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-GM07

To: **All Employees**	Subject: **Data Access and Data Security Policy**
Effective Date: December 2, 2019	Revision Date: February 3, 2026
Approved by: RORY J. RESPICIO, General Manager	

Policy reflects transition changes from AS400 to Oracle JD Edwards EnterpriseOne (E1), including updated systems, processes, and protocols.

I. INTRODUCTION

The Port Authority of Guam (PAG) maintains critical data that supports vessel and yard operations, administrative functions and business activities. This data is managed, protected, secured and controlled by the PAG Information Technology (IT) division, an autonomous agency of the Government of Guam (GovGuam).

II. PURPOSE

This policy secures and protects data stored, is accessible and utilized by end-users in support of the mission of PAG. The purpose of this policy is to ensure:

a. PAG's data confidentiality, integrity and availability is consistently maintained.
b. Authorized individuals are assured of timely and reliable access to necessary data.
c. Unauthorized individuals are denied access to computing resources or other means to retrieve, modify, view or transfer data.

This policy also defines the rights and responsibilities of authorized personnel in the handling, security, and protection of Port data. The objective of this policy is to ensure that all Port databases and information resources remain secure while minimizing impediments to its access.

III. SCOPE

This policy covers the following PAG-IT systems.

- JD Edwards EnterpriseOne (E1) Financial System
- Navis N4 Terminal Operating System (TOS)/N4 Billing System

- E-mail Access
- Shared Folder/File Server
- Remote Access
- Remote JDE E1

IV. POLICY

The Port Authority of Guam IT division will provide employees and contracted third parties with access to the information and system necessary to perform their duties effectively and efficiently, provided they follow the established request procedures and adhere to all guidelines for protecting and safeguarding that access.

1. Request Access Process

Personnel and contracted third parties requesting access to a covered system must complete an IT Service Request Form detailing the specific system and type of access required. The form must be signed by their supervisor. Before IT can process the request, the requestor must sign and acknowledge the Data Access and Security Policy. Once all requirements are met and the request is approved, IT will provide a user-ID and password via teleconference or email.

a. User-ID – Each user shall be identified by a unique user ID based on their first, middle and last name. For example, if the employee's name is Jane A. Doe, the user ID assigned will be *jadoe*. If there is an existing user-ID, PAG-IT will find the best suited ID for the requesting user.

The Terminal Operating System (TOS) uses a different user-ID structure. Each user is identified by the initials of their first, middle and last name, followed by their assigned employee number. Using the prior example stated above, the user-ID assigned would be *jad1234*, given that the employee number assigned was 1234.

b. Password – Password must contain alphanumeric characters and include at least one numeric number, unless otherwise specified by IT. Password will expire every 90 days.

c. JDE E1 – The EnterpriseOne Financial access and security is based on roles, with levels of access such as INQ (Inquiry), PROC (Processor), SUPR (Supervisor) and MNGR (Manager) for the following modules: Address Book (AB), Accounts Payable (AP), Accounts Receivable (AR), Budget (BG), Fixed Assets (FA), General Ledger (GL), Human Resources (HR), Inventory (INV), Job Costing (JC), Procurement (P2P), Payroll (PR), Safety (SAF) and Work Order (WO).

d. TOS Navis N4/N4 Billing – The N4 access and security is based on roles namely Gate Clerk, Handheld Gate Clerk, Handheld Yard Clerk, Handheld Hatch Clerk, Handheld Reefer Monitor, Ops Admin Office, Gate Configuration-PAG, IT Admin

Configuration Only, EDI only, Harbor Master, Temporary Configuration Account, Billing Setup, N4 User, Gate Admin, CAP Users, Warehouse Clerk, SUOps, Finance Division, Billing, IT SU, Test Config, Supervisor, Port Police and Vessel Planner for N4. N4 Billing have the following roles: Billing Configuration role, Tariff Techs and Superusers.

e. E-mail Access – Access to the e-mail system is based on the assigned user-ID and password provided or created by users.

f. Shared Folder/File Server Access – In the absence of Active Directory, file server access by department is currently granted to employees upon request. IT will establish and manage the shared access links accordingly.

g. Remote Access – PAG permits remote access via SSL VPN secured by the corporate firewall. All requests for remote access are subject to review and must include a valid business justification. Multi-factor authentication (MFA) is enforced where the capability is available.

h. Remote JDE E1 – Web access with MFA is available but limited to designated subject matter experts. Access requires prior approval from both the IT Department and the Chief Financial Officer.

Note: Any access to data from systems outside the scope of this policy is governed by 49 C.F.R. Part 1520 and will not be accessed by any means.

2. **Security Policy**

a. All authorized PAG users must be cognizant of the level of access they have been provided, and their responsibility to maintain the privacy and integrity of all Port data. Effective data security is not possible without the cooperation of users who understand the reasons for data security and comply with established security measures.

b. All authorized PAG users must not share usernames, accounts and passwords. Credentials must not be written down or recorded on unencrypted electronic files, devices or documents.

c. All authorized PAG users must secure their username, account, password, and system access from any unauthorized use.

d. Passwords will expire every 90 days, and it is the user's responsibility to update their password before the expiration date to maintain uninterrupted access.

V. ACCESS GUIDELINES AND REQUIREMENTS

a. Division Heads are responsible for authorizing data access requests for all employees within their division by submitting a completed IT Service Request form.

b. Division Heads or authorized personnel must submit a completed IT Service Request form that includes detailed information about the request and roles to be authorized.

c. Division Heads are responsible for reporting all user data access status and responsibilities within their division in accordance with Policy Memo No. 2022-GM03 User Access Rights/Privileges Annual Review.

d. Human Resources Division must submit a completed IT Service Request form for all employees that have a change in PAG employment status. The form must be accompanied with a copy of the Employee Separation Clearance form or other official documents.

e. Acknowledgement: All PAG employees are required to sign an acknowledgement confirming they have received and read the policy. A copy of the signed acknowledgement will be retained in the IT Division's records.

VI. VIOLATIONS

a. All 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 or supervisory personnel, with final authority of the General Manager.

c. All data access and e-mail privileges will be suspended pending final determination of the General Manager.

d. Depending on the severity of the violation, the General Manager may revoke the user's computers, digital equipment, data access, internet access and e-mail privileges.

VII. ENTIRE POLICY

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