PORT OF GUAM
ATURIDAT I 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 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:
Approved by: Rory J. Respicio RORY J. RESPICIO, General Manager	

I. INTRODUCTION

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

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 integrity and accuracy is consistently maintained.
B. Authorized individuals are assured of timely and reliable access to necessary
C. data.
D. Unauthorized individuals are denied access to computing resources or other means to retrieve, modify, view or transfer data.

This policy also addresses the issue of the rights and responsibilities of authorized persons in the handling, security, and protection of Port data. The objective of this policy is to ensure secure database while minimizing impediments to its access.

III. DATA SECURITY

A. All data should be secured, with access granted to PAG users on a 'need-to-know' basis, and within the confines of predefined access guidelines and security requirement. Application/module owner has ultimate responsibility for determining the appropriate security requirements and access authorization, within the confines of predefined authorization guidelines based on the function.

B. 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 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.

C. All authorized PAG users must not share user names, accounts and passwords, be written down or recorded on unencrypted electronic files, devices or documents.

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

IV. CLASSIFICATION OF DATA

A. All PAG data is classified into a category of function (application), sensitivity, and risk level.

B. The higher the sensitivity of the data, the greater the amount of information security that must be applied for its protection. Similarly, data with lower levels of sensitivity can be protected with less rigorous measures.

C. Application/module owners working with Information Technology division are responsible for the application, and related setup/policy of systems, data, and other information resources.

D. Every user of the PAG Information System resources is responsible for the application and related policies to the systems, data, and other information resources in their care.

V. ENTERPRISE FINANCIAL SYSTEM – JD EDWARDS SYSTEM

A. Record level Control by Action Code
   1. Access – Inquire only
   2. Access – Inquire, Add
   3. Access – Inquire, Add, Change
   4. Access – Inquire, Add, Change, Delete

B. Menu level Control by Skill and Responsibility Level
   1. Access – Inquire, Add, Change, Delete, Posting
   2. Access – Inquire, Add, Change, Delete, Posting, Monthly & Yearly processing
   3. Access – Inquire, Add, Change, Delete, Posting, Monthly & Yearly processing, Advanced Activity

4. Access – Inquire, Add, Change, Delete, Posting, Monthly & Yearly processing, Advanced Activity, System Setup

C. Application level Control by System – Ownership of Application

Application	Division
Human Resource and Benefit	Human Resource
Address Book for Employees only	Human Resource
Payroll	Payroll
Accounts Receivable	Financial
Accounts Payable	Financial
General Ledger	Financial
Financial Reports	Financial
Fixed Asset	Financial
Budget	Financial
A/B for Customers & Vendors only	Financial
Distribution and Logistic-Procurement	Procurement
Distribution and Logistic-Supply	Supply
Distribution and Logistic-Inventory	Inventory
Work Order Maintenance	Equipment Maintenance
Work Order Maintenance	Facility
Equipment/Plant Maintenance	Equipment Maintenance
Employee Mail	ALL divisions
World Writer	ALL divisions
Requisition Entry	ALL divisions
Requisition Approval	ALL divisions
Budget Request	ALL divisions

Library level Control

Production - Financial Production library
Production - Payroll Production library
Test - Financial Test library
Test - Payroll Test library

VI. NAVIS N4 SYSTEM (TOS)

Application	Division	Access Control by
N4	Financial	Invoicing – Password for division
N4	Tariff	Password by individual
N4	Harbor Master	Menu setup and password for division
N4	Terminal	Menu setup, passwords, and Super Users
N4	Facility	Reefer Monitoring

VII. OPERATION LOG AND OPERATION TIME ENTRY SYSTEM – SANFORD

Application	Division	Access Control by
OPSLOG	Stevedoring	Menu
OPSLOG	EQMR	Menu

Application	Division	Access Control by
OPS Time Entry	Terminal	Password by division
OPS Time Entry	Transportation	Password by division
OPS Time Entry	EQMR	Password by division
OPS Time Entry	Facility	Password by division
OPS Time Entry	Port Police	Password by division
OPS Time Entry	Safety	Password by division

VIII. BILLING SYSTEM - SANFORD

Selection	Division	Access Control By
Charge Rate Table	Tariff	Password by individual
Direct Labor	Tariff	Password by individual

IX. ACCESS GUIDELINES AND REQUIREMENTS

A. Division heads are responsible for signing off on data access requests for all employees under their division by submitting a completed IT Service Request form.

B. Division Heads or authorized personnel must submit a completed IT Service Request form, with detailed information of records, action mode, and menu access to be authorized, to the Information Technology division to setup access for the identified individual(s) in the request.

C. For Multi-tasks or Detailed assignments, step B must be performed. The time period from start to end dates must be indicated on the form(s).

D. Upon completion of the Multi-task or Detailed assignment, the Application Owner's/Division Head must submit a completed IT Service Request form restoring data access back to the original function(s).

E. Division Heads are responsible for reporting the state of all user data access status and responsibilities, within the division, annually by submitting a completed IT Service Request form.

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

G. Acknowledgement: 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.

X. ENTIRE POLICY

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

XI. 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. 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 forfeit the user's computers, digital equipment, data access, internet and e-mail privileges.