PORT OF GUAM
ATURIDAT I PUETTON GUAHAN
Jose D. Leon Guerrero Commercial Port
1026 Cabras Highway, Suite 201, Piti, Guam 96915
Telephone: 671-477-5931/5 | Facsimile: 671-477-2689
Website: www.portofguam.com

Lourdes A. Leon Guerrero
Governor of Guam
Joshua F. Tenorio
Lieutenant Governor

POLICY MEMORANDUM NO. 2019-GM08

To: All Employees	Subject: **Policy on the Use of Issued Computers, Laptop, Digital Equipment (i.e.: printer, scanner, camera, projector, phones, tablet, etc.), Internet Access, VPN Access and E-mail Services**
Effective Date: December 2, 2019	Revision Date: September 12, 2024
Approved by: RORY J. RESPICIO, General Manager	

I. POLICY

A. The Port Authority of Guam (PAG) provides its employees (users) with computers, laptop, digital equipment, internet access, Virtual Private Network (VPN) access and e-mail services as required for the performance and fulfillment of their job responsibilities. This is the responsibility of the Information Technology Division (IT).

B. PAG users must understand that the issuance of computers, digital equipment, internet access and e-mail is for the purpose of increasing productivity and not for non-PAG/Government of Guam (GovGuam) activities. Users must also understand that any computer log-in and/or connection to the network and the internet provides an opportunity for non-authorized users to view or access PAG corporate information. All issued equipment must be handled and access by authorized users only. All connections must be secured, controlled, monitored and logged off of all devices when leaving the work area.

C. PAG users have no expectations of privacy while using government of Guam-owned or leased equipment. Information passing through or stored on GovGuam equipment can and will be monitored. Users should also understand that management and IT maintains the right to conduct periodic audits of PAG computers, digital equipment, internet access and e-mail communication usage to ensure compliance with the policy.

D. Users accessing PAG N4 & JDE databases must also conform to the Data Access and Data Security policy. (See Policy Memorandum No. 2019-GM07)

II. PERMITTED USE

A. PAG issued computers, laptop, digital equipment, internet connection, VPN access and e-mail systems are primarily for business use. Occasional and reasonable use is permitted, provided that this does not interfere with the performance of work duties and responsibilities.

B. Users may use PAG issued computers, laptop, digital equipment, VPN access and internet services for personal improvement or outside of scheduled hours of work, provided that such use is consistent with professional conduct and is not for personal financial gain.

C. Authorized PAG users may send and receive e-mail attachments that do not exceed 10 megabytes in size, provided that all attachments are scanned before they are opened by PAG anti-virus software.

D. Authorized PAG users may send and receive occasional personal e-mail messages, provided that this does not interfere with the performance of work duties and responsibilities. Personal e-mail must be forwarded to the employee's personal e-mail account and viewed outside of working hours.

III. PROHIBITED USE

A. Users with PAG issued computers, laptop and digital equipment are prohibited from doing the following activities:

1. Vandalize, damage, or obvious misuse of the issued equipment.
2. Install privately owned software without permission.
3. Violate copyright or use illegal and impermissible software.
4. Play games, watch movies or for any other non-GovGuam purpose.
5. Create, view, store data or software that is disrespectful, offensive, and hateful or suggest violence towards any person, sex ethnic group or race.
6. Attempt to hack, defeat or circumvent any security measures, controls, accounts, or record-keeping systems.
7. Use the systems for unauthorized access and/or personal gain. This will cover any/all abuses as determined by Management/IT upon infraction.
8. Intentionally alter, misappropriate, dismantle, disfigure, disable, or destroy any computing information and/or services owned by the Port.
9. Use the equipment for unlawful purposes including fraudulent, threatening, defamatory, harassing, or obscene display.
10. Use the equipment to invade the privacy rights of anyone.

B. Utilize PAG internet access and e-mail services to download, save, receive or send any material or messages in the following categories:

1. Offensive content of any kind, including pornographic material.
2. Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion or disability.
3. Threatening or violent behavior.
4. Illegal activities.
5. Commercial messages.
6. Gambling.
7. Personal financial gain.
8. Forwarding e-mail chain letters.
9. Spamming e-mail accounts from PAG e-mail services or GovGuam machines/devices (to include all types of computers).
10. Material protected under copyright laws.
11. Sending business sensitive information by e-mail or over the internet without authorization.
12. Dispersing corporate data to PAG customers or clients without authorization.
13. Opening files received from Internet without performing a virus scan.
14. Tampering with PAG computer identification (handle) in order to misrepresent you and the entity to others.

IV. RESPONSIBILITIES

A. PAG authorized users of computers, laptop, digital equipment, internet. VPN access and e-mail shall:

1. Respect and abide by the user policies of networks accessed through PAG issued computers, internet and e-mail services.
2. Abide by existing federal, state, and local telecommunication and networking laws and regulations.
3. Abide by the copyright laws regarding protected commercial software or intellectual property.
4. Seek to endeavor to minimize unnecessary network traffic that may interfere with the ability of others to make effective use of PAG network resources.
5. Not overload networks with excessive data or otherwise limit PAG's use of these technical resources.
6. Do not attempt to open or fix computers and digital equipment if you are not qualified and authorized.
7. Treat your equipment with care and clean it occasionally to maintain a working performance.
8. Obtain permission if you will connect privately owned digital equipment, such as scanner, printers and external storage devices.

9. Refrain from plugging un-related appliances on Uninterruptible Power Supply (UPS) dedicated for PAG computers and digital equipment.
10. Return all PAG issued/assigned equipment listed on the signed Property Receipt form to the IT office when clearing via Human Resources (HR) Employee Separation Clearance process.
11. PAG employees are required to sign an acknowledgement receipt that they have received a signed copy and read the policy. A copy of the signed receipt will be retained in the IT division records and Human Resources personnel employee jacket.

B. **PAG Laptop Physical & Data Security:** Each employee provided with a laptop by PAG is responsible for the physical & data security of the laptop. All laptops acquired for or on behalf of PAG are deemed to be company property and must adhere to the following:

1. When not in use, the laptop must be locked with a password and caution taken when entering any user-id and passwords on the laptop.
2. Store the laptop in a safe environment when not in use.
3. Do not leave your laptop in your vehicle. If it is necessary to leave the laptop in your vehicle for a very short period of time, the laptop must be locked in the trunk of the vehicle.
4. When using the laptop in public areas, do not leave the laptop unattended for any length of time.
5. Employee will be responsible for maintaining the confidentiality of any data stored or access on this laptop. In the event of loss or theft, please inform Port Police and PAG-IT right away.
6. If the laptop is lost, damaged or stolen, employees will be responsible for its replacement.
7. External VPN access is permitted but limited to certain users with approval of the Division Manager.

During travel:

1. Do not pack your laptop in checked luggage.
2. Attach a name tag or business card to your laptop to easily identify it during security checks or if lost.
3. Store the laptop in a hotel room safe or locked suitcase when you are not in the room.
4. If the laptop is lost, damaged or stolen, employees will be responsible for its replacement
5. PAG-IT will provide a temporary admin password. However, this access is used for emergency purposes only and should not be used as a typical user-id. Admin password will be disabled upon return of the user.

C. **PAG VPN (Virtual Private Network) Security:** Approved users provided with VPN access must adhere to following:

1. It is the responsibility of the employee with VPN privilege to ensure that unauthorized users are not allowed access to the PAG network.
2. Approved PAG Employees may utilize the benefits of a VPN, which is a "user-managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing the required software.
3. Only traffic destined for PAG networks will travel across the VPN tunnel.
4. VPN users should disconnect right after each use.
5. Users will be responsible for the safety, confidentiality and security of their VPN credentials.

V. ENTIRE POLICY

All prior policies or memoranda in conflict with this policy are hereby rescinded.

VI. VIOLATIONS

A. Violations will be reviewed on a case-by-case basis.

B. If it is determined that a user has violated one or more of the above guidelines, appropriate disciplinary action will be taken by the division head/supervisory levels and ends ultimately at the General Manager.

C. Depending on the severity of the abuse, the General Manager may forfeiture the user's computers, digital equipment, internet and e-mail privileges.

D. If a breach of PAG system security is determined, all data access and e-mail privileges will be suspended pending final decision by the General Manager.

E. In the event of damages incurred, the General Manager may have the user reimburse the Port for repair costs of the equipment.

F. HR Employee Separation Clearance forms will not be approved by IT if all PAG issued/assigned equipment is not returned and inventoried.