

**POLICY & PROCEDURES
GOVERNING COMPUTING
& TECHNOLOGY
RESOURCES**




**POLICY & PROCEDURES GOVERNING COMPUTING & TECHNOLOGY RESOURCES IN
THE JUDICIARY OF GUAM**

ADMINISTRATIVE POLICY #UJ 05-03

Adopted: June 16, 2005

MANAGEMENT INFORMATION SYSTEMS

Policy & Procedures Governing Computing & Technology Resources



JUDICIARY OF GUAM
Guam Judicial Center
120 West O'Brien Drive
Hagatna, Guam 96910

POLICY & PROCEDURES GOVERNING COMPUTING & TECHNOLOGY RESOURCES IN THE JUDICIARY OF GUAM

Judiciary computer systems are provided to employees in order to assist them in their work for the Judiciary of Guam. Policies governing all branch employees' use of judiciary computer systems are set forth here.

Privacy Expectations

In using judiciary-provided computer systems, employees should have no expectation of privacy. Employees' use of these systems may be monitored at any time to assure compliance with these or any other judiciary policies. Reports on computer system activity, including Internet communications, may be regularly reviewed to ensure that systems are functioning efficiently and that computer usage is work-related. Such reports might disclose for instance, the addresses of outgoing Internet e-mail, the senders of incoming Internet e-mail, and the addresses of Web sites that have been visited. Monitoring may require more detailed information if there is reason to believe that computer systems have been used inappropriately. Issuance of a password is not an indicator of personal privacy.

Responsibilities of Employees

In General

❖ Obey the law.

Use judiciary-provided computer systems only for legitimate, business-related purposes. Do not use judiciary-provided computer systems for any illegal activities. Because any electronic communication is subject to existing laws governing speech, you could violate the law by electronically communicating libelous or sexually harassing statements. You could also violate the law by using or reproducing copyrighted material found on the Internet without permission. You should not transmit information if any doubt exists regarding its copyright status or legality.

In addition to the criminal penalties that could result from the actions described in the preceding paragraph, violating these policies may be grounds for discipline up to, and including, termination of employment or imposition of penalties such as reprimands, restitution, suspensions and other adverse actions. The Judiciary may advise appropriate law enforcement authorities of known or suspected violations of any local or federal law or regulations and will cooperate with all legitimate criminal or disciplinary investigations.



POLICY & PROCEDURES GOVERNING COMPUTING & TECHNOLOGY RESOURCES IN THE JUDICIARY OF GUAM


- **Comply with judiciary policies.**

Adhere to existing judiciary personnel rules and regulations, Code of Conduct of Non-Judicial Employees, and other workplace policies and procedures. One such policy you are expected to comply with is the policy against sexual harassment.

Use good judgment, adhere to high ethical standards, and avoid situations that create an actual or potential conflict between your personal interests and the interests of the judiciary. Avoid both the fact and the appearance of a conflict of interest. If you are unsure as to whether a certain transaction or activity constitutes a violation of workplace policies, consult your immediate manager, supervisor or Human Resources for clarification.

- **Use computer systems for work.**

Do not use judiciary computer systems to conduct the business of for-profit or nonprofit organizations, to solicit funds, or to advance political, religious, or other ideological causes.



The judiciary computer systems are to be used for proper judicial purposes. However, this policy will not be construed to prohibit incidental and minimal use of judiciary resources, such as computer equipment, for non-work activities. Employees are expected to exercise good judgment and restraint in their personal use of the Internet and incidental and minimal use should not interfere with work. Incidental personal use must not:

- consume more than a trivial amount of judiciary resources;
- disrupt the operation of the judiciary's computer network; or,
- preempt or impede any judiciary business or activity

Management reserves the right to prohibit any personal use of computer resources and to block computers or individuals from Internet access.

Prohibited Internet Uses.

- A. Material accessed on the Internet or sent from the judiciary on Internet E-mail that can in any way be seen as insulting, disruptive, offensive, or harmful to morale by another person is prohibited. Examples of forbidden transmissions include: sexually explicit messages and pictures, and messages that can be construed to be harassment or a disparagement.
- B. Possession or distribution of child pornography is a federal crime. Anyone caught with child pornography on a judiciary computer may be prosecuted. The judiciary does not

POLICY & PROCEDURES GOVERNING COMPUTING & TECHNOLOGY RESOURCES IN THE JUDICIARY OF GUAM

recognize any legitimate reason for the use of any variety of pornography on the judiciary's computer system. Intentionally accessing any pornographic site or transmitting pornographic material through e-mail is an abuse of judiciary resources that must be reported to the Administrator of the Court.

- C. Intentionally accessing, transmitting, storing, or distributing offensive material (e.g. racist literature, material, or symbols) is a prohibited Internet use. Participating in "chat room" or "instant messaging" discussions that are not for official judiciary business is a prohibited Internet use. Accessing "hacker" sites and downloading hacking tools is a prohibited Internet use unless specific authorization has been granted. Lobbying or advocacy on behalf of any political organization or religious group is a prohibited Internet use.
- D. Viewing, damaging, deleting, or interfering with the functioning of any judiciary system or any other person's files or communications is prohibited.
- E. Attempting to circumvent or disable any Internet security or auditing system is prohibited. This prohibition includes disabling virus detection mechanisms. Modifying or altering the operating system of the hardware used to connect to the Internet is prohibited.

- **Exercise reasonable care in using computer systems.**

You are responsible for any damage attributable to your failure to comply with these policies.

You will be personally responsible for the repair and/or replacement costs of any judiciary property that is lost, stolen or damaged because of your negligence or your failure to comply with these policies. This includes damage caused to the judiciary's computer system by downloading viruses or other malicious, incompatible or damaging programs.

Because operational efficiency is vitally critical to business operations, avoid any usage, such as sending or downloading large image or sound files that degrade or impair the performance of computer systems. Restrictions are subject to definition by management but employees should not download, install, store or use software from the Internet in violation of any patent, copyright, or license agreement

A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet

program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.

An e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk or log your keystrokes for hackers to gain access to your passwords, pin numbers or account numbers). Trojan horses have no way to replicate automatically.

Blindly downloading files from the Internet is a sure way to fall victim to a virus, worm or Trojan horse. Program files or other executable files may contain a virus, worm or Trojan horse program that could cause irreparable damage to software or data. Users should always exercise extreme care before opening any attachment to an e-mail, even if the e-mail is from a known source, because some malicious programs attach themselves to e-mails without the sender's knowledge. Some programs after infecting your computer send e-mails containing the virus, worm, or Trojan horse without the user's knowledge by infiltrating the sender's address book.

If you have any questions, contact your manager or supervisor.

Confidentiality and Access

- **Safeguard confidential information.**

Provide access to judiciary systems or information only if your work requires you to do so. Adhere to the judiciary's confidentiality guidelines, as set forth in the Code of Conduct for Non-Judicial Employees. You may make statements regarding judiciary practices or policies only if you are authorized to do so. You may share information regarding pending judiciary matters only if your work requires it.

Disseminate information only if you have verified its accuracy.

Since any e-mail that originates from a judiciary address may be given undeserved credibility, you must exercise caution in sending e-mail. For example, you should not forward e-mail containing warnings or rumors unless you have verified that the information originates from a reliable source and that the information is accurate.

Avoid using e-mail to send confidential or attorney-client information to other than judiciary employees.

If you must use e-mail to send confidential or attorney-client information to other than judiciary employees, observe the following procedures. Mark the e-mail as confidential, either in the subject line or in the body of the message. Do not forward or otherwise disseminate any information contained in an e-mail marked as confidential without the permission of the author of the message. Compose the message in Microsoft Word or WordPerfect, password-protect the document, and then include it as an attachment to your e-mail message. Inform the recipient by voice as to the document's password.

- **Access only those computer systems or files for which you have authorization.**

You may access only those computer files, including electronic mail, to which you normally have access. You may not access another employee's computer system or files unless your work requires you to.

Management may access your files for any reason and may require that you provide logins or passwords for such access.

- **Identify yourself appropriately.**

Addresses that you use for Internet e-mail or any other computer function should identify you as clearly as possible. Use of pseudonyms or personal aliases is prohibited. Use of another person's name or e-mail address is prohibited.

Software and Licenses

- **Comply with software licenses.**

The judiciary observes the terms of software licenses to which it is a party.

Copying provided software is permitted only within license terms. Questions about licenses should be directed to the Management Information Systems Administrator. Using illegally copied software, regardless of who has provided it, is prohibited.

- **Use standard hardware and software.**

Personal computer hardware and software are standard if your employer provides and supports them. Consult the Management Information Systems support staff before undertaking any modification or customization of standard hardware or software. Questions about the hardware or software covered by this term should be referred to Management Information Systems support staff.

Installing or downloading any software or files (including screen savers, wall papers and games) onto the judiciary's computer systems or network without the prior consent of management. Such software and files must have a direct business use, must be properly licensed and registered, and must be used in conformity with copyright laws and licensing agreements.

If management provides written approval of your use of nonstandard software, you are responsible for checking the software for viruses and contacting the Management Information Systems support staff to see that the software's data files are backed up to a network drive. Use approved virus detection software to check any software from outside sources, such as a personal computer at home, the Internet, or an external network. Management Information Systems support staff will provide training in the use of such software. You will be responsible for any loss of data that occurs because of a failure to comply with this policy. No backup is provided for non-standard software unless you or your manager or supervisor has arranged for network backup of the data files. No training or support is provided for nonstandard software.

- **Computer Management Procedures.**

Network

User Id: Existing judiciary employees with network accessibility will be required to obtain a new user id, upon notification from the M.I.S. Administrator.
(See example 1)

After notification from the M.I.S. Administrator, a request for a new user id must be completed by the employee and have the approval of the immediate supervisor or division head.

User id's will reflect the first character of their first name and utilize the full last name.
(See example 1)

Employees with the same first character and the same last name, your first character of your middle name will be added to your user id.
(See example 2)

An employee will not be permitted to request to reset or provide a new password for another employee unless authorized by the supervisor or division head. Passwords will only be given strictly to the rightful owner of the user id. If a user receives a temporary password, the user shall change the password immediately after logging into the network.

Supervisors, acting supervisors or division heads requesting to reset an employee's user id may contact the Management Information Systems Office by telephone or by completing a *Service Request Form*.

No ink stamp signature will be permitted.

Example 1.

<i>Employee's Full Name</i>	<i>Network User Id</i>
Jane Michelle Doe	jdoe
Michael Beckan Doe	mdoe

Example 2.

<i>Employee's Full Name</i>	<i>Network User Id</i>
Jane A. Doe	jadoe
John B. Doe	jbdoe
Jess R. Doe	jrdoe

Folder Access:

Division or department directories will be created in the server. Under each division, personnel folders that reflect your user id will be created and activated.

Each employee's folder is private and shall be accessed only by the authorized users. Users requesting access to any folder in the server that he/she does not otherwise have authority to access must obtain the approval of the employee whose folder is being accessed and the user's immediate supervisor or division head.

Supervisors, Acting Supervisors or Division Heads and employees allowing access to another employee must complete and sign the *Folder Access Request Form*.

Folder access must be explained in the request box.
(See example 3)

No ink stamp signature will be permitted.

Example 3

*Jane Doe to have access to John Doe's folder **or** Jane Doe to have access to John Doe's folder for only 2 days, starting today*

AS400

User ID & Employees with existing AS400 access will keep their current user id.

Access:

A request for an AS400 user id must be completed by the employee and have the approval of the immediate supervisor or division head.

Supervisors, acting supervisors or division heads who request to mirror a user id to another user id for an employee must provide both employee's user id's in the request box. With this option, the user will lose all existing programs and options to the mirrored user id and reflect new programs and options.

(See example 4)

Supervisors, acting supervisors or division heads requesting for additional programs or options to an employee's user id must attach a print screen copy of the requested program to the request form. With this option, your existing user id programs and options are not deleted but new programs and options are added.

(See Example 5)

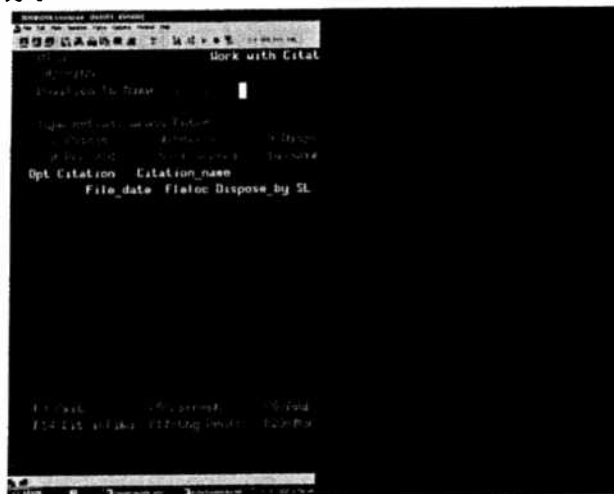
Supervisors, acting supervisors or division heads are the only allowed personnel to request any modification on an employee's user id. Supervisors, acting supervisors or division heads must fill out the signature section at the end of the form.

No ink stamp signature will be permitted.

Example 4

**CSM400 to mirror CSM200
Copy all of PRO210 to PRO12**

Example 5



POLICY & PROCEDURES GOVERNING COMPUTING & TECHNOLOGY RESOURCES IN THE JUDICIARY OF GUAM

Reports: Justices, judges, supervisors, acting supervisors, division heads and authorized employees are the only allowed personnel to request any report.

Justices, judges, supervisors, acting supervisors, division heads may provide a list of authorized employees to query limited access AS400 reports.

Supervisors, acting supervisors or division heads are responsible to attach a list together with the request form of authorized employees to the Management Information Systems Administrator.

Supervisors, acting supervisors or division heads are responsible to update, modify or delete authorized employees from their list.

Justices, judges, supervisors, acting supervisors, division heads and authorized employees requesting for reports must provide specific and detailed information to query in the request box.

No ink stamp signature will be permitted.

E-mail: Existing judiciary employees with e-mail id's will be changed to reflect their network user id.
(See example 6)

Request for a new e-mail user id, employees must fill out the information at the end of the form and have the approval of the immediate supervisor or division head.

No ink stamp signature will be permitted.

Example 6.

<i>Employee's Full Name</i>	<i>E-mail User Id</i>
Jane Michelle Doe	jdoe@guamcourts.com
Michael Beckan Doe	mdoe@guamcourts.com

Work Request: Divisions requesting to transfer CPU's, monitors, battery back-ups, printers, or other computer related hardware to another division, office, section, or employee's desk or cubicle must have approval by the immediate supervisor or division head. Transfer of property must be explained in the request box.

(See example 7)

Before any request of the removal or disposal of CPU's, monitors, battery back-ups, printers, or other computer related hardware, a transfer of property form must be filled out first provided by the Procurement and Maintenance Office.

Any computer books or software found within their division, office or section to be disposed of must contact the Management Information Office for review before disposal. There will be no placing or dropping of computer books or software at the front door of the Management Information Systems Office.

Responsibilities of Management

- **Inform employees about their responsibilities under these policies.**

Inform new employees of these policies immediately.

Remind all employees on a periodic basis about their responsibilities under these policies.

- **Authorize appropriate access to computer system resources.**

Determine and enforce the appropriate level of access to judiciary computer systems by employees or consultants under your supervision. Use the standard form for authorization, a copy of which is available from Human Resources. Notify computer support staff immediately when an employee's system access rights have been withdrawn. Security considerations or expenses require additional authorization to access some systems, such as the Human Resources system or the Fiscal system, and some services, such as Lexis and Westlaw.

Once the policy is implemented, training sessions are recommended to raise employees' awareness of the rules and to educate them on the risks of inappropriate use. Too many employees are simply unaware that a seemingly harmless joke sent by e-mail could lead to legal proceedings against the judiciary, or in some cases, the individual. As a means of reinforcing the policy principles, particularly after an incident of misuse, the judiciary should send periodic reminders to all employees regarding appropriate usage.



POLICY & PROCEDURES GOVERNING COMPUTING & TECHNOLOGY RESOURCES IN THE JUDICIARY OF GUAM

- **Report any violations of these policies.**

Notify your computer support staff and your supervisor immediately concerning possible security breaches and investigate any suspected misuse of computer systems. If technical assistance is required to investigate possible misuse, request it of your computer support staff.



AUTHORIZATION & ACKNOWLEDGEMENT FORM

I have read and reviewed the Policy & Procedures Governing Computing & Technology Resources in the Judiciary of Guam and consent to be bound by the terms and provisions set forth.

To be completed by the user:

Name: _____
First, Middle, Last

Division: _____ Start Date: _____

Signature: _____ Date: _____

To be completed by user's immediate supervisor:

Name: _____
First, Middle, Last

Signature: _____ Date: _____

To be completed by Administrator of the Court (If necessary):

Name: _____
First, Middle, Last

Signature: _____ Date: _____

Approved: Disapproved:

Management Information Systems Official Use Only

Assigned To _____ MIS Administrator _____

Completed Date _____ Date Enabled _____

SERVICE REQUEST FORM

To be completed by the user:

Name: _____
First, Middle, Last

Division: _____ Deadline: _____

Signature: _____ Date of Request: _____

DESCRIPTION:

Management Information Systems Official Use Only

Assigned To

MIS Administrator

Date Completed

FOLDER ACCESS REQUEST FORM

To be completed by the user:

Name: _____
First, Middle, Last

Division: _____

From _____ to _____
Effective Date Expiration Date

For the purpose of: _____

Signature: _____ Date of Request: _____

To be completed by immediate supervisor:

Name: _____
First, Middle, Last

Signature: _____ Date: _____

Approved: Disapproved:

Management Information Systems Official Use Only

Assigned To _____ MIS Administrator

Effective Date _____ Expiration Date



..

