GOR ICT GENERAL DIRECTIVES

TABLE OF CONTENTS

1. INTRODUCTION

1.1 RWANDA INFORMATION SOCIETY AUTHORITY

Rwanda Information Society Authority was constituted by the Law No. LAW N°02/2017 of 18/02/2017, and its main missions are:

- To implement national Information and Communication Technologies (ICT) policies and programs in order to fast-track socio-economic growth;
- To implement strategies, which expand the access and affordability of Information and Communication Technologies;
- To accelerate community development through mainstreaming Information and Communication Technologies in national socio-economic sectors;
- To prepare and coordinate programs that increase the required skills in the field of Information and Communication Technology in order to achieve a knowledge-based economy;
- To strengthen programs on Information and Communication Technology innovation;
- To coordinate the implementation of projects that deliver Information and Communication Technology services;
- To cooperate and collaborate with other regional and international institutions with a similar mission.

1.2 PURPOSE OF THE DOCUMENT

This document is meant to serve public entities by setting the direction of ICT implementation in the organization in order to allow consistency and ensure standards and compliance in terms of ICT deployment and related decisions across government institutions.

1.3 SCOPE OF ICT GUIDELINES

The guidelines provided in this document are to be supplemented by another detailed ICT standards document, which is in the process of being drafted and to be validated by competent entities. This document will provide basic guidelines for Institutional ICT strategy development, ICT project initiation, ICT deployment, ICT staff performance to support institution business, and ICT security across the Public Sector. It is intended to guide both IT and non-IT people for informed decision making as far as government digital transformation is concerned.

1.4 THE STRUCTURE OF THE DOCUMENT.

This document is organized in different sections starting from the basic guidance for a GoR's institution to be able to draft a sound ICT strategic plan comprising the analysis of the as-is situation, the analysis of the to-be situation and coming up with a list of ICT projects to leverage ICT for better corporate performance, and to close any information and technical gaps. The document further provides reference procedures for:

- ICT project management,
- ICT staff management and capacity building,
- ICT technical specifications,
- ICT acquisition,
- ICT documentation, and
- ICT security.

2. ICT STRATEGIC PLAN

2.1 Introduction

As standard practice, GoR's institutions are required to develop strategic plans for their mandates and businesses. Strategic planning is where institutions take their current business environment and decides where they want to be in the future. They then construct a strategic plan on how to get from the current to the future state. A very analogous process can be applied to Information and Communication Technology – where the current infrastructure is examined, then the desired future architecture is laid out based on both the business plans as well as what is known about future technology. A set of projects is then constructed to achieve this goal. It is important that both business needs and technical needs are considered. Upgrades, replacements and improvements can't be performed for technology's sake unless there is a business need for it. Conversely, it wouldn't make a lot of sense to build complex business processes on top of obsolete information technology infrastructure.

It is therefore very important to put together and maintain ICT strategic plans at both institution and sector levels. The establishment of ICT strategic plans should be done with a direct involvement of RISA for guidance, alignment and harmonization. On the other hand, according to the Smart Rwanda Master Plan (SRMP), each of the following sector should have a proper ICT strategic plan developed through sector consultation and with the support of RISA:

- Finance,
- Health,
- Education,
- Agriculture,
- Women empowerment through technology
- Trade and industry, and
- Governance.

However due to the proven impact of ICT on service delivery and operations' efficiency, other sectors are also required to make ICT a key component of their strategic and implementation plans. These include:

- JRLOS

- Social protection
- Infrastructure (Energy, transport),
- Capacity building and Employment promotion sector,
- Water and sanitation,
- Youth
- Private
-

2.2 The guidelines for Institutional ICT strategic plan development

2.2.1 The purpose

An ICT strategic plan defines the way a public entity proposes to manage and enhance its ICT assets to support its current and future business needs. The ICT strategic plan should make sure that all ICT activities and investments are aligned with:

1. Sector strategic objectives,
2. Institutions mandate (core business, and functions), and
3. The national ICT policy, and strategy.

2.2.2 Development of the Institutional ICT Strategy

a. Assessment of existing situation

- The development of an ICT strategic plan should start by the mapping of an institution's business information, applications, 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 "Blueprint"
- The strategy is a living document; hence it should be reviewed within each three (3) years
- The template to be used and detailed guidance on the 4 domains mapping process are provided as annexes.

b. Definition of the target position

The definition of the target position is arrived at by systematically connecting future business needs to technology evolvement. The target position should aim at achieving goals as set by the organization mandate, the organization strategic objectives, the sector strategic objectives, and the SRMP. For a period of 3 years, future business needs should be first collected and once the target business domain is described, remaining target domains (data, information and technology) should be derived taking into account the impact of technology evolvement.

A detailed reference document is attached for the mapping of future situation.

c. Definition of gaps

With reference to the above mapped information on the existing situation and future situation, a gap matrix should be developed to highlight shortages in the four domains.

A template gap matrix is annexed for reference.

d. Establishing a road map to close the gaps

In order to address the gaps this section should highlight:

- 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, timeframe and schedule.

2.2.3 Role 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 which outlines clearly respective roles and responsibilities.

A sample stakeholders' matrix is attached for reference.

2.2.4 Funding and resourcing

This last section should summarize the amount of resources (human and financial) needed to implement the strategy and potential sources of funds.

3. ICT PROJECT MANAGEMENT

3.2 ICT project initiation

All ICT projects should be derived from the assessment as indicated in the above section of ICT strategic planning.

3.3 ICT project documentation

Proper documentations of all ICT projects across the GoR should include:

- The background and rationale.
- The projected output and outcome.
- The project components.
- The implementation plan.
- The project implementation risk analysis and mitigation.
- The proposed resources (human and financial).
- The proposed monitoring and evaluation framework.

Template are attached for reference.

4. ICT FUNCTION, STAFFING AND TRAINING

4.2 IT Committee

- It is imperative that all GoR's entities establish an IT committee
- The IT Committee's primary role is to define the IT Strategy of the entity and ensure all IT projects within respective entities are well coordinated and aligned to the overall strategic goals of the entity.
- Members of the IT committee can vary from entity to entity but all IT committee should at least be comprised of:
    - Head of IT (Chair)
    - Planning Head,
    - Director of Finance

4.3 Structure of the ICT unit.

- The ICT structure of public entities is established through consultation between the concerned entity, RISA and MIFOTRA.
- The reporting line for ICT function should be the Chief Budget Manager.
- The responsibilities and job requirements should be aligned to the standard job requirements and responsibilities as published by RISA on regular basis. (Refer to RISA website).

4.4 Recruitment process

- The recruitment of ICT staff is done jointly by the recruiting institution and RISA.
- The ICT job vacancy advertisement is initiated at institutional level with reference to ICT job requirements and responsibilities as published and regularly updated by RISA.
- Institutions should contact RISA in writing at least with 15-day notice in order to plan for joint written and oral interviews.

4.5 ICT skills sets and capacity building

- All ICT staff across the GoR should comply with the requirements in terms of skills sets and trainings as set and regularly updated by RISA.
- All ICT staff should follow a consistent career path development as proposed and regularly updated by RISA.
- All ICT training needs should be consolidated at institutional level on yearly basis and shared with RISA for approval before submission to Capacity Development and Employment Services Board (CESB).
- RISA will consolidates annual training plans for trainings that can be conducted locally.
- RISA will initiate tenders, MoUs and agreements on yearly basis for all ICT trainings that can be conducted locally or online.

5. GENERAL TECHNICAL SPECIFICATIONS

5.1 GoR's domain names

- All GoR's entities should have their domain names set as a subdomain of "***gov.rw"***
  E.g. For an institution ***xxx***, the domain name should be created as ***"xxx.gov.rw".***

5.2 GoR's staff emails

- Email account of all staff in the GoR should be created by appending the last name to the first name separated by a dot. E.g. for a staff named Sonia Umutoni, the email account should be created as ***"sonia.umutoni@xxx.gov.rw"***
- For staff sharing the same first name and last name, numbers should be added as in: ***sonia.umutoni1@xxx.gov.rw*** **and** ***sonia.umutoni2@xxx.gov.rw***

- All staff should create an email signature comprising the full name, job position, phone number, and information on other accounts such as TWITTER and SKYPE.
- Staff should use an institution template to create email signature for uniformity.
- Link with OGS on this

5.3 Software

5.3.2 OS, Database, Application.

- Proprietary and open sources products are treated equally. Procedures for software development and procurement across the GOR are set in the section on ICT procurement and acquisition.
- For interoperability purpose RISA should be consulted to approve development languages and platforms.
- GoR's entities should on regular basis seek advice from RISA on updates, vulnerability, obsolescence of their systems.
- Applicable standards for Operating systems, Database, and Applications are provided in a separate document.

5.3.3 Software licenses

- Only genuine licenses are allowed in the GoR.
- The choice of licensing mode (user based or server based) should take into account cost effectiveness.
- The procurement of commonly procured licenses like ORACLE and MICROSOFT should be done through a centralized framework process at RISA.

5.4 Hardware.

This section on hardware helps establish a standardized way of determining technical specifications of commonly procured hardware items like desktops, laptops, servers, printers, copiers and scanners.

5.4.1 Desktops

The use of desktops across the GoR should be reduced to strict minimum in order to promote mobility.

The table below summarizes the minimum technical specifications for desktops.

Items	Specifications
Minimum processor capacity	– For simple office use, a minimum i5 processor is advised. – For other uses, an i7 processor can be used based on the amount of resources as dictated by the applications to be installed.
Size of the screen	– For simple office use, a screen of 14' is advised. – For other uses like multimedia, the screen size can be made bigger.
Minimum RAM	– For simple office use a minimum RAM of 4GB is advised. – For other uses, the RAM's can be made 8GB based on the amount of resources as dictated by the applications to be installed.
Minimum Storage	– For simple office use, a minimum storage of 500 GB is advised. – For users dealing with heavy data like videos and audio, a larger capacity of 1TB should be planned.
Storage types (SSD vs HDD).	– The choice between SSD and HDD disks should be made based on specific requirements and also taking into consideration the cost. – For simple office use, cheaper HDD disks should be preferred.

	– SDD disks should be purchased in specific cases whereby faster boot time, faster application launch/ run and faster file transfers are key requirements.
Graphic Card	– Most computers are equipped with basic graphic cards. – For some special cases like heavy multimedia applications, more powerful graphic cards are to be installed.
Minimum USB ports.	– Computers should be equipped with a minimum of 3 USB ports distributed on the front and the back of the computers. – The USB ports should all be of USB 3.0 standard.
HDMI ports	– Desktops should be equipped with at least with one HDMI port.
VGA ports	– VGA ports are optional
Installed OS	– For simple office use, desktops can be installed with Windows/ Mac OS/Linux.

5.4.2 Laptops

The use of laptops should be privileged over desktops to promote mobility.

The minimum specifications for laptops across the GoR are summarized in the table below:

Items	Specifications
Minimum processor capacity	– For simple office use, a minimum i5 processor is advised. – For other uses, an i7 processor can be used based on the amount of resources as dictated by the applications to be installed.
Size of the screen	– For simple office use, a screen of 14' is advised. – For other uses like multimedia, the screen size can be made bigger.

Minimum RAM	– For simple office use a minimum RAM of 4GB is advised. – For other uses, the RAM's can be made 8GB based on the amount of resources as dictated by the applications to be installed.
Minimum Storage	– For simple office use, a minimum storage of 500 GB is advised. – For users dealing with heavy data like videos and audio, a larger capacity of 1TB should be planned.
Storage types (SSD vs HDD).	– The choice between SSD and HDD disks should be made based on specific requirements and also taking into consideration the cost. – For simple office use, cheaper HDD disks should be preferred. – SDD disks should be purchased in specific cases whereby faster boot time, faster application launch/ run and faster file transfers are key requirements.
Graphic Card	– Most computers are equipped with basic graphic cards. – For some special cases like heavy multimedia applications, more powerful graphic cards are to be installed.
Minimum USB ports.	– Computers should be equipped with a minimum of 3 USB ports distributed on both sides of the laptop. – The USB ports should all be of USB 3.0 standard.
HDMI ports	– Laptops should be equipped with at least one HDMI port.
VGA ports	– VGA ports are optional
Installed OS	– For simple office use, desktops can be installed with Windows/ Mac OS/Linux.

5.4.3 Tablets

– The following three types of tablets can be used by GoR's entities:

- Apple tablets
- Microsoft tablets
- Android tablets

- The technical specifications for the above tablets are to be updated by RISA and published on yearly basis.

5.4.4 Servers

- For all servers' needs, GoR's entities are required to subscribe for cloud services at the NDC (National Data Center).
- The NDC proposes four categories of service levels:
  - Bronze
  - Silver
  - Gold
  - Platinum
- GoR's entities should subscribe for at least Gold or Platinum service levels for critical GoR's systems as these levels include the Disaster Recovery options.

5.4.5 Printers, copiers, scanning

- GoR's entities are advised to hire printing, scanning and copying services instead of acquiring, operating and maintaining printers, scanners and copiers.
- In case the hiring of printing, scanning and copying services is not cost effective, GoR's entities can procure printers, scanners, and copiers. Related technical specifications are to be published and updated on yearly basis by RISA.

5.5 Network designs.

- Buildings that host GoR's offices should comply with all requirements for telecommunication installations including general requirements, telecommunication pathways, and cabling network systems as set in Rwanda Building Code in its section 9: Telecommunication installations.
- The high level generic LAN design provided as annex should serve as reference for LAN design across GoR's entities.

- For small entities (small number of users) the routing function can be combined with the traffic filtering. A firewall can be installed to play both the roles of routing and traffic filtering.
- As best practice, the LAN should be divided into:
    - Core layer.
    - Distribution layer.
    - Access layer.
- All network nodes including routers, firewall and switches should allow for a remote and secure management.
- The access layer should be configured into VLANS in such a way that access to the organization's core systems is limited.
- For wireless LAN:
    - Deployed access points should support the 2 channel bands: 2.4 GHZ and 5 GHZ, should support latest wireless standards (IEEE 802.11), and should have a minimum throughput capacity of 300 Mbps. The minimum users per band should be 256.
    - The wireless network should be separated into staff network and guest network.
    - In case many access points are deployed, a centralized management system should be installed for better operation and monitoring.

5.6 Network management.

For proper network management, it is mandatory to install and configure basic and free network monitoring tools like PRTG and CACTI for bandwidth monitoring and network nodes graphing.

5.7 Datacenter and server room specifications.

- GoR's entities are required to host all GoR's data in the NDC as per the March 2012 ministerial instructions.
- Server rooms that are kept on premises should comply with the minimum standards in terms of room size, UPSs, Racks, Labelling, Cooling, and firefighting.

- GoR's entities that host critical GoR's systems on premises should comply with the guidelines as set in the section **IX** on **DATA BACKUP GUIDELINES.**

6 ICT HARDWARE AND SOFTWARE ACQUISITION.

6.5 Submission of annual ICT procurement plan to RISA.

- On yearly basis, all GoR's entities should consolidate and share with RISA their ICT procurement plans.
- 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 GoR's entities.
- References: Ministerial Instructions of N0 001/MINICT/2012 12/03/2012 and RISA's letter Ref: RISA/CEO/420/17.

6.6 ICT centralized procurement.

6.6.1 Centralized hardware procurement

- On yearly basis, RISA selects commonly procured ICT items from submitted ICT procurement plans.
- RISA sets technical specifications based on GoR's 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 GoR's entities.
- GoR's 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.
- GoR's entities that want to procure ICT items that are part of the centralized framework contracts but with different specifications should seek approval from RISA.

6.6.2 Centralized software procurement

- The procurement of all commonly procured Application Software and System Software across the GoR (like ORACLE software and MICROSOFT software) should be done through a centralized framework process at RISA.
- All application software across the GoR shall be acquired in line with the principles of information sharing, compatibility, unified support, cost saving, improved staff productivity and user satisfaction.
- GoR's entities should seek RISA's approval before embarking on major application software acquisition.
- GoR's entities should provide to RISA clear ICT gap analysis and ICT gap bridging road map to back the initiation of any application software acquisition. The road map should be in line with the guidelines as set in the section **II** on **ICT STRATEGIC PLAN.**
- In order to minimize cost and to avoid duplication, RISA shall confirm that there is no already existing application software within GoR that can provide equivalent functions and that can be replicated.
- In the same line and to the extent possible:
    - Multi-tenancy application software shall be privileged to allow sharing of development and maintenance costs.
    - Multi-tenancy application software shall be either centrally procured through RISA or procured with participation and close supervision of RISA.
    - GoR's entities shall to the extent possible, adhere to the use of open standards.

6.7 Decentralized ICT tenders

- GoR's entities shall obtain approval from RISA to initiate any procurement processes.
- RISA shall confirm the relevance of the hardware/software item to be acquired based on submitted ICT gap analysis and ICT gap bridging road map (Refer to the section II on "ICT strategic plan")

- GoR's entities should in addition seek validation of drafted ToRs/ requirements from RISA before publication of ICT tenders.
- GoR's entities can request RISA's participation at any stage of the tender evaluation of ICT tenders.

6.8 Development vs acquisition of software across GoR.

- GoR's entities should seek advice from RISA about the decision to acquire or develop the software.
- The below criteria should be used to take a decision between acquisition and development:

  GoR's entities 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 provided by the vendors.

  GoR's entities can go for acquisition in case:
  - The software is readily and cheaply available on the market.
  - The delivery time is critically short.
  - The software reliability is very critical.

- Minimum requirements that should be considered while determining the best solution are:
  - Total lifecycle cost: Including initial cost, installation, training, and recurrent cost for maintenance and support.
  - Maintainability: The ease of which (Cost and effort) the software can be modified to correct faults, improve performance or other attribute or adapt to a changed environment.
  - Interoperability: This 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.

6.9 Internet bandwidth procurement

- GoR's entities should source all their internet services (4G internet connection and Fiber internet connection) needs to BSC ltd as instructed by the March 2012 ministerial instructions.
- Depending on the size of the institutions the minimum bandwidth on Fiber Internet connection should be:
  - 5 Mbps for institutions having between 5 – 15 staff
  - 10 Mbps for institutions having between 15 – 30 staff
  - 12 Mbps for institutions having between 30 – 40 staff
  - 15 Mbps for institutions having between 40 – 50 staff
  - 18 Mbps for institutions having beyond 50 staff.
- For 4G internet connection, the bandwidth shall be decided based on the requirements of the intended user, but the minimum data volume should be kept at 1GB per day.

6.10 Procurement of hosting and cloud services.

- GoR's entities should source all their hosting and cloud services needs to AOS Ltd as instructed by the March 2012 ministerial instructions.
- Prices for hosting and cloud services are jointly fixed by AOS Ltd and RISA and shared to all GoR's entities.
- GoR's entities sign individual contracts with AOS Ltd and sample contracts as well as sample Service Level Agreements are shared by RISA.
- Any AOS's contract management issue which persists should be automatically escalated to RISA for resolution.

7 ICT ASSETS DOCUMENTATION

7.5 Hardware, systems and infrastructure

- All GoR's entities should record properly all ICT assets using the online template provided by RISA.
- The filled information should be instantly updated in case of any change.
- Consistent labelling should be proposed by RISA and adopted across the GoR.

7.6 Network diagrams

- For the network design and configurations, the network drawings should clearly depict the following base information:
    - Nodes
    - IP information (IP addresses, etc.)
    - Names of links and equipment
- Network diagrams should be made using open source tools such as NeDI with SNMP capability, to allow for automatic updates.
- Alternatively, the diagrams can be built using Microsoft Visio if the deployed equipment does not run SNMP protocol.

7.7 Routers, firewalls, switches, Access points, server configurations

- The Network equipment should have basic configurations.
- There should be a centralized authentication system to allow user access privileges to network equipment (Ex TACACS or Radius)
- Remote access to network equipment should be made using SSH access. Telnet should be disabled.
- IP addresses deployment should be planned, recorded and managed through a dynamic tool like PHP IPAM.
- Access points should have basic configurations (this might differ according to vendor):
    - Access point SSID name
    - WAN IP address
    - LAN IP address
    - VLAN configuration (if applicable)
    - NAT function established
    - Channel bands of 2.4 Ghz and 5Ghz

7.8 Datacenter and server room

Proper and consistent documentation for UPS, Racks, Labelling, Server power rating, Cooling, Firefight, Storage technology should be followed across the GoR

7.9 Changes, Faults and incidents documentation

All changes, faults and incidents should be properly documented to serve as a reference for future faults and interventions.

A template to capture the above information is attached for reference.

8 CYBER SECURITY GUIDELINES

These guidelines aim at:

- Hardening IT infrastructure and information access.
- Insuring high availability of data and systems for dedicated services
- Protection against malware and other related intruders which can compromise the integrity and privacy of data

8.1 Minimize the exposure of Systems to External Networks

GoR entities are advised to:

- Separate their internal network and Internet network by means of firewall and IPS/IDS devices.
- Maintain an accurate inventory of each system connectivity to both internal and external network. This will help determine which system is allowed to connect to which network depending on the service it provides.
- DMZ (Demilitarized Zone) should be set up to contain and expose organization's external-facing services to an untrusted network, such as Internet.

8.2 Implement Network Segmentation

GoR's entities are advised to:

- Classify their IT assets, data, and personnel into specific groups, and restrict related access through VLAN (Virtual Local Area Network).
- Restrict access to VLANs 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.

8.3 Use Secure Remote Access Methods

- Any remote access to the organization network or system should be secure; VPN (Virtual private network) should be used as a secure remote access method if remote access is required.

- Remote access should be further hardened by limiting the number of IP addresses that are allowed to connect remotely.
- The security and safeness of the connected device matters a lot as an infected computer can introduce vulnerabilities in the accessed network.

8.4 Establish Role-based Access Controls and Implement System Logging

- Role-based access control grants or denies access to network resources 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.

8.5 Implement Passwords Policy

GoR's entities are required to:

- Strictly use strong passwords.
- Have different passwords for different accounts.
- Change all default passwords upon installation of new software or new OS.
- Limit many incorrect passwords to be entered for short-term intervals.
- Set up a two-factor authentication for critical applications and/or systems.

8.6 Schedule Internal Cyber Security Awareness

GoR's entities must plan for regular internal cyber security awareness for end users at least 3 to 4 times per year

8.7 Put in place an Incident Response Plan

GoR's entities 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.

8.8 Regular Vulnerability Assessment and Penetration Testing

GoR's entities should plan for IT infrastructure vulnerability assessment and penetration testing at least once a year.

9 DATA BACKUP GUIDELINES.

According to the 12th March 2012 Ministerial Instructions, in its Article 16 (Security of Government critical data and systems) and Article 17 (Hosting Critical Government data and Information), 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.

The data to be protected is classified in the following five categories:

1. Applications and databases
2. Email systems
3. Websites
4. Operating systems
5. Personal Computers' data

The following guidelines apply to the above 5 categories of GoR's data to be secured. They provide general guidance on government data backup. A detailed data backup schedule is also provided **in section** 2.1 for further guidance.

- For critical IT systems and applications hosted in NDC, GoR's entities 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, GoR's entities 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, GoR's entities are required to comply with the detailed data backup schedule as set forth in **section 2.1.**
- For other IT systems and applications deemed non-critical and kept on premises, GoR's entities are required to comply with detailed GoR backup schedule in **section 2.1.**
- For government data that resides on personal computers (Laptops & Desktops), GoR's entities 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 and that all Windows 7, 8 are up to date with the latest updates/patches

9.1 Data Backup Schedule

SN0	Data types	Criticality	Backup type	Backup frequency				On-site	Off-site	Recommendations
				Daily	Weekly	Monthly	Annual			
1	Email systems	High								
			Incremental	V	-	-	-	V	-	
			Full		V	V	V	-	V	
2	Databases	High								
			Incremental	V	-	-	-	V	-	
			Full	-	V	V	V	-	V	
3	O.S.	Low								
			Full system	-	-	V	-	-	V	
			VM image	-	-	V	-	-	V	
			Restore point	-	V	-	-	N/A	N/A	
			Shadow copy	-	V	-	-	N/A	N/A	
4	File server	High								
			Full	-	-	V	-	-	V	The new backup copy should overwrite the previous month backup copy.
5	NAS	High								
			Full	-	V	V	V	-	V	The Off-site backed up data should be at the NDC.
6	Applications	High								
			Full	Full backup should be done after fresh installation and after any change made in terms of configuration and source code					V	
7	Websites	Medium								
			All GoR's websites should be hosted at the NDC under security standards as set forth by NDC.							

9.2 Backup Control and Restoration

- GoR entities should regularly conduct test restorations to ensure that backups are working correctly and make sure that restorations can be successfully executed. Such exercises should be conducted on regularly basis (At least quarterly) and records of such restorations test should be kept within IT teams.
- Prior to any disposal of hardware that was used to store government electronic data, all data after following the recommended backup procedures included in this document should be properly wiped/formatted. Care should be taken to leave no GoR's data on a drive which is disposed of.

9.3 Backup Retention

Where not specified otherwise, the following backup retention schedule shall apply

Types of backups	**Retention**	**Recommendation**
Daily backups	Two weeks	Backup media can be reused once the specified retention period expires.
Weekly backups	Two months	
Monthly backups	One year	
Yearly backups	10 years at minimum or as otherwise recommended by applicable legislation for the type of backed up data.	

9.4 Responsibilities

- Heads of IT Departments/Units are responsible for ensuring regular backups and data restoration tests. They are also responsible for the security of the network connection for online remote backups.
- Heads of institutions are responsible for enforcement and should request on regular basis data restoration tests reports from their respective IT teams. They are also responsible for the secure off-site backup drives/media.