GOVERNMENT OF SAMOA

HEALTH INFORMATION COMMUNICATION TECHNOLOGY ACCEPTABLE USE AND INFORMATION SECURITY POLICY

Ministry of Health

Table of Contents

1. INTRODUCTION:

Health information is an asset, which like any other asset owned by the Ministry of Health, has significant value to stakeholders of the Ministry and 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 Ministry to perform its activities and operational practices.

This policy document has been developed to establish and uphold the minimum requirements that are necessary to protection information against unavailability, unauthorized or unintentional access, modification, and destruction or improver disclosure.

2. OBJECTIVE:

The main objectives of this policy are to:

(i) ensure consistent, authorized, lawful management and use of MOH information systems and technology as well as defining baseline responsibilities for all its information system security, equipment and file storage;
(ii) provide sanctions in cases of breach of violation of the policy terms;
(iii) support the legal obligations of MOH to maintain the security and confidentiality of all its information under the Ministry of Health Act 2019 and also supports adherence to the Telecommunications Act 2005, National Cyber security Strategy 2016-2021, Samoa Crimes Act 2013 and Samoa Internet and Email Policy 2016; and
(iv) raise awareness of the importance of IT security in the day-to-day business of the Ministry of Health.

1.1. Scope

This policy applies to all employees, contractors, consultants and individuals accessing MOH network and ICT devices or electronic data in any format by any means and from any MOH site or location.

1.2. Equipment covered by this Policy

1.2.1. ***Desktop Computers*** – Personal Computers (PC) issued or provided to staff in the course of carrying out their duties.
1.2.2. ***Laptops/Notebooks/Tablets*** – Portable devices issued or provided to staff in the course of carrying out their duties
1.2.3. ***Mobiles Phones/devices*** – Digital communication devices issued or provided to staff in the course of carrying out their responsibilities.
1.2.4. ***Desk/Landline Phones*** – Telephone/ voice communication devices connected to the network including conference telephones, analogue telephony adaptors, and cordless phones.
1.2.5. ***Media/Portable Media*** - Electronic storage devices such as DVDs, CDs, memory sticks and hard drives issued or provided
1.2.6. ***Network Infrastructure***- equipment used to enable provision of MOH IT network, including servers, enclosures, cabling, switches/hubs, routers, wireless access points, firewalls, proxies, authentication system and devices and remote access systems.
1.2.7. ***External Communication Infrastructure*** – means used to connect MOH to the external world including wide area network, analogue telephone lines, digital

telephone lines, leased lines, LES/WES/Ethernet first mile circuits, ADSL circuits, SDSL circuits and all related equipment and services.

1.2.8. ***All related equipment and facilities controlled IT media used in meeting and conference rooms***.

3. ROLES AND RESPONSIBILITIES:

Defining responsibilities ensure that all users are aware of their responsibilities to minimize the risks to ICT security and operations

Ultimately, responsibility for ICT Security rests with the Director General who has delegated this much of the responsibility to the A.CEO HEALTH it & Communications. Routinely the ICT Unit is responsible for developing, managing and implementing ICT Security policies and processes on a daily basis.

3.1 HITC Division

- Ensuring compliance with relevant legislation, policies and good practice for all equipment and services listed in section 1.2
- Make sure users are aware of this policy and to ensure that users understand and are able to abide by them when carrying out their work.
- Processing requests for hardware, software, network and ICT related service deployments for MOH to ensure value for money, consistency and compliance.
- Maintaining an ICT Asset Register.
- Creating, deleting or disabling computer accounts, including electronic storage areas and email accounts while observing MOH data retention periods.
- Managing, implementing auditing and monitoring information backup schedules and process.
- Maintaining the confidentiality, integrity and availability of MOH systems and data they contain.
- Monitoring for actual or potential IT security breaches within the MOH ICT systems and reporting to the appropriate people as need be.
- Invoking and conducting disaster recovery operations when required.
- Controlling external connections to the MOH networks in accordance with MOH policies.
- Provision of external remote connections for authorized users.
- Day to day responsibility for the management and security of all MOH infrastructure and systems.

3.2 Human Resource Division

- Ensuring that, as part of their contract of employment, all staff to sign confidentiality undertakings.
- Confirm with the HITC Division before departure of an employee from the Ministry whether any ICT device is in their possession.

3.3 Divisional Managers

- Ensuring that all staff under their management who use computers for work purposes, plus all external users of MOH computers under their management, are aware of this and associated policies and procedures.
- Advice the ICT Unit immediately when an employee has resigned, terminated or suspended to ensure appropriate modifications to systems they use such as database, email or internet.
- Ensuring they inform the ICT helpdesk where the member of their staff proceed for any leave of absence for a period that exceeds 2 months.
- Request for creating staff user accounts for new staff or new accounts.

- Arranging for the use or return of any ICT equipment in the possession of their staff member.
- Ensuring they advise the ICT Unit immediately once an employee is to resign, terminated or suspended for the HICT to immediately action suspension or termination of their computer, email and internet access.

3.4 All MOH Staff and authorized users, without exception must:-

- Abide by this and associated policies and procedures.
- Keep all passwords and remote log in data secure (except where necessary to disclose to the ICT Unit for administrative purposes) and to deny unauthorized third party access to MOH network.
- Change their password after logging on for the first time or if a compromise if suspected.
- Not allow others to access, use or share their individual user accounts for any purpose. *(Note: where they may be a clear and justified need for a shared account, this should be discussed with the ICT Unit and if approved by the HICT Manager, a shared account will be created)*
- Change their password regularly and not exceed the enforced 90 day period.
- Never disclose their system, database as well as log on password to anyone including other computer users. The only exception to this may be during telephone ICT support provided by the ICT Unit. If this occurs the user must change their password on completion of the telephone support.
- Keep computer locked using Control Alt Delete or logged off if left unattended: in ward areas the user may have to log off in order to prevent other users being locked out.
- Not connect any privately owned/procured hardware to any MOH computing equipment or network without prior notification of and approval from the ICT unit. This is because of the risk of virus contamination and also to avoid unauthorized copying of confidential MOH information.
- Not install or attempt to install any software on MOH computing equipment without prior written endorsement from the ICT Unit.
- Ensure that all reasonable care is taken to protect the security of IT equipment they are issued together with the data and information stored in it whether used internally or taken outside of the office.

4. PROCESS FOR ACCESS TO THE NETWORK:

Users requiring access to the network must complete an *ICT Access Form* which must be justified and endorsed by their divisional Manager and handed over to the HITC A.CEO for approval and action by the ICT Unit. Signing this form indicates the user has read, understood and agrees to comply with the policies.

Access will not be approved if there is not enough justification to allow it especially for internet and email access.

Access to the network will be discontinued upon termination of an employee, completion of contract, end of service of temporary employee or disciplinary action resulting from violation of this policy or other related policies.

5. PROCESS FOR PROCUREMENT OF ICT EQUIPMENT:

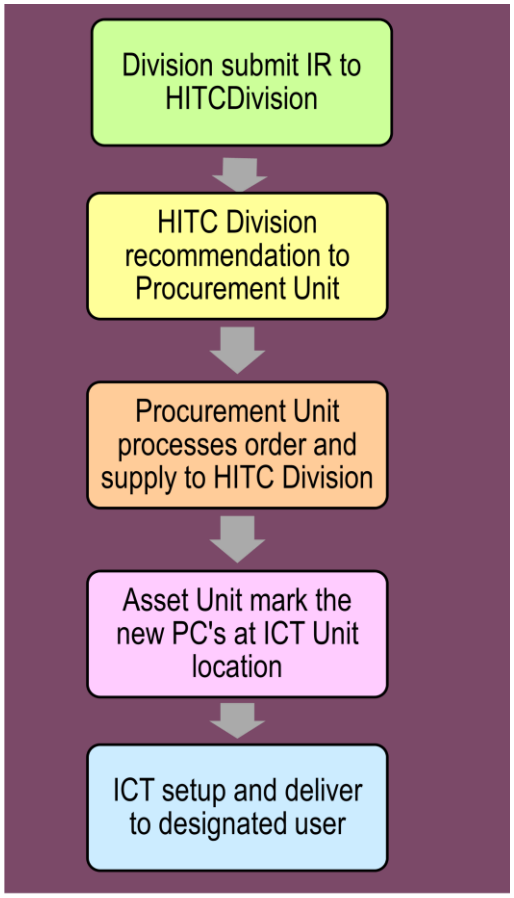
5.1 New Requests

- All requests for Procurement of new equipment's must be directed to the HICT division and must be accompanied by a budget confirmation from the Procurement Unit. ed. Request must include justification and endorsement and approval of the output manager.

- request for quotation will then be carried out in accordance with the ICT minimum specification requirements.

- ICT Unit recommendation will be done and referred with all relevant documents to Procurement Unit to action the relevant procurement process.

- Equipment must be handed directly to the ICT Unit upon their receipt, for confirming the correct specifications and for relevant network setup before handing over to the user.



5.2 Replacements

- ICT Unit will check the equipment and confirm status of equipment for write off.
- ICT Write Off Recommendation report will then be given to the Asset Unit to initiate the formal Write Off process.
- Action *section 4.1* of this policy with the Asset Unit Write Off report as supporting document for the procurement of a replacement equipment

6. ICT ASSET MANAGEMENT:

The ICT Unit must keep accurate and up to date register of new, transferred and written off equipment's. All MOH ICT equipments must be marked accordingly and the ICT Unit will refer to the Asset Unit request to label equipment's whose marks have faded through the years if encountered during their service calls or are being used without asset numbers.

A full equipment stock take should be completed at least once a year.

Equipment allocated to an individual user must not under any circumstances be reallocated within the division (or any other user) without prior notification of the ICT Unit. This is to ensure correct management of sensitive information and account setup. As well as ensuring whether the equipment will work in its planned location.

In the event that a staff member leaves MOH or is in a long term leave, then all loaned ICT assets ***must*** be returned to the HITC Division for checking whether it will need to be replaced or damaged and lost equipment cost must be deducted from end of employment benefits.

6.1 Process for marking new ICT Assets

- Once new equipment arrives, the Asset Management Unit (AMU) must be notified immediately to mark the assets before setup and before they are disseminated to the relevant division.
- Once marked the details will then be entered into the ICT Asset Register.

6.2 Process for Reallocation/ Transfer of ICT Assets

- The Division must inform the Asset Management Unit of their request for equipment transfer.
- Once asset transfer process is complete the ICT unit will then move to action setup of user account, files and information.

7. ACCEPTABLE USE:

The following are prohibited across all of MOH

- The use of MOH network to convey, share or store indecent and/or profane materials.
- The use of MOH infrastructure and resources to store information or conduct activities for privately owned businesses.
- The use of privately owned and bought removable media to import data onto the MOH network and assets without using the Antivirus scanning software beforehand.
- Removing covers of MOH ICT assets for any purpose including changing or adding components.
- Adding /installing ICT equipment to the MOH network without prior written approval from the ICT Unit.
- Leaving workstations logged-on whilst unattended.
- Installing or attempting to install any software including privately owned software onto MOH ICT asset without prior written approval.
- Permitting others to access your individual computer account, even if they themselves are authorized MOH account holders.
- Disclosing or providing access to MOH information to anyone that does not have a legitimate need to know.
- Users must not deliberately mispresent themselves or represent neither other users nor the MOH.
- Attempting to access MOH information systems for which they have no legitimate right to, and may only access systems for which they have been authorized to do so and for a legitimate business reason.
- Copying or transferring movies and music files onto MOH asset, taking up storage space and posing threat to the security of MOH network by way of virus transfers. (If such files are found by the ICT Unit during their maintenance visits, these will be deleted without warning)
- Storing personal and private photos and data on MOH ICT equipment are forbidden.
- Storing music files of any format on MOH equipment are forbidden.
- Storing of entertainment video files of any format are forbidden.

8. PASSWORD MANAGEMENT:

All MOH systems feature password control as part of the identification and authentication methods. Sharing of passwords is strictly forbidden and users must be fully aware of their responsibilities to the network once they are approved access.

The MOH password management procedures include the following requirements:-

- Initial passwords are given to users once registration is complete.
- Initial password changed by the user after first successful log on.
- Complex password made up of mixture of letters and numbers, minimum 8 characters.
- System enforces a password change every 90 days.
- Password is not displayed when user types in the password dialogue box.

9. ANTIVIRUS/ANTI-MALWARE:

MOH has deployed an enterprise Antivirus solution to protect against malicious software and this is deployed to all clients and servers.

Receipt of junk/SPAM email is a nuisance and in some instances could be a threat; all users should be cautious about any potential unsolicited emails and delete them at the earliest possible opportunity.

Use of removable/USB drives is limited to Senior level up to Management level. For any user below Senior level that requires access to use flash drive, their divisional Manager must authorize their usage. This is to control the entrance of Trojan viruses into our network.

10. ACCESS CONTROL:

Access control is an integral part of the controlling software and restricts access to MOH machines and internet by using a log-on feature requiring authentication. This assigned User ID and password is issued by the ICT Unit.

User Accounts: When user fills in their application for computer log on access using the access form (*Appendix 1*), they must read the policies carefully and must sign the confidentiality section.

- Divisional Managers/A.CEOS's must request access for any MOH system including network log on account for new staff by communicating with the HITC Manager.
- When accounts are closed, any data held within the account including email folders and files will be deleted after having been archived for a period of
  - 12 months on ceasing employment;
  - 12 months after the date of last access if the account has not been accessed for 90 days.

11. INFORMATION BACKUP:

The ICT Unit is responsible for controlling and implementing MOH's backup strategy.

- Servers only backup information stored on user Home drives.
- Users must take necessary measures to ensure their information is safe by keeping copies of their work on their USB drives.
- Divisions must have procedures in place to ensure data is retained in accordance with MOH policies. This may require archiving of divisional data or storage on shared homes drives. Please contact ICT for further guidance.
- Users must ensure local hard disk drives are not being used for backing up MOH information.

12. NETWORK SECURITY:

External connections in and out of MOH computer networks, supporting MOH services are subject to rules set by the HITC Division. Anyone requiring an external connection, either for support services or extended organizational activities, must contact the ICT Unit.

Remote access is forbidden. However, if the need warrants access, then endorsement by the HICT Divisional Manager will be needed and referred to the Director General for official approval.

13.MONITORING:

Users should expect no privacy when using the corporate network or MOH resources, such use may include but is not limited to; transmission and storage of files, data and messages.

MOH reserves the right to monitor any and all use of the computer network. To ensure compliance with MOH and national policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks and removable media upon approval of the Director General.

In the event of a requirement to investigate user activity or disciplinary proceedings being conducted by the HR Division and officially approved by the Director General, the ICT Unit will gather and make available all appropriate information from various sources to assist the investigation.

In the event that a divisional staff of any level requests the ICT Unit to provide report about user activity, these can only be actioned upon approval of the Director General following endorsement by the divisional Manager/A.CEO has been obtained. These requests ***must*** be supported by a clear rationale justifying the suspicions held about a certain user's activity. *(This will be required before any request for any investigation is completed)*

14.INCIDENT REPORTING:

Any member of the MOH staff observing an ICT Security incident must raise an incident report in accordance with MOH process and provide the ICT with relevant details. Typically these incidents include, but not limited to

- Virus attacks
- Password violation (disclose and sharing)
- Loss of equipment
- Theft of equipment
- Account sharing (users sharing account log on)
- Accessing inappropriate websites
- Storage of music files of any format, private/personal digital images and data
- Storage of entertainment video files of any format
- Visible evidence of ICT equipment being tampered with.

15.POLICY REVIEW:

The review of this policy will be lead by the Strategic Planning, Policy and Research Division in collaboration with the Health Information and Communication Technology Division of the Ministry of Health. The policy review will be conducted on annual basis or when the need arises within the year.