

**PORT OF GUAM**

ATURIDAT / PUETTON GUAHAN

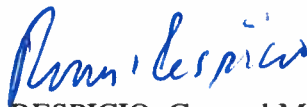
Jose D. Leon Guerrero Commercial Port

1026 Cabras Highway, Suite 201, Piti, Guam 96925

Telephone: 671-477-5931/35 Facsimile: 671-477-2689/4445

Website: www.portguam.com

Lourdes A. Leon Guerrero
Governor of GuamJoshua F. Tenorio
Lieutenant Governor**POLICY MEMORANDUM NO. 2023-GM02**

To: IT & Crane Maintenance Employees	Subject: Crane Diagnostic PC/Laptop Usage Policy
Effective Date: November 20, 2023	Revision Date:
Approved by:  RORY J. RESPICIO, General Manager	

I. INTRODUCTION

The Port Authority of Guam (PAG) maintains and diagnoses its Cranes using a Port issued laptop and/or Desktop PC, connecting remotely via Cat-5 hardline at the base of the crane, and PC via wireless bridge connection. These clients are isolated from the Port's corporate network and does not have internet connectivity.

These assets are managed, protected, secured and controlled by PAG's Information Technology (IT) & Crane Maintenance divisions.

II. PURPOSE

This policy is aimed to secure and protect PAG Cranes and their controllers from any Cyber-Security attack and/or IT related threat actors, which include but are not limited to the following.

- a. PAG's Cranes are protected from any Cyber-Attacks coming from the connecting Desktop PC's and laptop.
- b. PAG's Cranes are protected from any Cyber-Attacks coming from any misuse and/or mishandling of the PC & Laptop.
- c. PAG's Cranes are protected from any Cyber-Attacks by keeping its Operating System (OS), software & anti-virus up-to-date.
PAG's Cranes are protected from any Cyber-Attacks by keeping the equipment physically secured when not in use.

This policy also addresses the issue of the rights and responsibilities of authorized persons in the handling, security, and protection of Port Cranes. The objective of this policy is to ensure that the PC & Laptop clients are secured while restricting access to authorized users.

III. SCOPE

This policy covers all laptops and PCs connecting to the Cranes controllers.

IV. POLICY

Usage of Desktop PC & Laptop

- Users of the equipment must sign and adhere to Policy Memorandum No. 2019-GM08 (Policy on the Use of Issued Computer digital equipment (i.e.: printer, scanner, camera, projector, phones etc.), Internet Access and E-mail Services).
- User(s) of the laptop must be an employee of PAG only, if a third party must use it, a port employee must accompany and monitor its usage at all times.
- Desktop & laptop must ONLY be used for the sole purpose of diagnosing the crane.
- Desktop & PC must never be connected to the corporate network. If remote troubleshooting from off-island vendor is needed, connection to the corporate network can be scheduled with IT for proper port opening and configuration. **REMINDER: It is very important to have the PC/laptop disconnected from the corporate network as soon as the troubleshooting is completed.**
- Never connect a USB & peripherals coming from any unknown source. When in doubt, contact IT.
- The laptop must ONLY be used for the sole purpose of connecting to the crane.
- The laptop must not be used, loan or taken outside of the Port.
- Always log-off and shutdown the PC/laptop when not in use. Laptop must be secured in a locked office when not in use.
- The user must inform IT of any suspicious activity that may arise while using the system.

Access Guidelines

- Employees requesting access to the diagnostic system, must fill-out a request form and sign all the usage and access policies provided by IT.
- IT will provide a user-id and 8-10 character password with number, symbol and uppercase.
- IT must secure the administrator-id, by creating a 16+ password with number, symbol and uppercase.

Updates and Anti-virus

- IT must install Anti-virus on all crane diagnostic systems.
- Laptop must be returned to IT every 6 months to run updates on OS, Anti-virus and complete scan.

Privacy

- All authorized users must be cognizant of the access they have been provided, and their responsibility to maintain the integrity of the system. Effective security is not possible without the cooperation of users who understand the reasons for security and comply with established security measures.
- All authorized PAG users must secure their username, account, password, and system access from unauthorized use.

V. VIOLATIONS

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/supervisor with cause for submittal to the General Manager for final disposition.

Any User in violation of this Policy will have all access and privileges suspended pending a complete internal review.