

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
- Computers and Communication devices
- Power Supply and backup
- Scanners and printers
- End-use equipment
- Hardware maintenance

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 devices 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 cause 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.