GUAM POWER AUTHORITY **STANDARD OPERATING PROCEDURE**	**Prepared By:** RUDOLPHO MANIBUSAN Computer Technician Supervisor
TITLE: Network and Data System Access	**Concurred By:** MELVYN K. KWEK, CISA, GICSP Chief Information Technology Officer JOHN J. CRUZ, P.E., CEA, CEM, MBA Asst. General Mgr, Engineering & Technical Services
NO: SOP-150 **Supersedes: AP-056, dated 05/28/03** **SP-150, dated 07/19/11** **Page 1 of 14**	**APPROVED BY:** for 1-2-2019 **JOHN M. BENAVENTE, P.E.** **General Manager** **Dated:**

1.0 * PURPOSE OVERVIEW

The purpose of this standard operating procedure is to outline Guam Power Authority's (GPA's) connectivity, use, and management of its network infrastructure at **all** GPA sites. References to "Authority" applies to GPA

This policy is one of GPA's cybersecurity policies, which informs all authorized users of their responsibilities for the use and protection of technology and information assets. This policy represents the commitment of GPA to ensuring that system and information integrity policy is appropriately defined and implemented, in order to protect GPA systems from intentional or unintentional acts that may negatively impact its system. This policy establishes guidelines for the access and use of the network infrastructure. These guidelines facilitate the preservation, integrity, availability, safety, and confidentiality of GPA's information.

This shall also be construed as an Authority security policy, which identifies guidelines, standards, and responsibilities. This policy represents the commitment of the Authority to protect its systems and information from intentional or unintentional acts that may negatively impact system security.

2.0 * SCOPE

This policy applies to **all** employees, board members, contractors, consultants, vendors, temporary, volunteers, and other workers of the GPA with GPA owned or personally-owned computer or workstation used to connect to GPA networks and any information resource. This policy also applies to onsite and remote access connections used to do work on behalf of GPA.

This guideline supports GPA's objective of a network infrastructure to operate securely, reliably, and to provide dependable Local Area Network (LAN) and Wide Area Network (WAN) communications. The LAN and WAN processes and activities within GPA include but are not limited to: Advanced Metering Infrastructure (Tier 1, 2, and 3 Networks), Substation Automation, Outage Management, and Remote Office connectivity.

This policy provides guidelines for acceptable and unacceptable uses of GPA:

i. Network Access, Security, and Management;

ii. Physical Connections to Authority Network;

iii. Network Infrastructure and Bandwidth;

iv. Responsibilities of Authorized Network Users;

v. Remote Access and Devices;

vi. System Security, Confidentiality; Integrity and Availability

vii. Standard of Conduct.

3.0 * RESPONSIBILITIES

The Information Technology (IT) Division is responsible for granting all network access to GPA computer systems network.

3.1 Chief Information Technology Officer (CITO) and IT Division – The team, which is led by the CITO or a designee, is responsible for providing oversight and guidance in complying with GPA Information Technology Security and Network Infrastructure. The team assists with the implementation of security controls and monitors GPA systems to ensure compliance with regulatory requirements and standards. The team is also responsible for providing guidance and clarifying security controls.

3.2 Managers and Supervisors – Managers and Supervisors must ensure that employees and users are informed of appropriate uses of GPA equipment and information technology resources through training and awareness.

3.3 It is the responsibility of **every** user to know these guidelines, and to conduct their activities accordingly. When GPA computer and system users are confronted by a situation not covered by these policies/procedures or they do not clearly apply to a situation, users are encouraged to clarify with their respective supervisor or officials with their IT Division.

This policy will be reviewed and updated by the IT Division annually to ensure compliance with the law, standards, operational functions, contractual obligations, and regulatory requirements.

4.0 * DEFINITIONS

4.1 Users – For the purpose of this policy, these are **all** employees, board members, contractors, consultants, vendors, temporary, volunteers, third party, and other person in a position to know or obtain information about computer or devices on GPA network.

4.2 Local Area Network (LAN) – A computer network within a small geographical area such as office building. It is composed of interconnected workstations and personal computers that are each capable of accessing and sharing data and devices, such as printers, scanners and data storage devices, anywhere on the LAN.

4.3 Wide Area Network (WAN) – A telecommunications network or computer network that extends over a large geographical distance or between different LAN. WAN networks allow an organization to effectively carry out its daily function regardless of location.

4.4 Remote Access – Access to the LAN from any location outside the firewall by any method, including but not limited to Virtual Private Network (VPN), dial-in modem, frame-relay, SSH, cable-modem and any other method of accessing the LAN from outside the firewall.

5.0 * GENERAL OWNERSHIP & PRIVACY EXPECTATION

GPA's operations are highly dependent on its network communications, system processes, and data storage. The Authority's IT Division are the custodian and has end-to-end responsibility and control of the network infrastructure.

All connections to the network to include access points, wireless devices, wall sockets, data cabling (RJ45) and everything connected to such is the sole responsibility of the IT Division and shall not to be accessed, changed or modified by anyone unless specifically authorized by the CITO or a designee. GPA owned or leased equipment, devices or units that are or may be connected wirelessly or plugged into Authority network are also subject to this policy.

GPA network and the data contained therein are government property. User has no expectation of privacy with GPA network and computer systems, Internet access, E-mail, voice mail, and electronic data or documents produced, stored or located on Authority computers, devices or systems. GPA reserve the right to inspect computers, other electronic data devices and associated systems, audit networks and systems, and to monitor computer systems at any time for legitimate government purposes to assure compliance with law, with this policy, and with other government or regulatory requirements.

6.0 * NETWORK POLICY & GUIDELINES

6.1 Network Access

Only authorized users are granted access by IT Division to information systems, and users are limited to defined, documented, and approved applications and levels of access rights. Computer and communication system access control are to be achieved via user and permissions (role/title role) that are unique to each individual user to provide individual accountability.

The following applies to all GPA authorized network users.

6.1.1 Access to the resources on the GPA WAN and LAN networks shall be strictly controlled to prevent unauthorized access. No device may be connected to the Authority's network, and no wireless connection devices may be activated within GPA facilities and building spaces, without the prior written approval of the CITO or a designee.

6.1.2 There will be no connections to GPA computer systems network, to include but not limited to: wireless access points; network routers; tethering devices; switching equipment or hubs; key loggers or any device to capture data or store data (both hardware and software); laptops or computers that have not been authorized by the IT Division; or outside Internet connections to GPA equipment not authorized by the IT Divisions.

6.1.3 Use of external resources to conduct Authority business must have prior written approval of the CITO or a designee.

6.1.4 Network security for GPA shall be protected by an established Firewall, Secured Web Gateway and/or other Application/Appliance that provides controlled acces and security protection. Access Control Lists (ACLs) are used to control and limit access, network traffic and are managed by the IT Division.

a) All traffic and systems will be monitored for a variety of reasons subject to pertinent GPA policies.

b) All personal computers connected to GPA networks (with prior written approval of the CITO or a designee) must have an active virus detection and protection software installed with the latest updates and signatures and configured for automated scanning updates of signature pattern files.

c) All systems and devices on GPA's network may be subject to a security assessment with appropriate follow-up action taken to mitigate any compromised system or device.

d) Any device found providing unauthorized services shall be immediately disconnected from the network and inspected by IT officials to ensure data/information has not been compromised.

e) Connected devices must be maintained in accordance with the manufacturers' recommendations. Operating System and application software must be kept up-to-date to ensure risks from security vulnerabilities are minimized.

f) Devices are required to meet security standards for operating system security patch levels and authentication.

g) Devices shall be removed or shall not remain connected to the Authority's network after the manufacturer, operating system, and application vendor has designated End of Life.

6.2 Network Security

In the event the IT Division has discovered or otherwise been informed that a system on the GPA network is threatening the stability, availability, integrity or security of the network, or has otherwise been compromised, hacked, is sending out malicious traffic or is the source of SPAM, the IT Division has the right to:

a) Gain access to and inspect the configuration of device (s) and take remedial actions as necessary.

b) Remove from the network any device(s) that it believes could be the source of the problem, or otherwise block inbound and outbound traffic, as appropriate.

c) Disable as necessary any part of the network in order to remove the source of the problem.

Every effort will be made to contact the system user, owner, Supervisor, Division Manager, and/or other appropriate official(s). All services will be reconnected at the first opportunity after the problem has been remediated.

6.3 Network Management

GPA's LAN and WAN shall be managed by IT Division staff to oversee its day to day operations and to preserve its confidentiality, integrity, and availability. Where network infrastructure is not managed by the IT Division, read-only access to GPA owned devices shall be provided, on request, for the purpose being able to monitor the network activities. All network management staff shall be given significant training and awareness with information on cybersecurity and related IT issues.
As part of the IT Division's network oversight role, they will:

a) Maintain appropriate logs to monitor and trace who/what device was using a particular IP address at a particular time. Logs will be retained for at least 6 months in compliance and archived for historical purposes.

b) In the event of a security event involving the network affecting the LAN/WAN, the IT Division personnel has the right to gain access to and inspect the configuration of devices or equipment and to require the immediate removal of any devices or equipment that it believes could be the source of the risk.

c) In collaboration with individual owners/users, IT Division has the right to disable portions or all of the LAN/WAN, as necessary, to diagnose and/or remove the source of the threat, risk or problem.

d) Systems or devices shall be disconnected from the network by the IT Division, when a threat or risk may cause problems with users of the network, to an external network and/or following a security breach. Systems shall not be reconnected without the explicit prior authorization of the Network Operations Center, Computer Technician Supervisor and approved by the CITO or a designee.

6.3.1 All network addresses, including IP addresses, Server/Device/DNS Names, within GPA's LAN and WAN shall be allocated and administered by the Network Operations Center of the IT Division. Any configuration changes, additions, deletions shall be under the instruction of the Network Operations Center with the approval of the CITO or a designee.

6.3.2 To proactively protect the integrity, security and operations of the network and the systems, the IT Division may carry out both manual and automated systematic vulnerability scans and penetration tests on computer systems connected to the network. Best efforts will be undertaken to minimize any disruption, and any unavoidable or unrecoverable damage will be immediately investigated.

6.4 Physical Connections to Authority Network

New connections of equipment into GPA LAN/WAN network may only be made with the prior approval of the Network Operations Center, Computer Technician Supervisor, and approved by the CITO or a designee.

6.4.1 Physical connections to GPA's network switches and/or backbone must be coordinated with the PC Support Group, or Network Operations Center with the explicit prior approval of the CITO or a designee.

6.4.2 No extensions and/or modifications to the physical infrastructure of GPA network, including wireless, may otherwise be made. This includes, but is not limited to, the addition and/or removal of: network switches; Routers; Wireless Access Points; Cabling other than connecting a patch cable to a provided network wall socket; or any device which acts in such a capacity of a Switch, Router or

Access Point, (e.g. a PC configured as a router). Network Address Translation (NAT) boxes are specifically prohibited.

6.4.3 Specialty devices will be individually assessed, and approval will be given in writing by IT officials where appropriate. Special consideration will be given to lab equipment and/or other specialty devices.

6.5 Network Infrastructure and Bandwidth

All network infrastructure equipment, devices and/or network wiring within GPA's LAN and WAN is managed by the Network Operations Center of the IT Division. With the approval of the CITO or a designee, Network Operations Center is responsible to monitor and may restrict/suspend excessive use of network bandwidth by any system or user.

6.5.1 Network equipments are stored in network cabinets in the Data Center's Main Distribution Center (MDF) and/or throughout the various Intermediate Distribution Frames (IDF) equipment rooms. Only those who are specifically authorized may have access to the Data Center and/or MDF or IDF rooms.

6.5.3 All requests for changes such as the connection of additional switch ports shall be made through the IT Division Helpdesk with the prior approval and in collaboration with the Network Operations Center and the CITO.

6.6 Responsibilities of Authorized Network Users

Only authorized users are permitted to connect to and use of GPA network. Users who have agreed to the Authority's terms and conditions, read and signed the Authority ***Network and Data System Access Acknowledgment*** (see Attachment 1) form and shall be issued a personal username and password in GPA's Lightweight Directory Access Protocol (LDAP) directory or Active Directory.

a) It is unacceptable for users to share their username and their password or to allow unauthorized individuals to use it for any facilities to which it gives access.

b) Users are not permitted to plug in client machines or devices without the written prior approval by IT Division personnel and shall not extend the network in any way.

c) Users shall not advertise wireless networks within GPA's compounds.

d) Users shall not connect any device that will act as a wireless access point. Access to the GPA's network shall not be shared with unauthorized user(s).

e) GPA users who have completed, accepted, signed and submitted all required cybersecurity documents and provided proof of identity, will be issued a temporary username and password (valid for a period not exceed the contract corresponding to the scheduled work hours and days). The cybersecurity documents, to include but are not limited to:

1. Background Check (BGC Form)
2. Logical Access Request Form
3. None-Disclosure Form
4. Master Access Agreement Form
5. Physical Access Request Form
6. Proper and Acceptable Identification

Only when all of the above requirements are met, will a user name and password to temporary visitors be issued by the IT Division.

7.0 # REMOTE ACCESS AND DEVICES

Remote access into GPA networks is essential in maintaining productivity, but in many cases, remote access originates from networks that may already be compromised or are at a significantly lower security posture than GPWA's networks.

While these remote networks are beyond the control of the IT Divisions, all authorized users must mitigate these external risks to the best of our ability. Users with remote access privileges into GPA corporate network are responsible to ensure that their remote access connection is given the same security approach as connection made within GPA.

7.1 Use of external resources to conduct GPA business must have prior written approval of the CITO or a designee and the user's appropriate business unit manager.

7.2 While using a GPA-owned or leased computer to remotely connect to the network, authorized users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorized user or third party.

7.3 System users using any remote device must ensure that such device is updated with the most recent security patches for their Operating System.

7.4 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs) and strong and complicated password or pass-phrases.

7.5 All hosts that are connected to GPA internal networks via remote access technologies must have updated anti-virus software.

7.6 Authorized users shall protect their login and password, even from family members.

8.0 # SYSTEM SECURITY AND CONFIDENTIALITY

The security and confidentiality of GPA data and records are matters of great concern. Employees and users with access to information are in a position of trust in maintaining security and confidentiality of GPA information and data records.

8.1 Security of System

System users must adhere to the following:

a) Unauthorized use of or access to any GPA data records is strictly prohibited.

b) System users are prohibited from personally benefiting or allowing others to benefit by knowledge of any confidential information gained by virtue of their work assignments.

c) System users are prohibited from exhibiting or divulging the contents of any record or report to any person except in execution of their normal duties and responsibilities.

d) System users may not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.

e) Users may not delete or cause to be deleted data from any record or report without prior explicit authorization.

f) No official record or report, or copy may be removed from the office where it is maintained except when performing duties.

g) System users shall not leave a workstation unattended without properly and completely locking the workstation.

h) Each system user has unique access profile (a login userID and password). No system user may divulge or allow anyone else to use his/her access. If a system user suspects someone of knowing or using their access, they will immediately notify their supervisor and the IT Division.

i) Users, who believe that their computer systems have been subjected to a security incident or has otherwise been improperly accessed or used, should immediately report the situation to their supervisor or manager and the IT Division. The user shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

j) No one is to aid, abet, or act in conspiracy with another to violate any part of the system access.

8.2 Information Security

It is essential that each user never divulge even the most seemingly innocent detail about the Authority's Information Technology to a third party. While it may seem inconvenient or rude, all employees and users must treat as suspicious any request from any third party person not personally known to that them.

Any caller not personally known to the employee or user who requests sensitive information must be immediately referred to the IT Division or to the CITO or designee. If such referral is not possible or practical, then the employee or user must request from the caller a callback number, to be given to the appropriate IT personnel or Division official.

9.0 **# STANDARD OF CONDUCT**

Standards of ethical conduct and appropriate behavior apply to the use of all GPA information technology resources, including but not limited to, hardware, software, Internet, storage media, and computer and network.

9.1 Performance of illegal activities through GPA network by any user is prohibited.

9.2 When accessing GPA network from a personal computer, users are responsible for preventing access to any GPA computer resources or data by non-authorized users.

10.0 **# POLICY ENFORCEMENT & COMPLIANCE**

Violation of this policy may result in suspension, limitation or revocation of access to GPA's computer workstations, other electronic data devices and associated systems, Internet access, E-mail usage, etc. in addition to other disciplinary action determined to be appropriate by management.

Users are expected to report suspected violations of this policy to the IT Division; their supervisor or manager; or the Internal Audit Office. Where guidance or interpretation of this policy is needed concerning the appropriateness of a particular use, users are advised to discuss the situation with their Supervisor, Manager or IT Division staff for guidance and direction.

The IT Division will include in its Cybersecurity Trainings elements of this policy in its efforts to build a robust awareness program. Users shall also be provided and comply with the Authority's ***Network and Data System Access Acknowledgment*** (Attachment 1).

10.1 **Compliance Measurement**

The IT Division team will verify compliance to this policy through various methods, including but not limited to; IT tools, internal and external audits, and reports, to include abuse and or noncompliance. Employees and users are expected to report suspected violations of this policy to the IT Division; their Supervisor or Manager; or the Internal Audit Office.

Potential, detected, or reported deviations from this policy will also be documented in the IT Division's ***IT Network Incident Form*** (Attachment 2).

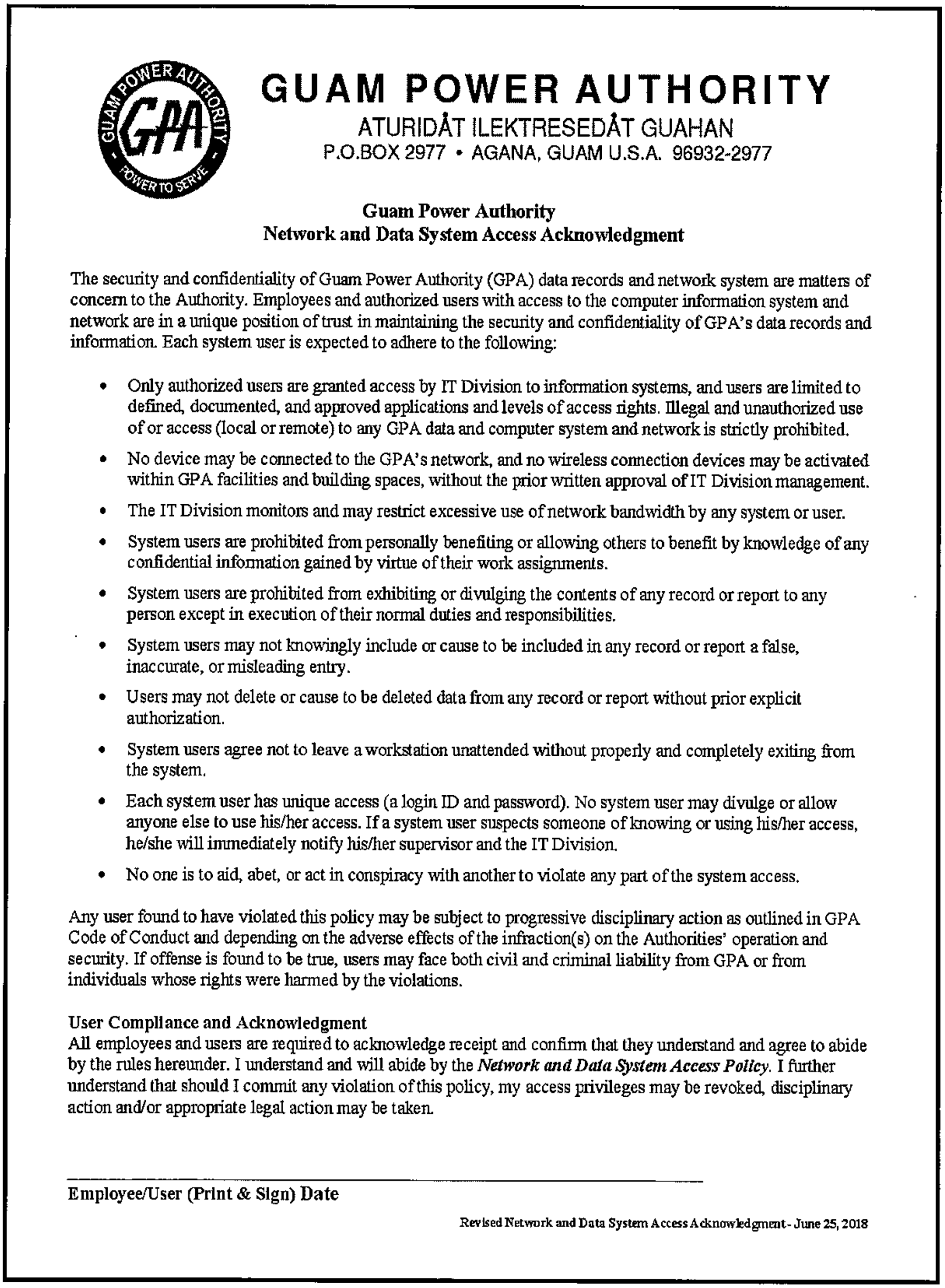
10.2 **Exceptions**

GPA IT Division acknowledges that under rare circumstances certain users may need to employ systems that are not compliant with the policies. All such instances must be reviewed and approved in advanced and in writing by the CITO.

10.3 **Non-Compliance**

Any user found to have violated this policy may be subject to progressive disciplinary action ranging from a verbal warning to dismissal or as outlined in the Authority's Codes of Conduct and depending on the severity and/or adverse effect(s) of the infraction(s) on GPA's operation and security. If offense is found to be true, users may be held personally liable for damages caused by any violations of this policy. Users may alaso face both civil and criminal liability from GPA or from individuals whose rights and information were harmed by the violation(s).

ATTACHMENT 1: System and Network Access Acknowledgment



GUAM POWER AUTHORITY
ATURIDÅT ILEKTRESEDÅT GUAHAN
P.O.BOX 2977 • AGANA, GUAM U.S.A. 96932-2977

Guam Power Authority
Network and Data System Access Acknowledgment

The security and confidentiality of Guam Power Authority (GPA) data records and network system are matters of concern to the Authority. Employees and authorized users with access to the computer information system and network are in a unique position of trust in maintaining the security and confidentiality of GPA's data records and information. Each system user is expected to adhere to the following:

- Only authorized users are granted access by IT Division to information systems, and users are limited to defined, documented, and approved applications and levels of access rights. Illegal and unauthorized use of or access (local or remote) to any GPA data and computer system and network is strictly prohibited.
- No device may be connected to the GPA's network, and no wireless connection devices may be activated within GPA facilities and building spaces, without the prior written approval of IT Division management.
- The IT Division monitors and may restrict excessive use of network bandwidth by any system or user.
- System users are prohibited from personally benefiting or allowing others to benefit by knowledge of any confidential information gained by virtue of their work assignments.
- System users are prohibited from exhibiting or divulging the contents of any record or report to any person except in execution of their normal duties and responsibilities.
- System users may not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.
- Users may not delete or cause to be deleted data from any record or report without prior explicit authorization.
- System users agree not to leave a workstation unattended without properly and completely exiting from the system.
- Each system user has unique access (a login ID and password). No system user may divulge or allow anyone else to use his/her access. If a system user suspects someone of knowing or using his/her access, he/she will immediately notify his/her supervisor and the IT Division.
- No one is to aid, abet, or act in conspiracy with another to violate any part of the system access.

Any user found to have violated this policy may be subject to progressive disciplinary action as outlined in GPA Code of Conduct and depending on the adverse effects of the infraction(s) on the Authorities' operation and security. If offense is found to be true, users may face both civil and criminal liability from GPA or from individuals whose rights were harmed by the violations.

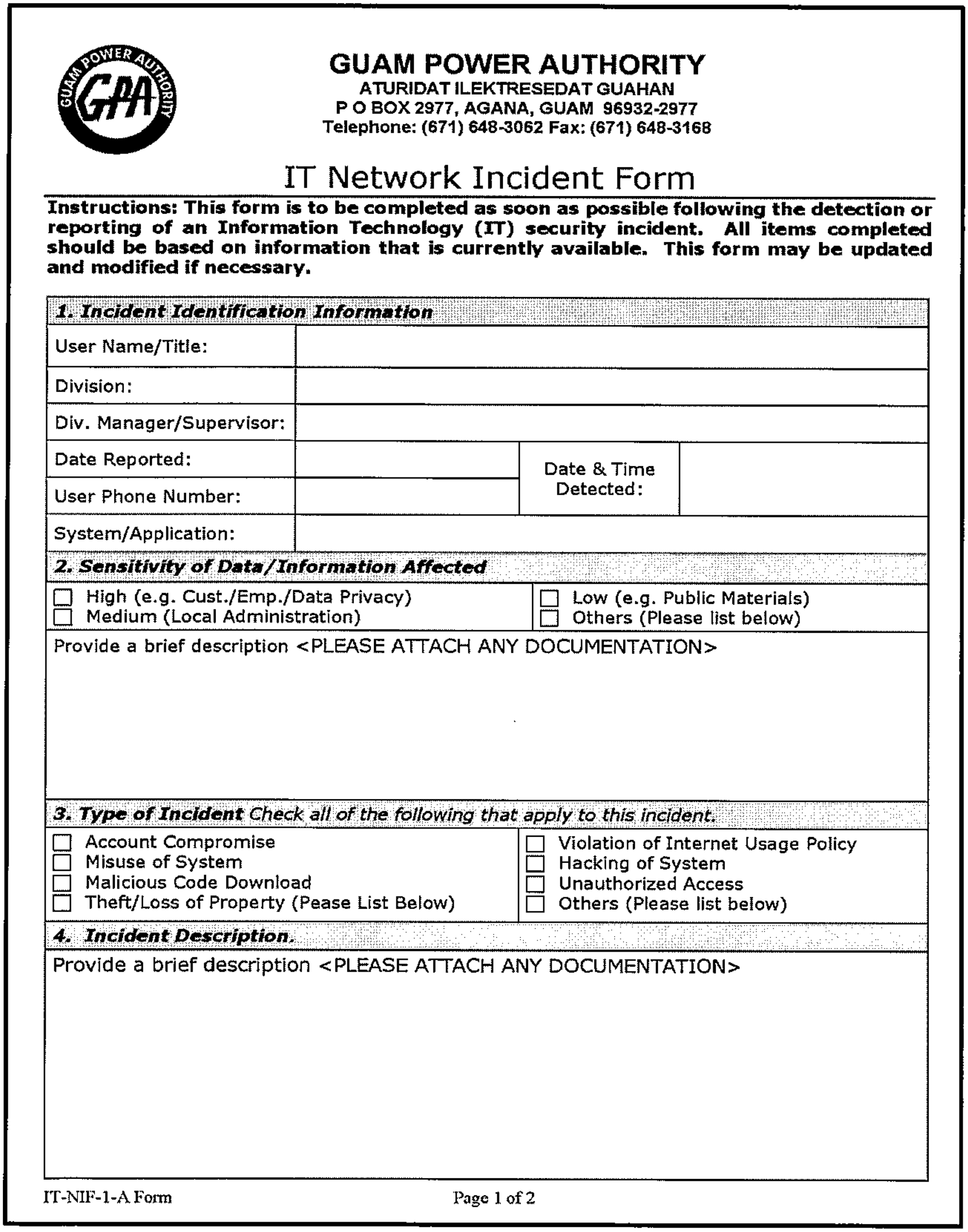
User Compliance and Acknowledgment
All employees and users are required to acknowledge receipt and confirm that they understand and agree to abide by the rules hereunder. I understand and will abide by the ***Network and Data System Access Policy.*** I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

____

Employee/User (Print & Sign) Date

Revised Network and Data System Access Acknowledgment - June 25, 2018

ATTACHMENT 2: IT Network Incident Form



GUAM POWER AUTHORITY
ATURIDAT ILEKTRESEDAT GUAHAN
P O BOX 2977, AGANA, GUAM 96932-2977
Telephone: (671) 648-3062 Fax: (671) 648-3168

IT Network Incident Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. Incident Identification Information

User Name/Title:			
Division:			
Div. Manager/Supervisor:			
Date Reported:		Date & Time Detected:	
User Phone Number:			
System/Application:			

2. Sensitivity of Data/Information Affected

□ High (e.g. Cust./Emp./Data Privacy)
□ Medium (Local Administration)
□ Low (e.g. Public Materials)
□ Others (Please list below)

Provide a brief description <PLEASE ATTACH ANY DOCUMENTATION>

3. Type of Incident *Check all of the following that apply to this incident.*

□ Account Compromise
□ Misuse of System
□ Malicious Code Download
□ Theft/Loss of Property (Pease List Below)
□ Violation of Internet Usage Policy
□ Hacking of System
□ Unauthorized Access
□ Others (Please list below)

4. Incident Description.

Provide a brief description <PLEASE ATTACH ANY DOCUMENTATION>

IT-NIF-1-A Form   Page 1 of 2

ATTACHMENT 2: IT Network Incident Form

5. What Steps Have Been Taken So Far? *Check all of the following that apply to this incident.*	
□ No action taken □ System Disconnected from network □ Updated virus definitions & scanned system	□ Restored backup from tape □ Log files examined (saved & secured) □ Other – please describe:
Provide a brief description <PLEASE ATTACH ANY DOCUMENTATION>	

6. Incident Details	
Has the incident been resolved?	□ YES □ NO □ PENDING
Approx. # of sites affected incident:	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5+
Approx. # of systems affected:	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5+
Approx. # of users affected incident:	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5+
Any additional information that is important but has not been provided elsewhere on this form.	

7. Remediation of Employee *(To be completed by the affected Division Supervisor/Manager)*
Provide a brief description <PLEASE ATTACH ANY DOCUMENTATION>

Investigated By

Name:______________________________Title:_______________________Date:___________

Concurred By:

_____________________________________ _____________________________________

IT Supervisor Date
<Please Print Name>

Division Supervisor/Manager Date
<Please Print Name>

cc: Human Resources
Internal Audit
Employee Division:_______________________