes occur.

The institution shall have documented operating procedures for information processing facilities. Operating procedures shall be available to personnel who need them and are reviewed at planned intervals, and if significant changes occur.

Minimizing the exposure of systems to External Networks

- Install and configure gateway firewall.
- Configure inbound and outbound Access Control List (ACL) to control only required and legitimate traffic only to be allowed to go in and out of the network.
- Close all the ports and only open the required port.
- Avoid “any” “any” rules set up in all the configurations.
- All rules must be configured to ensure no “unwanted services” or “hosts” are exposed to the internet, web protection anti-malware, web and app visibility, control, and protection.
- Implement network segregation by having Demilitarized Zone (DMZ) for public facing servers, server zone and user zone.
- All remote access to digitalization infrastructure shall be done via VPN.

Access Control

- The institution shall limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- The institution shall limit system access to the types of transactions and functions that authorized users are permitted to execute (role-based access control).
- The institution shall have a procedure for removal of access rights (termination) for all departing or resigning personnel, both employees and contractors/third parties. This procedure shall coordinate management decisions with the system administrator/personnel who is responsible for executing system access termination.
- In case of malicious activity done by the employee, or contractor (third-party employee), access rights shall be immediately revoked according to the incident response procedure.

Implement network segmentation

- **Access control:** It shall start with IT assets, data, and personnel classification into specific groups, and restrict related access through VLAN.
- **Access management**: access to VLANs shall be restricted by isolating them from one another and dispatching resources into different VLANs, so that a compromised system in one segment does not translate into exploitation of the entire network.
- **Use of secure remote access methods:** any remote access to the institution network or system shall be secured through VPN for any remote access required. Remote access shall be further hardened by limiting the number of IP addresses that are allowed to connect remotely for security and safeness.

Institution awareness and Training

The institution shall ensure that executives, senior management, managers, systems administrators, and users of institutional systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

The institution shall ensure personnel are trained to carry out their assigned cybersecurity-related duties and responsibilities. It is advised to Provide ongoing security awareness and training programs for government staff to educate them about security best practices as well as data protection law for the safety of personal data mostly on technical and institutional measures required for the compliance.

Audit and Accountability

The institution shall create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. The institution shall ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

Configuration Management

The institution shall establish and maintain baseline configurations and inventories of institutional systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. The inventory shall contain information about all users and all accounts in systems and applications.

The institution shall establish and enforce security configuration settings for information technology products employed in institutional systems.

Identity Management and Authentication

- The institution shall identify system users, processes acting on behalf of users, and devices.
- The institution shall authenticate (or verify) the identities of users, processes, or devices as a prerequisite to allowing access to institutional systems.
- The institution shall enforce a minimum password complexity and change of characters when new passwords are created.
- The institution shall allow temporary password to use for system logons with an immediate change to a permanent password.

Incident Response

The institution shall have an operational incident-handling capability for institutional systems, including preparation, detection, analysis, containment, recovery, and user response activities.

The institution shall notify the public authority in charge of cybersecurity about every incident. This also pertains to the incidents that can be handled by the institution itself. If the institution cannot handle the incident and/or the incident concerns critical public safety, the institution shall request support from the appropriate public authority.

The institution shall have documented and implemented procedures for responding to cybersecurity incidents.

The procedures shall include at least:

- Reporting information security incidents,
- Planning and preparing to respond to incidents,
- Monitoring, detecting, analyzing and reporting events and incidents related to information security,
- Response, including escalation, supervised post-incident recovery and internal and external communications.
- The public institution shall ensure that incident-handling capability is supported at the appropriate level by human, technical, information and financial resources.

Maintenance

- The institution shall perform maintenance on institutional digitalization systems.
- The institution shall provide controls on the tools, techniques, mechanisms and personnel used to conduct system maintenance.

Media Protection

- The institution shall protect (i.e., physically control and securely store) system media containing paper and digital media.
- The institution shall limit access to system media to authorized users.
- The institution shall sanitize or destroy system media before disposal or release for reuse.
- Conduct regular audits and assessments to ensure compliance.
- The public institution shall ensure identification of records and their retention period, considering legislation or regulations and community or societal expectations, if applicable.
- Law № 058/2021 of 13/10/2021 relating to the protection of personal data and privacy in Rwanda (article 52). Information systems shall permit the appropriate destruction of records after that period if the institution does not need them.

Personnel Security

- The public institution shall identify (inventories) its own human resources. For each official position with access, the scope of duties and the analyzed security requirements are defined (the level of access to zones, rooms, documents, systems etc.).
- The public institution shall verify the identity of employees and job candidates based on the submitted original documents (containing names, surnames, date of birth, address and photo).
- The institution shall screen individuals prior to hiring them as well as taking up a role related to access to sensitive information. In particular, it does so before authorizing access to digitalization systems of the institution.
- The institution shall ensure that institutional systems are protected during and
- after personnel actions such as terminations and transfers.
- The institution shall provide basic training on information security upon commencement of employment.
- The institution shall ensure the identification of people having access to the facilities by introducing mandatory identifiers (badges).
- The institution shall ensure that security personnel are immediately provided with information on the denial of access for the departing employee.
- The institution shall ensure periodic verification of physical access and authorizations for employees and external subcontractors related to position and work performed.
- The public institution shall provide all employees with awareness training in social engineering threats. Completion of the training shall contain the training program content, its duration, the instructor and the trainee's signature.
- The public institution shall have procedures for verifying the qualifications of candidates and employees.
- The institution shall ensure that people with no criminal record are employed in key positions. This is done by a successful job candidate submitting a Criminal Record Certificate.

Physical and Environmental Protection

- The institution shall divide the area it manages into security zones based on risk assessment to ensure physical security.
- The institution shall provide, limited by the scope of official duties, access to particular security zones. The principle of necessary access applies (need to have).
- The institution shall limit unauthorized individuals' physical access to institutional systems, equipment, and the respective operating environments.
- The institution shall provide employees in charge of systems and infrastructure with basic physical security training.

Risk Assessment

The institution shall periodically (at least once a year) assess the risk to institutional operations (including mission, functions, image, or reputation), institutional assets, and individuals resulting from the operation of institutional systems and the associated processing, storage, or transmission.

System and Communications Protection

- The institution shall monitor, control, and protect communications (i.e., information transmitted or received by institutional systems) at the external and key internal boundaries of institutional digitalization systems.
- The institution shall use architectural designs, software development techniques, and systems engineering principles that promote effective information security within institutional digitalization systems.

System and Information Integrity

- The institution shall identify, report, and correct system security flaws on time.
- The institution shall protect malicious code (malware) within institutional digitalization systems and update malicious code protection mechanisms when new releases are available to make sure that detected malicious software is addressed.
- The institution shall monitor system security alerts and advisories and take action as soon as they are published.

Personally identifiable information (PII) Processing and Transparency

The institution shall identify and meet the requirements for preserving privacy and protecting PII according to applicable laws and regulations and contractual requirements and especially comply with the law(s) relating to the protection of personal data and privacy in Rwanda.

Contingency Planning

- The institution shall ensure that backup copies of data, software and system images are regularly made and tested.
- The institution shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for institutional information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Supply Chain Risk Management

- In collaboration with a competent authority where applicable, the institution shall establish and agree on information security requirements with each supplier based on the type of supplier relationship.
- In collaboration with a competent authority where applicable, the institution shall define and implement processes and procedures to manage the information security risks associated with the use of supplier’s products or services.

Passwords Protection

- Users shall have different passwords for different accounts.
- All default passwords shall be changed upon installation of new software or new Operating System (OS).
- Passwords shall be securely hashed and stored. Never store plain text passwords, and use strong, industry-standard encryption algorithms.
- Failed login attempts shall be logged and limited to three times and then lock the user.
- Account lockout duration shall be a minimum of 20 minutes to a maximum of 1 hour.
- A two-factor authentication shall be set up for critical applications and/or systems.