12/18/2020

Puntland Ministry of Health

INFORMATION & COMMUNICATIONSTECHNOLOGY (ICT) POLICY & PROCEDURES

Puntland Ministry of Health ICT Policy and Procedures – December 2020

Prepared by Abdirashid Awad Dirie

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

CD	-	Compact Disk
DHIS2	-	District Health Information Software 2
DVD	-	Digital Versatile Disk
ICT	-	Information & Communication Technology
ISP	-	Internet Service Provider
IT	-	Information Technology
LAN	-	Local Area Network
LAN	-	Local Area Network
Mbps	-	Mega Hits per second
MOH	-	Ministry of Health
PDA	-	Personal Digital Assistants
SBP	-	Server Backup Policy
PSD	-	Portable Storage Devices
VPN	-	Virtual Private Networks.

DEFINITIONS

ICT Policy:

ICT in this policy refers to all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices that are owned, controlled or operated by the Puntland Ministry of Health.

User:

"User" means anyone who operates or interfaces with ICT. It includes Puntland Ministry of Health staff, officers (whether permanent, temporary or part-time), contractors, sub- contractors, consultants, business partners or official visitors or any other member of the Ministry of Health

Systems Authority:

While the Puntland Ministry of Health is the legal owner or operator of all ICT systems, it delegates oversight of particular systems to the head of a specific directorate or department ("Systems Authority"), or to an individual staff member, in the case of ICT systems purchased with funds for which he or she is responsible.

Systems Administrator:

Systems Authorities may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular ICT resources.

Certifying Authority:

This is the Systems Administrator or other Ministry authority who certifies the appropriateness of an official Ministry document for electronic publication in the course of Ministry.

Specific authorization:

This means documented permission provided by the applicable Systems Administrator or departmental manager.

SPAM:

Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail

1. INTRODUCTION

The Puntland Ministry of Health recognizes the importance of quality, efficient, user-friendly ICT systems in order to increase performance levels and provide excellent services to all Ministry staff and Health Centres. The purpose of this policy is to promote the efficient, ethical and lawful use of the Puntland Ministry of Health's computer and network resources. The Information and Communication Technology Policy 2020 outlines Ministry's intention to develop ICT policies and legislation.

Major technological advances have resulted in sweeping changes to the way information is transmitted. Today the internet is an integral component of modern life. Internet browsing and email are the key method of written communication in scores of organizations.

The Puntland Ministry of health has steadily expanded ICT resources and services since its inception. The number of computers in the Ministry has grown and most of which are networked. The ICT network comprises a fiber optic backbone and several Ethernet LANs that cover the ministry and administrative blocks. The LANs are managed from a central server room which hosts various servers, switches, routers and other data terminal equipment.

This policy sets out the expectations on employees of the Puntland Ministry of Health including contractors and temporary staff, who use the Ministry's IT facilities. IT facilities are provided to assist with day to day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal, professional and ethical obligations that apply to them. All users are responsible for IT activity which is initiated under their username.

2. PURPOSE OF THE POLICY

Purpose of this policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Puntland Ministry of health:

- Understand and follow procedures to ensure the safe and appropriate use of ICT at the service, including maintaining secure storage of information
- Take responsibility to protect and maintain privacy in accordance with Ministry's Privacy and Confidentiality Policy
- Are aware that only those persons authorised by the Approved Provider are permitted to access ICT at Puntland Ministry of health
- Understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.

3. SCOPE OF THE POLICY

This policy applies to all aspects of the use of ICT including:

- Backup Policy
- Security Policy For ICT Staff
- Network Control Policy
- ICT appropriate Use
- ICT Asset Disposal Policy
- Software Policy
- Hardware Policy
- Email Policy

4. BACKUP POLICY AND PROCEDURES

This document defines the backup policy for computer systems within the Puntland Ministry of health which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. The policy outlines the minimum requirements for the creation and retention of backups. The main purpose of this policy is to provide secure storage for data assets critical to the work flow of official Puntland Ministry of Health, prevent loss of data in the case of accidental deletion / corruption of data, system failure, or disaster and permit timely restoration of archived data in the event of a disaster or system failure.

This document outlines a set of policies and procedures for Data Backup and Retention to facilitate restoration of applications and associated data. Also it lays emphasis on verifying that backups and recoveries are completed without errors.

The purpose of back up is to ensure server and data continuity and to support the retrieval and restoration of archived information in the event of a disaster, equipment failure, and/or accidental loss of files.

The goals of this backup policy will be as follows:

- To safeguard the information assets of Puntland Ministry of health.
- To prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes should such events occur
- To manage and secure backup & restoration processes and the media employed within these processes.

4.1 Scope of server backup

Puntland Ministry of health's ICT Unit is responsible for providing policy-based, system level, network-based backups of server systems under its stewardship. This document outlines the policies for backup implementation that define:

- Selections: what information needs to be backed up on which systems?
- Priority: relative importance of information for purposes of the performing backup jobs.
- Type: the frequency and amount of information to be backed up within a set of backup jobs.
- Schedule: the schedule to be used for backup jobs.
- Duration: the maximum execution time a backup job may execute prior to its adversely affecting other processes
- Retention Period: the time period for which backup images created during backup jobs are to be retained.

4.2 Backup Creation

Backups will be created using industry standard data backup software that support "enterprise level" data assurance. The product, defined by the data backup standard, must support scheduled backups, full or differential or incremental backups, and centralized management.

4.3 System Backup Profiles

The MOH ICT Unit maintains the following type of backup profiles:

1. **Standard Backup:**

The standard backup is provided for most centralized Ministry computer systems.

- The backup could be full, differential or incremental. The frequency of backup could be daily, weekly or monthly and is dependent upon the application. The retention of these backups could vary from 1 week up to 2 months.
- For some applications backup is performed on a day and time agreed upon by the application owner.
- ANNEX I shows the applications along with backup type, frequency of backup –

.

4.4 Storage Locations and Retention Period of Backups

Unless a system supporting an application or business function requires a custom retention period, MoH ICT section will maintain full and incremental backups. Backup tapes for the current weekly backup period will be stored within the MoH ICT section for purposes of current backups and restores. Tapes representing backups from the former weekly backup period will be stored within a secured, fireproof place until such time as the backup images stored on these tapes expire and the tapes are re-used or destroyed. After a successful backup, it will be stored in a secure, off-site media vaulting location for an appropriate period for disaster recovery purposes. This will ensure that no more than one week of information would be lost in the event of a disaster in which campus systems and backup images are destroyed. After the period of six months has elapsed, the tapes may 'optionally' be returned to MoH ICT section and re-used or destroyed.

4.5 Backup Verification

On a periodic basis, logged information generated from each backup job will be reviewed for the following purposes: 14 Back to Contents

- To check for and correct errors
- To monitor duration of the backup job
- To optimize backup performance where possible Moh ICT section will identify problems and take corrective actions to reduce any risks associated with failed backups. Test restores from backup tapes for each system will be performed. Problems will be identified and corrected. This will work to ensure that both the tapes and the backup procedures work properly. MOH ICT section will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes

4.6 Policy date

The Server Backup Policy (originally approved and issued on 22 May 2020 with subsequent revisions as shown in the beginning of this document) will remain in force without time limit, and will be reviewed annually to ensure relevance.

4.7 Puntland Ministry of Health Servers

There are three servers in the Ministry of health including:

- DHIS 2
- Video Conference room server
- Finance server

5. ICT SECURTITY POLICY

5.1 security policy for ICT staff

The most important computer security issue is the security of data. Dedicated security infrastructure allows information systems to be provided a greater level of security than can be achieved through user vigilance alone. Without dedicated security infrastructure, the potential exists that vulnerability which cannot be mitigated by the capabilities inherent in Puntland Ministry of Health's systems will be exploited leading to a compromise of information system security. This Security Infrastructure Policy applies to all dedicated security systems that are deployed to protect the property of Puntland Ministry of Health including: perimeter protection platforms (i.e., firewalls); malware protection platforms (i.e., anti-virus, anti-spyware, etc.); intrusion protection platforms; and data protection platforms (i.e., content filters, encryption).

Intended audience:

This policy is specifically for Information and Communications Technology (ICT) staff responsible for security infrastructure, policy enforcement, and prevention of security breaches in their respective offices.

Policy statement:

Ownership: MOH ICT security infrastructure is owned by the organization. Technical approval for major configurations must be obtained from the Technology Services Section prior to implementation.

Monitoring: MOH reserves the right to monitor, review and log user use of its technology resources without notice. This includes but is not limited to email, Internet access, file access, log-ins and changes to access levels. Furthermore, and consistent with generally accepted business practices, MOH collects statistical data about its technology resources and ICT staff monitors its use to ensure the ongoing availability and reliability of the

system. Should a security or other relevant incident arise, MOH may review system logs to determine the cause and take appropriate action. If it is determined, for example, that the security incident arose, in whole or in part, due to user noncompliance with applicable regulations, rules, policies or procedures, this may result in forfeiture of the privilege to use technology resources as well as administrative, disciplinary or other legal action as applicable.

Infrastructure:

There are a number of ways data can be destroyed or stolen. The following items must be implemented in all Puntland MoH offices (for collocated offices, the infrastructure can be shared with other agencies) to ensure data security:

- Boundary network access should be protected by a firewall that monitors and controls data flow. The firewall will be configured to deny access by rule and allow by exception, to prevent public access to internal networks and to place controls on publicly accessible systems. Security standard firewalls should be utilized whenever possible.
- All information systems will be protected by antivirus protection systems where such solutions exist for the information system. At a minimum, antivirus protection should be performed at the network boundary, on e-mail and other communications systems, and on all workstations, servers and other endpoints
- Boundary network access points as well as all information systems will be protected by data protection platforms that monitor, control and restrict the flow of data into and out of systems and into and out of networks. These platforms will

include data encryption, session encryption and content filtering.

- If the need for additional remote access security is recognized by approved staff and authorized third parties may utilize Virtual Private Networks (VPNs). The user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing the required software. VPN gateways will be set up and managed. All computers connected to MOH internal networks via VPN or any other technology must use the most up-to-date anti-virus software; this includes personal computers. By using VPN technology with personal equipment, ICT staff must understand that their machines become an extension of MoH's network, and as such, are subject to the same rules and regulations that apply to Puntland Ministry of Health equipment.

Ethical behaviour:

Considering the responsibilities and high level of access to data and systems infrastructure provided to ICT staff, it is imperative that all act with the highest degree of professional responsibility and integrity.

Related Policies

Change authority:

The Ministry of Health ICT section and Infrastructure/Security Specialist have the authority to change the security policy for ICT staff.

5.2 Protect the Ministry of health's physical ICT assets

The Ministry has made considerable investments into ICT resources. These must be protected by ensuring information held is kept secure and physical assets are cared for. With data being held electronically, it is necessary to ensure the Ministry is kept
Protected from computer and software viruses which could potentially allow access to confidential data. Any protective measures taken must be frequently reviewed and updated. All equipment should also be password protected with access codes being
Changed at regular intervals.

The care of physical ICT assets is the responsibility of all Ministry employees. Permission should always be sought from a Manager or Director to temporarily remove such assets from Ministry property (e.g. taking laptops or cell phones home overnight). Any loss or damage to such ICT equipment is the employee's responsibility. Purchase of a similar asset of equal value or repair charges must be borne by the employee at fault.

6. NETWORK CONTROL POLICY

6.1 Acceptable Use Policy Objectives

The following are the objectives of acceptable use policy:

- Provide guidelines for the conditions of acceptance and the appropriate use of the computing and networking resources
- Ensure that ICT resources are used in an appropriate fashion, and support the Ministry's mission and institutional goals.

- Encourage users to understand their own rights and responsibility for protecting the Ministry ICT resources.
- Protect the privacy and integrity of data stored on the Puntland Ministry of health network.
- Elaborate the consequences of the inappropriate use of these resources.

6.2 Scope of network control policy

The ICT network at the Ministry of Health is comprehensive and includes all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices that are:

- controlled or operated by the Ministry of Health:
  - connected to the Ministry of Health network:
  - used at or for Ministry of Health activities:
  - Brought into a Ministry of Health site.

ICT includes but is not limited to; computers (such as desktops, laptops, PDAs), computer systems, storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), telecommunication equipment, networks, databases and any other similar technologies as they come into use.

7. ICT APPROPRIATE USE

Although this Policy sets out the general parameters of appropriate use of ICT systems, staff should also consult the Ministry's Personnel Policy and Procedures manual under.

7.1. Acceptable /Appropriate Use

ICT systems may be used only for their authorized purposes that is, to support the administrative, and other functions of the Ministry of Health. The particular purposes of any ICT system as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the user.

While the use of email distribution lists can be very effective, excessive use of email lists, especially with large messages, can cause congestion on network traffic. The forwarding of chain letters is considered to be spam and is not permitted.

The Ministry of Health recognizes that the Internet is an essential tool and as such the use of the Internet shall be treated as privilege given to those who have the approval of their respective Directors or Head of Ministry.

No one without specific authorization shall use any Ministry of Health computer or network facility for non-Ministry of Health business.

Acceptable Use ICT section provides access to networked computers to support staff's work. Our Acceptable Use Policy is an extension to the Ministry Rules. It includes guidelines for the safe and responsible use of the network and the internet, and identifies those activities which

constitute an abuse of our ICT facilities. In summary, users of the Ministry network are prohibited from:

- Logging on to the network with another user's account
- Creating or sending offensive or harassing materials to others
- Altering the settings of MoH computers or making other changes which render them unusable by others
- Tampering physically with the equipment
- Installing software without authorisation
- Hacking into unauthorised areas of the network
- Accessing inappropriate websites or trying to circumvent the system
- Attempting to spread viruses via the network
- Any form of illegal activity, including software and media piracy

7.2 Systems Administration

Ministry of Health system administrators are entitled to remove from any Ministry of Health computing resource data and programs that are found to be inappropriate and/or to terminate the computing privileges of any user who violates the MOH ICT Policies.

7.3 Proper Authorization

Users are entitled to access only those elements of ICT systems that are consistent with their authorization.

Specific Restrictions on Use

The following categories of use are inappropriate and prohibited:

- **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others**. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behaviour that may cause excessive network traffic or computing load is also prohibited.

- **Use that is inconsistent with the Ministry of Health's values and purposes**. The Ministry is a non-profit, government organization and, as such, is subject to public scrutiny and specific laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of ICT systems for non- Ministry purposes is prohibited, unless specifically authorized. Prohibited commercial

- **Harassing or threatening use**. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another.

- **Use that is damaging the integrity of Ministry or other ICT Systems**. This category includes, but is not limited to, the following activities:

- **Attempts to defeat system security**. Users must not defeat or attempt to defeat any ICT system's security – for example, by "cracking" or guessing and applying the identification or password of another user, or compromising room locks or alarm systems. (This provision does not prohibit, however, Systems Administrators from using security scan programs within the scope of their Systems Authority.)

- **Unauthorized access or use**. The Ministry recognizes the importance of preserving the privacy of users and data stored in ICT systems, particularly data related to patients. Users must honor this principle by neither seeking to obtain unauthorized access to ICT systems, nor permitting or assisting any others in doing the same. For example, people not employed by the Ministry of Health may not use Ministry ICT systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-Ministry organizations or individuals across the Ministry network without specific authorization. Similarly, users are prohibited from accessing or attempting to access data on ICT systems that they are not authorized to access. Furthermore, users must not make or attempt to make any deliberate, unauthorized changes to data on an ICT system. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

- **Disguised use**. Users must not conceal their identity when using ICT systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

- **Distributing computer viruses**. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

- **Modification or removal of data or equipment**. Without specific authorization, users may not remove or modify any Ministry-owned or administered equipment or data from ICT systems.

- **Use of unauthorized peripheral devices.** Without specific authorization, users must not physically, or use hardware specific cables (such as USB cables) to, attach any additional device (such as an external disk, printer, or video system) to ICT systems.

- **Unauthorized use of network resources.** Users are not permitted to connect non-ministry laptops or workstations onto the Ministry's network without specific authorization.

Use of antivirus scanning systems. All authorized connectivity of non-ministry laptops and workstations to the Ministry of Health network must consent to the use of Ministry security scanning programs on these systems.

Detection of security threats on these systems will result in immediate termination of privileges.

- **Other prohibited uses.** Examples of such uses are: promoting a pyramid schemes; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making threats.

- **Use in violation of law.** Illegal use of ICT systems that is, use in violation of civil or criminal law at the international or local level is prohibited.

With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

- **Use in violation of Ministry contracts**. All use of ICT systems must be consistent with the Ministry's contractual obligations, including limitations defined in software and other licensing agreements.

- **Use in violation of Ministry policy**. Use in violation of other Ministry policies also violates this policy. Relevant Ministry policies include, but are not limited to, those regarding sexual

harassment and racial and ethnic harassment, as well as Ministry policies and guidelines regarding incidental personal use of ICT systems.

- **Use in violation of external data network policies**. Users must observe all applicable policies of external data networks when using such networks.

7.4 Personal Account Responsibility

Users are responsible for maintaining the security of their own ICT systems accounts and passwords. Any user changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their ICT systems accounts.

7.5 Responsibility for Content

Official Ministry information may be published in a variety of electronic forms. The Certifying Authority is responsible for the content of the published document.

7.6 Conditions of Ministry Access

The Ministry places a high value on privacy and recognizes its critical importance in a clinical setting. There are nonetheless circumstances in which, following carefully prescribed processes, the Ministry may

determine that certain broad concerns outweigh the value of a user's expectation of privacy and warrant Ministry access to relevant ICT systems without the consent of the user. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

The Ministry may access all aspects of ICT systems, without the consent of the user, in the following circumstances:

- When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the ICT systems; or

- When required by law or administrative rules; or

- When there are reasonable grounds to believe that a violation of law or a significant breach of Ministry policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or

- When such access to ICT systems is required to carry out essential functions of the Ministry; or

- When required to preserve public health and safety.

Process

Consistent with the privacy interests of users, Ministry access without the consent of the user will occur only with the approval of the Secretary of Health and the user's supervising Director as appropriate, or their

respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The Ministry, through the Systems Administrators, will log all instances of access without consent. Systems Administrators will also log any emergency entry within their control for subsequent review by the Director of Funding and Planning and Secretary of Health. A user will be notified of Ministry access to relevant ICT systems without consent; depending on the circumstances, such notification will occur before, during, or after the access, at the Ministry's discretion.

User access deactivations

In addition to accessing the ICT systems, the Ministry, through the appropriate Systems Administrator, may deactivate a user's ICT privileges, whether or not the user is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the user of any such action.

Users will also have all their ICT privileges revoked upon retirement, resignation or termination from the Ministry of Health. The Systems Administrators will only proceed with user account deactivation once notification has been received from the Ministry's Human Resources Department on the user's employment status.

Logs

Most ICT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish and post policies and procedures concerning logging of user actions, including the extent of individually-identifiable data collection, data security, and data retention.

8. ICT ASSET DISPOSAL POLICY

The object is to minimise security risks associated with equipment disposal through ensuring the secure destruction of discarded data stores.

1. Disposal of ICT Assets is the responsibility of the custodian, or manager, of the asset. Prior to disposal, the following should be considered:

- Re-deployment options

- Asset value and cost recovery
- Recycling options
- Destruction of data and configuration information prior to disposal

2. The ICT Asset disposal process used will be based on an assessment of the data value performed by the responsible parties.

The disposal methods presented in this Procedure are intended as a minimum standard of operation; not as directive statements. Workstations that hold critical Information stores, for example, can be destroyed using processes of higher diligence than those described in this Procedure.

9. ICT SOFTWARE POLICY

The goal of this policy is to provide stable technology software solutions that appropriately address business needs. A lack of standards regarding what software can be installed on organizational devices, including desktop and laptop computers, can hinder provision of service. Controlling organizational software is not only a best practice for cost control, but also required for legal compliance. The Software Policy articulates what software is permitted on enterprise devices and who authorizes and carries out the installation task. The goal of this policy is to provide stable technology software solutions that appropriately address business needs. A lack of standards regarding what software can be installed on organizational devices, including desktop and laptop computers, can hinder provision of service. Controlling organizational software is not only a best practice for cost control, but also required for legal compliance. The Software Policy articulates what software is permitted on enterprise devices and who authorizes and carries out the installation task.

Following is a general listing of supported software:

- Microsoft Windows (7, 8, and 10) Professional versions

- Microsoft Office (Word, Excel, PowerPoint, Outlook)
- Google Apps (Gmail, Hangouts, Docs, Sheets, Slides)
- Google Chrome
- Mozilla Firefox
- Adobe Acrobat Reader
- Symantec EndPoint
- Skype

Prohibited software:

It is expressly forbidden to distribute or use computer programs for reasons such as scanning networks, intercepting information or password capture unless specific authority is obtained from the MoH ICT Section Chief.

Puntland Ministry of health users must comply with copyright laws and respect the intellectual property rights of others. It is therefore expressly forbidden for users to have possession of unlicensed software on Ministry of health premises or, during the course of carrying out their employment use unlicensed software on Ministry of health computers. Users of unauthorized copies of software will be disciplined as appropriate under the circumstances.

10. ICT HARDWARE P POLICY

This policy covers all users with MOH contracts over 6 months in duration. Users with contracts of less than six months are not assigned permanent MOH IT hardware. Users separating from the organization will return assigned IT hardware prior to departure.

This policy covers all users with MOH contracts over 6 months in duration. Users with contracts of less than six months are not assigned permanent MOH IT hardware. Users separating from the organization will return assigned IT hardware prior to departure.

This policy also covers IT hardware standards of equipment procured for MOH programmes, as these are a reflection on MOH. Deviations from current standards must be cleared by the MOH ICT section Manager.

All IT hardware has a replacement cycle of 4 years. Any replacements made prior to 4 years require MOH ICT section technical endorsement following provision of justification. The MOH ICT section may revise the replacement cycle depending on the rate of technological advancement.

11. EMAIL USAGE

The Puntand Ministry of health's email is limited personal use of email is permitted but must be in a responsible and professional manner and must not be misused or abused. The sending of any message which contains obscene material or offensive language is not permitted

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.

- Always include a disclaimer (refer to Definitions) which is common to all users, on emails to limit liability.
- Be cautious about opening files or launching programs that have been received as an attachment via email from the email itself. Instead, save an attachment to disk and scan with anti-virus software before opening, and keep an eye out for unusual filenames.
- Never open emails if unsure of the sender.
- Check email accounts on a regular basis and forward relevant emails to the Approved Provider or appropriate committee members/staff.
- Remove correspondence that is no longer required from the computer regularly.
- Respond to emails as soon as is practicable within the next working day.
- Consider the risks and determine whether or not to send personal and sensitive information via unencrypted email
- Ensure all material stored on an end point data-storage device is also stored on a backup drive.

UNACCEPTABLE/INAPPROPRIATE USE OF ICT FACILITIES

- Users of the ICT facilities (and in particular, the internet, email and social media) provided by Puntland Ministry of Health must not:
- Create or exchange messages that are offensive, harassing, obscene or threatening.
- Create, copy, transmit or retransmit chain emails (refer to Definitions), spam (refer to Definitions) or other unauthorised mass communication.
- Use the ICT facilities as a platform to gain unauthorised access to other systems.
- Use the ICT facilities to access, download, create, store or distribute illegal, offensive, obscene or objectionable material (including sexually explicit material). It will not be a defence to claim that the recipient was a consenting adult.
- Use the ICT facilities to make any personal communication that could suggest that such communication was made in that person's official capacity as an employee or volunteer of Puntland Ministry of Health.
- Conduct any outside business or engage in activities related to employment with another organisation.
- Exchange any confidential or sensitive information held by Puntland Ministry of Health unless authorised as part of their duties.
- Publish Puntland Ministry of Health's email address on a 'private' business card.

- Harass, slander, intimidate, embarrass, defame, vilify, seek to offend or make threats against another person or group of people
- Copyright laws through making copies of, or transmitting, material or commercial software.

ANNEX 1 MOH Puntland backup server checklist

Version	Review Date	Received by	Approval Date	Approval by	Summary of Changes	Next Review date
V14.11.2	May 2019	MOH ICT section	12.5.2019	Abdirashid Awad	corrected field names to properly display in Query Designer when query uses JDE SQL Server connection type	May 2022

ANNEX 2 MOH Puntland Authorised user agreement

Puntland Ministry of health Email Account

I, _____

- Acknowledge that I have received an email account belonging to Puntland Ministry of Health
- Will ensure that the email account:
  - Is used for work-related or committee of management purposes only
  - Log in details will not be shared with unauthorised persons
- Will notify the MOH ICT unit as soon as is practicable if any problems occur
- Have read the Puntland Ministry of health Information and Communication (ICT) Technology Policy and agree to abide by the procedures outlined within.

Log in details Account name:
Address:
Password:
Security Questions:

ANNEX 3 Authorised User Agreement for Portable Storage Devices (PSD)

This may include but are not limited to laptop, iPad, USB, external hard drive, SD card, mp3 player. Please read the Puntland Ministry of Health Information and Communication (ICT) Technology Policy and ensure that you abide by the procedures outlined within. By signing the register below, you agree to ensure that the PSD:

– Is used for committee of management purposes only
– Is password-protected where possible/necessary
– Will not be loaned to unauthorised persons
– Will be returned to Puntland Ministry of Health on cessation of involvement with the committee of management – if damaged, faulty or lost, you will notify the Director of Puntland Ministry of health , Administration Officer as soon as is practicable

No of equipment	Name of the person	Role	Date taken	Signature	Date returned	Received by