



Office of the Attorney General of Guam

590 S. Marine Corps Dr., Ste. 706, Tamuning, Guam 96913



Elizabeth Barrett-Anderson
Attorney General
Phone: (671) 475-3324
ext. 5015/ 5030
Fax: 477-4703
law@guamag.org

Jacqueline Z. Cruz
Chief of Staff
Administration
ext. 5010
jzcruz@guamag.org

Phillip J. Tydingco
Chief Prosecutor
Prosecution
ext. 2410
ptydingco@guamag.org

Karl P. Espaldon
Deputy AG
Solicitors
ext. 3115
kespaldon@guamag.org

Kenneth D. Orcutt
Deputy AG
Litigation
ext. 3225
korcutt@guamag.org

Fred S. Nishihira
Deputy AG
Consumer Protection
ext. 3250
fnishihira@guamag.org

Rebecca M. Perez
Deputy AG
Child Support
ext. 1610
rebecca.perez@guamcse.net

Carol M. Hinkle-Sanchez
Deputy AG
Juvenile
ext. 4040
csanchez@guamag.org

Pauline I. Untalan
Administrator
Victim Service Center
& Notary Unit
ext. 5030
puntalan@guamag.org

September 15, 2016

Memorandum

To: All Employees
From: Attorney General
Subject: **Computer Usage Policy**
RE: **Policy 2016-002**

Hafa adai. Attached is the OAG's Computer Usage Policy 2016-002. All employees are required to read, acknowledge, date, and return the last page to Human Resources Section by **Friday, September 30, 2016.**



ELIZABETH BARRETT-ANDERSON

Attachment



**OFFICE OF THE ATTORNEY GENERAL
COMPUTER USAGE POLICY
GOVERNING THE USE OF GOVERNMENT OF GUAM
COMPUTERS, ELECTRONIC DEVICES AND INTERNET ACCESS**

Policy Number 2016-002

Statement of Need

This policy applies to all staff of the Office of the Attorney General (OAG) of Guam. OAG automation systems to include Information Systems which access, store, or transmit OAG information; computers, voice mail, electronic pads, smart phones, fax machines and all forms of Internet/Network access, are for OAG business and is to be used for authorized purposes only.¹

OAG automation systems are OAG resources and are provided as business communications tools. Electronic communication “should not be used to solicit or sell products, distract coworkers, or disrupt the workplace.” (See the Government of Guam, Personnel Rules and Regulations, Department of Administration).

Use of OAG computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct including, but not limited to:

- Violating confidentiality of data contained in these systems and networks
- Sending chain letters
- Use of automation systems and computers for social media and/or social networking **unless** pre-approved in writing by the Attorney General for OAG business related activities
- Engaging in private or personal business activities
- Misrepresenting oneself or the OAG
- Engaging in unlawful or malicious activities / or violate any local or federal law.
- Violate copyright or intellectual property of another individual or organization
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages
- Sending, receiving, or accessing pornographic materials

¹ This policy is enacted pursuant to 4 GCA 4101.1 and 4105, personnel policies; 4 GCA 4508, employee email accounts protected; 4 GCA 1101 and 1102, government property; 5 GCA 20603 and 20604, government records; and 5 GCA 10103, Sunshine Reform Act of 1999.

- Becoming involved in partisan politics
- Causing congestion, disruption, disablement, alteration, or impairment of OAG networks or systems
- Infringing in any way on the copyrights or trademark rights of others
- Using recreational games
- Gambling, wagering, betting or selling chances; and/or
- Defeating or attempting to defeat security restrictions on OAG systems and applications.

Using OAG automation systems to create, view, transmit, or receive racist, pornographic, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Material" is defined as any visual, textual, or auditory entity. Such material violates the Government of Guam or OAG anti-harassment policies and is subject to disciplinary action. The Government of Guam's or OAG's electronic mail system must not be used to violate the laws and regulations of the United States or any other nation, state, city, province, or other local jurisdiction in any way. Use of OAG resources for these activities can lead to disciplinary action, up to and including, dismissal and criminal prosecution.

Unless specifically granted in this policy, any non-business use of the OAG's automation system is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action, up to and including, dismissal.

Ownership and Access of Electronic Mail and Computer Files

The OAG owns the rights to all data and files in any computer, network, or other information system used in the OAG. This data and these files are public records that are required to be maintained and retained for administrative, legal and fiscal purposes.² Removal or destruction of data or files on government automation systems shall be conducted by authorized employees only, consistent with Guam law and policy.

The OAG reserves the right to monitor computer and e-mail usage, both as it occurs and in the form of account histories and their content. The OAG has the right to inspect any and all files stored in any areas of the network or on any types of computer storage media in order to assure compliance with this policy and Guam and federal laws. The OAG will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual computer and e-mail activities. The OAG also reserves the right to monitor electronic mail messages and their content. Employees must be aware that the electronic mail messages sent

² See Records Management Act, 5 GCA 20601-2-611, and Sunshine Reform Act of 1999, 5 GCA 10101-1-113.

and received using OAG equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by OAG officials at all times. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Government of Guam or OAG official.

The OAG has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. No employee may add software, computer programs or applications to the OAG automation systems. Only authorized employees are permitted to add or remove hardware, software, programs or applications to OAG automation systems. Violation of this policy can lead to disciplinary action, up to and including, dismissal.

Confidentiality of Electronic Mail

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable Guam and federal laws and Government of Guam rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message or material you send or receive could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of Office of the Attorney General policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others. Employees found to have engaged in such activities will be subject to disciplinary action, up to and including dismissal. System administrators and supervisors may access the electronic mail and computer systems of others to carry out official duties.

Message Tone for Electronic Mail

Users are expected to communicate with courtesy, professionalism, and restraint with both internal and external recipients. Electronic mail should reflect the professionalism of the OAG and should not include language that could be construed as profane, discriminatory, obscene, sexually harassing, threatening, or retaliatory.

It is recommended that using all capital letters, shorthand, idioms, unfamiliar acronyms, and slang be avoided when using electronic mail. These types of messages are difficult to read.

In addition, consistent email standards are herein implemented as follows:

1. Font – Times New Roman
2. Font Size – 12 point
3. Font Color – Black or Blue

4. No background or border
5. Chamorro and or English greetings or salutations are acceptable
6. Employee's Name as follows:
 - (First, Middle Initial, Last Name)
 - Title
 - Division
 - Office of the Attorney General
 - 590 S. Marine Corps Drive, Suite 706
 - Tamuning, GU 96913
 - Tel. (671) 475-3324 ext. _____
 - Fax (671) 477-_____
7. Add disclaimer: **CONFIDENTIALITY NOTICE:** This email and any files transmitted with it may be legally privileged and confidential and is intended solely for the use of the individual or entity named above. If you are not the intended recipient, you are hereby notified that any review, dissemination or copying of this email, or taking any action in reliance on the contents of this information is strictly prohibited. If you received this transmission in error, please notify us immediately by email or telephone to arrange for the return of this email and any files to us or to verify that it has been deleted from your system.

Electronic Mail Tampering

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for Internet/Network Browser(s)

This policy applies to all users of the Internet, but does not supersede any Guam or federal laws or Government of Guam or OAG policies regarding confidentiality, information dissemination, or standards of conduct. The use of OAG automation systems is for business purposes only. Brief and occasional personal use is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense to the OAG.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Examples of inappropriate use are defined below in the section entitled "Inappropriate Use of the Internet/Network." Managers or supervisors determine the appropriateness of the use and whether such use is excessive.

The Internet is to be used to further the OAG's mission, to provide effective service of the highest quality to the OAG's customers and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Network access are OAG resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating OAG computer and internet access policy, security policy, copyright, and licensing agreements.

All OAG policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, Government of Guam or OAG information dissemination, standards of conduct, misuse of Government of Guam or OAG resources, anti-harassment, and information and data security.

Violation of these policies and/or Guam and federal laws can lead to disciplinary action, up to and including, dismissal and possible criminal prosecution.

Inappropriate Use of the Internet/Network

Use of OAG computer, network, or Internet resources to access, view, transmit, archive, or distribute racist, pornographic, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Materials" is defined as any visual, textual, auditory item, file, page, graphic or other entity. Such material violates the OAG's anti-harassment policies and is subject to OAG disciplinary action, up to and including, dismissal.³

Users should refrain from seeking to gain unauthorized access to information resources through OAG property. No employee may use the OAG's Internet/Network facilities to deliberately propagate any virus, worm, Trojan Horse, trap-door program code, or other code or file designed to disrupt, disable, impair or otherwise harm either the Government of Guam's or the OAG's networks or systems or those of any other individual or entity. Examples of such tools are those that facilitate illegal copying of copy-protected software, unintended discovery of secret passwords, unauthorized decipherment of encrypted data, or unauthorized scanning of the OAG network or systems.

Sharing of network identities, such as user names, passwords, PIN codes, proximity card badges, is strictly prohibited. Use of OAG information resources for commercial or private use (e.g., printing flyers, invitations, etc.), is strictly prohibited.

The use of personal computers or personal equipment on OAG networks, to include hardline or WiFi (e.g., home laptop plugged in to OAG network), is strictly prohibited.

The OAG's Internet/Network facilities and computing resources must not be used to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of OAG resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution.

³ Investigation exception. Authorized employees engaged in official investigative work may be permitted to engage in activities involving government computers and automation systems that would otherwise be a violation of this policy or a violation of law. Authorization for use of government computers and automation systems for official investigation purposes may be approved on a case by case basis and shall include written authorization and documentation.

Internet/Network Security

The OAG Internet use is not confidential and no rights to privacy exist. The OAG reserves the right to monitor Internet/Network usage, both as it occurs and in the form of account histories and their content. The OAG has the right to inspect any and all files stored in private areas of the network or on any types of computer storage media in order to assure compliance with this policy and Guam and federal laws. The OAG will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities.

Existing rules, policies, and procedures governing the sharing of work-related or other confidential information also apply to the sharing of information via the Internet/Network. Please refer to the Confidentiality Guidelines and the OAG rules regarding the release of confidential information. The Government of Guam has taken the necessary actions to assure the safety and security of our network. Any employee who attempts to disable, defeat, or circumvent OAG security measures is subject to disciplinary action, up to and including, dismissal.

Exiting Government Service

When an employee leaves the OAG or government service, attention must be paid to the proper retention and storage of public records in the computer used by the former employee. Concurrent with the retention of public records of the former employee, the ability of a former employee to access computers and automation systems shall be revoked. Computers and automation systems shall be modified so that access codes and personal passwords of a former employee will be disabled.

In addition, the Information Technology (IT) Section, Administration Division, is required to inventory a departing (through resignation or retirement) employee's computer system to ensure all components that were received by the employee remain with the OAG, prior to the IT Administrator signing the clearance of the employee from government service.

Disposition of Hardware

Computers and other electronic data devices are to be disposed of only by designated employees assigned to the IT Section. It is the policy of the OAG to remove and destroy all data storage components from government computers and other electronic automation devices (e.g., printers, copiers, scanners, etc.) at the time the device is permanently removed from further service through equipment survey. After the required retention of public records contained in computers and other devices, authorized IT personnel are to remove and destroy, by either breakage or mutilation, every disk, tape, chip or other data storage component contained in hardware prior to that hardware being sent to the General Services Agency for disposition.

Enhancement of This Policy

This policy represents the **minimum** policy of the OAG concerning this subject. An authority, department, agency or instrumentality of the OAG may enhance this policy, consistent with the requirements of the Administrative Adjudication Law so long as this policy is not diminished, reduced or abolished in any manner.

User Compliance*

I understand and will abide by this **Office of the Attorney General of Guam Computer Usage Policy**. I understand that should I commit any violation of this policy, my access privileges may be revoked and disciplinary action up to and including dismissal and/or appropriate legal action may be taken.

I further understand that emails remain confidential and cannot be taken with me when I leave the OAG (e.g., retire, resign, terminated).

Employee Name (typed)

Date

Employee Title

Assigned Division

Employee Signature

***Original file to be maintained in the employee’s personnel jacket by Human Resources Section, and a copy maintained by IT Section, Administration Division.**