Digital Adoption Implementation Guidelines

This document serves as a guide to support the government of Rwanda institutions herein referred to as public institutions and affiliated institutions during digitalization implementation and application to ensure consistency in terms of security, reliability, scalability, effectiveness and efficiency in service delivery.

- Introduction
  - Objectives
  - Benefits
  - Scope
- Principles
- Network and Communication Infrastructure
  - Network design
  - Network Implementation
  - Network Management
- Hardware & End-User Equipment
  - User devices
  - Precaution measures
  - Stolen computers
  - User responsibilities
  - Hardware acquisition, maintenance

    - Hardware disposal

- Software Applications and Data
    - Software applications
    - Data
    - Business Continuity (BC) and Disaster Recovery (DR)

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

- 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

- Sector Digital Strategic Plan
    - Assessment of the current situationge
    - Definition of the strategic target position
    - Definition of gaps
    - Establishing a roadmap to close the gaps.
    - Roles and responsibilities
    - Resources and Impact
- Digitalization Project Management
    - Digitalization project initiation
    - Digitalization project documentation
    - Digitalization project implementation
- Digitalization Office Function, Staffing and Training
    - Digitalization staff
    - Digitalization talent and capacity building
- Innovation and Creativity
    - Challenge Definition
    - Ideation Stage
    - Prototyping
    - Testing Stage
    - Implementation
- Consequences of Non-Compliance
- Document Review Cycle
- References

Introduction

This document serves as a guide to support the government of Rwanda institutions herein referred to as public institutions and affiliated institutions during digitalization implementation and application to ensure consistency in terms of security, reliability, scalability, effectiveness and efficiency in service delivery.

It requires institutions to be compliant to the guidelines, requirements and for them to use this guide as a reference document during strategic planning, acquisition, deployment, and governance in public institutions when digitalization and related digitalization services are to be relied on as an enabling environment.

This document henceforth replaces the ICT Implementation guidelines for the Government of Rwanda that were published in 2019.

Any inquiry about these guidelines shall be directed to Rwanda Information Society Authority via email: info@risa.gov.rw

Objectives

These guidelines aim at providing a uniform framework for the design, configuration, and management of digitalization across government institutions in Rwanda to:

1. Harmonize and ensure security and protection of critical systems, infrastructure, data and information as determined by available national laws, orders, directives and guidelines.
2. Improve and conform to best digitalization practices, standards and business continuity.
3. Enable shared infrastructure and services set up especially where different institutions may share buildings among others.

Benefits

Adoption of these guidelines will allow government institutions to:

- Have a high quality and reliable work environment.
- Efficiently deliver government services to citizens.
- Remove duplication and reduce costs related to digitalization operations.
- Enable scale up and easy integration of future technologies.

Scope

These guidelines shall be strictly adhered to by all government institutions, including institutions at central and local government as well as all their affiliated agencies and parastatals.
They cover areas including network infrastructure, hardware and end-user equipment, data, software Applications, system administration, cyber security, digitalization strategies and policy, digitalization project management, digitalization hardware and software acquisition, staffing, innovation and capacity development.

Principles

1. These digitalization implementation guidelines shall be used as best practices for digitalization deployment.
2. Digitalization offices shall submit sector level compliance reports annually as an assessment tool to evaluate enforcement of these guidelines.
3. All institutions shall have digitalization policies, user guides and manuals, network, hardware and system documentations.
4. All sectors shall have digital strategic plans and related policies to cater to sector specific digitalization needs.

Network and Communication Infrastructure

This section provides guidelines and requirements for deployment of IT networks across institutions. Any institution that is intending to build a new network or upgrade the existing network infrastructure shall first seek guidance from RISA.
For better network management practices, the following shall be considered:

Network design

The following parameters shall be based on while designing institution network:

1. **Number of users in the institution:** The number of network users shall be both employees and guests.
2. **Services accessed or offered by the institution:** Services shall be defined and categorized depending on operational and availability requirements.
3. **Broadband technology:** The technology to be used shall be chosen according to location, institutional business requirements, and offices set up. Wireless local area networks are advised for convenient and modernized work spaces.
4. **Physical network diagram:** The design of the physical network diagram will consider the number of users based on the institutional structure, the interior design/aesthetic of the building and sitting arrangement (i.e. whether all users sit on the same floor or on different floors) and shall also consider whether the infrastructure of the building is shared or not.
5. **Logical network diagram:** The design of the logical network diagram shall consider existing systems, services, and applications according to the institutional business processes. The design should also provide the capability for scaling up and growth.
6. **Network Security:** All Government institutions shall comply with the current cyber security directives for network and information systems issued by a competent authority.

The below recommended bandwidth allocated to the different categories of users considers the average number of end user devices to be two and these devices can be computers, smartphones or tablets among others.

Number of users using devices	Bandwidth in Mbps		Number of users using computers	Bandwidth in M
1-10	15		121-140	210
11-20	30		141-160	240
21-30	45		162-180	270
31-40	60		181-200	300
41-50	75		201-240	360
51-60	90		241-280	420
61-70	105		281-320	480
71-80	120		321-360	540
81-90	135		361-400	600
91-100	150		Above 400	Individual Cas Basis (ICB)
101-120	180			

Network Implementation

1. **Network equipment:** The network equipment and devices comprising the core network infrastructure to provide connectivity and security features shall among others include a rack, minimum routers, switches, and access points, as well as a firewall.
2. **Network cabling, labeling and physical layout:** Any network structure shall consider latest cabling and labeling standards.
3. **Network room:** Institutions shall have network rooms at their premises. Modular racks/containerized racks are recommended to be used. Note that this room will not serve as a data center for the institution.

They shall comply with the following minimum requirements for a modular rack:

Location	The network room at the institutional premises shall be in an isolated secure place away from mechanical shocks and/or excessive vibrations, clean and shall not be used for other purposes.
Size	Minimum depending on the number of network equipment
Room Temperature	The network equipment shall be put in a place where there is an environmental control installed i.e. air condition/cooling system that allows devices to remain in good condition.
Structural consideration (floor, ceiling, and walls)	Doors shall be metallic and no other materials that are fire prone. The network room shall not have exterior windows. In case of existing windows, frosting has to be implemented. Ceiling shall be fully closed and with a minimum height of 2.7 meters. Floor shall have a rack raiser. The walls shall not have water pipes that could burst and drench the system.
Environmental Control	Environmental control includes ventilation (natural and mechanical), filtration, ultraviolet germicidal irradiation, and other methods of air cleaning. A network room shall have sensors throughout the area that measure both temperature and humidity. In case of modular racks, environmental monitoring shall be inbuilt. Airflow Planning: A good airflow plan helps to avoid ‘hot spots’ and eliminates heat from the area so it doesn’t cause damage.

Cable Management Solutions	Cabling shall be properly routed, organized, and supported. This involves organizing your cabling and connectivity hardware in a way that makes it easy to identify components and troubleshoot problems. This makes future upgrades and repairs easier while keeping your IT spaces professional (Cable management and labeling).

Electrical system	The network room shall have two different power sources dedicated non-switched, power redundancy, supplies connected to UPSs on separate power circuits, a clear-labeled emergency power-off switch and monitor system. Shall have an automatic voltage regulator with circuit drawing and main switch board for all services, equipment grounding system and lighting rod. A regular maintenance and testing shall be performed. For proper load monitoring, Power Distribution Unit (PDU) installed in racks shall be smart PDUs.
Access control and safety	Physical access to the network room shall be limited to only authorized individuals. Such access control systems (access card or biometric keyboard or locking door) shall be used at all entry points 24/7, and clear procedure to ensure access is removed when an individual no longer has entry permission, and access list shall be reviewed periodically. Communication rooms shall have fire prevention system, electric all type fire extinguishers and dry pipe fire suppression. Alarm system and CCTV cameras shall be installed to monitor and record all events.
Network room cabinet systems	Racks enclosures shall have at least adjustable 19U, 24U with mounting rails and other sizes depending on the need. They shall also have terminals that allow cables for power and data pathways at the top and bottom. All cabinets shall be lockable.
Personal Protective measures	In order to safeguard Engineers' lives during the line of duty, protecting them from hazards and other injuries that they may sustain, adopting the use of personal protective equipment is recommended. These are key PPE to consider per personnel involved: • Safety footwear • Evolution 6121 Hard • Hat Safety glasses • Safety gloves

Noise protection Earplug
Class 3 high visibility vest Anti-static wrist strap.

RISA framework contract shall be used while procuring the network room equipment.

Documentation: This includes network drawings, network connection, network segmentation and configuration information, addresses of all devices on the network with static IP addresses, and logbooks. The document versions shall be reviewed periodically, and any changes shall be tracked.

Network Management

- **Network performance:** Redundancy, load balancing, application response time, and quality of service shall be controlled and assured.
- **Network maintenance:** Each institution shall elaborate a network maintenance plan together with the disaster recovery (DR), business continuity (BC) plan and an escalation matrix in reference to the DR and BC published by RISA. RISA maintenance framework contract shall be used.

Hardware & End-User Equipment

Hardware & End-User Equipment

User devices

Institutional devices used by employees shall be labeled (tagged), recorded and proper naming shall be done. They shall not be used to illegally process, distribute, or store any data protected by copyright of intellectual property. These devices shall not be used in activities that contribute to decreasing the employee’s productivity.

Precaution measures

- Offices with digitalization equipment shall be locked to prevent theft and other risks.
- Digitalization equipment shall not be placed next to air conditioners as humidity and heat can shorten the life of internal components.
- Users shall not eat, drink or smoke next to digitalization equipment as these may cause safety risks.
- Only suitable cleaning tools shall be used when cleaning computer keyboards, screens, printers and other digitalization equipment.
- Whenever possible, digitalization equipment shall not be connected to the same electric power as other power consuming devices.
- All other digitalization equipment taken into government premises shall be identified and recorded at the entrance security checkpoint.

Stolen computers

In case of a stolen computer, the user shall immediately report to the supervisor and to Rwanda investigation bureau (RIB) and to the administrator in charge. Institution’s rules and regulations governing loss of public properties shall be applied.

User responsibilities

- Users shall ensure proper use of digitalization equipment in accordance with all provisions of these guidelines.
- Users are required to report any misuse or potential threats to digitalization equipment.
- It is the user’s responsibility to seek guidance when in doubt of what constitutes acceptable or prohibited use of digitalization equipment.
- While the physical and logical security of digitalization equipment and data is primarily a responsibility of the Government, users as well shall take note that they share this responsibility.

Hardware acquisition, maintenance

All IT equipment shall be checked once in every quarter and maintained according to the elaborated maintenance plan. Institutions shall always refer to RISA hardware acquisition and maintenance framework contracts.

Hardware disposal

Following the institution’s disposal committee resolutions regarding digitalization equipment to be disposed, the current electronic devices’ disposal guidelines shall be adhered to.

Software Applications and Data

This section provides high level guidelines for software applications development, acquiring, usage and their security. It also provides guidelines for data processing, usage and protection.

Software applications

- **Architectural model for e-government applications:** All systems shall be documented in five viewpoints including the enterprise viewpoint (describing purpose, scope and processes), the information viewpoint (determining the structure and semantics of the system's information), the computation viewpoint, the engineering viewpoint and the technology viewpoint.
- **Software design:** Any new software design shall consider security by design, privacy by design, reusability, scalability, information sharing, user satisfaction, improved productivity, compatibility, interoperability, unified support, and cost-effectiveness, as principles. Each Government institution shall have comprehensive and detailed requirements and design documents for each software solution they manage.
- **Acquisition of new software or upgrade:** The digitalization office in collaboration with RISA shall determine whether the new software or upgrade is needed, and once justified, assess if it is to be developed internally or externally.
- The digitalization office can internally develop and implement the solution if they have the required resources, competencies and skills. In case the digitalization office cannot develop the solution internally, they shall utilize the RISA framework contract. In case the solution cannot be implemented under the framework contract, the institution shall officially request a non-objection from RISA to utilize other alternative options.
- Institutions should follow the ICT Spend Control Guidelines for Public institutions when acquiring new software.
- **Proprietary and open-source software:** Proprietary and open-source software shall be treated equally depending on the advantages and benefits to the institution according to the defined software design principles and regarding the needs and requirements at institution level. The institution with such a solution shall have the required training for its staff in order to have skills to maintain and support it.
- **Security Patch Management:** The institution managing the application/systems or a third party on behalf of the institution shall make sure that security patch management is done regularly and prioritize critical patches to address vulnerabilities promptly. The software source code for proprietary software shall reside in a centralized version control platform recommended by RISA.
- **Software development methodology:** Software solutions shall be developed following agile methodology and the development team shall focus on customer satisfaction, quick software delivery and response to change.
- **Software license:** Only genuine licenses are allowed in government institutions. The procurement of commonly procured licenses shall be done through a centralized framework. In case the licenses cannot be acquired under the centralized framework, the institution shall officially request for a non-objection from RISA. The choice of licensing mode (user based or server based) shall consider cost efficiency.
- **Software maintenance:** there shall be a focal team at institution level which shall elaborate the maintenance plan and collaborate with RISA on regular basis for periodic

system audits, maintenance, updates, vulnerabilities assessment, and obsolescence of their systems, so as to ensure maximum system availability. A vulnerability assessment plan shall be made available by the digitalization office for each institution and make sure that all systems are secured with updated antivirus software.

- **Systems and software phase out:** the phase out of any system or application shall be done in collaboration with RISA and the security of information contained in the system shall be considered. The phase out shall be based on each institutions criteria for the required phase out especially after a phase out assessment has been done, and related reports shall be availed for effective decision making.
- **Websites:** Websites of government Institutions shall be designed according to the official template provided by RISA. These websites shall be hosted at the National Data Center. Web Content shall be updated timely, and the website shall be monitored by the Institution. All websites of government institutions should be registered under the .gov.rw subdomain while those in the academic sector should be under .ac.rw. The requests for the .gov.rw domain should go through RISA before submission to the competent issuing institution for approval.

Data

Data produced or collected by government institutions is necessary for measuring effectiveness and developing public services. In that sense, institutions are expected to perform the following:

- Data discovery and metadata capture.
- Search and filtering.
- Business Glossary.
- Data Quality Monitoring.

This shall allow public institutions to reduce the time it takes to find the right data and to facilitate more data-informed decisions. Data shall also be classified by access level, specifying which data is accessible to the public, government institutions, Private and other partners.

- The value in data sharing between government institutions lies in the ability to use the data for meaningful insights. For guidelines on data sharing, refer to the data sharing policy.
- Categories of data to be protected shall include but not limited to applications and databases, email, websites, operating systems, data on personal computers among other data. Encrypt sensitive data both in transit and at rest, using strong encryption algorithms and ensure that encryption keys are securely managed and stored.
- All government data shall be hosted locally at the institution or within Rwanda and the institution owning it shall determine who to share the data with based on access levels. Depending on the type of data, the duration of retention shall be determined by the institution owning the data.
- Data and data storage breaches shall be avoided, and security safeguards shall be put in place by the institution holding the data. For effectiveness, personal and sensitive data shall be classified to cater for security and use by putting into consideration measures to conduct and have data backups to prevent data loss by all government institutions.
- All institutions shall also be obliged to enforce the requirements of the Data Protection and Privacy Law № 058/2021 of 13/10/2021.
- The Data Protection Law shall be used as a guide to determine the processing of Personal data and sensitive data, and all institutions shall be obliged to comply with this law. Under this law,
- processing of data is an operation or set of operations which shall be performed on personal data or on sets of personal data and sensitive data whether or not by automated means, such as access to, obtaining, collection, recording, structuring, storage, adaptation or alteration, retrieval, reconstruction, concealment, consultation, use, disclosure by transmission, sharing, transfer, or otherwise making available, sale, restriction, erasure or destruction.
- The Data protection and Privacy law also provides safeguards to process sensitive and personal data. In other words, security of processing this involves the ability to ensure confidentiality, integrity and availability of data. It is recommended to all public

institutions to perform a Data Protection Impact Assessment (DPIA).

- Data protection impact assessment helps to assess the impact of a process or project more specifically a processing that an institution is going to carry out. DPIA aimed at two important understandings; the understanding of the risks to individuals (data) as well as the understanding if the processing is necessary and proportionate and most importantly identifying security measures in place or needed and their adequacy level.

Business Continuity (BC) and Disaster Recovery (DR)

Business continuity management is a planning and holistic management through which institutions create and implement measures, strategies and plans which are effective to manage crises, respond to/ and recover from a disaster.

Business continuity is more than just a plan to recover from a disaster but a survival strategy for enterprises that enhances systems resilience, ensures high availability and continuous operations of solutions. All institutions shall therefore have Disaster Recovery plans as a measure and guide to use for Business Continuity in case disasters befall.

Disaster recovery consists of developing step-by-step procedures for ensuring a full recovery, however, when many think about DR, they usually think about Backup, while it is only one piece in BC-DR. Therefore, the following are recommended to be followed for best practices:

A. Based on the data and systems inventory and classification:

- All institutions shall have a backup mechanism for all data that is performed regularly and most importantly kept offsite; this means having taken your backups, stored them in a safe and accessible way. Local Backup on Recovery Devices shall be stored in house and then replicated
- to an offsite location where applicable. It is the local site that shall serve a master role and then the offsite backup.
- For important data and systems, all institutions shall have a Hot-standby DR solution based on both the Business Continuity and Disaster Recovery plans.
- For critical data and systems having a DR solution shall no longer be an option but an active-active DR solution by which both primary and secondary sites shall be active and processing requests in parallel. This solution shall not help in recovery and continuity of the business after the disaster but shall avoid a disaster altogether by minimizing the risk of losing data, systems and information The Recovery time objective and Recovery point objective (RPO and RPO shall be near to zero).
- For further clarifications and understanding about Disaster recovery and Business continuity refer to the current Business Continuity Management guidelines issued by RISA.
- For critical IT systems and applications hosted in the National Data Centre, the institution shall ensure that they subscribe to a minimum hosting plan that includes daily backups and disaster recovery services.
- For critical IT systems and applications hosted on premises, the government entity shall immediately consult RISA to devise a strategic road map for migration to the National Data Center.
- Pending full migration of critical IT systems and applications, to the National Data Centre and other IT systems and applications deemed non-critical and kept on premises,

Government institutions shall be required to comply with the institution’s detailed data backup schedule.

- For government data that resides on personal computers (Laptops & Desktops), government institutions shall set up a local file server that automatically synchronizes with users’ personal computers to keep copies of any data files as created/updated by users.
- Personal computers shall also be installed with an up-to-date Antivirus/Antimalware and no user shall be allowed to keep government data on a non-protected personal computer.
- Personal computers and servers shall have the latest Operating Systems installed or upgraded to the latest operating system.

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

- 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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Cyber Security

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.

Sector Digital Strategic Plan

All sectors are required to develop sector digital strategic plans to guide the sector’s digital adoption and implementation in accordance with each sector’s mandate, The Strategic plan shall be aligned to all relevant National guiding strategies. All plans where applicable shall have accompanying sector policies to enable effective implementation at the institution level.

The following is a summary of key steps to the development of digitalization strategic plan at the sector level:

Assessment of the current situationge

- The development of a digitalization strategic plan shall be initiated by the mapping of a sector’s business, information, applications, and technology and infrastructure domains.
- The mapping shall be aimed at highlighting the linkage between the above four domains to support the sector’s mandate and strategic objectives.
- The business domain shall focus on functions, services, processes, and roles.
- The information domain shall focus on data models, data source and data usage (internal and external).
- The application domain shall focus on applications portfolio, interfaces, and services.
- The technology and infrastructure domain shall focus on hardware and software assets as well as network infrastructure and configuration.
- The output of the above mapping process shall be the sector/institution’s IT landscape view known as the “As-Is Blueprint.”

Definition of the strategic target position

The desired situation and attainable targets shall be defined within a period of 3-5 years. The target position shall contribute to the overall goals and strategic objectives of the institution, the specific sector strategic objectives, and also aligned to the National digitalization strategy and existing digitalization initiatives by the government. Stakeholders’ needs and funding mechanism shall as well be considered.

Definition of gaps

Based on the assessed current situation, a gap matrix shall be developed to highlight shortages in the four domains.

Establishing a roadmap to close the gaps.

This stage shall highlight the following:

- Highlight Strategic interventions that bring about the desired results.
- Process changes that are needed and impact on institution’s business.
- Proposed new digitalization projects or existing digitalization projects that shall be re-focused and related description, priority, timeframe and schedule.

Roles and responsibilities

The success of the sector digitalization strategic plan depends on the endorsement, commitment, and ongoing support from the sector leadership and relevant stakeholders. It is important to establish a stakeholder’s matrix that clearly outlines respective roles and responsibilities for each party.

Resources and Impact

Resources (human and financial) needed to implement the strategy and potential sources of funds will be highlighted and a clear monitoring and evaluation matrix of the strategy to measure implementation progress and impact.

Digitalization Project Management

Digitalization project initiation

All digitalization projects shall be derived from the assessment as indicated in the above section of sector digitalization strategic planning. All institutions are advised to involve RISA starting with project conception stage onwards for better alignment and execution. Every institution shall ensure to have an approved project charter before the project is executed

Digitalization project documentation

Proper documentations of all digitalization projects across the government shall include the background and rationale of the project, projected output and outcomes, project key components, implementation plan, project implementation risk analysis and mitigation, proposed resources (human and financial), and proposed monitoring and evaluation frameworks.

Digitalization project implementation

The agile mode of implementation which allows visibility of project details and ability to manage changes is advised for digitalization project implementation across government institutions.

Digitalization Office Function, Staffing and Training

Digitalization staff

The digitalization office for public entities shall be established through consultation between the concerned entities, RISA and MIFOTRA.

The responsibilities and job requirements shall be aligned with the standard job requirements and responsibilities as published by RISA on a regular basis.

Digitalization talent and capacity building

All digitalization office staff across the Government shall perform team and individual self-skills assessment, skills development in accordance with respective job profile and duties.

All digitalization office staff shall leverage huge rich content and training available for continuous improvement of individual and team skills and capacity.

All training plans shall be done and consolidated at institutional level on yearly basis and shared with RISA for approval.

RISA shall establish the framework on yearly basis for all available training schedules for local, online, or abroad training and in collaboration with other external both national and foreign stakeholders, such trainings shall be offered.

Innovation and Creativity

All public institutions are called upon to embrace innovation and to adopt new ideas.

This section defines high level guidelines for user-centered Innovation processes as a framework to foster creativity and help develop appropriate solutions for addressing a broad range of challenges facing a public institution. This framework focuses on engagement with end-users in order to better understand and meet their needs.

The key stages of the user centered innovation processes are Challenge Definition, Idea Generation, Prototyping and then Implementation.

Challenge Definition

This stage describes the role of ideation within innovation processes, providing the designers with a range of different tools and techniques to get a deep dive understanding of the end-user’s problem, making them familiar with the problem.

It shall be encouraged to always start with the problem, never with a solution with first understanding of the problem to be solved. Every problem shall have a clear problem statement that consolidate and capture the end-users needs. A problem statement shall mark the starting ideation phase.

The methods to support the creation of a problem statement include:

- Context mapping which shall help to recognize contexts and patterns in the collected information.
- Cause-effect diagrams which shall help to differentiate the causes and the impact of problems.
- Questions to help to transfer the resulting problem definition into design opportunities.

Ideation Stage

After problem definition is ideation where the innovator shall learn as much as possible about a user and the user needs. Here, simple tools such as customer experience chains, personas, and explorative interviews shall be used.

Innovators shall be must be encouraged to use an empathy map as a tool to identify feelings, thoughts, and attitudes of existing or potential users and customers and understand their needs, speaking to experts who know the user-customer well and, of course, being active and doing what the user is doing. Some other tools to use shall include Customer Journey, Persona/User Profile and tasks to be done.

Prototyping

Building prototypes make ideas and proposed solutions tangible and perceptible. Prototypes shall range from simple critical function prototype to the final prototype. To build a prototype, simple materials that are good enough to test a function or an experience shall be used.

The “prototype” phase shall be closely connected to the “test” phase where feedback collected shall be used to learn more about the user and to improve or discard the proposed solution. It shall not be about solving the problem completely but instead to question elements of a possible solution. The experiments (or prototypes) shall be created in a very short period of time.

Testing Stage

The testing shall be conducted on potential users as a way to get feedback on the prototype but also to refine the view of the problem and the user. Tools such as a feedback capture grid and feedback techniques shall support the testing.

In addition, there are different test procedures. At this stage, the security of the systems and infrastructure shall be put into consideration before the final approval.

Among other things, testing shall help to learn as much as possible about the user and user needs by having the user interact with the prototype.

Implementation

A successful prototype will then be assessed for full development and implementation. This may lead to a new approved project that will be implemented at scale.

Consequences of Non-Compliance

Compliance to these guidelines is highly encouraged at all sector and institutional levels in order to mitigate risks, litigations and damage due to not complying with these guidelines. Exceptions to these guidelines shall be allowed only if approved by RISA.

Document Review Cycle

RISA and stakeholders shall review these guidelines every three years or when deemed necessary to address new issues arising from the use of IT systems and emerging technology trends in the industry.

The digitalization office in every government institution shall gather new inputs to use to update the document, investigate and follow-up on reported and suspected non-compliance and take necessary corrective actions.

References

1. Minimum Bandwidth for Broadband Internet Connectivity in Rwanda
2. Directives on Cyber Security for Network and Information System
3. Data Protection and Privacy Law
4. Guidelines for Disposal of Old IT Equipment
5. National Digital Talent Policy
6. ESO Grant Application Guidelines
7. National Strategy for Transformation (NST2)
8. ICT Sector Strategic Plan
9. National Cybersecurity Strategy of Rwanda
10. The National AI Policy
11. Cyber Crimes Law