MINISTRY OF HEALTH
PO Box 84 KIGALI
www.moh.gov.rw

HEALTH SECTOR INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SECURITY POLICY

REPUBLIC OF RWANDA

MINISTRY OF HEALTH
PO Box 84 KIGALI
www.moh.gov.rw

Health Sector Information and Communication Technology (ICT) Security Policy

January *2016*

Table Of Content

List of Acronyms:

AAA:	Authorization, Authentication and Accounting
AC:	Alternative Current
AP:	Access Point
BCP:	Business Continuity Planning
DRP:	Disaster Recovery Planning
EAP:	Extensible Authentication Protocol
HIS:	Health Information Systems
HR:	Human Resources
ICT:	Information and Communication Technology
ID:	Identification
IP Address:	Internet Protocol Address
IPR:	Intellectual Property Rights
ISMS:	Information Security Management System
ISO:	International Standards Organization
IT:	Information Technology
ITSMF:	Information Technology System Monitoring Forum
LAN:	Local Area Network
MAC Address:	Media Access Control Address
MOH:	Ministry of Health
NAC:	Network Access Controller
NDA:	Non-Disclosure Agreement
NTP:	Network Time Protocol
PDA:	Personal Digital Assistant
SLA:	Service Level Agreement

SQL:	Structured Query Language
SSH:	Secure Shell
SSID:	Service Set Identifier
SSL:	Secure Sockets Layer
TLS:	Transport Layer Security
UPS:	Uninterrupted Power Supply
VPN:	Virtual Private Network
WAP2:	Wireless Application Protocol version 2
WEP:	Wired Equivalent Privacy
WLAN:	Wireless Local Area Network
XSS:	Cross-Site Scripting
XST:	Cross-Site Tracking

List of Figures:

DEFINITION OF KEY TERMS

Health Security Policy: Health security policy refers to a set of mechanisms that allow for the Ministry's information security objectives to be defined, attained and monitored.

Confidentiality: In this context, confidentiality refers to the concept of protecting information, ensuring that only people authorized to have access to certain information are able to do so.

Integrity: In this context, integrity refers to the concept of maintaining the value and the state of information protected from unauthorized modification. A major objective of information security policy is to ensure that information is not modified or destroyed, thus challenging its integrity.

Availability: In this context, availability refers to the concept of information access, meaning that information and information systems are available and operational, as they are needed. A major objective of an information security policy must be to ensure that information is always available to support critical Ministry of Health service processing.

FOREWORD

The Ministry of Health has a responsibility to develop and adhere to the Information and Communications Technology (ICT) Policy in order to ensure that all information and communications across the Rwandan Health Sector are protected and held to a standard of confidentiality, integrity, availability and non-repudiation of data. A policy guided by these principles will ensure that information in the Health Sector is protected and that improper disclosure of information and inaccuracies in data are prevented, while timely use and dissemination of high quality data is ensured to those who have been granted access to information.

This policy aims to inform all Health Sector staff and users of the significance of ICT Security as it relates to the health information of patients, populations and systems as its collected processed, stored, and used. As technologies advance rapidly, both globally and throughout Rwanda, information and communication also advances. As ICT pervades the area of health, bringing new manners of collecting, analyzing, storing, using and sharing protected health-related data, new protective measures must be taken to ensure confidentiality, integrity and proper access. The ethical and legal protection of personal health data, patient-level health data and intellectual property across the Health Sector must be a responsibility that we each hold as individuals and as members of the Health Sector.

This policy will provide guidance on the acceptable use and organization of health information, health information asset management, personnel security, physical and environmental safety, communication and operational management, access control, systems and application testing related to health information systems.

Dr. Agnes BINAGWAHO
Minister of Health

CHAPTER 1. INTRODUCTION

The main purpose of this document is to define the Information and Communications Technology security policies of the Health Sector, as well as the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which, like any other asset owned by the MOH, has significant value to the stakeholders of the Government. Information security is a critical component that is required to enable and ensure the availability, integrity, and confidentiality of data, network, and processing resources, which are required for the Health Sector to perform its activities and operational practices.

In accordance with the Information Technology System Monitoring Forum of the Ministry, this policy document has been developed to establish and uphold the minimum requirements that are necessary to protect information (assets) against unavailability, unauthorized or unintentional access, modification, destruction or improper disclosure.

The scope of this document is intended to cover any information asset owned, leased or controlled by the MOH as well as the methodologies and practices of external entities that require access to Health Sector information resources. These assets include information hardware, software, data and patient and population data.

This document applies to all full- and part-time employees of the Health Sector as well as all third parties, contractors or vendors who work on Government premises or remotely access the Health Sector computing platforms.

By establishing an appropriate policy framework and utilizing the documented policy development process that includes all stakeholders, the Government aims to obtain maximum voluntary compliance. The policy development and implementation process includes input from Health Sector information technology (IT) professionals and approval by the Information Technology System Monitoring Forum.

All information resources and information systems owned by the Health Sector shall be protected from unauthorized disclosure, use, modification or destruction in order to maintain the value, sensitivity and criticality to the business and operation of the government and those they serve. Access to information technology assets will be granted using the principle of least privilege.

Having identified the relevant security requirements, it is necessary to select and implement appropriate controls to ensure risks are reduced to known and acceptable levels. Controls will be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors, such as inability to deliver a service or the loss of reputation must also be taken into account.

All of the approved policies will support the requirements of the Information Technology System Monitoring Forum of the MOH, as well as the Government Information Security Policy of the Government of Rwanda (GoR). Portions of this security policy are drawn from Rwanda Development Board's ICT security policy.

This Information security policy is issued by the Ministry of Health, referring to a Ministerial order for ''Government Information Security Policy'' protecting Government information assets and information systems. All exceptions to any of the security policies shall be subject to review and approval by the Minister of Health.

The rest of this document is organized as follows: Chapter two: Situation analysis, which talks about the current situation in ICT in Rwanda and specifically in Cyber Security; Chapter three relates to Policy orientation, which encloses key points such as acceptable use, organization of information, asset management, personnel security, access control and systems & application testing; Chapter four, which is the Governance framework, outlines the structure of ICT Personnel in Health Sector and finally the conclusion is found in the fifth Chapter.

CHAPTER 2: SITUATION ANALISYS

The Ministry of Health is aware that cyber security threats are posing a global danger to the integrity, security and privacy of information worldwide, and that in the twenty-first century and beyond, every country shall have to protect its cyber-space in order to protect its citizens.

Although there have been significant investments and government interventions to address cyber security challenges through various institutions, there is a need for a strong Health Sector ICT Security policy to coordinate cyber security initiatives with an integrated approach to fully realize cyber security strategic objectives. The absence of such an ICT Security Policy has often led to inconsistency and duplication of efforts among stakeholders.

The Policy, Legal, and Regulatory Framework and Standards governing ICT, addresses issues related to ICT Services and Security. This includes ICT Policy and regulatory functions, consumer protection, matters of Health Sector interest and data security, regulation of electronic certification service, computer misuse, cyber-crime, and protection of personal information.

The comprehensive ICT law under final review for enactment shall supersede several ICT related laws including "Law relating to electronic messages, electronic signatures and electronic transactions". Even though the penal code and the current ICT bill outline provisions for cyber security, there are still gaps due to the absence of an adopted Health Sector security policy. This absent Health Sector security policy has resulted in inconsistency of security policies in each health facility.

Several infrastructure and initiatives have been implemented in cyber security which include: the establishment of an Internet Security Center (ISC) to monitor the status of Internet security, the National Public Key Infrastructure (PKI) to provide confidentiality, integrity, authenticity and non-repudiation of e-Transactions, and the establishment of a National Computer Security and Incident Response Team (CSIRT) tasked with preventing and responding to cyber security incidents in public and private cyberspace.

All the above will protect critical infrastructure such as the Health Information Systems, MOH Applications at the National Data Center (NDC), 4G LTE last mile network.This infrastructure needs to be highly protected both logistically and physically.

2.1. The Health Information Security Challenge

Information technology (IT) solutions are driven by the demands of our daily Health Sector activities. On a daily basis, the Health Sector is facing different types of challenges. The Health Sector recently digitized their records, which turned out to be extremely valuable to criminals, while hospitals, clinics and other organizations are still learning how to protect them.

On top of that, healthcare organizations face additional challenges, outlined below.

Personnel issues

In hospitals, health centers, doctor's offices, and other related organizations, a large number of people need access to patient records to do their jobs. Thus access control need to be adequately monitored and maintained to preserve proper security.

Mobile device issues

Health information sensitive data are spread across a number of devices, not just servers and desktops but also laptops, mobile devices, and specialized devices for inputting medical record data. All devices with sensitive data will be able to be encrypted at all times and have the ability to remotely wipe these devices if lost.

Medical equipment issues

In Health Sector, there is specialized medical equipment that could pose particular security challenges. Those medical devices cannot be easily scanned for malware.

CHAPTER 3. POLICY ORIENTATION

3.1. Vision

The Ministry of Health's ICT Security Vision is to make timely informed decisions with practical security mechanisms for the protection of Health Systems and patient data.

3.2. Mission

The Health Sector ICT Security Policy sets forth our mission to exceed expectations in the implementation of and compliance with our internal security standards. We aim to deliver quality protection to Health Services consumers by providing the fastest, most reliable health services without exposing them or ourselves to security related risks.

3.3. Guiding principles

The following eight information security principles provide comprehensive governance guidelines for the security and management of information at the Ministry of Health.

i. Information will be classified according to an appropriate level of confidentiality; integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements.

ii. Staff with particular responsibilities for information are responsible for ensuring the classification of that information; for handling that information in accordance with its classification level; and for any policies, procedures or systems needed for meeting those responsibilities.

iii. All users covered by the scope of this policy, must handle Health information appropriately and in accordance with its classification level.

iv. Health Information must be complete, accurate, timely and consistent.

v. Health Information will be both secure and available to those with a legitimate justification for needing access to said information, in accordance with its classification level.

vi. Health Information will be protected against unauthorized access and processing, in accordance with its classification level.

vii. Health Information will be protected against loss or corruption.

viii. Breaches of this policy must be reported in timely manner.

3.4. Goal and Policy Objectives

The Goal of the Health Sector ICT policy relates to the secure use of information assets (both physical and system based) owned by the Ministry of Health, all privately owned systems when connected directly or indirectly to Ministry's network and, all MOH-owned and/or licensed or sanctioned software, data and equipment. Below are specific objectives:

1. To provide users with relevant guidance concerning use of various information and information assets in Health Sector.
2. To ensure effective information security management framework, within the organization with clearly laid down roles and responsibilities.
3. To sustain appropriate protection of organizational assets.
4. To ensure that employees of Health Sector understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risks of human error, theft, fraud or misuse of facilities and address security responsibilities prior to and during employment.
5. To prevent unauthorized access, damage and interference to business premises and information.
6. To ensure secure processing, storage and movement of the Health Sector's information through adequate planning, operating procedures, backups, change management, media handling and network management.

To prevent unauthorized access to the Health Sector's information, to protect it from unauthorized disclosure, deletion or modification and to ensure its continued availability.

7. To prevent errors or misuse of information during application development and maintenance.
8. To ensure that the organization avoids breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements in the operation, use, and management of information systems.

10. To ensure that a well-defined and tested business continuity plan exists in the Health Sector while ensuring a timely resumption of its critical business processes, information, and information processing facilities and safeguarding its personnel in the event of disasters, long term outages and disruptions due to security failure.

3.5. ACCEPTABLE USE

3.5.1. Purpose

The main objective is to provide users with relevant guidance concerning use of various information and information assets in the Health Sector.

3.5.2. General Requirements

- End-users are responsible for exercising good judgment regarding appropriate use of Government resources in accordance with Government policies, standards, and guidelines. Government resources may not be used for any unlawful or prohibited purpose.
- For security, compliance, and maintenance purposes, authorized personnel shall monitor and audit equipment, systems, and network traffic.
- Devices that interfere with other devices or users on the Government network may be disconnected.
- The ownership assigned to the user of the information assets and information processing facilities will be approved and reviewed regularly, in specifics the owner will follow the NDA (Non-Disclosure Agreement), Government Information Security Policy and Procedure.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized Government user access to a Government resource; obtain extra resources beyond those allocated; circumvent Government computer security measures.
- Government Information Resources must not be used for personal benefit.

3.5.3. Information Classification

- All information in Government is classified to indicate the need, priorities and expected degree of protection that will be ensured while handling the information. Refer to the Health Sector Data Sharing and Confidentiality Policy for specific examples of this in the health sector.

  The Classification Categories are:
  - Strictly Confidential
  - Confidential
  - Internal
  - Public
- It is the responsibility of MOH to define the Classification of the asset, periodically review it, and ensure it is kept up-to-date and at appropriate level.
- MOH will also specify the access rights and approve authorization of users to access the assets.
- It is responsibility of the information users to ensure compliance to the defined categories.
- The detailed information classification is referred to Asset Management Policy.

3.5.4. Password Use

- Users will not keep copy of password in any written form or electronic form. If absolutely required, passwords of critical user accounts shall be maintained securely.
- Users will change passwords whenever there is any indication of possible system or password compromise.
- Users will change passwords at regular intervals of 90 days, or based on the number of times accessed (passwords for privileged accounts will be changed more frequently than normal passwords). Users will avoid reusing or cycling old passwords.
- Users will change temporary passwords at first logon
- Users must not include password in any automated logon process, e.g.: stored in a macro or function key
- Users will not share their passwords with anyone
- Users will ensure that nobody is watching when the password is being entered
- Wireless access points shall be secured with help of a security key

3.5.5. Password construction

- Users will choose passwords that are easy to remember but difficult to guess. Some of the guidelines for password constructions are:

  - Quality password with sufficient minimum length 8 characters long
  - Easy to remember
  - Not based on anything, somebody else could easily guess or obtain using persons related information (e.g.: Names, Telephone No's, Date of Birth, Company Name, Spouse Name, etc.)
  - Not vulnerable to dictionary attack (i.e. do not consists of words included in dictionaries)
  - Free of consecutive identical, all-numeric or all alphabetic characters

- Do not use word or number patterns like aaabbb, qwerty, zyxwvuts,123321, etc.
- Not use the same password for MOH and non-MOH purposes
- Strong passwords would have a minimum length of 8 characters and can be constructed through a mix of numerals (1,2,3 etc), special characters (!,@,#,$ etc) and capital letters (A,B,C etc).
- One way to create complex but easy to remember passwords is to take a known word or passphrase and convert it using numerals, special characters and capital letters. For example, the passphrase/word might be "complex" and password could be: "cOmp1@x".

  NOTE: Do not use either of these examples or any examples given in seminars, workshops, training etc. as your passwords.

3.5.6. Unattended User Equipment, Clear Desk and Clear Screen

- All users are responsible for implementing security procedures for protecting unattended equipment.
- All users shall terminate active sessions by using Ctr+Alt+Del on windows and Command+Option+Esc on Macintosh
- Sensitive or critical business information, e.g.: on paper or on electronic storage media, will be locked away (ideally in a safe or specialized cabinet or other forms of security furniture) when not required, especially outside the normal working hours.
- Computers and terminals will be left logged off or protected with a screen and keyboard locking mechanism controlled by a password when unattended and will be protected by key locks, passwords or other controls when not in use.
- Incoming and Outgoing mail point and unattended machines will be protected
- Unauthorized use of photocopiers and other reproduction technology like scanners, digital cameras, will be prevented.
- Documents containing sensitive or classified information will be removed from printers immediately.
- System administrators shall ensure that the active directory system is configured to automatically lock systems, which are inactive for more than 5 minutes.

3.5.7. Secure Log-on Procedures

- System Administrators shall develop guidelines for secure exchange of information; these shall be approved by the IT Security Officer/ICT Unit/HIS Unit/IT Manager together with ITSMF.
- The Information Security Team shall communicate these guidelines to all the users of the Health Sector information systems on an annual basis via the information security awareness sessions.

3.5.8. Information exchange Policies and Guidelines

- Appropriate controls will be implemented for protection against malicious code, when transmitting information electronically.
- Sensitive information will be protected using encryption, password or any other suitable method especially when being sent as an attachment in an email.
- Disposal procedures will be followed to destroy sensitive information.
- End-users will,
  - Not leave sensitive information unattended at Scanners, printers etc.
  - Not auto-forward mails to external mail ids.
  - Not reveal sensitive information in public.
  - Not leave sensitive messages on answering machines.
  - Check the recipients email ID before sending an email respectively.

3.5.9. Reporting Information Security Incidents and Weaknesses

- All employees, contractors and third party users of the Health Sector will be aware or made aware of their responsibility to report any information security incidents and/or weaknesses in systems or services.
- All users shall report Information security related events and weaknesses through the quickest mode to the ICT unit through a defined reporting procedure.

3.5.10. Prevention of misuse of information processing facilities

- All employees, contractors and third party users of Health sector IT resources will use the information processing facilities for business purposes only.
- Any use of these facilities for non-business purposes without management approval or for any unauthorized purposes, will be regarded as improper use of facilities or breach of confidentiality. The unauthorized activity may be identified by monitoring or other means.
- Intrusion detection, intrusion prevention, content inspection, and other monitoring tools shall be used to detect and prevent misuse of information processing facilities.

3.5.11. Anti-Virus

- All workstations and laptops will have anti-virus installed, running and updated. A corporate anti-virus will be implemented in the Health Sector.
- All hosts used by the employee that are connected to the Institution Internet/Intranet/Extranet, whether owned by the employee or by the Institution shall have approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
- Users will not change the anti-virus settings.
- Users will not disable the installed anti-virus agent or change its defined settings during installation. This includes settings for daily virus scan; anti-virus server address and signature update schedules.
- Users will not disrupt the auto virus scan scheduled on their desktop. If the scan is affecting system performance, users will contact system administrator for resolution.
- All external media will be used only after authorization and subjection to anti-virus scan and users are advised to run anti-virus scan when any external media is used.
- Users will report any virus detected in the system to System Administrators or to a reporting manager within their respective department.
- Employees must exercise extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse codes.
- Users will exercise caution when copying files. Only download from reputable sites, and carry out a virus check on the file.

3.5.12. Internet Usage

- Users shall not use or access the Internet for non-business purposes and restrict personal use to minimum limited to educational, knowledge and news sites. Users will strictly avoid visiting non-business, offensive and unethical sites, which violate security policies.
- Users will not use Internet facilities to:
  - Download or distribute malicious software or tools or to deliberately propagate any virus.
  - Violate any copyright or license agreement by downloading or distributing protected material.
  - Upload files, software or data belonging to the Health Sector to any Internet site without authorization of the owner of the file, software, or data.
  - Share any confidential or sensitive information of the Health Sector with any Internet site unless authorized by a Superior or Management.
  - Post any Health Sector proprietary information on Internet share drives/Briefcase, public forums, newsrooms or bulletin boards. This is strictly prohibited and any violation will be subject to disciplinary process that include legal consequences.
  - Post remarks that are offensive, aggressive, insulting, obscene or not in line with Health Sector's policy on the subject.
  - Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting the organization.
- In case such misuse of the Internet access is detected, authorized personnel shall terminate the user Internet access and take other disciplinary action.
- Users will ensure that they do not access websites by clicking on links provided in emails or in other websites. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.
- Users shall be aware that their information systems (computer, internet, email, messenger and telephone conversations), their usage and information exchanged are not private and the company reserves the right to monitor and audit these on ongoing basis and during or after any security incident.
- Users must be aware that Health sector accepts no liability for their exposure to offensive material that they may access via the Internet.
- Users will ensure that security is enabled on the Internet browser as per guidelines given below:
  - Configure browser not to remember web application passwords.
  - Set browser security setting to medium.
- Any bundled software that the user has obtained with mobile phones/PDAs and IPADs etc. will be explicitly approved by reporting head and IT Security Officer/ICT Unit/HIS Unit/IT Manager.

- The Health Sector reserves the right to monitor and review Internet usage of users to ensure compliance to this policy. Any such monitoring will be authorized by ITSMF and or IT Security Officer/ICT Unit/HIS Unit/IT Manager.

3.5.13. User Privacy

- Users will have no expectation of privacy while using company-owned or company-leased equipment. Information passing through or stored on company equipment can and will be monitored as and when required for security and compliance reasons.

3.5.14. Email Usage

- Email is a business communication tool and users must use this tool in a responsible, effective and lawful manner.
- Users shall comply with Health Sector's e-mail policy on proper and effective use of e-mail.
- Users shall archive his/her emails on regular intervals. Users will protect their email account on the server through strong password and will not share their password or account with anyone else. All such locally stored emails on critical laptops/desktops shall be protected by a password.
- Users shall conduct the necessary housekeeping of his/her email at regular intervals.
- Users will promptly report all suspected security vulnerabilities or problems that they notice with the email system to the designated System Administrators.
- The Health Sector has the authority to intercept, disclose or assist in intercepting or disclosing email communications.
- Users will not use any email account other than the one provided by the Health Sector for transmitting official information.
- Confidential information will be secured before being sent through e-mail by way of compression, password protection or other advanced cryptographic means.
- Language used will be consistent with other forms of business communications
- Health Sector employees will treat electronic-mail messages with sensitive or confidential information as 'Confidential' and take due care as per the "Information Handling Guidelines".
- Users shall avoid opening mail from unknown users/sources and also avoid opening suspicious attachments or clicking on suspicious links.
- The Health Sector shall restrict attachments size on the company mail system. Outgoing mail sizes are restricted to less than 20MB.
- The Health Sector reserves the right to monitor email messages and may intercept, disclose or assist in intercepting or disclosing email communications to ensure that email usage is as per this policy.
- Users shall avoid sending or forwarding unsolicited email messages; "chain letters", "Jocks", "junk mail", etc. from other internal users and external networks or other

advertising material to individuals who did not specifically request such material (email spam).

- Users will avoid using "reply to all" for messages that are sent to large distribution groups, especially when the reply only concerns only a few recipients.
- Users shall avoid any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Users shall avoid unauthorized use, or forging, of email header information.

3.5.15. Laptop Security

- Laptop users will take additional responsibility for the security of their laptop and the information it contains. Users will adopt the following measures and consult System Administrators for any clarification:
  - Ensure that laptop is configured as per the secure configuration. Do not install unlicensed or doubtful software or applications.
  - All sensitive data on laptop will be secured either through password protection or by using encryption.
  - Whenever connecting to the LAN, ensure that anti-virus agent is installed with latest signatures on the laptop.
  - Consult with System Administrators and periodically update all necessary security patches and hotfixes for the operating system and applications installed on laptop.
  - Log off laptops when not working for extended periods and enable a screen saver with password for protection during short periods of inactivity.
  - Backup critical files from laptop on the network location.
  - Take adequate measures for physical protection of laptop including, but not limited to, not leaving laptops unattended in public places or while travelling.
  - Personal Digital Assistant (PDAs) devices, laptops, wireless phones and miniature hard drives will not be connected to the LAN without prior permission from the reporting manager and IT Security Officer/ICT Unit/HIS Unit/IT Manager. If the laptop has modem or dial up facility for Internet, users will disconnect Internet connection before connecting it to the LAN. Users having dialup facility are recommended to have a personal firewall installed to prevent unauthorized access to their laptop while connected to Internet.
  - Loss of laptop will be reported immediately to HR Department / ICT Department / IT Security Officer/ICT Unit/HIS Unit/IT Manager. If the laptop contains sensitive information, necessary steps need to be taken by the Department head/ IT Security Officer/ICT Unit/HIS Unit/IT Manager to control damage.
- In case any laptop is connected to the company network without authorization, the ICT/ Security Department shall take appropriate action against it.

3.5.16. Cloud Computing

Some of the health sector systems are located on the cloud because as we know cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. However, without adequate controls, it also exposes health data to online threats such as data loss or theft, unauthorized access to health sector networks, and so on.

In this policy we included the cloud computing to ensure that health sector cloud system based are not used without the IT Security Officer/ICT Unit/HIS Unit/IT Manager`s knowledge. It is imperative that employees NOT open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of health-related data or communications without the IT Security Officer/ICT Unit/HIS Unit/IT Manager`s input. This is necessary to protect the integrity and confidentiality of health data.

3.5.17. Exchange Agreements

- In case of an exchange of information between The Health Sector and an external party, an appropriate agreement will be established addressing the following points:
  - Traceability and non-repudiation
  - Courier identification standards
  - Responsibilities and liabilities in the event of an incident
  - Labeling system as per the sensitivity of the information
  - Cryptography

3.6. ORGANIZATION OF INFORMATION

3.6.1. Purpose

The objective of this policy is to ensure an effective information security management framework within the organization with clearly laid down roles and responsibilities.

In a large Government organization, a cross-functional forum of management representatives from relevant parts of the organization is necessary to coordinate the implementation of information security controls.

3.6.2. Management commitment to information security

- The Health Sector shall form an IT Security Monitoring Forum consisting of senior management representatives from different departments/divisions and functions.
- The Information Security Management Forum (ITSMF) shall oversees the implementation of this policy and approve the detailed security policies of the Institution.
- ITSMF shall review the information security policy at least once a year or on a need basis.
- ITSMF meetings will be conducted at least twice a year to review the effectiveness of the implementation of the information security policy.
- ITSMF shall ensure adequate resources are allocated for information security initiatives.

- ITSMF shall form an Information Security Implementation Team to assist in implementing these policies.
- ITSMF assisted by the IT Security Officer/ICT Unit/HIS Unit/IT Manager shall coordinate the implementation and maintenance of information security controls.
- The size of the ITSMF and IT Security Officer/ICT Unit/HIS Unit/IT Managerwill depend on the structure and size of the Institution/Ministry.

3.6.3. Information security co-ordination

The ITSMF shall take overall responsibility for Information security, including:

- ITSMF shall be responsible for forming the Information Security Implementation Team (IT Security Officer/ICT Unit/HIS Unit/IT Manager) who will drive Information Security initiatives in the organization.
- ITSMF shall comprise of the Senior Management of the Institution.
- ITSMF shall be responsible for assigning roles, responsibilities and authority to the IT Security Officer/ICT Unit/HIS Unit/IT Manager to function effectively and efficiently.
- The ITSMF along with IT Security Officer/ICT Unit/HIS Unit/IT Manager shall be responsible for approving all the Security Policies in the Institution.
- The ITSMF Team shall meet once every quarter to review the policies and minutes of these meetings shall be maintained as records.
- Every institution shall have an Information Security Officer appointed by the ITSMF.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that security activities are executed in compliance with the information security policy.
- The ITSMF team shall assess and review risk management for the processing facilities at least once a year or whenever there is a change.
- The ITSMF team shall ensure periodic information security education, training and awareness for employees and third party personnel.
- The ITSMF team in quarterly meetings shall review, evaluate information security incidents, and recommend appropriate corrective or preventive actions.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager /ITSMF team shall ensure internal audits are conducted once every six months to ensure that the information security policies, procedures are implemented and to assess the effectiveness of the policies.

3.6.4. Allocation of information security responsibilities

- ITSMF shall be responsible for allocating Information security roles and responsibilities. IT Security Officer/ICT Unit/HIS Unit/IT Manager shall be appointed to coordinate and be the focal point for all information security activities in the organization.
- The Information Security Officer shall be responsible for preparing, maintaining and communicating the Information Security Policies & Procedures.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure all assets of business processes are listed with an identified owner.

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure the responsibility of asset owners are defined, documented and communicated to the asset owners.
- The asset owners along with the IT Security Officer/ICT Unit/HIS Unit/IT Manager shall be responsible for the identifying and assessing the risks to the assets on need basis or at least once a year.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure the authorization levels are defined and documented and reviewed at least once a year.

3.6.5. Authorization process for information processing facilities

- ICT department shall authorize acquisition of new information processing facilities.
- ICT and the Administrative department/unit heads shall authorize hardware, and software after evaluating their compatibility with other systems and requirement of security controls.
- Legal department approval shall be sought to ensure compliance to legislative requirements for new information processing facilities.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure all employees and external party users are briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information processing facilities.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager on a need basis shall approve the usage of personal or privately owned information processing facilities (e.g. laptops, home-computers or hand-held devices) for processing business information.

3.6.6. Confidentiality agreements

- Human Resource and ICT team will develop a confidentiality agreements form.
- Human Resource Manager shall ensure confidentiality agreements with employees and third party organizations and their respective users are signed before granting access to sensitive information or information processing facilities
- The Legal Head shall ensure the Confidentiality and non-disclosure agreements comply with all applicable laws and regulations applicable to the health sector.
- All employees and third party users shall maintain confidentiality of information and this shall be maintained as per the information classification policy.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure the signed confidentiality agreements address the requirements to protect confidential information. This shall be based on legally enforceable terms and conditions.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager along with Legal Head shall ensure the confidentiality agreement's address the duration of agreement, confidential information to be protected, and actions to be taken upon termination or breach of agreements.
- The confidentiality agreement shall address ownership of information, trade secrets, intellectual property, responsibilities to avoid unauthorized disclosure of information, permitted use of information and the Health Sector's right to audit and monitor activities that involve confidential information.
- The Confidentiality agreement shall address the notification and reporting procedures for unauthorized disclosure or confidential information breaches.

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager along with Legal Head shall review the Confidentiality and non-disclosure agreement clauses at least once a year and when there is a change in agreement.

3.6.7. Independent review of information security

- The institution shall conduct an independent review of the implementation of these policies every year.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure recommendations for improvement are implemented within one month's time where applicable.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure the results of the independent review shall be discussed in the Information Security Management Forum meetings. These records shall be maintained.

3.6.8. Identification of risks related to external parties

- The Information Security Implementation Team shall evaluate information regarding security risks from external parties before deciding the engagement of external parties.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall review the risks from third party access once every year.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall, based on the criticality of the Health Sector system or process involved, reassess the risks and service levels whenever there is a requirement to change external party services.
- The relevant department will assess the access levels required (physical and logistic) for the external parties. Access shall be approved by the IT Security Officer/ICT Unit/HIS Unit/IT Manager and respective department head/manager.

3.6.9. Addressing security when dealing with customers

- The Health Sector shall include all relevant security requirements in agreements (e.g. NDA) with external parties involving accessing, processing, exchanging, communicating or managing the organization's information and information processing facilities.
- The Health Sector shall ensure that the security controls, service definitions and delivery levels included in the external party service delivery agreement are implemented, operated and maintained by the external party.
- Relevant service unit heads shall do regular review and monitoring of the services, reports and records provided by the external party.
- The Health Sector shall require external party users to apply security in accordance with the organization's established policies and procedures.
- Physical and logistic access to the third party shall be granted only after approval from the interfacing department head and the IT Security Officer/ICT Unit/HIS Unit/IT Manager.
- Third party users shall be provided with unique user IDs.
- Physical and logistic access to applications or devices shall be revoked immediately after the service term/period of activity is concluded.

- All third party access to The Health Sector's information or information systems and devices shall be monitored.
- It shall be ensured that the service level agreement (SLA) is adhered to by the third party.
- The Health Sector shall monitor and review the services provided by third parties.

3.6.10. Addressing security in third party agreements

- The Health Sector's institutions shall address responsibility and legal actions for information security in the terms and conditions of all agreements.
- The Health Sector shall ensure that it maintains agreements with external parties to provide service and agreed level of service continuity as per Business Continuity Plan.

3.6.11. Management Responsibility

- The HR department in consultation with the relevant business line head or manager shall ensure that the job profile listing the various responsibilities of the employee is created. (Making sure that information security is applied in his/her duty)
- The job profile shall include and emphasize the responsibilities related to information security. These shall appropriately be modified in case of change in profile.

3.7. ASSET MANAGEMENT

The objective of this policy is to maintain appropriate protection of organizational assets.

Every Health Sector institution will ensure that all information and information processing assets are identified, classified and adequately protected by the owners of these assets. It will also ensure that boundaries of acceptable use are clearly defined for anyone that accesses any of the information assets.

3.7.1 Inventory of ICT assets

"All assets will be clearly identified and an inventory of all important assets drawn up and maintained."

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure Inventory of all in ICT assets are drawn and maintained with each department.
- The information asset inventory shall be updated by respective team representative and reviewed once every year by the IT Security Officer/ICT Unit/HIS Unit/IT Manager.
- The asset inventory shall include type of asset, owner, location, backup information, manufactured date, purchase date, license information and the assetvalue based on Confidentiality, Integrity and Availability (i.e. type of assets are hardware, software, information, service, people, etc.).
- The Respective Information Asset Owners will classify, label and handle information based on the classification scheme and guidelines.
- The Respective Information Asset Owner shall note in the asset inventory all the critical information the assets require to be recovered in case of a disaster.
- Lifetime of ICT equipment will be reviewed every year by ITSMF.

3.7.2. Ownership of assets

"All Health sector information and assets associated with information processing facilities will be ownedby a designated department."

- Each information asset will have an identified owner who will be responsible for safeguarding the asset.
- The Respective Information Asset Owners shall be responsible for assigning and maintaining appropriate information classifications based on the information classification schemes.
- The Respective Information Asset Owners shall be responsible for deciding the allocation of access rights and classifications of the Information assets.
- Respective Information Asset Owners shall review access to information assets every quarter.
- Respective Information Asset Owners shall review information classification of the asset inventory at least once a year.

3.7.3. Acceptable use of assets

"Rules for the acceptable use of information and assets associated with information processing facilities will be identified, documented, and implemented"

- The Information Security Implementation Team shall ensure all employees, contractors and third party users follow information assets acceptable usage guidelines.

- The Information Security Implementation Team and HR shall be responsible for communicating acceptable usage guidelines to all employees, contractors and third party users at the time of engagement with the organization.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that acceptable usage guidelines shall be a part of the Non-Disclosure Agreements signed by the contractors and third party users.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure acceptable usage guidelines shall be communicated to employees during induction and through various channels such as awareness mailers.

3.7.4. Classification guidelines

"All health sector information will be classified and secured in terms of its value, legal requirements, sensitivity and criticality."

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that a procedure for defining, allocating and reviewing information classifications is documented.
- The designated information asset owners shall classify all assets as per the classification schemes specified in information security guidelines.
- The Respective Information Asset Owners shall review access and classify critical information.
- All users shall classify information as per the information classification procedure.
- Asset owners shall take due care of classifying and maintaining contracts of clients.
- This is contradictory information is to be classified into different levels of confidentiality or public access.
- The Respective Information Asset Owners shall ensure access is based on need to know basis (Read, write access based on individual role).

3.7.5. Information labeling and handling

"An appropriate set of procedures for information labeling and handling will be developed and Implemented in accordance with the classification scheme adopted by the organization."

- The ICT and Administrative Team shall ensure all assets are labeled using asset tags.
- Employees shall be made aware of their responsibilities regarding handling of sensitive information.
- Information no longer useful shall be permanently deleted from the system.
- All critical information shall be securely protected; files shall be password protected and critical information shall be encrypted.
- Media with confidential information shall be physically labeled.
- The ICT and Administrative Team shall be responsible for disposing media securely using media destroyers.
- Users shall ensure all paper information no longer needed will be shredded.
- Media tapes shall be stored in lock and key at all times.

- Backup media shall be labeled and stored in locked fireproof cabinets.
- Media in transit shall be securely stored using bubble wrap or boxes.

3.8. PERSONNEL SECURITY

The objective of this policy is to ensure that employees of the Health Sector understand their responsibilities, are suitable for the roles they have been considered for, to reduce the risks of human error, theft, fraud or misuse of facilities and to address security responsibilities prior to and during employment.

Security responsibilities will be addressed at the recruitment stage, included in contracts, monitored during an individual's employment, and considered during the contract termination process.

3.8.1. Prior to employment

- The job description for all designations will be documented and security roles and responsibilities will be part of the same. These responsibilities will include any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets or for the execution of particular security processes or activities.
- Background checks will be carried out on all health sector employees, contractors and third party users prior to the commencement of employment. A record of the reference checks will be maintained. If necessary, detailed checks of criminal records will be performed for positions with access to extremely sensitive information.
- Confidentiality or non-disclosure agreements from all employees and contract employees reflecting the organization's need for the protection of information will be obtained.
- All Employees, Contractors and Third party users will sign the Health Sector Information Security Policy before employment.

3.8.2. During employment

- Appropriate awareness trainings and regular updates on organizational policies and procedures will be provided to all Health Sector employees, Contractors and Third party users of the organization as relevant to their job functions. Awareness training will continue to be part of the induction process.
- All Health Sector employees, Contractors and Third party users are required to follow the information security policies and procedures.
- All employees not on duty (i.e.: on study leave) for at least 2 weeks, shall be temporarily suspended from accessing organizational information resources.
- A formal disciplinary process will be initiated against employees violating laid down policies and procedures or perpetrating security breach. This may include termination of employment or legal action.

- All employees, contractors and third party users will report immediately an asset stolen or destroyed.

3.8.3. Termination or change of employment

- HR department in conjunction with the concerned head of department will follow the termination and change in role process.
- In case of termination, a clearly defined exit procedure will be followed and a record of the same will be maintained. This will include the return and review of all previously issued information and information processing assets.
- The access rights of all employees and contract employees to information and information processing facilities will be removed on termination of their employment or termination of their contract or agreement. It will be modified for any change in their designation or status.
- All employees, contractors and third party users will return all Health Sector assets in their possession upon termination of their employment, contract or agreement.
- HR department will ensure that all the assets of the organization e.g. Service ID cards, laptops are returned by the outgoing employee or contract employee upon termination of their contract or at the end of employment.

3.9. PHYSICAL AND ENVIRONMENTAL SECURITY

The objective of this policy is to prevent unauthorized access, damage and interference to business premises and information.

It is essential that critical information processing facilities be housed in secure areas, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls. They will be physically protected from unauthorized access, damage and interference, corresponding with the identified risks. The practices of “clear desk” and “clear screen” will be encouraged to reduce the risk of unauthorized opportunist access to facilities.

3.9.1. Physical Security Perimeter

- Security perimeters for the office premises, server rooms, and other sensitive business areas will be defined to form a physical boundary
- Different areas of the Institution will be categorized under following classifications:
  - Green Zone - Areas accessible to public. (i.e. Reception)
  - Blue Zone - Areas not accessible to public, but accessible to all employees.
  - Red Zone - Secure Areas. (i.e. Data center, server rooms, network equipment rooms, etc.)
- All entrances and exits to the premises will be managed 24/7 and red and blue zones will have an access card system.
- All the critical or sensitive information processing facilities shall be housed in secure areas.
- An entry and exit log for all the visitors entering red zone areas will be maintained.
- External party personnel entry to red zone areas will be allowed only after prior authorization by the IT Security Officer/ICT Unit/HIS Unit/IT Manager.
- Visitors to red zone areas will be escorted throughout their stay.
- Visitors will be asked to declare their belongings at entry and this will be returned upon the visitors exit.

- A separate list of external party personnel who require long term access will be maintained.
- All Health Sector employees, contractors and third party users are required to wear an Institution Identification.
- A list of personnel having access to red zone areas will be maintained.
- All delivery will be received in green zone areas. If access to blue zone or red zone areas is required, the delivery personnel will be escorted throughout their stay.
- Photographic, video, audio or other recording equipment, such as cameras in mobile devices, will not be allowed in red zone, unless authorized by the IT Security Officer/ICT Unit/HIS Unit/IT Manager.

3.9.2. Environmental Security

- The backup files and sensitive paper documents will be kept securely off-site. The backups will be stored in appropriate environmental conditions as per the manufacturers' specifications taking into account air conditioning, humidity etc.
- Firefighting mock drills and power outage mock drills will be conducted at least once a year.
- The Health Sector will ensure that the security personnel and personnel often working in the secure area are trained in using fire extinguishing equipment.
- Environmental conditions like humidity, pests etc. will be considered when securely storing the IT equipment, paper documents, backup tapes etc.
- The power supply equipment, air-conditioning and other equipment will be protected from disruptions such as, power surges. All such equipment will be under annual maintenance contracts with service level agreements. Records will be kept for all suspected or actual faults, and all preventive and corrective maintenance.
- Adequate backup time for UPS will be ensured to cater to the availability of the server for orderly shutdown in case of normal power outage to avoid data and file corruptions.
- Cabling (power and telecommunication) carrying data or supporting information services will be properly labeled (point to point) with necessary identification methods and protected from interception or damage.
- Power and telecommunications lines feeding into information processing facilities will be underground, when possible, or subject to adequate alternative protection.
- A documented patch list will be used to reduce the possibility of errors.
- A service assets register shall be maintained to record the maintenance activities carried out for critical equipment like UPS, ACs etc.
- All organizational physical security systems will be properly managed by both Administration department and the ICT department to effectively and securely operate them.

3.10. COMMUNICATION AND OPERATIONS MANAGEMENT

The purpose of this policy is to ensure secure processing, storage and movement of the Health Sector's information through adequate planning, operating procedures, backup, change management, media handling and network management.

All the information, its communication and processing facilities, flow of information within the Health Sector and outside the Health Sector's institutions, will be protected by appropriate system and network planning, management and through well-established operating procedures.

3.10.1. Operational procedures and responsibilities

Documented Operating Procedures

- Operating procedures for information systems will be documented and authorized by the management and will be made available to all users who need them. These procedures include:

  - Backup
  - Equipment maintenance
  - Media handling, computer/ server room and mail handling management, and safety.
  - Operating procedures that require specific instructions for the detailed execution of each job including the interdependencies, if any, and instructions for dealing with exceptions or errors that may arise during job execution.

Change Management

- Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all changes to equipment, applications and procedures are required to be followed.
- The change management form needs to be completed for each scheduled, unscheduled or emergency change following the steps contained in the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management log will be maintained for all changes. The log must contain, but is not limited to:

  - Date of submission and date of change
  - Owner and custodian contact information
  - Nature of the change
  - Indication of success or failure

Segregation of Duties

- Roles and responsibilities will be assigned, implemented and reviewed for each critical process.

- Due care will be exercised to segregate the roles and responsibilities. Whenever it is practically not feasible to segregate the roles and responsibilities, appropriate supervision will be carried out.

Separation of development, test, and operational facilities

"Development, test, and operational facilities for critical systems shall be separated to reduce the risks of unauthorized access or changes to the operational system"

- The IT Security Officer/ICT Unit/HIS Unit/IT Managershall ensure that there is separation of development, test and production environment for all the changes to the operational systems.
- The Development Manager shall ensure that there are defined rules for transfer of the system/software from development to its production environment.
- The IT Security Officer/ICT Unit/HIS Unit/IT Managershall ensure that utilities like compilers, editors and other development tools or such systems utilities are removed from the production system.
- The IT Security Officer/ICT Unit/HIS Unit/IT Managershall monitor and control the access to the utilities.
- The Testing team shall ensure that sensitive data is not copied into the test environment.
- The IT Security Officer/ICT Unit/HIS Unit/IT Managershall ensure that users are given different user profiles for operational and test facilities.
- The IT Security Officer/ICT Unit/HIS Unit/IT Managershall ensure that the installation of system/software on its production systems is controlled in order to prevent corruption of systems and information.
- The separation of development, testing and operational facilities requirements must be planned and documented.

3.10.2. Third Party Service Delivery Management

Service Delivery

- The third party service delivery agreement will include Service Definition, Security Controls and Arrangements and Delivery Levels.
- The Third Parties' capability to provide service and agreed level of service continuity as per Institution's Business Continuity Plan will be assessed and ensured by the respective head of the unit.
- An SLA (Service Level Agreement) that meets the Institution's requirements will be clearly defined to every outsourced service from a Third party.

Monitoring and Reviewing Third Party Services

- Third party service delivery will be continuously monitored and reviewed by the head of the ICT unit/ Head of Concerned Unit. This includes:

    - Service performance level and adherence to agreements
    - Regular review of service reports and meetings with vendors, if necessary
    - Review of records of security events, faults, failures and disruptions to service
    - Process of resolving and managing problems and incidents

Changes in Third Party Service

- Changes in third party service can occur because of internal changes in the institution or variations to existing service delivery. The head of the ICT unit/ Head of Concerned Unitin the institution will ensure security policies; procedures and controls are maintained or improved during and after the process of change.

3.10.3. System Planning and Acceptance

Capacity management

- Performance of the Health Sector's critical information processing and communication facilities will be monitored daily to ensure respective set standards are met.
- The performance monitoring reports will be analyzed and any bottlenecks will be identified. For each new and on-going activity, capacity requirements will be identified. System tuning and monitoring will be carried out to ensure and improve the availability and efficiency of systems.
- The IT Security Officer/ICT Unit/HIS Unit/IT Managerwill use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system or services, and plan appropriate action.

System acceptance

- For all new information systems, upgrades to existing systems or new versions, acceptance criteria will be clearly defined and if met it will be subsequently approved.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager will be consulted in order to define the
- Criteria relating to information security.
- A detailed checklist will be prepared for various parameters to be incorporated in the acceptance test. The acceptance criteria can be based on process requirements and/or user requirements.
- Acceptance test criteria will invariably include Risk Assessment.

3.10.4. Protection against Malicious and Mobile Code

Controls against malicious code

"Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented"

- To prevent the spread of and exploitation by malicious code, the IT System shall be configured to prevent users from installing unauthorized software.
- The IT Systems Support Team shall ensure that appropriate detective and preventive measures are implemented at key network locations to protect the organization against risks introduced by malicious code.
- The IT Systems Support Team shall ensure that the anti-virus software is running the latest virus signatures and the usage of the anti-virus is proper.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager along with IT Systems Support Team shall ensure that appropriate business continuity plans are drafted to guarantee timely recovery of all IT Systems due to a malicious code attack.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall research and actively inform users periodically about information on real (vs. hoax) threats and the procedures for handling each type of attack.
- The IT Systems Support Team shall ensure that all users log into their desktops using "normal user" privileges.
- All emails messages shall be scanned before entering and leaving the organization for presence of any malicious code.
- All users shall be trained on the best practices to be followed while using computer systems to prevent the outbreak of a virus incident.
- IT systems support must ensure that local schedule backups of each computer system are activated and configured to facilitate the recovery in case of malicious code.

Controls against mobile code

Background: Malicious mobile code is malware that is obtained from remote servers, transferred across a network, and then downloaded on to your computer. This type of code can be transmitted through interactive Web applications such as ActiveX controls, Flash animation, or JavaScript.

- Mobile code, e.g Java, activeX may contain malicious code; hence appropriate technical measures will be activated to ensure that the same are managed.
- The Network Security Team shall ensure that all types of malicious mobile code are blocked at the Internet Gateway/Firewall.
- The Network Security Team must ensure that the firewall is running the latest signatures.

Protection and treatment guidelines

Necessary technical and operational procedures will be in place for centralized Antivirus definition updates.

- It will be ensured that the Anti-virus software is installed, configured and active on every machine. The configuration of Anti-Virus software will be protected to avoid any unauthorized modifications.
- Updating of anti-virus software on all computers will be managed centrally.
- Systems will be implemented to review the anti-virus software activity logs, to check whether anti-virus software is running regularly on respective computers.
- Machines will be scanned for virus at least once a day and it will be properly scheduled, preferably during the lunch hours of the office.
- Every storage media shall be scanned for virus before use.
- Controls will be implemented to protect the network from spyware software.
- The Anti-Virus software for messaging system (e-mail) will be implemented. If the virus is found in mail attachment file, this file will be deleted and the sender will be informed. The recipient will get the remaining message.
- The IT Security Officer/ICT Unit/HIS Unit/IT Managermust be regularly updated about the latest information on malicious code through internal communication mail.
- Unauthorized or any pirated software will not be used by Health Sector employees.
- Any files or data obtained from outside sources, through any media required for business, will be tested for viruses before being used.
- Appropriate recovery procedures will be in place for recovering from malicious code attacks, including all necessary data and software backups and recovery arrangements.
- Necessary procedural protection will be taken to protect against the introduction of malicious code during maintenance and emergency procedures, which may bypass normal malicious code protection controls.

3.10.5. Back-up

Information backup and archival

"Back-up copies of information, system, servers and software will be taken and tested regularly in accordance with the agreed backup policy"

- The IT Security Officer/ICT Unit/HIS Unit/IT Managershall maintain a record of all data that needs to be backed up along with the schedule for each backup.
- The IT Security Officer/ICT Unit/HIS Unit/IT Managershall ensure that backup logs are reviewed on a monthly basis.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager in coordination with the [Backup Administrator] shall ensure that backup and restoration procedures are drafted and made available at all times.
- The IT Security Officer/ICT Unit/HIS Unit/IT shall ensure that all backup tapes are moved to an offsite secure location on a monthly basis.

- The IT Security Officer/ICT Unit/HIS Unit/IT in coordination with the Administration Unit shall ensure that all backup equipment and tapes are given adequate physical protection, both onsite and off-site.
- The IT Security Officer/ICT Unit/HIS Unit/IT shall test all backup media quarterly to test the completeness of the backup.
- The IT Security Officer/ICT Unit/HIS Unit/IT in coordination with the IT security officer shall carry out restoration procedures every six months to ensure that systems are restored as per the BCP/DRP regulations.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall identify suitable encryption technologies to ensure that highly confidential data is encrypted on backup tapes.
- The IT Security Officer shall ensure that the retention period of all data being backed up is identified. The same shall be communicated (retention period) to the ICT Team who shall maintain the same.
- The IT Security Officer/ICT Unit/HIS Unit/IT must ensure that the backup of users' important files is performed (local computer backup and domain users' folder redirection)
- The system administrator must ensure that all key servers and their configuration must be cloned (copied) and will have to be cloned after any change made to them or after a certain period (6 months).

3.10.6. Network security management

Network Controls

"Networks will be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit."

- Overall responsibility for network activity will be clearly assigned to an individual (i.e. the network 'owner'). Responsibilities for key tasks will be assigned to one or more individuals who are capable of performing them.
- The risk of staff disrupting the running of the network either in error or by malicious intent will be reduced by:
    - Segregating the duties of staff running the network. In case this is not practically feasible, suitable audit trails and quarterly review of the activities will be incorporated.
    - Ensuring all network and external staff sign non-disclosure and confidentiality agreements
    - Minimizing reliance on key individuals (i.e. by automating tasks, ensuring complete and accurate documentation, and arranging alternative cover for key positions)
    - Organizing duties to minimize the risk of theft, fraud, error and unauthorized changes to information (i.e. by supervising and recording activities, prohibiting lone working and the segregation of duties)

Security of Network Services

- The IT Security Officer/ICT Unit/HIS Unit/IT Mangers shall ensure that sufficient technology controls are implemented whilst taking security and network services from a service provider. The controls shall take into account the confidentiality, integrity and availability of the data being transmitted between the client and the service provider.
- The IT Security Officer/ICT Unit/HIS Unit/IT Mangers shall ensure that Operational Level Agreements are signed with units providing network and security services.
- The IT Security Officer/ICT Unit/HIS Unit/IT Mangers shall regularly monitor the services provided by these unit/departments. Corrective and Preventive actions shall be carried out to ensure that these units/department provides services as agreed to in the agreement.

Wireless communication security

- Wireless router will be tested prior to selection, the test will include but not be limited to, the below points;
    - Inter compatibility with other network devices
    - Will support strong encryption and authentication protocol (i.e.WAP2)
    - Will have a logging mechanism
- Wireless Access Point (WAP) in the Health Sector corporate networks must not be used by third party; it shall be used where only required and after approval from the IT Security Officer.
- All access to wireless networks shall have strong authentication mechanisms to prevent unauthorized users.
- The SSID of the wireless device shall be configured in such manner so it does not contain or indicate any information about the organization, its departments, or its personnel including organization name, department name, employee name, employee phone number, email addresses, or product identifiers.
- WEP & WAP must not be used for Wireless deployment (since these are vulnerable) only WAP2 with EAP-TLS will be used.
- Institutions shall require that parts of the network containing and supporting wireless devices directly (the wireless network) be separated from the part of the network that does not support wireless connections. The part of the network supporting wireless devices or connections shall be considered less trusted than the part of the network that does not.
- All file servers and internal domain controlling servers shall be separated from the wireless network using a firewall.
- Wireless access to third parties shall only be provided after adequate verification and authorization.
- Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in WLAN) to fully understand the wireless network security posture.
- Default Administrator password on AP must be strictly changed.
- Wireless AP access password must be changed periodically (every 3 months).

3.10.7. Media handling

Management of Removable Media

- Movement of media containing information will be supported by a suitable authorization process.
- Movement of media will be initiated by filling out an authorization form (Gate Pass).
- In case the confidential information needs to be printed on a common printer, then a responsible person will supervise while the information is getting printed and ensure that no printouts are left on the printer.
- While transporting information media to other locations, care will be taken to protect the media from damage or unauthorized modification. The procedure for 'Security of Media in Transit' will be followed strictly.

Disposal of Media

When an information media becomes unusable or not is no longer required in the Health Sector, it will be disposed of securely and safely. If proper care is not taken while disposing the media, critical Health information can be disclosed and misused. Procedures for disposal of such media will be followed to reduce the risk of a corresponding security breach.

Information handling

Information media such as tapes and paper documents containing confidential organization information, shall be maintained in safe custody, and wherever necessary, in a fireproof cabinet. The key to the cabinet shall be available only with the concerned department manager and the duplicate shall be kept with the head of the department for emergency use. Access to the information will be given only to selected personnel on a "need-to-have" basis and the names of these personnel will be documented.

Security of System Documentation

- The Health Sector will ensure that all system documentation is handled as per its classification.
- Access to system documentation shall be approved by Reporting manager to prevent possible data loss. Logs of all such approvals will be maintained and reviewed every quarter by the IT Security Officer/ICT Unit/HIS Unit/IT Manager.
- Process owners shall ensure that the system documentations within their department are stored securely to avoid possible misuse or disclosure from unauthorized users.

"System Documentation" means those operational manuals, tables, access control lists, or other documentations that contain sensitive information such as the descriptions of application processes, procedures, data structures, addressing schemes, and authorization

processes, which if divulged could compromise the security of the systems referenced within such documentations.

3.10.8. Exchange of information

Information Exchange Policies and Guidelines

"Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities"

- Appropriate controls will be implemented for protection against malicious code, while transmitting information electronically.
- Sensitive information will be protected using encryption, passwords or any other suitable method, particularly when being sent as an attachment in an email.
- Disposal procedures will be followed to destroy sensitive information.
- End users will:
  - Not leave sensitive information unattended at scanners, printers, photocopiers, barcode reader machines, etc.
  - Not auto-forward mails to external mail IDs.
  - Not reveal sensitive information in public
  - Not leave sensitive messages on answering machines
  - Check the recipients email ID before sending an email.

Exchange Agreements:

In case of an exchange of information between the Health Sector and an external party, an appropriate agreement will be established addressing the following points:

- Traceability and non-repudiation
- Courier identification standards
- Responsibilities and liabilities in the event of an incident
- Labeling system as per the sensitivity of the information
- Cryptography

Electronic messaging

- Information present in electronic messages will be appropriately protected according to its criticality.

Health Information Systems

Interconnection of Health information and communication systems including phone calls, conference calls, emails etc. shall be adequately protected.

3.10.9. Electronic Medical services

Publicly available information

The integrity of information being made available on a publicly available system will be protected to prevent unauthorized modification.

- Unauthorized modifications to electronically published information on an Institution's website may harm its reputation. The IT Security Officer/ICT Unit/HIS Unit/IT Manager will implement appropriate controls to protect Health information from unauthorized access and modification. Heads of the pertinent units will be the internal authorities responsible for the proposed content to be published publicly online.
- Reviews and comments from Chief budget's office and/or Legal department will be obtained for publishing information and the IT Security Officer/ICT Unit/HIS Unit/IT Manager will be responsible for reviewing it, from an information security standpoint.
- It will be ensured that the information to be published is in compliance with applicable legislation and contractual obligations. The data collection over web will also comply with the applicable legislation.

3.10.10. Monitoring

Audit Logging

"Audit logs recording user activities, exceptions, and information security events will be produced and kept for an agreed on period to assist future investigations and access control monitoring."

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager will maintain Operational and Maintenance logs of all activities.
- The logging will be automated as much as possible. Implementation of automatic recording of logs whenever feasible will be in applied, as it is useful to maintain the integrity of the logged information. Logs will include, but will not be limited to:
    - Date, time and other details of key events, e.g. log-on and log-off
    - Records of successful and rejected system access attempts
    - Changes to system configuration
    - Use of privileges
- All activities of system administrator/system operator will be logged and reviewed at least once in a quarter by the IT Security Officer/ICT Unit/HIS Unit/IT Manager or the responsible person.

Fault Logging

"Faults shall be logged, analyzed, and appropriate action taken"

- Users will report problems encountered with information systems and communication systems to the system administrator.
- The faults reported will record the nature of problem, date and time of the report and user identity.
- The details of action taken will be recorded along with date and time of action and person performing the action.

Review of Logs

- The System/Network logs shall be reviewed daily to initiate timely actions for system and/or network errors. Regular review of the logs is essential to maintain maximum uptime of the system, which leads to continuity of business process.
- An internal appointed audit team will conduct a periodic reviews of the logs. These reviews are helpful in ensuring that operating procedures are performed properly and that information security controls are effective.

Protection & Retention of Logs

- Logs will be protected from unauthorized access and changes.
- Logs will be backed up automatically on a daily basis, these logs will be archived quarterly.
- The log retention period will be determined based on business needs, legal and contractual obligations.

Monitoring System Use

- It is essential to monitor the use of information systems to safeguard the information from unauthorized activities.
- Level of monitoring will be determined by a risk assessment of individual systems.
- Review of event logs is an important function in monitoring system use. The system administrator will monitor their respective systems daily and report any unauthorized activity noticed. The Head of technical services and the IT Security Officer/ICT Unit/HIS Unit/IT Manager will be notified about said unauthorized activity.
- An audit team will review the process of monitoring system use periodically. This process will be assessed at least once in a year and necessary corrective/preventive action will be initiated.

Clock Synchronization

- The correct setting of computer clocks is important to ensure accuracy of logs. The logs may be required for investigations or as evidence in legal or disciplinary process.
- All information systems and devices, which have real time clocks, will be set to Rwanda Standard Time Zone.
- The system administrator will regularly check and maintain the clocks using an NTP server as per the standard time settings as mentioned above.

3.11. ACCESS CONTROL

The purpose of this policy is to prevent unauthorized access to the Health Sector's information, to protect it from unauthorized disclosure, deletion or modification and to ensure its continued availability.

Access to Health sector's information processing facilities, application systems, databases, network, communication and operating systems will be restricted to the Health Sector, to ensure confidentiality, integrity and availability of its information.

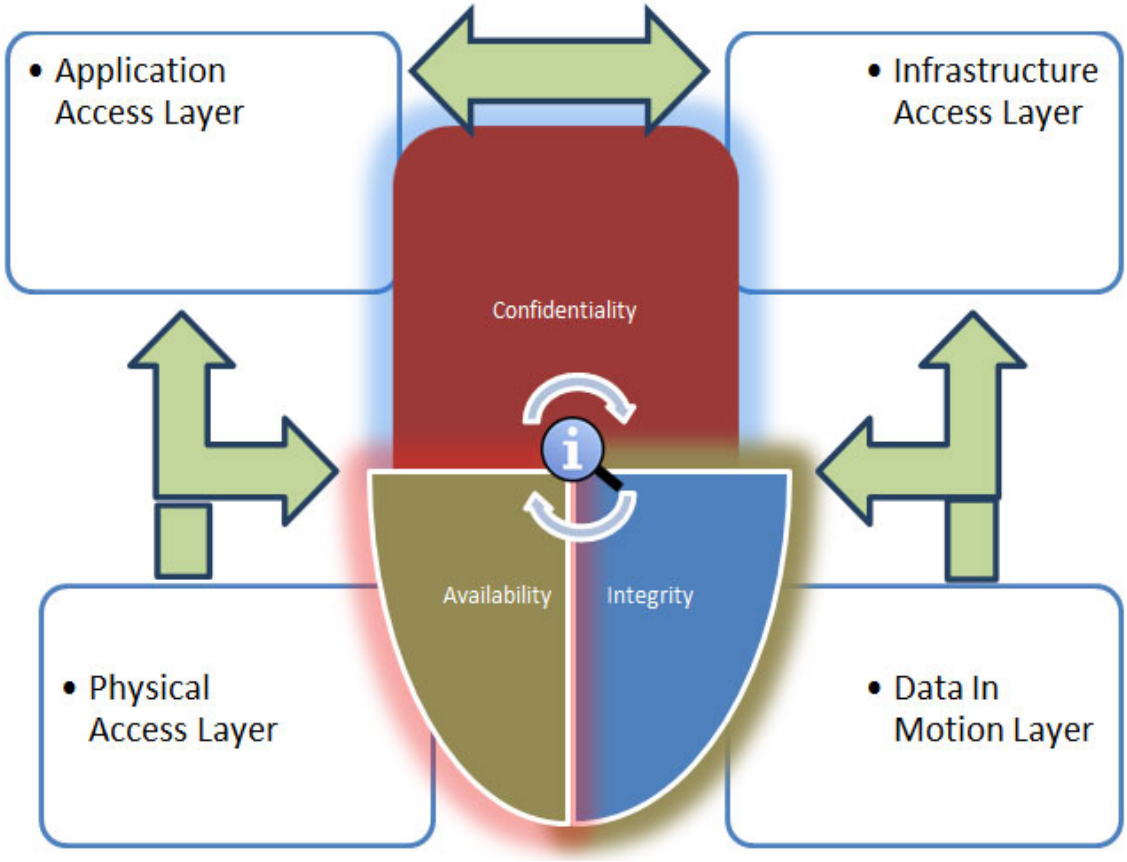

Figure1: Access control layout

3.11.1. User registration

- All users will have a unique identifier (username/ ID) for their personal and sole use so that his/her activities can be subsequently traced to assign responsibility for actions or in case of any system misuse.
- All users having a need to use any of the organization's information systems will require an authorization from their respective managers/heads of departments. Access to the information systems will not be granted unless the authorization procedure has been completed and approved.
- The level of access granted to each user will be based on business requirement only.

- All users will clearly understand the Acceptable Usage Policy, to ensure that the information systems are used as required by the Ministry of Health.
- A formal record of all persons registered to use the information systems will be maintained.
- Access rights of all users who have changed roles/jobs or have left the organization will be revoked immediately. In certain cases where the user ID or account needs to be maintained for a certain period, sufficient controls will be put in place to prevent any misuse.
- The information systems will be checked on a quarterly basis to ensure redundant user IDs and accounts do not exist.

3.11.2. Privilege Management

- The privileges associated with each information system (i.e. for each operating system or application) assigned to each individual user will be identified.
- Privileges will be allocated to individuals on a "need-to-use" basis.
- An authorization process will be followed and a record of all privileges allocated will be maintained. Privileges will not be granted until the authorization process is complete and has been approved.
- All activity related to privileged users will be logged and reviewed on a quarterly basis to detect any misuse of privileges.

3.11.3. User Password Management

- All users will be required to keep personal passwords confidential.
- All newly created user IDs will be assigned a temporary password, which will be changed immediately upon first logon.
- Any user requesting a change in password will be duly verified.
- The exchange of temporary passwords over insecure mediums (for example clear text electronic mail) will be avoided.
- Temporary password will follow the complexity rule.
- Default vendor passwords will be changed or disabled following the installation of the system or software.

3.11.4. Review of user access rights

- User access rights will be reviewed regularly and always after any change in employment of the user such as promotion, demotion or termination by the respective reporting manager.
- Privileged user access rights will be reviewed quarterly.
- Necessary controls such as removal of extra access rights will be conducted in case of any ambiguity found during the review.

3.11.5. User Responsibilities - Password Use

- All users working with Health sector premises will be informed to keep passwords confidential and not share it with anyone.
- If there is an indication of a possible system or password compromise, the password associated with the concerned system will be changed immediately.
- Passwords of information systems will be of a minimum length of 8 characters.

- The characters in the password will be a combination of numeric, alphabetic and special characters.
- The passwords will be difficult to guess or derive and towards this end will avoid using personal information such as names, telephone numbers, date of births etc.
- Passwords will be changed every 90 days.
- Password history will be maintained for 5 past used passwords.
- All temporary passwords will be changed at first log-on.
- Passwords in any automated log-on process will be avoided.

3.11.6. Unattended user equipment

Unattended equipment will be provided with adequate protection viz:

- By providing appropriate locking or password protected screen saver or
- By logging off.

3.11.7. Clear desk and clear screen policy

- All sensitive documents and storage media containing sensitive documents will be locked away when not required and especially when the office is vacated.
- All sensitive documents being printed will be immediately removed from printer areas to prevent unauthorized access.
- The organization will make use of shredder systems to get rid of paper documents that may no longer be required or left unattended near printer areas.
- All computer screens will be set to lock automatically after 5 minutes of inactivity.
- All computer screens will be locked when left unattended.

3.11.8. Policy on use of network services

Network Services users shall have access to the services that they are authorised to use only with specific privileges

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that a Network Policy is drafted taking the following points into consideration:
  - Reporting manager and head of IT Security Officer/ICT Unit/HIS Unit/IT Manager need to approve network access to the users
  - Documentation of the type of network access that will be granted to the users under the various scenarios
  - Reference to procedures, if any, to grant network access
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall perform a risk assessment before formally approving the commissioning of any new network service.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall document and highlight any serious concerns with issuing or commissioning a particular network service to users.

3.11.9. User authentication for external connections

- Strong Authentication mechanism must be implemented to control external and Internal connections to Health sector networked services (e.g “Two factor Authentication technique i.e., VPN techniques, etc...
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall perform a risk assessment to decide the level of protection required before formally approving the type of remote access authentication technology.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure two factor authentication is used to control access by remote users.

3.11.10. Equipment identification in networks

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that connection to network devices for administrative purposes is identified through an IP Address or MAC Address.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that all network devices are configured to control access to and from the network using identifiers such as IP Addresses or MAC Addresses
- Network Access Control (NAC) may be considered for auto identification of devices on the network.
- Any new devices connected to Health Sector networks shall be identified and monitored

3.11.11. Remote diagnostic and configuration port protection

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that all servers and network equipment are placed in locked cabinets/rooms to prevent the direct access to remote diagnostic ports.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that all default enabled ports and services that are not required for business purposes are disabled.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager shall maintain Operating Security Guidelines for each of the technologies and systems used.

3.11.12. Segregation in networks

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that a risk assessment is performed to analyze the security requirements of the network and the need to segregate the same into various domains.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that the criteria for segregation of networks are based on the business needs for access control and security access requirements.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that access controls are implemented between the various domains.

3.11.13. Network Connection Control

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that access control rules are implemented on the network devices to ensure that users access to health information services is secure.

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that Internet services are available.

3.11.14. Network Routing Control

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that controls are applied on Internet firewalls to hide the IP address schema used inside the company.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that filters are applied on the Internet router or Internet firewalls to ensure any "internally" reserved IP address does not appear as the source at the externally facing interface.

Note: The firewall security policy is needed for more details on this policy

3.11.15. Secure log-on procedures

- All access to systems, applications and Network Devices must be secure and traffic encrypted using technologies such as SSH, SSL, Tokens, etc.
- The use of weak log-on procedures (e.g.: telnet) is prohibited while accessing Health sector Systems, Applications and Networks Devices
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that access to information services is controlled by secure log-on process.
- The log-on procedure will disclose minimum of information about the system, in order to avoid providing an unauthorized user with unnecessary assistance.

3.11.16. User identification and authentication

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that the super user on the systems will be two and only one is used by system administrator and the second one its credentials will be documented and kept by the head of the organization with a signed non-disclosure agreement.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that all the users have a unique user ID.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that prior management approval is taken for creating shared user ID and generic ID.
- The users will ensure that a strong password is used for authentication.
- By default, any new users shall have minimum level of privileges; higher privileges required for the job shall be subject to approval by the reporting manager.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that privileged IDs are created only after authorization from the Head of the department/unit. Privileged IDs shall be different from those used for normal business use.

3.11.17. Password management system

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall follow a formal password management process for the allocation of passwords.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that users are given temporary passwords for initial login and the same shall be communicated securely.

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that all default passwords provided by the vendor shall be changed following installation of system or software.
- The users shall ensure that passwords are not stored on computer systems in an unprotected form.
- The System Administrators shall define procedures for password resets.
- The users shall follow complexity guidelines in the selection of passwords to ensure their quality.
- The System Administrators shall implement controls to change passwords at a frequency of 90 days.
- The System Administrators shall ensure that password history of previous passwords is maintained to prevent re-use.
- The System Administrators shall ensure that all the systems and applications used will adhere to password policy.
- The institution shall ensure that all passwords are kept confidential and not shared unless otherwise authorized by the IT Security Officer/ICT Unit/HIS Unit/IT Manager, if there is a legitimate business reason.

3.11.18. Use of system utilities

The System Administrators shall restrict and control the use of utility programs that might be capable of overriding system and application controls.

3.11.19. Session time-out

- The System Administrators shall ensure that all computing equipment are configured to lock after 5 minutes of inactivity.
- The System Administrators shall ensure that wherever feasible, all inactive sessions are configured to shut down after a period of 10 minutes.

3.11.20. Limitation of connection time

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall enforce restrictions on connection time for sensitive applications to normal office hours (07AM-5PM) if there is no requirement for over-time or extended-hours of operation.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall enforce re-authentication at timed intervals.

3.11.21. Information Access Restriction

- The Application Owner shall ensure that the access to information through the applications is controlled by the use of menus. The menus shall be designed such that access to sensitive information is controlled through the use of a confidential password.
- The Application Owner shall ensure that users are given varied access rights (i.e. read, write, and execute) depending on his/her business requirement.

3.11.22. Sensitive System Isolation

- The Application Owner shall define and document the sensitivity of the application in terms of Confidentiality, Integrity and Availability. This shall be reflected in the asset inventory file.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall conduct a risk assessment on an annual basis of all those applications that are critical to the business and that run on shared environments.
- Application Owners shall require formally approving the sharing of environments for critical business applications.
- Critical information systems shall be strongly secure and isolated to the rest of the other systems.

3.11.23. Mobile Computing and Communications

- All users using mobile computing devices such as laptops, smart phones, iPads and similar hand held devices for business purposes shall be trained on the best security practices towards these devices. This training will be part of the end user awareness training conducted annually for all employees.
- A risk assessment shall be performed on the potential threats associated with the various forms of mobile computing for new devices that become available.
- Users of mobile computing devices (i.e. Laptop, smart phones, iPad and similar hand held devices) shall be required to sign a statement of their understanding and compliance to the mobile computing policy. This statement will be included in the policy acceptance letter signed during orientation.
- Users shall reasonably ensure mobile devices are physically secure at all times if they contain Health Sector sensitive data. Examples of physically securing devices include:
  - Mobile devices will never be left visible in a car, and will never be left in the trunk or other storage location overnight.
  - Mobile devices will always be carried on-board aircraft and not put in checked luggage.
- If a mobile device contains additional things other than public Health Sector Data, it shall have some form of access control (i.e. username and password) to access this information. If access to the device is not controllable, access to the data must be controlled.
- If a mobile device contains sensitive Health Sector Data, it shall be encrypted by the encryption systems put in place, that will be managed by the IT security officer. Encryption may be on a file-by-file basis, or on a volume-by-volume basis.
- Users are strongly encouraged to back up their Health Sector Data stored on ICT devices. Backup may be done when connected to the Health Sector Network (file shares and other backup facilities), or may be backed up to removable media. If backed up to removable media, this media must be physically protected and the data must be encrypted.
- Remote connections to the Health Sector Network shall be made from mobile devices at public places only after obtaining prior approval from the respective division/unit manager, the Infrastructure Owner and the IT Security Officer from the respective institution.
- Before connecting to the company network from the public network, the following points shall be considered:

- Users must use an approved personal firewall, and have it running and actively filtering traffic, when connecting to Health Sector Networks from public places.
- Users must also have current and active anti-virus software running before connecting.
- Remote connections will be made through VPN tunnels to safeguard the connection traffic.

3.12. SYSTEMS AND APPLICATION TESTING

The purpose of this policy is to prevent errors or misuse of information during application development and maintenance.

IT Systems, application development and maintenance will be secured, to prevent unauthorized development, modification, change by means of implementing robust testing prior to acceptance and deployment in either of the following existing systems like;
-moh.gov.rw
-Exchange Server
-Domain Controller
-IHRIS (Integrated Human Resource Information System)
-Health Resource Tracking Tool (HRTT)
-Ebola System (to be integrated to eIDSR)
-RHMIS (Rwanda Health Management Information System)
-MEMMS (Medical Equipment Maintenance Management System)
-E-LMIS (electronic Logistic Management Information System),
-Community Health Workers management and badge system,
-Community Health Worker Reporting Information System (RapidSMS),
-Laboratory Information System (LIS),
-Blood bank system, EMR (Electronic Medical Records),
-Rwanda Health Information Exchange Project (RHIE Project)

- Client Registry: Holds the details of all antenatal care clients of government health services in the Rwamagana District. Each client is assigned a unique identifier, which is used by health workers to access their records from the Shared Health Record.

- Facility Registry: Contains details of all government health care facilities in Rwanda

- Interoperability Layer: A communication layer that allows information from care applications to be validated and stored in the respective registry.

- Provider Registry: A database containing details of all antenatal care health providers working in government health facilities in the Rwamagana District.

- Shared Health Record: The central repository of electronic patient records around which the health information exchange is built.
- Terminology Service: A system to verify the maintained terminology standards for diagnosis, procedures, medications etc. in the Health Sector.
- Finger Print

  - The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that the application is tested for compliance, security and regulatory requirements before deployment. This will also include checking for input controls, audit and logging capabilities, account policy etc.
  - The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall be consulted in order to define the criteria relating to information security.
  - Once deployed, the testing shall be carried out whenever there is a major software change including, but not limiting to, version upgrade.
  - The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure input data validations with adequate checks and controls are incorporated into the applications.
  - The testing for software's will cover the following areas:

    - Authentication and Authorization
    - Audit log generation
    - Processing security controls
    - Input validation checks
    - Output security controls
    - Integrity checks
    - Encryption
  - Security testing for Web application will additionally include:

    - SQL injection
    - Cross Site Scripting (XSS)
    - Cross Site tracking (XST)
    - Web Page code analysis
    - Parameter Manipulation
    - Form Field Manipulation
    - URL Manipulation
    - Session ID Security
    - Access Control
    - Directory traversal
  - All activities shall be logged and reviewed quarterly by the IT Security Officer/ICT Unit/HIS Unit/IT Manager.
  - The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that a system acceptance test plan is documented.

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that results of the tests are recorded to determine whether the system is performing as expected and so can be accepted.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that regression tests are planned so as to test upgrades or new versions.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that failure of any parameter during the acceptance test shall be recorded and action shall be initiated.
- Access to Application Development machines shall be restricted to the Application Development Team members only.
- Application security checks shall be done by personnel that are not developing the application and the results will be analyzed by the IT Security Officer/ICT Unit/HIS Unit/IT Manager. Along with the identification of risks, recommendations shall be provided for the risks identified by the IT Security Officer/ICT Unit/HIS Unit/IT Manager.
- Compliance with the recommendations provided shall be monitored.

3.13. COMPLIANCE

The objective of this policy is to ensure that the organization avoids breaches of any law, statutory, regulatory or contractual obligations and conforms to any and all security requirements in the operation, use, and management of information systems.

All relevant legal, regulatory and contractual requirements will be identified and complied, including those related to intellectual property rights and privacy of personal information. Compliance to security policies and procedures including technical compliance will be periodically checked through Internal/External Information System audits.

3.13.1. Compliance with Legal Requirements

Identification of applicable legislation

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager along with the Legal Department shall identify and document all relevant statutory, regulatory, and contractual requirements applicable to the organization.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager along with the Legal Department shall identify the controls to be implemented to help the Health Sector meet the expectations of all the applicable legislations.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall assign the implementation of the controls to the respective process owners.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall document all responsibilities towards implementation of the necessary controls required to meet the expectations of the applicable legislations.

Intellectual Property Rights (IPR)

- The e-Health Unit shall ensure that all software to be used in the organization is licensed and procured from reputable vendors.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall train its users on the various policies applicable to IPR on an annual basis.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall maintain an asset register highlighting all those assets with requirements to protect intellectual property rights.
- Users shall not download or install any third party pirated software on Health Sector systems.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that the IT Department maintains all copies of licenses purchased.
- The IT Department shall develop a procedure to ensure that the licenses issued do not exceed the maximum number purchased.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall on an annual basis audit all IT systems for presence of unauthorized software.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall define a procedure to maintain an accurate track of all licenses during the transfer or disposing of software.

Protection of organizational records

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall identify and document all records that need to be maintained to meet statutory, regulatory, contractual and business requirements.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall also identify the retention period for the records.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that appropriate protection measures are taken to protect the Confidentiality, Integrity and Availability of the records.

Data protection and privacy of personal information

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall identify and ensure compliance towards any legislation that deals with the collection, processing, and dissemination of personal information.
- Confidential information entrusted to Health Sector employees by members, Health partners, suppliers, and other third parties shall be protected in accordance with Health Sector's Security Policies and shall be protected with the same care as Health Sector confidential information.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall advise data owners on policies and procedures concerning the protection and storage of personal data.

Prevention of misuse of information processing facilities

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that all users are presented with a login banner at the time of accessing an IT System.
- The HR Department shall ensure that all users are made aware of their responsibilities towards the proper use of information processing facilities.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that appropriate detection mechanisms are implemented to ensure the proper use of IT facilities.
- All users need prior approval from their reporting manager before requesting use of any new information processing facilities.
- Legal/Disciplinary action shall be taken against any user found misusing any of the information processing facilities.

3.13.2. Compliance with Security Policies and Standards, and Technical Compliance

Compliance with Security Policies and Standards

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager in coordination with the IT Security Implementation Team shall review and ensure on a quarterly basis that each department under the scope of the ICT Security Policy complies with the security policies and standards.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that all non-compliances reported during the review shall be addressed appropriately keeping in mind the risks to the Health Sector.

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall maintain a record of all review findings along with the actions carried out to close them.

Technical Compliance Checking

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall be responsible for initiating a review on an annual basis to ensure that the controls implemented on the IT Systems are in agreement with Health Sector policies and standards.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall invite external security experts in case the technical compliance activity cannot be performed by the internal IT Team.
- The Institution shall carry out vulnerability assessments (from inside the network) and penetration tests (from outside the network) on an annual basis to ensure the controls are adequate to mitigate the current risks to the organization. The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall initiate this activity.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that the compliance checks are always done under supervision of a member from the ICT unit.

3.13.3. Information Systems Audit Considerations

Information Systems Audit Controls

- Health sector shall conduct audit exercises on a regular basis including at least an external audit from a trusted audit firm once a year.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall be responsible for documenting and communicating specific audit requirements if any to the concerned departments prior to being audited.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall seek prior approval from the management before proceeding with any auditing activity on the Information Systems.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that the Audit team has read access only to the software or data being audited.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that all audit activity on IT systems is carried out in the presence of a member from the IT Team.
- All access to data/systems by the auditor shall be logged.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that the persons conducting the audit are independent from the activities being audited.

Protection of information systems audit tools

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall identify and securely store all audit tools that will be used for audit purposes.
- Any user seeking access to audit tools shall take prior approval from his/her reporting manager and the IT Security Officer/ICT Unit/HIS Unit/IT Manager.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager is responsible for maintaining records of all access given to system audit tools.

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that any system audit tools are uninstalled once the audit activity has been completed.
- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that any system audit tool built into the OS or application that could serve as a potential threat is disabled prior to commissioning the system.

3.14. BUSINESS CONTINUITY MANAGEMENT

The objective of this policy is to ensure that a well-defined and tested business continuity plan exists in the Health Sector to ensure timely resumption of its critical business processes, information, and information processing facilities and safeguard its personnel in the event of disasters, long term outages and disruptions due to security failures.

A practical and well-defined Business Continuity Plan will be prepared to ensure that adequate procedures are in place to recover from disasters and resume normal business operations in the Health Sector. Recovery teams will be formed with clear, well-defined roles and responsibilities, to safeguard personnel and property in case of any disaster. The HIS Director shall identify critical functions, emergency response team with contact details and ensure that a well-documented BCP is in place. The plan must be maintained current and tested / exercised regularly.

3.14.1. Including information security in the business continuity management process

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure a critical assets inventory is maintained and reviewed at least yearly by the respective process owners.
- Institutions shall ensure that a business impact analysis is carried out once in a year, or when major changes to the business occurs, to determine the potential impact of the interruptions and subsequently put alternate controls and processes in place.

3.14.2. Business continuity and risk assessment

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager / shall ensure BCP is based on a formal Risk Assessment, which identifies the risks associated with various system information processes of the institution while simultaneously performing business impact analyses.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure a risk assessment for unavailability of information assets is done at least once a year.

3.14.3. Developing and implementing continuity plans including information security

- IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure user awareness training on emergency procedures is conducted once every year.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure roles and responsibilities for handling crisis situations shall be documented and communicated to relevant teams and personnel.
- Floor wardens shall be responsible for evacuation of all employees.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager along with System Admin shall ensure fire evacuation drills are conducted at least once a year.
- Crisis management teams shall be trained once a year on crisis management situations.

- BC and DR plans shall be communicated to relevant teams. The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure latest copy is maintained at the DR site.

3.14.4. Business continuity planning framework

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure a business continuity planning framework is defined in order to maintain or restore business operations in the required time frames to cause least disruptions to business.
- The business continuity plans includes established emergency procedures and existing fallback arrangements for all critical services.
- A business continuity framework shall be designed so that it states the conditions for activation and identifies the personnel responsible for execution of each component of the plan.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure that business continuity plan is in line with the Incident Management Policy.

3.14.5. Testing, maintaining and re-assessing business continuity plans

- The IT Security Officer/ICT Unit/HIS Unit/IT Manager will be responsible to ensure BCP plans are tested at least once a year to ensure that they are effective and up to date.
- IT Security Officer/ICT Unit/HIS Unit/IT Manager shall ensure a test plan and test schedule is established for timely testing of BCP.
- BCP test results shall be communicated to the ITSMF (IT Security Monitoring Forum) and the results shall be discussed in the six monthly security management meetings.
- Records of the Business Continuity Tests shall be maintained, analyzed and reviewed for improvements.

CHAPTER 4. GOVERNANCE FRAMEWORK

4.1. Organization & Management

The effective implementation of this security policy will depend upon the availability of resources to purchase and license the required security hardware and software (security equipment, central anti-virus, firewalls, VPNs) and adequate staffing to manage infrastructure, train users and conduct routine security audit procedures. Similarly, several committees will need to be set up and meet regularly to provide leadership and governance for the ICT team. The chart below highlights the minimum staffing and committee structure required to implement this policy:

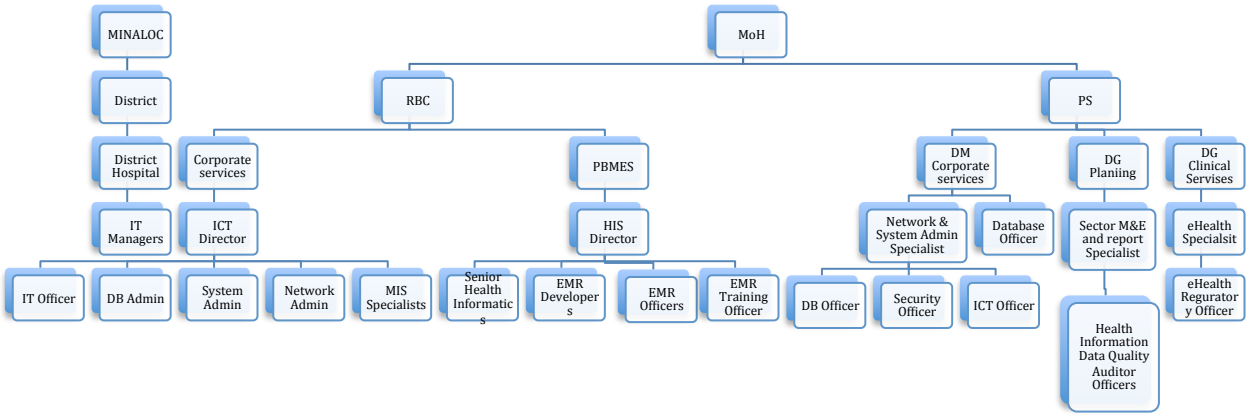

Figure2: Structure of ICT Personnel in Health Sector

4.2. Partnership and Coordination

The section below section describes the role and responsibilities of the stakeholders

1. Ministry of Youth and ICT

Developing general policies and strategies and providing political oversight and coordination.

2. Rwanda Development Board ICT (RDB)

Under RDB-ICT it was established that the National Computer Security and Response Team (RW-CSIRT) has the mandate to detect, prevent and respond to cyber security threats and simultaneously play a role in incidents response. Providing human resources as well as adequate capacity building resources will strengthen the National CSIRT operation capabilities.

3. Rwanda Utilities Regulatory Authority (RURA)

- Developing a cyber security regulatory framework and ensuring that Rwandan cyberspace within an environment of open and robust competitive ICT industry is secure.
- Promoting awareness and addressing cyber security threats and vulnerabilities.
- Taking part in cyber security capacity building efforts.
- Promoting and enforcing compliance of technical and operational standards.

4.3. Monitoring & Evaluation

ICT security policy developers and some of the senior managers shall oversee the implementation of this policy and approve the detailed security policies in the Health Sector, to ensure the protection of information resources (assets) against unauthorized or unintentional access, modification, destruction or disclosure.

CHAPTER 5. LEGAL IMPLICATIONS

After the approval of this policy by Minister of Health, it will be followed by the review of the legal framework related to ministerial order regarding administrative sanctions to ensure that all applicable ministry's legislation are implemented. It is recommended that a Privacy and Confidentiality of Health sector Information Act be passed and promulgated into law. It is also recommended that a law enforcement body be set up to provide legal oversight of the Privacy Act.

CHAPTER 6. CONCLUSION

The purpose of this policy is to ensure that the staff and all the users in the Health Sector understand the importance of Information Security Management as defined in this policy. This information security policy sets out the Ministry's approach to information security management. It focuses on the three main principles: confidentiality, integrity and availability of information.

This comprehensive policy provides guidance for acceptable use and organization of health information, asset management, personnel security, physical and environmental safety, communication and operational management, access control, and systems and application testing relating to health information. Consequently, the governmental framework has highlighted the roles and responsibilities of stakeholders such as: MYICT, RDB-ICT, RURA, whereby staff and communities are required to implement this policy.

Reference

1. Rwanda: “Rwanda Cyber Security Policy”. Kigali, Rwanda. March 2015
2. Rwanda: “ICT Sector Profile for Web”. Kigali, Rwanda. June 2014
3. Maria Korolov, cso online “Healthcare organizations face unique security challenges“ “http://www.csoonline.com/article/2932978/data-protection/health-care-organization-face-unique-security-challenges.html”. Jun 9, 2015
4. Republic of Rwanda “SMART Rwanda Master Plan 2015 ~ 2020”.Kigali Rwanda, 2015.
5. Institute of Education, University of London “Information_Security_Management_Policy_0910”.November 2010
6. Feidhmeannacht na Seirbhise Slainte Health Service Executive, “Information Technology (I.T.) Security Policy”. February 2012