
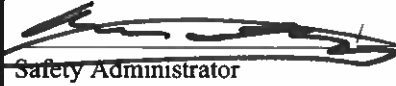

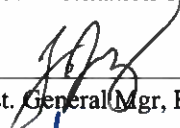
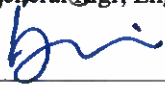



<p align="center">GUAM POWER AUTHORITY STANDARD OPERATING PROCEDURE</p>	<p>Prepared & Amended by:  / <u>Rudy C. Manibusan</u> Computer Technician Supervisor  / <u>Kenneth J. Gutierrez</u> Safety Administrator</p>
<p>TITLE: DATA CENTER AND SERVER ROOM SECURITY</p>	<p>Concurred by:  / <u>Melvyn K. Kwek, CISA, GICSP</u> Chief Information Technology Officer  / <u>John J. Cruz, P.E., CEA, CEM, MBA</u> Asst. General Mgr, Engineering & Technical Services  / <u>Beatrice P. Limtiaco</u> Asst. General Manager, Administration</p>
<p>NO: SOP- <u>168</u></p> <p>Page 1 of 12</p>	<p>Approved:  <u>2/18/2021</u> John M. Benavente (P.E.) General Manager Dated:</p>

1.0 PURPOSE OVERVIEW

The purpose of the Guam Power Authority's (GPA) Data Center Security policy is to provide and ensure a secured, resilient and monitored environment for the Data Center which includes Server Room and all the equipment hosted therein; the Information Technology (IT) Office areas and premises; and all other remote Server/Communication Rooms throughout GPA Facilities where IT Resources and Network Infrastructure are hosted. These guidelines and procedures are to safeguard and restrict access to authorized personnel only.

2.0 SCOPE

The objective of this standard operating procedure is to minimize security risks and vulnerabilities from possible external and or internal threats, and ensure the safety and protection for all IT personnel and all the equipment hosted within the authority's Data Center and Server Room. Data center security includes but not limited to physical access into the GPA IT's offices and Server Room, which hosts ALL Servers, Systems Controllers, Disk Arrays, Main Distribution Facility (MDF), and all internal and external (inside plant and outside plant) Intermediate Distribution Facilities (IDF) or Remote Server/Communication Rooms within the Gloria B. Nelson Public Service Building (Fadian) and throughout the various GPA Compounds and facilities.

CODES:

★ REVISED

ADDED

This policy is intended to create a governance and guidelines for the Data Center Security. This policy applies to all employees, contractors, consultants, vendors, interns, temporary, as well as other workers or third-parties who are doing work on behalf of the Authority (referred collectively as “users” within this document).

3.0 **DEFINITIONS**

- 3.1 ***Data Center:*** A secured, and environmentally controlled area that includes the Authority’s Information Technology Offices, personnel work area, and the Server Room.
- a) ***Server Room:*** A highly secured and environmentally controlled room which hosts GPA’s IT, GPA’s Power Systems Control Center (PSCC) Systems and GWA’s Dispatch Servers, Storage Devices, Controllers, and the Main Distribution Facility (MDF) for all Local Area Network (LAN), Wide Area Network (WAN), and Metropolitan Area Network (MAN) communication devices and equipment.
- b) ***Main Distribution Frame/Facility (MDF):*** A termination point and the distribution Frame/Facility for connecting internal equipment (inside plant) to cables and carrier equipment (outside plant).
- c) ***Intermediate Distribution Frame/Facility (IDF):*** A frame or facility that provides interconnectivities and cable/wiring management between the MDF and the end points (workstations, printers, and other Internet Protocol (IP) devices.
- 3.2 ***IT Personnel:*** GPA personnel who works under the Information Technology Division’s organizational chart or who are assigned (detailed) in a temporary capacity.
- 3.3 ***Authorized Personnel:*** GPA personnel whose roles and responsibilities require physical access in the Data Center and or IT offices and premises.
- 3.4 ***Authorized Vendor/Contractor:*** Non GPA personnel through contractual arrangements for access must have all required Cyber Security documents completed, and submitted to their respective sponsors. Refer to Section 4.2 for these requirements.
- 3.5 ***Visitors:*** All other personnel who is visiting GPA’s Data Center.

4.0 **PHYSICAL AND ENVIRONMENTAL SECURITY**

Security for the IT Divisions’ offices, perimeters, Data Center, and all other remote Server/Communication Rooms shall be defined to protect areas that contain confidential or sensitive data, information and/or information systems. Accordingly, these procedures provide the requirements and security protocol by appropriate access controls.

4.1 Security Standards and Requirements.

- a) All visitors must sign in and out of the IT Division, and or the Visitors Log Book for or the Server Room documenting their Name, Company, and purpose of visit. Log book shall be maintained by the GPA IT Division and may be audited unannounced and/or as necessary by the Internal Audit Office, Safety, or pertinent division/officials.
- b) All visitors must be briefed by their sponsors and must adhere to this policy and other GPA policies and procedures as it applies.
- c) All visitors must wear a valid GPA/GWA visitors badge issued by the respective Human Resources Division while in the IT Division's perimeters.
- d) All visitors must be escorted by their sponsors while within the Data Center perimeters at all times.
- e) In cases where deliveries require the main doors to be kept open, the authorized personnel receiving the deliveries (point of contact) is responsible for watching the door until it is closed and secured.
- f) Access Control Badges shall not be shared when entering the Data Center and or Server Room. Piggybacking or tailgating is prohibited.

4.2 Required Clearances and Documents for Vendors/Contractors

Non GPA personnel through contractual arrangements for access must have all required Cyber Security documents completed and submitted by their respective sponsors. The sponsors are responsible for submitting the Cyber Security documents to the IT Division for approval by the Chief Information Technology Officer (CITO) or designee or from the GWA's IT Manager or designee prior to access into the GPA Data Center and IT office areas and premises. These documents include but are not limited to the following:

- a) Physical Access Request Forms for US Passport Holders (*Attachment 1*)
- b) Physical Access Request Forms for Non-US Passport Holders (*Attachment 2*) AND Foreign National or Non-US Passport Holders Clearances Requirements (*Attachment 3*)
- c) GPA Confidentiality & Nondisclosure Agreement Form (*Attachment 4*)
- d) GPA Background Investigation Requirements (*Attachment 5*)

5.0 **DATA CENTER ACCESS AND ETIQUETTE**

5.1 Data Center Policy on Access and Requirements

- a) Entrance into the Data Center shall be kept locked at all times.

- b) Access into the Data Center is restricted to GPA IT and GPA PSCC Personnel, and GPA authority personnel with approved access, vetted vendors, external auditors, and government regulatory officials.
- c) Each authorized personnel must swipe the access control system prior to entering the Data Center. Piggybacking or tailgating is not permitted and shall not be practiced.
- d) Manual key entries for the Data Center and the Server Room shall be used **ONLY** when the access control system is inoperable.
- e) All system/servers rack doors in the Server Room must be closed and locked when not being accessed to prevent unauthorized access and or intruders.
- f) All visitors granted access into the Data Center must be escorted at all times by their sponsors or authorized personnel.
- g) Access Control Badges into the Data Center shall not be shared.
- h) Individuals or visitors requiring access into the GPA Server Room to perform maintenance work relating to equipment hosted within, or environmental equipment within, must be arranged and approved in writing by GPA's CITO or designee or GWA's IT Manager or designee in advance.
- i) Equipment installations, removals, and changes within the Server Room must have prior written approval by the CITO or designee and with an approved Scope of Work (SoW). Entry will be denied to authorized staff or visitors who intend to install, remove, or change equipment without presentation of proper approved SoW documentation.

5.2 In order to maintain a clean and safe environment and not obstruct work performed in the Server Room, all individuals must adhere to the following rules of etiquette:

- a) Under no circumstances shall food or beverage of any type and/or any kind be brought into the Server Room.
- b) All work areas must be kept clean and free of debris. Upon completion of any work, personnel performing the work must ensure that the area is clean before leaving the work area.
- c) Unpacking of boxed systems, equipment and devices must be done in a designated staging area outside the Server Room prior to mounting installation. Unpacking of any system, equipment and device are not allowed in the Server Room.
- d) Avoid obstructing aisles, walkways, or leaving the raised floor tiles unsettled in the Server Room. This will help to reduce safety hazards in the Server Room.

- e) All rack enclosures must be kept neat and free of manuals, cables, etc. Doors to each rack must be locked at all times and upon completion of approved work.
- f) Un-racked equipment, i.e., operating equipment outside of cabinets or racks, is strictly prohibited.
- g) Cables shall not be strung outside of rack enclosures. Designated cable pass-throughs must be used for connectivities to adjacent racks. Cable trays must be used for all external Data and FiberOptic Cabling.
- h) No cleaning fluids or water are allowed inside the Server Room.
- i) No cutting of any type of materials (pipes, floor tiles, wood, etc...) shall be performed inside the Server Room. Data and Fiber Cabling are exceptions as cables are terminated at length.
- j) Taking photos and/or capturing videos are strictly prohibited inside the Server Room.
- k) Only authorized personnel shall be issued keys to racks as assigned per roles and responsibilities.
- l) Decommissioned systems, equipment and devices shall be removed immediately upon written approval by the GPA's CITO or designee or GWA's IT Manager or designee.
- m) All hard drives must be sanitized and disposed properly after removal from any and all system by authorized GPA IT personnel.
- n) All equipment hosted within the Data Center must be inventoried with configuration as assets.

6.0 **POLICY ENFORCEMENT & COMPLIANCE**

All users are responsible for complying with this standard operating procedure, protecting information resources in their possession, and to immediately report unauthorized or suspicious activities or violations of this or any other IT policy or procedures to their Supervisor, Manager, the CITO, and/or the Safety Division.

Where guidance or interpretation of this standard operating procedure is needed, users are to discuss the situation with their immediate supervisor/manager or IT personnel for proper guidance and direction. The IT Division enforces this standard operating procedure and related operations standards at all times. Anyone who has reason to suspect a deliberate and/or willful violation of this standard operating procedure must promptly report it to their immediate supervisor, manager, GPA's CITO, Internal Audit Office, and/or the Safety Division.

Users found in willful violation of this standard operating procedure may be subject to progressive disciplinary action ranging from a verbal warning to dismissal as outlined in the Authority's Codes of Conduct. The severity and/or adverse effect(s) of the infraction(s) on GPA's operation and security will be considered.

Exceptions to the Data Center and Server Room Security Policies and Procedures may be granted by the CITO or designee as necessary. It is to provide immediate and or emergency access to include but not limited to Facilities Division personnel, Emergency First Responders (i.e., Medical, Fire, Police, etc.), and/or Federal Officials.

ATTACHMENT 1: Physical Access Request Form for US Passport Holders



PHYSICAL ACCESS REQUEST FORM

Rev 4 02/04/20

Physical Access Request Form for US Passport Holders

Required Non-GPA User Information: Important: This form will not be processed unless all fields are completed. Fields preceded by an "*" are mandatory and must be filled in. Indicate N/A for non-applicable fields

Requestor Information			
* Requestor Name - Print:			
* Requested Access Start Date:		* Requested Access End Date	
* Company Name:			
* Company Address:			
* Requestor's Office Phone #:		* Project Manager's Phone #:	
* Requestor's Email:		* Project Manager's Email:	
* Project P.O. #/Expiration:		* Sponsor's Division:	
* Sponsor Name/Title:			
* Project Name/Title:			
Access Requirements similar to (state name): <i>May help to expedite your request</i>			
* List of Facilities with the associated access permissions being requested:			
* Business Justification:			
***** Requestors: Do not write anything below this line *****			
GPA HR Background Investigation (BGI) Letter Verification Information			
* GPA Human Resource Approver Name:			
* Date of Requestor BGI Letter:			
* Requestor BGI Approved (Y/N):	/ / (Yes) / / (No)		
GPA Physical Access Approvals			
Approved Access Start Date:		Approved Access End Date:	
Approvers	Name	Signature	Date
GPA Requesting Division Manager:			
Assistant General Manager (Admin, Operations, Engineering & Technical Services), or Chief Financial Officer:			
GPA Safety Administrator:			

CODES:

* REVISED

ADDED

ATTACHMENT 2: Physical Access Request Form Non-US Passport Holders**PHYSICAL ACCESS REQUEST FORM**

Rev 4 02/04/20

Physical Access Request Form for Foreign Nationals (Non-US Passport Holders)

Required Non-GPA User Information: Important: This form will not be processed unless all fields are completed. Fields preceded by an "*" are mandatory and must be filled in. Indicate N/A for non-applicable fields

Requestor Information			
* Requestor Name – Print:			
* Requested Access Start Date:		* Requested Access End Date:	
* Company Name:			
* Company Address:			
* Requestor's Office Phone #:		* Project Manager's Phone #:	
* Requestor's Email:		* Project Manager's Email:	
* Project P.O.#/Expiration:		* Sponsor's Division:	
* Sponsor Name/Title:			
* Project Name/Title:			
Access Requirements similar to (state name): <i>May help to expedite your request</i>			
* List of Facilities, with the associated access permissions being requested:			
* Business Justification:			
***** Requestors: Do not write anything below this line *****			
GPA Cyber Security – Non-US Passport Holders - Verification Information			
*Flight Itinerary:			
*Hotel Accommodations:			
*Passport Country/Number:			
GPA Physical Access Approvals			
Approved Access Start Date:		Approved Access End Date:	
Approvers	Name	Signature	Date
GPA Requesting Division Manager:			
Assistant General Manager: (Admin, Operations, Engineering & Technical Services), or Chief Financial Officer:			
GPA Safety Administrator:			

CODES:

* REVISED

ADDED

ATTACHMENT 3: Foreign National or Non-US Passport Holders Clearance Requirements

All GPA foreign national visitors, vendors, or contractors (including sub-contractors) are required to provide clearance documents and information to the GPA Safety Division (Safety Administrator). The submission of personal information, also known as Personally Identifiable Information (PII) is required to establish identity and for vetting purposes to determine if authorized access may be granted. A Foreign National is defined as a person who was born outside the jurisdiction of the United States, who is subject to some foreign government, and who has not been naturalized under U.S. law. The following information and document listed below are required and must be submitted two weeks prior to the subject vendor/contractor's actual visit into the facility.

1. *A clear copy of the individual's passport.*
2. *Following information about the individual:*
 - a) Full Name (Last, First, Middle)
 - b) Known Alias(es)
 - c) Gender
 - d) Date of Birth
 - e) Place of Birth
 - f) City/Country of Residence
 - g) Country of Citizenship
 - h) Company Name and Contact Information
 - i) Occupation/Title
 - j) GPA Host/Sponsor (Division/Department/Section)
 - k) GPA Point of Contact (Name, Title and Phone Number)
 - l) Address while in Guam (Hotel Name)
 - m) Nature or Purpose of Visit
 - n) Duration of Stay
 - o) Date and Time arrival and departure

Failure to furnish the requested information in a timely manner or altogether may delay or prevent the requested access to Authority IT Resources, Facilities or Programs.

ATTACHMENT 4: GPA Confidentiality & Nondisclosure Agreement Form**Confidentiality and Nondisclosure Agreement**

**GUAM POWER AUTHORITY
CONFIDENTIALITY AND NONDISCLOSURE
AGREEMENT**

This Confidentiality and Nondisclosure Agreement ("Agreement") dated _____, 20____
is between Guam Power Authority, and _____.

In consideration of the promises contained herein, the Parties hereby agree as follows:

1. Either party (the "Disclosing Party") may supply the other party (the "Recipient Party") with information or data that is confidential, proprietary, or secret to the Disclosing Party. This includes information pertaining to the Disclosing Party's activities, business, or work related, to activities performed in support of Guam Power Authority's _____.
_____. Such information and data shall be deemed "Confidential Information" as discussed in this Agreement.
2. Information shall not be deemed to be Confidential Information where: (i) it is or becomes public information or otherwise generally available to the public through no act or fault of the Recipient Party; provided, Recipient Party shall not disclose such information unless, and then only to the extent, such information is obtained from a source other than the Disclosing Party and such source did not receive the same directly or indirectly from the Disclosing Party; (ii) it was, prior to the date of this Agreement, already in the possession of the Recipient Party and was not received by the Recipient Party directly or indirectly from the Disclosing Party; (iii) it is hereafter rightfully received by the Recipient Party from a third person who did not receive the same directly or indirectly from the Disclosing Party; or (iv) it is at any time independently developed by employees or consultants of the Recipient Party who have not had access to Confidential Information in the possession of the Recipient Party. The Recipient Party shall bear the burden of proof that such employees or consultants have not had access to Confidential Information. Specific information shall not be deemed to be within the exceptions of subparts (i) through (iv) merely because it is embraced by more general information within such exceptions, nor shall a combination of features be deemed to be within such exceptions merely because the individual features are within such exceptions.
3. The Recipient Party agrees that any Confidential Information which has been or will be disclosed directly or indirectly to it by or on behalf of the Disclosing Party shall be maintained in confidence, and shall not be disclosed to any third person without the Disclosing Party's prior express written consent. Such consent may only be granted by a duly authorized representative of the Disclosing Party.

ATTACHMENT 3: GPA Confidentiality & Nondisclosure Agreement Form

Confidentiality & Disclosure Agreement

4. The Recipient Party agrees that it will not make use of any Confidential Information received pursuant to this Agreement except for the limited purposes for which expressly given without the express prior written consent of the Disclosing Party. Such consent may only be granted by a duly authorized representative of the Disclosing Party.
5. The Recipient Party may disclose Confidential Information to any governmental or regulatory authority requiring such disclosure under color of law, provided that: (i) the Recipient Party notifies the governmental or regulatory authority that the materials are Confidential Information; and (ii) prior to such disclosure, the Disclosing Party is given prompt notice of the required disclosure so that it may take whatever action it deems appropriate, including intervention in any proceeding and the seeking of an injunction to prohibit such disclosure.
6. This Agreement shall not be construed as a license or authorization to the Recipient Party to utilize the Confidential Information for any purpose.
7. This Agreement is for the benefit of the Disclosing Party and, without prejudice to the rights and remedies otherwise available to it, the Disclosing Party shall be entitled to equitable relief by way of injunction if the Recipient Party breaches or threatens to breach any of the promises of this Agreement. In addition, the Disclosing Party shall be entitled to recover all reasonable attorney's fees incurred in seeking such remedies.
8. This Agreement shall be interpreted, governed, and construed under the laws of Guam excluding provisions thereof which refer to the laws of another jurisdiction.
9. This Agreement may be executed in multiple counterparts, each of which shall be deemed to be an original.
10. This Agreement is effective as of the date fully executed by both Parties and shall terminate three (3) years thereafter.

GUAM POWER AUTHORITY_____
(Company Name)By: _____
(Print)By: _____
(Print)By: _____
(Signature)By: _____
(Signature)

Title: _____

Title: _____

Date: _____

Date: _____

UA-NDA-1.1

Page 2 of 2

ATTACHMENT 5: GPA Background Investigation Requirements

Applies to all non-GPA employees through contractual arrangements requiring access into GPA, IT Resources, facilities and work areas. These information are required to be submitted to GPA Human Resources Division.

- 1) **Background Investigation (BGI)** documents must be sent/mailed directly from the vendor company's Human Resource (HR) Department with respective contact information, to the GPA HR Department contact(s) provided below. Additional members can be cc'd on the email for information and coordination purposes.

- 2) **GPA HR Contact information:**
Sandra Perez
Guam Power Authority
Personnel Services Administrator
Human Resources Division
Gloria B. Nelson Public Service Building
688 Route 15 Fadian
Mangilao, Guam 96923
671-648-3130
sperez1@gpagwa.com

- 3) **The BGI documents must include the following required information:**
 - a. Name of employee(s) that the successful BGI was performed on.
 - b. Date the Background Investigation(s) was performed for each employee.
 - c. The name of the company/agency that conducted the background investigation on each subject employee.
 - d. Background investigation criteria:
 - i. 7-year criminal background check at federal & local state/county level for mainland individuals.
 - ii. 7-year Police and Court background/criminal investigation for Guam residents.
 - iii. Screening for Sex Offenses and National Sex Offender Registry (NSOR).
 - iv. Identity/Social Security Number Verification.