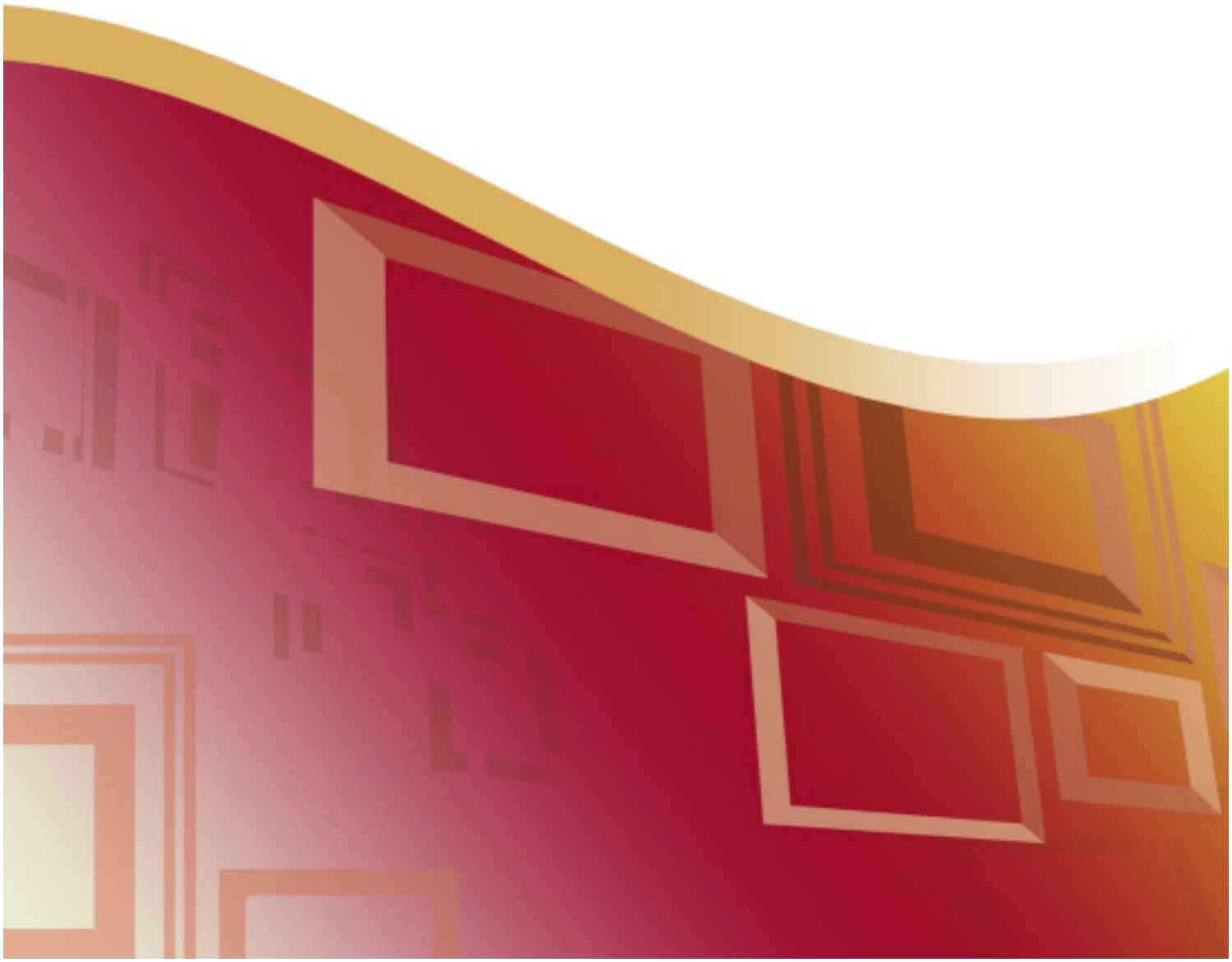
Government of Samoa

Ministry of Communication and Information Technology

GOVERNMENT INTERNET AND ELECTRONIC MAIL POLICY 2016



Ministry of Communications and Information Technology,
Private Bag,
Level 6,
Tui Atua Tupua Tamasese Efi Building,
Apia,
SAMOA.
Telephone: (685) 26117
Facsimile: (685) 24671
Email: www.mcit.gov.ws

Table of Contents:

Acronyms:

GoS	-	Government of Samoa
e-Mail	-	Electronic Mail
LAN	-	Local Area Network
Government Organisation	-	Ministry, Constitutional Authorities, Corporations, Authority, SOE's, etc)

Introduction:

The GoS encourages Government Organisations and their employees to use e-Mail, Internet, organisational intranet, websites and other means of electronic communications for government day-to-day operations, to communicate extensive range of information resources and services across Government, businesses, partners and with the general public.

Electronic communications offer unique benefits and challenges. There are technical aspects to any electronic system that an Organisation may need to consider.

Purpose:

The Government Internet and Electronic Mail Policy defines and outline acceptable use of internet and e-Mail in Government Organisations.

It complements on a higher level, internal policies, procedures and guidelines put in place by individual Government Organisations to minimize risks and costs to the Government, while realising valuable potential of these communication tools.

Vision Statement:

Effective and Efficient Communication Services for all.

Policy Objectives:

This policy aims to;

- Encourage communication access to facilitate and enhance government services;
- Improve the quality of work and employee productivity;
- Create security standards to protect and maintain Government resources.

Scope:

This policy applies to Users of all resources and information technology equipment owned, leased or hired by the GoS regardless of the time of day, location, or method of access. Any third parties such as Visitors, Project Contractors, Consultants or Suppliers must have prior authorisation from a designated Authority to use Government Internet and/ or e-Mail resources and networks.

Legislative Framework:

All Government Organisations are responsible for assuring that employees and users under its authority have been made aware of the provisions of this policy, that compliance by the employee is expected, and that intentional, inappropriate use of Internet and e-Mail resources may result in disciplinary action and up to dismissal.

Legal action may proceed if necessary pursuant to the following legislations:

- Electronics Transactions Act 2008
- Telecommunications Act 2005

- Public Service Act 2004
- Copyright Act 1998
- Patents Act 1972
- Criminal Procedure Act 1972
- Crimes Act 2013
- Public Finance Management Act 2002

Policy:

This policy requires all Government Organisations, employees and other users to comply with the acceptable use provisions, to protect both the user and the GoS.

All government organisations are different, and it is vital that all its policies are relevant to its needs. Some Organisations will need to have a detailed policy, others maybe less so, but the following features are to be in common:

- How much personal use of Intenet and e-Mail can be made, if any;
- Securuing information and data through privacy policy and confidentiality agreements.
- Good housekeeping practices, including locking keyboards and password security use of language and appropriate etiquette (no capitalisation of text, correct forms of address and signing off);
- Prohibition of inappropriate messages, for instance any that might cause offence or harassment on grounds of age, sex, race, disability, religion etc;
- Prohibition of deliberate accessing of offensive, obscene or indecent material from the Internet, such as pornography, racist or sexist material, violent images, incitement to criminal behaviour etc;
- Being aware of copyright and licensing restrictions that might apply to downloaded and forwarded material, whether Internet or e-Mail, and including unauthorised software, games, magazine, disc items etc. The importation of viruses is often through downloading files and programs from external sources;
- What monitoring, if any, will be carried out by the Organisation;
- What might happen if a breach of the policy occurs.

Once a policy is in place, it must be communicated to everyone. Communication methods may include:

- Via e-Mail, although that does not guarantee that the recipients will open it!
- A follow-up circular, or incorporation into a staff handbook (hardcopy or intranet) is sensible. Some Organisations may wish to consider including any such policies into individual contracts;
- A presentation to staff to explain the system and its use might be appropriate in smaller Organisations, discrete Departments or Teams;
- Training in effective use should be available to all. Some Organisations may consider including policy consultation during induction trainings for new recruits.

Policy Guidelines

Internet Services

The Internet is a valuable tool for research and provide a great source of information to users. Some Organisations allow reasonable personal use of internet, perhaps outside working hours, some allow no personal use at all. If personal use is granted, the Organisation has to be aware of some of the issues that may arise, and a policy for use should be drawn up and communicated to everyone. Factors to consider include:

- Internet connection costs can be high;
- Viruses can be imported into the Organisation's system;
- Inappropriate sites may be visited (pornographic, racist, sexist etc);
- People may spend too long on personal surfing during working hours.

Website

With the rapid increase of internet, more and more people are accesing information from Government websites. Therefore, Government Organisations are encouraged to create its own respective website to improve the standard of information and service delivery through electronic media and demonstrate its commitment to enhance government public interaction through application of internet technologies.

Accessibility

When developing websites, Organisations should consider the needs of a broad spectrum of visitors, including the general public, specialised audiences, people with disabilities, those without access to advanced technologies, and those with limited english proficiency.

Copyright

Web developers must ensure that published Web materials follow applicable laws and regulations, and respect the intellectual property and privacy rights of others.
Copyrighted photographs, text or graphics created by another person may not be placed on a web page without permission of the photographer, artist or author. Developers should be aware of all legal issues, especially copyright.

Outdated, incomplete, or inaccurate information is of little use and Organisations should routinely review and update their respective website pages.

Social Media

Social media refers to social networks, video and photo file sharing, social bookmarking, blogs, micro-blogs, podcasting, wikis and other similar tools. It refers to freely accessible online social media tools used to produce, post and interact using text, images, video, and audio to communicate, share, collaborate, or network.

Government Organisations should consider the following before making use of social media tools:

- Keep postings legal, ethical and respectful;
- Respect copyright laws;

- Ensure that information published on-line is accurate and approved;
- Keep Government-confidential information confidential;
- Keep personal social media activities distinct from Government communication;
- Government logos and other Government branding symbols may not be used in personal social media posts, without explicit permission in writing from the Organisation Authority;
- Respect Government time and property.

Failure to control when and how social media sites are being created and used on behalf of the Government sets the stage for losses.

Electronic Mail (E-mail)

The Organisation may allow full personal use of e-Mail, or limited use, or prohibit any personal use. If personal use is allowed, staff should be made aware of the possibility of importing viruses into the system, and what action to take if, for instance, an e-Mail has a suspect attachment, or they are sent a 'chain' letter. The Organisation should have a nominated personnel who can advise on security issues. Medium to Small range Organisations, who may outsource their computer support, will probably be able to include security issues within their maintenance contracts.

The following broad policy guidelines on e-Mail will be considered for the provision of e-Mail services within a Government Organisation.

i. Head of a Government Organisation will retain the Administrative Control of the network established in his/her domain;
ii. Head of a Government Organisation will decide as to which employee of his / her Organization should be provided with e-Mail addresses. External e-Mails should have disclaimers attached;
iii. Necessary software for the purpose of e-Mail and Internet filtering should be in place. This will enable Network/System Administrator(s) to reduce the SPAM traffic on their network(s);
iv. e-Mail can be used for exchange of draft Documents, exchange of general information, scheduling of internal office meetings, comments/draft minutes of meetings, circulation of office messages, other drafts, engagement activities, etc. within Government Offices;
v. To serve as legal documents, all e-Mails must be maintained on the mail server for legal/audit/documentary purposes;
vi. Electronic Mail signatures must be attached to e-Mails sent for all official correspondences. This practice identifies the source and serves as a record keeping;
vii. Government Officials may use Public e-Mail addresses (gmail, hotmail, etc.) for official correspondence, if required.

Security

Network Protection

Network Administrator(s) will ensure that properly configured Firewall and filtering systems

are in place to technically support the access requirements defined by this policy.

Hardware or software firewall must be installed and configured to protect the network from unauthorised access and intrusion into an Organisation‘s LAN from the Internet.

Virus Protection

The LAN should be protected from viruses by using standard Antivirus software. This should be scheduled to automatically update the clients and servers after daily centralised downloading of latest virus from the Internet or e-Mail attachments, and any other devices connected to the organisation network.

Software Installation

Employees must not install software on any Organisation’s computing devices operated within the government network. Software requests must be approved by the IT Manager/ACEO Corporate Services and CEO, and then be made to the Information Technology Division in writing or via e-Mail. Software must be selected from an approved software list, maintained by the Information Technology Division, unless no selection on the list meets the requester’s need. The Information Technology Division will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

Backup and Recovery

Backup specifics and procedures vary according to the needs of an Organisation. Periodically reviewing your backup-and-restore process is a key part of ensuring data security.

Prohibited and Unacceptable Uses:

Government Organisations must ensure that its employess and other users must not engage in any activity that may reasonably be anticipated to cause damage to the GoS’s hardware or software. Precluded activities include but are not limited to;

Illegal Downloading

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, including but not limited to, the downloading, installation or distribution of pirated software, digital music and video files.

Viruses and Hacking

Engaging in illegal activities or using the Internet or e-Mail for any illegal purposes, including initiating or receiving communications that violate any laws of the Independent State of Samoa and regulations. This includes malicious use, spreading of viruses, and hacking. Employees must not attempt to gain unauthorised access to any information resources, systems or networks, databases, data or electronically stored information or interfere with another user's work.

Commercial Manner

Using the Internet and e-Mail for personal business activities in a commercial manner such as buying or selling of commodities or services with a profit motive.

Offensive Material

Using resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, whether through language, frequency or size of messages. This includes statements, language, images, e-Mail signatures or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, and disability, religious or political beliefs.

Abusive Languages

Using abusive or objectionable language in either public or private messages.

Pornographic Sites

Knowingly accessing pornographic sites on the Internet and disseminating, soliciting or storing sexually oriented messages or images.

Misleading e-Mail

Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or e-Mail. This includes the use of false or misleading subject headers and presentation of information in the distribution of e-Mail.

e-Mail Account of Another Employee

Employees are not permitted to use the e-Mail account of another employee without receiving written authorisation or delegated permission to do so.

e-Mail Header Forgery

Employees are not permitted to forge e-Mail headers to make it appear as though an e-Mail came from someone else.

Chain Letters and Pyramid Schemes

Sending or forwarding chain letters or other pyramid schemes of any type.

Unsolicited Commercial E-mail

Sending or forwarding unsolicited commercial e-Mail (spam) including jokes.

Religious and Political Activities

Soliciting money for religious or political causes, advocating religious or political opinions and endorsing political candidates.

Fraudulent Offer

Making fraudulent offers of products, items, or services originating from any Government account.

Unwarranted Invasion of Personal Privacy

Using official resources to distribute personal information that constitutes an unwarranted invasion of personal privacy.

Personal Webpage
Developing or maintaining a personal web page on or from a Government device.

Non-Government Service
Any other Non-Government service related activities that will cause congestion, disruption of networks or systems including, but not limited to, Internet games, online gaming, and e-Mail attachments.

Government Managers and Supervisors Responsibilities:

Government Managers and Supervisors are required to identify Internet and e-Mail training needs and resources, to encourage use of the Internet and e-Mail, to improve job performance, to support staff attendance at training sessions, and to permit use of official time for maintaining skills, as appropriate.

Government Managers and Supervisors are expected to work with employees to determine the appropriateness of using the Internet and e-Mail for professional activities and career development, while ensuring that employees do not violate the general provisions of this policy.

Government Managers and Supervisors who suspect that an employee is using Internet and e-Mail inappropriately, must gain access to the employee's Domain and E-mail account.

Monitoring, Maintenance and Review:

Internet and e-Mail systems are subject to random monitoring and recording by or on behalf of the GoS by each Government Organisations. Accordingly, while the Government will at all times seek to act in a fair manner, employees and other users should be aware that there can be no legitimate expectation of privacy when using Government's Internet and e-Mail facilities.

The Government Internet and Electronic Mail Policy must be regularly monitored and reviewed by the Ministry of Communications and Information Technology (MCIT) through its Policy Division every twelve month cycle.

Modification History:

Version	Document	Date	Changes
1.0	Government Internet and Electronic Mail Acceptable Use Policy	2010	Initial Release
2.0	Government Internet and Electronic Mail Policy	2016	First Review with major changes and additional guidelines

Annex 1: List of Government Organisations

The Government Internet and Electronic Mail Policy 2016 applies to the follwoing Government Ministries, Authorities, Corporations and State Owned Enterprises.

Accident Compensation Corporation
Attorney General's Office
Audit Office
Central Bank of Samoa
Development Bank of Samoa
Electric Power Corporation
Land Transport Authority
Legislative Assembly
Ministry for Revenue
Ministry of Agriculture & Fisheries
Ministry of Commerce Industry & Labour
Ministry of Communications and Information Technology
Ministry of Education Sports & Culture
Ministry of Finance
Ministry of Foreign Affairs & Trade
Ministry of Health
Ministry of Justice & Courts Administration
Ministry of Natural Resources & Environment
Ministry of Police
Ministry of Public Enterprises
Ministry of the Prime Minister & Cabinet
Ministry of Women Community & Social Development
Ministry of Works, Transport & Infrastructure
National Health Services
National University of Samoa
Office of the Electoral Commissioner
Office of the Regulator
Ombudsman's Office
Public Service Commission
Public Trust Office
Samoa Airports Authority
Samoa Bureau of Statistics
Samoa Fire & Emergency Services Authority
Samoa Housing Corporation
Samoa International Finance Authority
Samoa Land Corporation
Samoa Law Reform Commission
Samoa Life Assurance Corporation
Samoa National Kidney Foundation
Samoa National Provident Fund

Samoa Ports Authority
Samoa Post
Samoa Prisons & Correction Services
Samoa Qualifications Authority
Samoa Shipping Corporation
Samoa Shipping Services
Samoa Sports Facilities Authority
Samoa Tourism Authority
Samoa Trust Estate Corporation
Samoa Water Authority
Scientific Research of Samoa
Unit Trust of Samoa

Annex 2: Statement of Compliance

The Government of Samoa's Internet and e-Mail resources must be used in a responsible, lawful and ethical manner and must be solely used for purposes that serve the Government mission and goals. Internet and e-Mail access will only be provided to authorised personnel. Usage for personal or unauthorized activities is strictly prohibited and could result in criminal prosecution under applicable legislations.

You should have no expectation of privacy, rights or ownership in anything you may access, create, store, send, or receive within the Government network. This application constitutes your waiver, and consents to monitoring, retrieval and disclosure of any information in this network, for all purposes deemed appropriate by the Government of Samoa.

You are responsible for the secure handling of sensitive personnel, financial and/or security related information you may be authorized to handle, and conform to your organisation privacy and confidentiality for data handling and disposal.

You must use Government Internet and e-Mail solely for business-related communications. Abuse of Internet and e-Mail may lead to suspension of your computing privileges and possible disciplinary action.

Accessing, viewing, downloading, e-mailing, or storing pornography is strictly prohibited. Pornography is considered sexual harassment and will not be tolerated.

Downloading or installing software is prohibited. Software requests must be made to the IT Division who will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation upon approval from IT Manager/ACEO Corporate Services and CEO.

The User ID and password being issued to you must not be shared with any other individual. You must assume full responsibility for the security of your password. If you forget your password or believe your password has been compromised, contact your IT Administrator immediately.
You are not permitted to use the e-Mail account of another employee without receiving written authorisation or delegated permission to do so.

Chain mail is prohibited. Please do not forward chain letters, games, virus alarms, or solicitations for donations. These are non-productive within the public sector.

Adhere to all licenses, copyright laws, contracts, and other restricted or proprietary information.

Government Managers and Supervisors reserve the right to take action as it deems appropriate against any user that knowingly violate the conditions of the Government Internet and Electronic Mail Policy and will be treated seriously and subject to disciplinary action up to and including dismissal.

User Acknowledgement

☐ I have read and understand the Statement of Compliance above.

☐ I understand that any violation of these Terms and Conditions may result in suspension and/or termination of my access to the Internet and/or e-Mail.

☐ IT Administrator may access my domain and email account for monitoring and auditing.

Signature *Print Name* *Date*

_____ _____ _____

Supervisor

My signature below certifies that the above applicant is an employee / user of_____ {*Organisation Name*} under my supervision. I am responsible to ensuring this employee / user complies with the above terms and conditions and receives possible disciplinary actions if he/she violates the general provsisions of the Government Internet and Electronic Mail Policy.

Signature *Print Name*

_____ _____

Position Title *Date*