GOVERNMENT OF SAMOA

MINISTRY OF HEALTH
E-MAIL POLICY

OCTOBER 2020

Table of Contents

INTRODUCTION

The Electronic mail (email) is an integral part of MOH' communications with healthcare organizations, government agencies, business and members of the public. It is widely used in all areas of the Health Sector, often as the primary communication and awareness strategies within the Ministry. At the same time, misuse of email can post many legal, privacy and security risks. It is therefore important for users / employees to understand the appropriate use of electronic communications.

The Ministry of Health provides email to all authorized employees. Email is a business tool to help the Ministry's employees serve our customers, communicate with vendors, streamline internal communications and reduce unnecessary paperwork. The email system is intended primarily for business purposes of the Ministry. This email policy outlines the acceptable use of business email for the Ministry of Health.

PURPOSE

The purpose of this email policy is to help employees ensure the Ministry email is used appropriately, and make users aware of what the Ministry considers as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within the Ministry of Health's (MoH) Network. It also provides sanctions in cases of breach of violation of the policy.

SCOPE

This policy is intended to detail the rules of conduct for all staff of the Ministry of Health who use email and related services. This email policy applies and covers appropriate use for the purpose of any email sent from a Ministry email address, email messages and attachments, of any IT facilities including hardware, software and networks provided by the Ministry. The policy applies to all MoH employees and individuals granted the privilege to have access and/or use the MOH email services regardless of location and source of connectivity. They are here on referred to as '*users*'.

OBJECTIVES

The objectives of this policy:

- Increasing understanding of the requirements for the use and management of email in the Ministry of Health
- Reduce corporate exposure from inappropriate email practices and to ensure compliance with legal requirements such as freedom of information requirements and the Confidentiality Agreement
- Increase understanding by employees that their actions may have legal implications and could adversely affect them, if they act outside of this policy
- Promote acceptable use of email in the MoH

POLICY

1. STRUCTURE OF E-MAIL ACCOUNT

All email accounts adhere to a specific naming convention. "*Firstname.Lastname@health.gov.ws*". For example, "george.washington@health.gov.ws"

2. OWNERSHIP OF MOH E-MAIL ACCOUNTS.

Although primarily all MOH email accounts are given for the purpose of conducting MOH work related activities, MOH allows reasonable personal use and for usage to be in accordance with this policy. All MOH email accounts are the property of MOH therefore the Ministry, authorized personnel(s), have the right to investigate, read and keep record of any emails that users transmit via the MOH' email system. The DG is the only authority to authorize investigations of this nature unless otherwise delegated.

3. E-MAIL ACCESS REQUEST AND APPROVAL

Access to an MOH email account and usage is a privilege provided only on an as-needed basis to support the user's professional duties in performing MOH activities to achieve its goals.

3.1 Usage Request

Users requiring access to an email account must first read this Email Policy plus other relevant policies before completing and signing the ***ICT Access Form***. Signing this form indicates the user has read, understood and agrees to comply with the policies. This request must then be justified and endorsed by the relevant ACEO and submitted to the ACEO of Health ITC Services.

3.2 Usage Approval

The ACEO of Health ITC Services will assess and approve or disapprove the submitted request before passing it to the IT department for the necessary action to be taken.

3.3 Usage Disapproval

The request for access to an email account will be denied if the justification for an account is not satisfactory.

3.4 Removal of Access to an Email account

Access to email accounts 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.

4. HOW TO ACCESS MOH E-MAIL

There are two methods of accessing MOH email.

1) After an email request has been approved, the IT Unit then comes around to the user workstation and setup email in Microsoft Outlook.

2) Another method of accessing MOH emails either from within MOH or when the user is outside of the office or on duty travel is-
Step 1: Open browser (either Internet Explorer, Google Chrome, Mozilla Firefox).
Step2: In the address bar, type *email.MOH.gov.ws*
Step 3: Press Enter.
Step 4: Then enter your Username (which is the same as your email account) and Password.

5. PASSWORDS

Accessing contents of a user email account requires login passwords. The user is responsible for taking reasonable steps to ensure that no person has unauthorized access to their password or account login information. It is the user's sole responsibility to control and monitor the use of their passwords and to inform the IT department as soon as they suspect unauthorized access and/or usage of their email account.

6. ACCEPTABLE E-MAIL USAGE

The following lists the acceptable use and security measures that one must exercise when using their MOH emails.

- Emails sent and received via MOH' email system should be kept as private as possible by senders and recipients. MOH management and its email system administrators will not access or read emails unless necessary in the course of their duties (e.g. including investigation, report of inappropriate usage or as directed by the Director General of Health.
- Communication between employees and its stakeholders for business purposes.
- Employee professional development.
- Informing employees about upcoming meetings and events.

7. UNACCEPTABLE / MISUSE E-MAIL USAGE

Strictly prohibited activities include, but are not limited to:

7.1 Usage of MOH email account for sign up to social media sites is prohibited as these are a doorway for entrance of spam or virus attacks.

7.2 Usage of email to harass or intimidate others.

7.3 Sending emails that are offensive, obscene, defamatory, abusive or otherwise unlawful. Email messages can be used as evidence in a court of law.

7.4 Creation, posting, transmission or voluntary receipt of any unlawful offensive, libelous, threatening, harassing material including, but not limited to comments based on race, nationality, gender, sexual orientation, age, disability, religion, social or political beliefs.

7.5 The acquisition, storage and dissemination of data which is illegal, pornographic or which negatively depicts race, sex or creed is specifically prohibited.

7.6 MOH also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

7.7 Deliberate pointing or hyper-linking of the MOH website to other sources whose contents may be inconsistent with or in violation of the policies of the company.

7.8 Use, transmission, duplication or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets or patent rights of any person, group or organization. Users are to assume that all materials on the internet are copyright and/or patented unless specific notices state otherwise.

7.9 Use, transmission or duplication of any proprietary, confidential or otherwise sensitive information about patient or other staff members without the proper controls.

7.10 Usage of email to adversely affect the reputation of MOH.

7.11 Any form of gambling is strictly prohibited.

7.12 Playing of any online games.

7.13 Participation in any online contest or promotion.

7.14 Forwarding of chain letters.

7.15 Acceptance of promotional gifts.

7.16 Transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind

All authorized users of the MOH email accounts should be aware that deleting an email may not remove all instances of that message. There may be copies of the message elsewhere, for instance, the recipients system or backup files held on central servers.

Using email for illegal activities is strictly prohibited. Illegal use may include, but is not limited to obscenity, child pornography, threats, harassment, theft, attempting unauthorized accss to data or attempting to breach any security measures on any electronic communications system, attempting to intercept any electronic communication transmissions without proper authority, and violation of copyright, trademark, or defamation law.

8. PERSONAL USE

Employees are allowed to use their email for personal reasons like register for classes or set up meetings, send email to families and friends as long as they do not spam or disclose confidentiality information. Employees must adhere to this policy at all times, in addition to our confidentiality and data protection agreements.

8.1 All users must follow the corporate principles regarding resource use and exercise good judgment when using the email. Usage of email by personnel that is inconsistent with corporate needs of MOH results in the misuse of resources.

8.2 Usage of MOH computer resources to access the MOH email for personal purposes without approval may be considered cause for disciplinary action.

8.3 All users must be aware that the company network creates a log of all access activities reflecting what times email was accessed and whether it was a legitimate log in.

8.4 Users who choose to store or transmit personal information such as bank pin numbers or related details as well as credit card numbers on email do so at their own risk. MOH is not responsible for any loss of information, such as information stored online and accessed through MOH ICT resources, or any consequential loss of personal property due to such processes.

8.5 Any ordering (shopping) of items or services on email, or request for services and goods against government or MOH policies for personal gain or use is strictly prohibited.

8.6 All users must adhere to this policy at all times, and should at all times refrain from conflict of interest, harassment, defamation, copyright violation, or illegal activities

9. ACCESS TO E-MAIL ACCOUNTS UPON DEPARTURE

Authorization or entitlement to access an individual's email account will normally automatically cease on the date on which an individual's employment with MOH has ended. If additional access is required to an email account then this must be authorized by the Chief Executive Officer.

10. E-MAIL DISCLAIMER

To ensure confidentiality of patient information and other MOH confidential documents and information from being disseminated by unauthorized users and viewed by unauthorized viewers, all email users of MOH must have the following disclaimer as part of their email signatures.

"This e-mail and any files transmitted with it are the property of Samoa National Health Services, are confidential and intended solely for the use of the recipient(s) or entity to whom they are addressed. If you are not the intended recipient(s), you should not disseminate, distribute or copy this e-mail and you should notify the sender immediately and delete this e-mail from your system. You are hereby notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited and you might be liable for punishment."

11. E-MAIL SECURITY

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment.

Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every two months.

Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of click bait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can ask our IT Team.

We remind our employees to keep their anti-malware programs updated.

12. DISCIPLINARY ACTION

Employees / Users who do not adhere to this Policy will face disciplinary action.

REFERENCES

Brown university (2015) **Workable Corporate Email Usage Policy**. Downloaded from: https://it.brown.edu/computing-policies/enail-policy

Government of Western Australia (2004). Guidelines to Assist Agencies in Developing Email an Internet Use Policies. Department of the Premier and Cabinet. Office of e-Government. Perth, Western Australia.

Heathfield Susan M. (2019). **Company Internet and Email Policy**. Downloaded from: http://www,thebalancexareers.com/internet_and_email-policy-sample-1918869

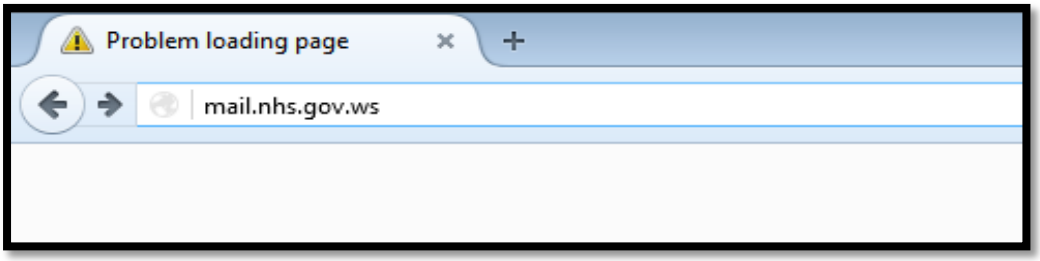
University of Arizona (1998). **Electronic Mail Policy**. Downloaded from: https://policy.arizona.edu/infomration-technology/electronic-mail-policy

APPENDIX

Step 1: Double click to open browser (either Internet Explorer, Google Chrome, Mozilla Firefox).

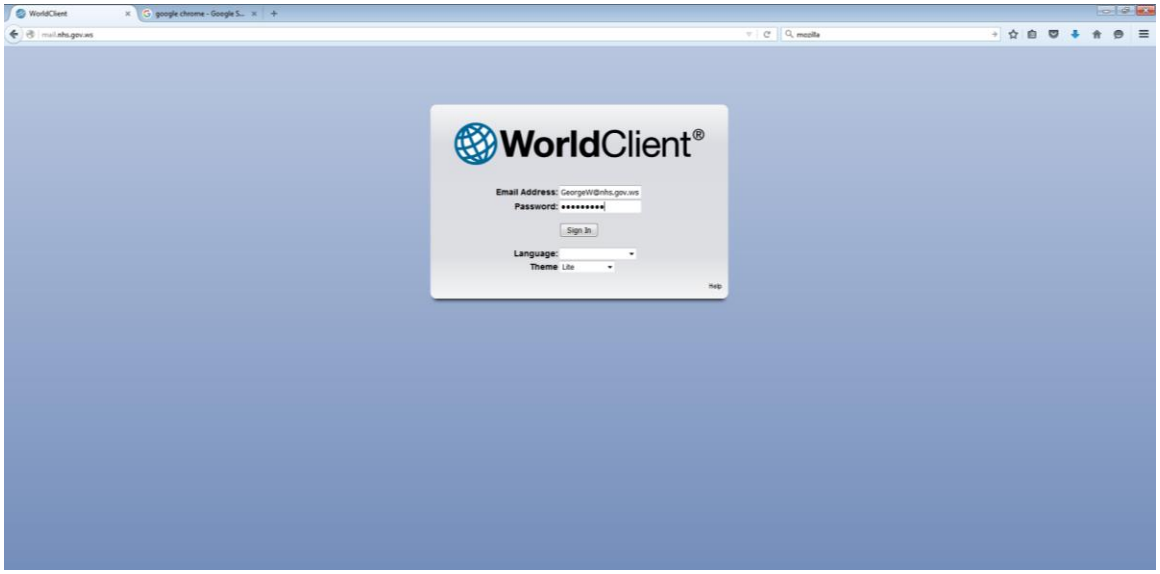
… Or (Internet, Safari) on other mobile devices.

Step 2: In the address bar, type *mail.MOH.gov.ws*



Step 3: Press Enter.

Step 4: Then enter your Username (which is the same as your email account) and Password.



ICT Access Form