


**JUDICIARY OF GUAM  
POLICY AND PROCEDURES  
ADMINISTRATIVE POLICY NO. UJ20-02**

  <b>Judiciary of Guam</b>	Division:  <b>ADMINISTRATIVE OFFICE OF THE COURTS</b>
<b>TITLE: LAPTOP AND MOBILE DEVICE INTERIM POLICY AND PROCEDURES</b>	EFFECTIVE DATE: <i>5/6/2020</i>
REVISED DATE:	APPROVED BY: <i>Kristina L. Baird</i> Kristina L. Baird, Administrator of the Courts

**A. PURPOSE**

The purpose of this Laptop and Mobile Device Interim Policy (“Interim Policy”) is to establish guidelines for the appropriate use of Judiciary of Guam (“Judiciary”) owned laptops and mobile devices, and non-Judiciary owned computing (e.g., laptops, tablets, etc.) and mobile devices – i.e., personally owned computing and mobile devices if such personally owned computing and mobile devices are used for work that is performed remotely and/or which accesses the Judiciary network -- by Judiciary employees, consultants and contractors. This Interim Policy is necessary to preserve the integrity, confidentiality and availability of information.

This Interim Policy has been developed to address the exigent circumstances created by the COVID 19/Coronavirus situation, including the emergency state of the island, lockdown and modified/limited work and operational status of the Judiciary. This Interim Policy is intended to be consistent with and to supplement currently existing and implemented policies established by the Management Information Systems (MIS) Division of the Judiciary.

**B. APPLICATION**

This Interim Policy applies to all Judiciary employees, consultants and contractors who utilize Judiciary owned laptops and mobile devices, and non-Judiciary owned computing and mobile devices, for work that is performed remotely and/or which accesses the Judiciary network.

**C. POLICY GUIDELINES AND GENERAL RESPONSIBILITIES**

**1. USE**

The use of Judiciary owned laptops and mobile devices is for authorized purposes only.

**2. PROHIBITED USE**

**a. General Prohibition of Use**

The following activities are prohibited on any Judiciary owned laptop and mobile device:

- Gambling.
- Visiting and downloading material from pornographic websites.
- Lobbying the legislature or any government agency.
- Campaigning or other political activity.
- Online stock trading activities.
- Online real estate activities except as required and authorized as part of one's official duties pursuant to Judiciary policies and applicable Guam and federal rules, regulations and/or laws.
- Online activities that relate to any type of outside work or commercial activity, including any trading.
- Endorsements of any products, services, or organizations.
- Fundraising for external organizations or purposes.
- Any type of continuous audio or video streaming from commercial, private, news, or financial organizations except as required and authorized as part of one's official duties pursuant to Judiciary policies and applicable Guam and federal rules, regulations and/or laws.
- Any activity that would constitute a violation of any Guam and/or federal rules, regulations or laws.

#### **b. Forwarding of Email**

The Judiciary issues e-mail accounts and disk storage to all Judiciary employees, and authorized and approved consultants and contractors. Unless approved by the Chief Justice of the Supreme Court of Guam or the Administrator of the Courts, Judiciary employees, consultants and contractors must not forward e-mail from their Judiciary e-mail address to a different e-mail address, such as one obtained from an external Internet Service Provider (e.g., AOL, Gmail, Hotmail, etc.). The Judiciary has no control over the delivery of e-mail that has been forwarded outside of the Judiciary domain to external providers.

### **3. PASSWORDS**

The Judiciary makes every effort to secure its computer systems, networked resources, and e-mail accounts, but cannot guarantee the infallibility of these systems to unauthorized intrusion, or the authenticity of the sender of an electronic communication. To mitigate unauthorized access, Judiciary employees, consultants and contractors must ensure their accounts and devices are password protected in compliance with **Administrative Policy No. UJ20-03 (MIS-005-Password Management Policy)**.

Judiciary employees, consultants and contractors are responsible for keeping their Judiciary e-mail passwords confidential, and should never share this information or access to the Judiciary network and information resources with others including family members and friends.

### **4. OWNERSHIP, RIGHT TO MONITOR, AND RIGHT OF INSPECTION**

The Judiciary owns the rights to all data and files in any laptop, network or other information system owned by the Judiciary, and to all data and files sent or received using any Judiciary owned laptop, network or information system.

The Judiciary reserves the right to monitor e-mail messages and their content, as well as all use by Judiciary employees, consultants and contractors of the internet and of computer equipment used to create, view or access e-mail and internet content. Judiciary employees, consultants and contractors must be aware that the e-mail messages sent and received using Judiciary owned equipment or Judiciary provided internet access are subject to viewing, downloading, inspection, release and archiving by authorized Judiciary officials, as designated by the Chief Justice of the Supreme Court of Guam or the Administrator of the Courts.

The Judiciary has the right to inspect all files stored in any area of the Judiciary network, individual computers, or storage media in order to ensure compliance with Judiciary policies and Guam and federal rules, regulations and laws. Accordingly, employees, consultants and contractors should assume that whatever they do, type, enter, send, receive and view on Judiciary owned equipment or electronic information systems is electronically stored and subject to inspection, monitoring, evaluation and use by the Judiciary at any time.

**D. PROCEDURE FOR ASSIGNMENT, AUTHORIZATION AND APPROVAL  
PROCESS RE: JUDICIARY OWNED LAPTOP OR MOBILE DEVICE**

1. The Procurement Administrator will assign, authorize and approve the Judiciary owned laptop or mobile device to the Division Manager. A Division Manager may be assigned, authorized and approved more than one laptop or mobile device depending on the needs of the division and the availability of devices.
2. The Division Manager will assign, authorize and approve the Judiciary owned laptop or mobile device to his/her division employee, consultant or contractor.
3. The Division Manager is required to complete the appropriate request form indicating the Judiciary owned laptop or mobile device requested and the employee, consultant or contractor to whom the device will be assigned.
4. Prior to the assignment of a Judiciary owned laptop or mobile device to a Division Manager, the device will be configured by the MIS Division to comply with established laptop or mobile device security requirements.
5. Following assignment to the Division Manager and division employee, consultant or contractor, the Division Manager and division employee, consultant or contractor are prohibited from changing the security configuration on the laptop or mobile device.
6. Judiciary work product, documentation, communications and all other official information must be shared, stored and/or disseminated using the Judiciary Google account, i.e., the Judiciary e-mail address and associated Google drive, and/or via the hard drive of the assigned Judiciary owned laptop or mobile device.
7. Judiciary employees, consultants and contractors remotely accessing the Judiciary network are required to use Judiciary owned laptops and mobile devices.
8. The Judiciary employee, consultant or contractor is authorized to take the Judiciary owned laptop or mobile device to his/her home and/or for his/her remote use, on weekdays and weekends, including after working hours, in order to ensure its availability in the event a

disaster or crisis occurs affecting the Judiciary's operations. Employees, consultants or contractors assigned a Judiciary owned laptop or mobile device are required to securely transport the laptop or mobile device to his/her home and/or for remote use on weekdays and weekends, including after working hours, in order to ensure the availability in the event of a disaster or crisis affecting the Judiciary's operations.

9. Each employee, consultant or contractor assigned a Judiciary owned laptop or mobile device must acknowledge his/her understanding that in the event of a disaster or crisis, the laptop or mobile device may be reclaimed by the Procurement Administrator or the Administrator of the Courts for deployment to another Judiciary employee, consultant or contractor.

10. If the Judiciary employee, consultant or contractor assigned a laptop or mobile device terminates his/her employment or contractual relationship for any reason, it is the responsibility of the Division Manager of the division employee, consultant or contractor, or higher official of the Division Manager, whichever situation is applicable, to reasonably ensure the return of the laptop or mobile device to the Procurement Administrator.

11. If the terminated Judiciary employee, consultant or contractor, or Division Manager, whichever situation is applicable, refuses to return the laptop or mobile device upon termination, law enforcement will be contacted and a complaint for theft will be made by the Judiciary.

12. If any Judiciary owned laptop or mobile device is lost, stolen or damaged, as set forth in **Administrative Policy No. 001-92 - Loss, Damage or Theft of Court-Issued Property**, the employee, contractor or consultant must immediately report the incident in writing to the Division Manager or higher official of the Division Manager, whichever situation is applicable. The Division Manager or higher official of the Division Manager, whichever situation is applicable, must immediately report the incident in writing to the Procurement Administrator. The procedure found in **Administrative Policy No. 001-92** must be followed.

#### **E. PROCEDURE FOR ASSIGNMENT, AUTHORIZATION AND APPROVAL PROCESS RE: NON-JUDICIARY OWNED LAPTOP OR MOBILE DEVICE**

1. The use of non-Judiciary owned computing (e.g., laptops, tablets, etc.) and mobile devices to access the Judiciary network is prohibited unless authorized for use for official work by the MIS Division.

2. All non-Judiciary owned computing and mobile devices authorized for use for official work must be protected with a password required at the time the device is powered on. The password must meet the requirements of and comply with **Administrative Policy No. UJ20-03 (MIS-005-Password Management Policy)**.

3. All non-Judiciary owned computing and mobile devices must have active up-to-date anti-virus and anti-malware protection. The MIS Division will assess this device security requirement.

4. Judiciary work product, documentation, communications and/or all other official information must be shared, stored and/or disseminated using the Judiciary Google account, i.e., the Judiciary e-mail address and associated Google drive.

5. No Judiciary work product, documentation, communications and/or all other official information are to be stored on non-Judiciary owned computing and mobile devices -- i.e., personally owned mobile and computing devices, or on external or removable devices (e.g., DVDs, CDs, thumb drives, external storage devices, etc.).

6. MIS instructions on how to use the Judiciary Google account, i.e., the Judiciary e-mail address and associated Google drive, are provided in Appendix A.

7. For assistance, please contact:

MIS Division  
Judiciary of Guam  
671-472-9710 (office phone)  
671-787-9101 (cell phone)  
[jmannion@guamcourts.org](mailto:jmannion@guamcourts.org) (email address)

## **F. VIOLATIONS**

Any Judiciary employee, consultant or contractor found to have violated this Interim Policy may be subject to disciplinary action, up to and including termination.

## **G. REFERENCES**

1. Administrative Policy No. 001-92 - Loss, Damage or Theft of Court-Issued Property
2. Administrative Policy No. UJ 05-03 - Policy and Procedures Governing Computing and Technology Resources
3. MIS Policy No. 002 - Workstation Use Policy
4. MIS Policy No. 003 - Workstation Security Policy
5. MIS Policy No. 0014 - Email Policy

## **APPENDIX A: MIS Instructions to Access Google Drive**

Login to Judiciary of Guam e-mail account in Chrome browser  
Find Google apps grid on top right of browser window  
Click on grid  
Click on Drive icon (green/yellow/blue triangle)  
Your Google drive will open

### **To upload a file:**

Click on My Drive  
Click Upload on drop down menu  
Select file from local hard drive folder  
Click open  
To find file click on Recent on left side menu

### **To download a file:**

Right click on file to download in your Google Drive  
Select Download  
File will download to the Downloads folder on your local hard drive