# ICT Implementation Guidelines in Government Institutions

This document is meant to guide ICT implementation and application cross all government institutions in Rwanda, in order to ensure consistency in terms of security, reliability, scalability and efficiency.

- Hardware and End-User Equipment
    - Services
    - Computers and Communication devices
    - Power Supply and backup
    - Scanners and printers
    - End-use equipment
    - Hardware maintenance
- Software Applications and Data
    - Software applications
    - Data
- System Administration
    - Password Protection
    - Email Accounts
    - System access
- Cyber Security
    - Minimizing the exposure of systems to external networks
    - Implement network segmentation
    - Establish role-based access controls and implement system logging
    - Implement passwords policy
    - Institution level cyber security awareness
    - Perform regular vulnerability assessment and penetration testing
- ICT Strategic Plan
- ICT Project Management
- ICT Function, Staffing and Training
    - ICT Committee
    - ICT Unit
    - ICT staff recruitment process
    - ICT talent and capacity building
- ICT Hardware and Software Acquisition

    - Submission of annual ICT procurement plan to RISA
    - ICT centralized procurement
    - Decentralized ICT tenders
    - Development vs acquisition of software
    - Minimum requirements to determine the best solution
    - Internet bandwidth procurement
    - Procurement of hosting and cloud services

- Consequences of Non-Complience
- Document Review Cycle
- References

# Introduction

This document is meant to guide ICT implementation and application cross all government institutions in Rwanda, in order to ensure consistency in terms of security, reliability, scalability and efficiency. It provides compliance requirements and should serve as reference for ICT strategic planning, acquisition, deployment and governance in public institutions.
Any inquiry about these guidelines should be directed to Rwanda Information Society Authority via **email: support@risa.gov.rw**

# Objectives

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

1. Harmonize and ensure maximum security
2. Improve and conform to best ICT practices and standards
3. Enable shared infrastructure and services set up
4. Allow real time monitoring, back up, and business continuity

# Benefits

Adoption of these guidelines will allow government institutions to:

1. Have high quality and reliable ICT environment
2. Efficiently deliver government services
3. Remove duplications and reduce cost related to ICT operation
4. Enable scale up and easy integration of future technologies

# Scope

These guidelines are expected to 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 and software applications, system administration, cyber security, ICT strategies and policy, ICT project management, ICT hardware and software acquisition, as well as staffing and IT human capacity development.

# Principles

These ICT Implementation guidelines will be used as best practices for ICT deployment.

- Regular ICT audits will be conducted periodically by RISA to ensure compliance and enforcement.
- All institutions should have individual 3 years ICT strategic plans that are linked to the overall strategies of the institutions.

# Network and Communication Infrastructure

This section provides guidelines and requirement for deployment of IT networks across institutions in three categories:

# Network Design

- **Number of users in the institution:** identify the number of network users both onsite and offsite.
- **Services accessed or offered by the institution:** services should be defined and categorized depending on processes and availability requirements
- **Broadband technology:** should be chosen according to location, institutional business requirements, and offices set up. Wireless local area networks are advised for convenient and modernized work spaces
- **Bandwidth requirement1:** minimum bandwidth requirement should be according to user needs.

| *Number of staff using computers* | *Bandwidth in Mbps* | | *Number of staff using computers* | *Bandwidth in Mbps* |
|---|---|---|---|---|
| 1-10 | 2 | | 121-140 | 28 |
| 11-20 | 4 | | 141-160 | 32 |
| 21-30 | 6 | | 162-180 | 36 |
| 31-40 | 8 | | 181-200 | 40 |
| 41-50 | 10 | | 201-240 | 48 |
| 51-60 | 12 | | 241-280 | 56 |
| 61-70 | 14 | | 281-320 | 64 |
| 71-80 | 16 | | 321-360 | 72 |
| 81-90 | 18 | | 361-400 | 80 |
| 91-100 | 20 | | Above 400 | Individual case basis |
| 101-120 | 24 | | | |

- **Physical network diagram:** should consider the number of users based on the organizational structure, interior design of the building and sitting arrangement (i.e. whether all users sit on same Floor or on different Floors)
- **Logical network diagram:** should take into account systems, service, and applications according to the institutional business processes.
  The physical and logical network infrastructure design in Government institutions should be put in four categories based on the number of users:

  - **Category 1:** Small-sized network infrastructure for up 30 users
  - **Category 2:** Medium-sized network infrastructure for up 50 users
  - **Category 3:** Large-size network infrastructure for about 100 users
  - **Category 4:** Network infrastructure for more than 100 users

- **Network security:** all government institutions should comply with the cybersecurity directives adopted in June 2018 for network and information systems.

# Network Implementation

- Network equipment: network equipment and devices comprising the core network infrastructure to provide connectivity and security features include rack, minimum routers, switches, and access points, as well as a firewall.
- Network cabling, labeling and physical layout: any network structure should consider latest cabling and labeling standards.
- Communication room: institutions should have communication rooms at their premises when proven necessary and should comply with the following minimum requirements:

| | |
|---|---|
| – ***Location*** | The communication room at the institutional premises should be located in an isolated place and only be accessed by authorized people |
| – ***Size*** | Minimum depending on the number of network equipment |
| – ***Temperature and humidity control*** | Temperature to be maintained between, and air humidity must be controlled at level that is compliant with the equipment (17.7°C - 23.8°C, and 30%-55% for humidity) |
| – ***Structural consideration (floor, ceiling, and walls)*** | The floor should be raised and well prepared to facilitate cleaning, cooling inside the room, and cabling installation, to allow elimination of dust. Floor tiles to facilitate cleaning<br>Walls should have no external windows nor electrical conduits, should have wall block sensor, door frame size should be sufficient to allow easy removal of equipment, doors must open 180° outwards, minimum 90 cm wide and 2m high. Only equipment related to the communication room should be present in the room. |
| – ***Electrical system*** | The communication room should have two different power source dedicated non-switched, power redundancy, supplies connected to UPSs on separate power circuits, a clear-labeled emergency power-off switch and monitor system.<br>Should have automatic voltage regulator with circuit drawing and main switch board for all services, equipment grounding system and lighting rod. A regular maintenance and testing should be performed. |
| – ***Access control and safety*** | Physical access to the communication room must be limited to only individuals with legitimate responsibilities justifying such access. Access control system (access card or biometric keyboard, or locking door) should 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 must be reviewed periodically. |
| | Communication rooms should have fire prevention system, electric fire extinguishers and dry pipe fire suppression alarm system and CCTV cameras must be installed to monitor and record all events |
| – ***Communication room cabinet systems*** | Racks enclosures should have at least adjustable 19U or 24U mounting rails, with access points for power and data pathways at the top and bottom. All cabinet must be lockable, and must be set in secure area within the Communication room. |

In addition to the above minimum requirements, the following are guidelines for network equipment in the communication room:

− **Switches:** small medium and large institutions are advised to use 24 ports, PoE, 10/100/1000, 4 T/Small Form-Factor Pluggable (SFP) LAN Base image. A 48 ports switch may be used for larger institutions.
− **UTP data patch panels:** should be of CAT6, 24 ports or more depending on latest technology.
− **Routers:** should support high-bandwidth module-to-module communication at higher speeds based on the platform, some of the 10/100/1000 Ethernet ports can support small-form factor pluggable (SFP) based on connectivity in addition to RJ-45 connections, enabling fiber or copper connectivity.
− **Firewall:** latest firewall network security should be implemented. (For more details on requirements refer to Cyber Security directives)
Access Points: the number of access points may vary depending to the building configuration, advisable wireless standards are 802.11a/b/g/n/ac (2.4 GHz/5 GHz)
− **LAN Ethernet cabling:** CAT6 FTP or advanced types.

- **Documentation:** this includes network drawings, network connection and configuration information, addresses of all devices on the network with static IP addresses, and log documents. The document versions should be reviewed periodically, and any changes should be tracked.

# Network Management

- Network performance: redundancy, load balancing, application response time, and quality of service should be controlled and assured.
- Network maintenance: each institution should elaborate a network maintenance plan, together with the disaster recovery and business continuity plan.

# Hardware and End-User Equipment

This part is focused on Hardware devices including servers, desktop computers, scanners and printers. It specifies the recommended hardware configuration and the operating system wherever applicable.

# Services

Government institutions are required to host all government data in the National Data Center (NDC) as per the Ministerial instruction in March 2012). However in case of colocation, institutions may rent space for servers and other computing hardware at the Data Center. These servers may include Web Servers, Mail Servers, File Server (Application), storage and other computer systems.

# Computers and Communication devices

The following are the minimum requirements that shall guide Government institutions during the acquisition of computers and communication devices for office use or any other administrative purpose. However, the detailed technical specifications are found in the framework agreement between RISA and providers on behalf of public institutions.

- **Desktop/Laptop:** the following are the minimum requirements depending on the purpose of use.

- Hard Drive: 500 GB or 1TB
- Processor: Core i5 or i7
- Memory: 4GB RAM or 8 GB RAM
- Screen size: 14” or more
- Operating system: Windows/ Mac OS/Linux (Genuine)
- Uninterruptible Power Supply (UPS) for Desktop

- **IP Phone:** should be used where deemed necessary
- **Personal mobile devices:** (mobile phones, tablets, pads) can be used and a bring- your-own-device (BYOD) policy should be defined to ensure secured access to the institution’s network.

# Power Supply and backup

The computer network infrastructure at the institutional premises should have main power supply and power backup battery. General specifications are provided in the framework contract that governs the acquisition of the computer devices and related power supply as well as backup solutions.

# Scanners and printers

Government institutions are recommended to acquire printing, scanning and copying as services instead of procuring, operating and maintaining printers, scanners and copiers. Institutions’ system administrators should have control usage and ensure access credentials are strictly managed. In some exceptional cases where institutions have to acquire such hardware devices, the recommended best practice is to use all-in-one devices.

# End-use equipment

- **User devices:** institutional devices used by employees should be labeled and recorded. Proper naming should be done, in accordance to advised network set up. They should not be used to illegally process, distribute, or store any data protected by copyright of intellectual property. These devised must not be used in any activities that contribute to decrease employee's productivity.
- **Housekeeping rules:** offices with ICT equipment should be locked to prevent theft and other risks; ICT equipment should not be placed next to air conditioners as humidity and heat can shorten the life of internal components; users should not eat, drink or smoke next to ICT equipment as these may causes safety risks; only damp cloths with suitable cleaning fluids shall be used when cleaning computer keyboards, screens, printers and other ICT equipment; whenever possible, ICT equipment should not be connected to the same electric power as other power consuming devices; all other ICT equipment taken into government premises should be identified and recorded at entrance security check point.
- **Stolen computers:** in case of a stolen computer, the user should immediately report to the supervisor and to Rwanda investigation bureau (RIB) and to the administrator in charge; institution's internal rules and regulations should be applied.
- **User responsibilities:** users should ensure proper use of ICT equipment in accordance with all provisions of these guidelines; users are required to report any misuse of ICT equipment or alert IT managers of potential threats to ICT equipment; it is the user's responsibility to seek guidance from IT department or any related division in the department when in doubt of what constitute acceptable or prohibited use of ICT equipment; while the physical and logical security of ICT equipment and data, is primarily a responsibility of the Government, users as well must take note that they share this responsibility.
- **IT department's responsibility:** IT departments in every government institution should implement mechanisms and technological controls to ensure, monitor and enforce compliance to ICT policy and these guidelines.

# Hardware maintenance

**Maintenance plan:** All IT equipment should be checked once in every quarter, and maintained according to the elaborated maintenance plan.

**Maintenance contract with equipment supplier:** After the warranty period, there should be agreements with equipment suppliers and service providers and maintenance services should be provided at least every quarter. Extended service items such as training, phone, preventative maintenance visits, and trade-in benefits should be captured, and each type of contract needs to be reviewed and evaluated on its own merit whereby the decision is
made as to whether it’s necessary to enter into such an agreement before the warranty
period expires.

**IT Toolbox:** The IT unit should be equipped with the IT tool box for computer hardware and network maintenance. Before the acquisition of the aforesaid toolbox, the institution will seek for the technical assistance from RISA.

# Software Applications and Data

# Software applications

- **Architectural model for e-government applications:** all systems should be documented in five viewpoints including the enterprise viewpoint (describe purpose, scope and processes), the information viewpoint (determines the structure and semantics of the system's information), the computational viewpoint, the engineering viewpoint, and the technology viewpoint.
- **Software design:** any new software design should consider security by design, reusability, scalability, information sharing, user satisfaction, improved productivity, compatibility, interoperability, unified support, and cost-effectiveness, as principles.
- **Acquisition of new software:** competent team (EA team at institutional or sector level) has to be consulted in order to determine whether the new software is needed, and to assess if it is to be developed internally or externally.
- **Proprietary and open sources software:** should be treated equally depending on the advantages and benefits to the Government according to the defined software design principles and in regards to the needs and requirements at institution level.
- **Software development:** RISA should be consulted to approve development languages and platforms.
- **Software license:** only genuine licenses are allowed in government institutions. The choice of licensing mode (user-based or server-based) should take into account cost-effectiveness. The procurement of commonly procured licenses should be done through a centralized framework.
- **Software maintenance:** there should be a focal team at institution level, which should elaborate the maintenance plan to collaborate with RISA on regular basis for periodically system audits, maintenance, updates, vulnerabilities assessment, obsolescence of their systems, so to ensure maximum system availability.
- **Systems and software phase-out:** the phase-out or upgrade of any system or The application should be done in collaboration with RISA, and the security of information contained should be considered.
- **Messaging and collaboration:** the use of official emails should be enforced, and each institution should comply with the information security policy.
- **Antivirus:** Antivirus software should support a local license server and update server and provide automatic updates of the license server from the vendor site. Clients should get automatic updates from the local license server in case of non-availability of the update license server. The antivirus should support all available versions of the Microsoft Windows operating system (on the market) and should be browser/version independent. The network deployment feature should include virus updates status, license usage, client status, and installed machines.
- **Websites:** the web should be designed according to official template for government institutions; should be hosted at the national data center; web content should be update timely, and the website should be monitored.

# Data

- **Data availability:** Data should be available round the clock (24-hour access) to access from different time zones.
- **Data creation:** single point of capture, duplication of data capture should be avoided as much as possible.
- **Standardization of shared data:** should comply with any interoperability framework defined at institutional or sector level.
- **Data identifiers:** each shared data object should be identifiable by a globally unique identifier.

  **Data backup and recovery:** every institution should have in place a backup and recovery strategy; all data should be available both onsite and offsite.

  GoR's entities are required to host all IT systems and applications, which process, store and provide critical Government data and information in the National Data Center (NDC). These include core business applications and databases, emails systems, and websites.
- **Categories of data to be protected:** application and databases, email systems websites, operating systems, data on personal computers in institutions:

  − For critical IT systems and applications hosted in NDC, the institution should 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 should 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 NDC, Government institutions are required to comply with the detailed data backup schedule as
  section I.

  − For other IT systems and applications deemed non-critical and kept on premises, entities are required to comply with detailed backup schedule.

  − For government data that resides on personal computers (Laptops & Desktops),
  government institutions are required to set up a local file server that automatically synchronize with users' personal computers to keep copies of any data files as created/updated by users.

  − Personal computers should also be installed with an up-to-date
  Antivirus/Antimalware and no user should be allowed to keep government data on a non-protected personal computer.

  − Personal computers and servers installed with Windows Operating Systems
  should be upgraded to Windows 10 (for desktops and laptops) and to at least Windows Server 2008 (For servers). In the meantime, IT teams should ensure that there is no single machine still running Windows XP in any institution, and that all Windows 7, 8 are up to date with the latest updates/patches.

# System Administration

System administration is a core function in ICT implementation, it involves a range of activities from installation, support of servers or computer systems as well as service outage response and other related problems. In this section we are going to focus on user management, general network management utilities, password policies, and IP numbering conventions. Mechanisms by which data stored on every government institution’s owned computing systems and utilized by government employees is defined.

# Password Protection

- Password should not be written down on paper;
- Password should not be sent through email,
- Password should not be included in a non-encrypted stored document,
- Password should not be revealed over the phone,
- Password should not be revealed or hinted on a form on the Internet;
- Password should not be “remembered” if the “Remember Password” feature in the application program such as Internet Explorer, Google Chrome, Safari and Mozilla Firefox is used;
- Password should not be used on an account over the Internet which does not have a secure login (https);
- password should not contain common acronyms;
- Password should not have reverse spelling;
- Password should not use part of your login name;
- and password should not have part of numbers easily remembered such as birthdays, phone numbers, etc.

# Email Accounts

Official Government of Rwanda (GoR) employees as well as administrative visitors of departments must request for a generic user account to facilitate operations and communications. A request must be made to IT departments. Generic accounts created are not to be linked to a personal account (i.e. gmail, yahoomail, etc.) Email accounts will be vetted so as not to include names that are associated with other departments for example: helpdesk (IT Services);

> All email accounts belonging to government institutions must have a domain with a suffix of gov.rw e.g. @risa.gov.rw.

# System access

- **Connection to the local area network (LAN):** personal computers that have been out of office shall be automatically updated with the latest antivirus signature file by a server.
- **Computers:** users should terminate active sessions or log out of their computers when moving away from the workstation unless they lock the computer in which case they would be required to re-enter the password. Offices, computer rooms and storage facilities should always be locked when unattended. Failure to apply necessary protection for equipment shall constitute neglect and the user may be held liable for the loss. In addition, all users should be responsible for the safety and custodianship of the laptop 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.
- **Password requirement:** minimum password recommended length is 8 characters; minimum complexity of password should use lowercase, uppercase, numbers, special characters such as!@#${}:”>?<; passwords should be created keeping the sensitivity in mind; maximum password age should not exceed 60 days; minimum password age is 2 days; a password safe should be used to keep the passwords in a safe.
  Computers should be locked and enabled when the user is not attending it or there is inactivity. Rules being applied to password should also apply to passphrases that are used for public/private key authentication such as VPN, or any other system.
- **Printers and scanners operation:** users shall be required to share printers on the network based on physical proximity and division in order for resources optimization where applicable. IT administrators should ensure that all management interfaces of printers are protected by a password to prevent unauthorized use or configuration. Individuals must 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 should carry out printer repairs.

# Cyber Security

Cyber Security

# Minimizing the exposure of systems to external networks

- nstall and configure gateway firewall, IPsec and SSL VPN, and wireless;
- 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;
- Ensure that the network is secure by segregating different administrative duties; consider network protection including IPS, REB, HYML5 VPN, ATP, and Security Heartbeat.
- All remote access to ICT infrastructure should be done via VPN.

# Implement network segmentation

- **Access control:** should start with IT assets, data, and personnel classification into specific groups, and restrict related access through VLAN.
- **Access management:** access to VLANs should 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 organization network or system should be secured through VPN for any remote access required. Remote access should be further hardened by limiting the number of IP addresses that are allowed to connect remotely for security and safeness.

# Establish role-based access controls and implement system logging

- **Role-based access control:** access to network resources should be granted or denied based on job functions. Permissions should be defined based on the level of access needed to perform job functions and related duties.
- **Standard operating procedures:** should be established to allow the removal from network access of former employees and contractors.
- **Logging capability for each system:** should be implemented for each user and for each activity.

Cyber Security

# Implement passwords policy

- Strictly use strong passwords with minimum 8 characters comprised of alpha numerical and special characters, as was described in section 6.3;
- Users should have different passwords for different accounts;
- All default passwords must be changed upon installation of new software or new Operating System (OS);
- Failed login attempts should be limited to three times and then lock the user;
- Account lockout duration should be at minimum 20 minutes at maximum 1hour.
- A two-factor authentication should be set up for critical applications and/or systems.

Cyber Security

# Institution level cyber security awareness

Government institution must plan for and conduct regular internal cyber security awareness for end users at 3 times per year in partnership with RISA.

Cyber Security

# Perform regular vulnerability assessment and penetration testing

- **Preventive maintenance:** government institutions should plan and perform IT infrastructure vulnerability assessment and penetration testing at least once a year.
- **Incidence response:** government institutions should be prepared to mitigate or to respond as quickly as possible to a cyber-incident, which can hit the organization. A proper disaster recovery plan should also be put in place to insure business continuity while recovering from such an incident.

# ICT Strategic Plan

All public institutions are advised to develop an ICT strategic plan to guide the adoption and implementation of ICT in accordance to each institution's functions, in line with Smart

Rwanda Master Plan, the enterprise architecture blueprint development guidelines for GoR, the specific sector ICT strategy, and also aligned to other institutional strategic plans.
The following are key steps to the development of an ICT strategic plan at institutional level:

- Assessment of the current situation:

The development of an ICT strategic plan should start by the mapping of an institution's business, information, applications, and technology and infrastructure domains. The mapping is aimed at highlighting the linkage between the above four domains to support the institution's mandate and strategic objectives.
− The business domain focuses on functions, services, processes and roles.
− The information domain focuses on data models, data source and data usage (internal and external).
− The application domain focuses on applications portfolio, interfaces and services.
− The technology and infrastructure domain focuses on hardware and software assets as well as network infrastructure and configuration.
The output of the above mapping process is the institution's IT landscape view called "As-Is Blueprint"
Detailed guidelines on the 4 domains mapping process are provided as annex. **(Enterprise Architecture Blueprint Development Guidelines for GoR)**

- **Definition of the target position:** the desired situation and attainable targets should be defined within a period of 3 years. The target position should contribute to the overall goals and strategic objectives of the organization, the specific sector strategic objectives, and also aligned to the National ICT strategy and existing ICT initiatives by the government. Stakeholders' needs and funding mechanism should as well be considered.
- **Definition of gaps:** basing on the current position, a gap matrix should be developed to highlight shortages in the four domains. (Refer to the EA Blueprint Development Guidelines for GoR).
- **Establishing a roadmap to close the gaps:** should highlight the
  - Process changes that are needed and impact on organization's business,
  - Software, hardware assets that need to be purchased or retired,
  - New ICT projects that should be initiated or existing ICT projects that should be re-focused and related description, priority, timeframe and schedule.
- **Roles and responsibilities:** the success of the ICT strategic plan depends on the endorsement, commitment and ongoing support from different decision makers within the institution and outside the institution. It is important to establish a stakeholder's matrix that clearly outlines respective roles and responsibilities.

- **Funding and resources:** should summarize the amount of resources (human and financial) needed to implement the strategy and potential sources of funds.

# ICT Project Management

- **ICT project initiation:** all ICT projects should be derived from the assessment as indicated in the above section of ICT strategic planning. All institutions are advised to involve RISA at the starting of the project, since the project concept elaboration.
- **ICT project documentation:** proper documentations of all ICT projects across the government should include the background and rationale of the project, projected output and outcome, project key components, implementation plan, project implementation risk analysis and mitigation, proposed resources (human and financial), and proposed monitoring and evaluation framework. ICT project implementation: the agile mode of implementation which allows visibility of project details and ability to manage changes is advised for ICT project implementation across government institutions.

# ICT Function, Staffing and Training

# ICT Committee

- **ICT committee:** it is imperative that all government institutions establish an ICT committee.
- **Role of the ICT Committee:** the primary role of the IT committee is to define the institution’s ICT Strategy and ensure all ICT projects within respective entity department and agencies are well coordinated and aligned to the overall strategic goals of the institution.
- **Members of the ICT committee:** can vary from entity to entity but all ICT committees should at least be comprised of: Head of ICT, Head planning, and Head of Finance and the chair shall be elected among the team.
- **Operations of the ICT committee:** this committee should meet at least by quarterly; the institution’s ICT committee is expected to ensure ICT is leveraged to improve business process within the institutions and better services to constituents. This committee should closely collaborate with the sector ICT technical working group, and should report to the Chief Budget Manager of the institution.

# ICT Unit

The ICT structure of public entities is established through consultation between the concerned entity, RISA and MIFOTRA. Ideally, the reporting line for ICT function should be direct to the Chief Budget Manager, where it is not the case, ICT unit is advised to keep the chief budget manager updates and aware of ICT operations and plans in the institution. The responsibilities and job requirements should be aligned with the standard job requirements and responsibilities as published by RISA on regular basis.

> (More details can be found on RISA website)

# ICT staff recruitment process

- **Recruitment procedure:** the recruitment of ICT staff is done jointly by the recruiting institution and RISA.
- **ICT job vacancy advertisement:** is initiated at institutional level and each institution will submit ToRs to RISA ahead of time for review.
- **Candidates assessment:** institutions should contact RISA in writing with at least 15- day notice in order to plan for joint written and oral interviews

# ICT talent and capacity building

- All ICT staff across the Government should perform team and individual self-skills assessment, skills development in accordance to respective job profile and duties.
- All ICT staff should leverage huge rich content and trainings available for continuous improvement of individual and team skills and capacity.
- All ICT training plans should be done and consolidated at institutional level on yearly basis and shared with RISA for approval.
- RISA will establish framework on yearly basis for all ICT trainings schedule for locally, online or abroad.

# ICT Hardware and Software Acquisition

# Submission of annual ICT procurement plan to RISA

- **ICT procurement plans:** all government institutions should consolidate and share with RISA at centralizedprocurement@risa.gov.rw their ICT procurement plans on yearly basis in accordance to the government planning cycle. RISA compiles and harmonizes submitted ICT procurement plans to establish a single national ICT procurement plan. The national ICT procurement plan is shared back to all government entities.
  References: Ministerial Instructions of **N0. 001/MINICT/2012 12/03/2012 and RISA's letter Ref: RISA/CEO/420/17.**

# ICT centralized procurement

- **Centralized hardware procurement**

  − On yearly basis, RISA selects commonly procured ICT items from submitted institutional ICT procurement plans.
  − RISA sets technical specifications based on government needs and technology trend.
  − RISA initiates annual centralized tender of the above commonly procured ICT items.
  − RISA signs annual framework contracts based on unit prices and share them with all government entities.
  − Government entities issue purchase orders to selected bidders for acquisition of needed items.
  − Other ICT items that are not part of the centralized framework contracts, should be procured using the normal procurement process at institutions' level and RISA should be involves for technical support and advice.
  − Government entities that want to procure ICT items that are part of the centralized framework contracts but with different specifications should seek approval from RISA.

- **Centralized software procurement**

  The procurement of all commonly procured Application Software and System Software across the government should be done through a centralized framework process at RISA.

  − All application software across the government shall be acquired in line with the principles of information sharing, compatibility, unified support, cost- effectiveness, improved staff productivity and user satisfaction.
  − Government institutions should seek RISA's approval before embarking on major application software acquisition.
  − In order to minimize unnecessary redundancies and to avoid duplications, RISA shall confirm that there is no already existing application software within government that can provide equivalent functions and that can be replicated.
  − In the same line and to the extent possible:

    o Multi-tenancy application software shall be privileged to allow sharing of development and maintenance costs.
    o Multi-tenancy application software shall be either centrally procured through RISA or procured with participation and close supervision of RISA.
    o Government institutions shall to the extent possible, adhere to the use of open standards.

# Decentralized ICT tenders

- **Procurement process:** institutions should obtain approval from RISA to initiate any ICT procurement process
- **Relevance of the hardware/software item:** RISA shall confirm the to be acquired based on submitted ICT gap analysis and ICT gap bridging roadmap in reference to the section 8 on institution “ICT strategic plan”)
- **Validation of drafted terms of reference (ToR)/ requirements:** Government institutions are advised to collaborate with RISA on ToR’s development before publication of ICT tenders. Institutions can request RISA’s participation at any stage of the tender evaluation of ICT tenders.

# Development vs acquisition of software

- **Decision to acquire or develop the software:** government institutions should seek advice from RISA about the acquiring or developing the software.
  The below criteria should be based on in order to take a decision between acquisition and development:
- **Government institution can go for development in case:**

  – Requirements are very specific and cannot be found on the market;
  – Commercial solutions have prohibitive prices;
  – Commercial solutions' vendors do not supply source codes;
  – The support is critical and it is not to be provided by a vendors; and
  – The institution should have and ensure the development and software maintenance capabilities are available in house or locally by Rwandan companies.

- **Government institution can go for acquisition in case:**

  – The software is readily and cheaply available on the market;
  – The delivery time is critically short; or
  – The software reliability is very critical.

# Minimum requirements to determine the best solution

- **Total lifecycle cost:** including initial cost, installation, training, and recurrent cost for maintenance and support.
- **Maintainability:** the ease of how (cost and effort) the software can be modified to correct faults, improve performance or other attribute or adapt to a changed environment.
- **Interoperability:** ihis includes additional support required to integrate with existing systems. It also includes flexibility to accommodate changes over time and among multiple systems.
- **Portability:** usability of the same software in different environments. A computer environment can include hardware, operating systems, and interfaces with other software, users and programmers.
- **Scalability:** ability to support future growth and increased through put.
- **Availability and accessibility:** robust and redundant (fault tolerant) software to achieve required level of service without disruption from software failure.
- **Reusability:** ability to make repeated use of the software for additional requirements with minimum additional cost.
- **Functionality/performance:** ability to achieve operational requirements effectively and efficiently.
- **Security:** ability to protect system data and operational environment from loss or compromise.
- Additional criteria include: vendor viability, licensing restrictions, product market share, customer recommendations, frequency of upgrades, and potential obsolescence.

# Internet bandwidth procurement

- **Internet services:** government institutions should source all their internet services (4G internet and Fiber Internet connection) needs through the established framework as per the March 2012 ministerial instructions. (See annex)
- **Bandwidth capacity to be purchases:** bandwidth shall be decided based on the requirements of the intended user and usage purpose as detailed in section 3.1

# Procurement of hosting and cloud services

**Hosting and cloud services:** government institutions should source all their hosting needs through the established framework asper **the March 2012 ministerial instructions.**
Government entities sign individual contracts with the provider and a sample contracts as well as sample Service Level Agreements are shared by RISA. Any contract management issue which persists should be automatically escalated to RISA for resolution.

# Consequences of Non-Complience

Non-compliance of these guidelines may lead to disciplinary actions, where the individual will stand for all risks and damage caused by not implementing these guidelines.

> Exceptions to these guidelines shall be allowed only if approved by RISA.

# Document Review Cycle

RISA shall review these guidelines annually or when deemed necessary to address new issues arising from the use of IT systems and emerging technology trends in the industry. IT department in every government institution shall investigate and follow-up on reported and suspected non-compliance and take necessary corrective actions

# References


1. Guideline on minimum Bandwidth for Broadband Internet Connectivity in Rwanda
2. Directives on Cyber Security for Network and Information System