GUAM POWER AUTHORITY **STANDARD OPERATING PROCEDURE**	**Prepared By:** RUDOLPHO MANIBUSAN Computer Technician Supervisor
TITLE: Acceptable Use of Information Technology (Computer, Software, License, E-mail, Internet, and Standards of Conduct)	**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-110 **Supersedes: SP-110, dated 4/21/03** **Page 1 of 13**	**APPROVED BY:** **JOHN M. BENAVENTE, P.E.** **General Manager** **Dated:** 10/12/18

1.0 * PURPOSE OVERVIEW

Computer Uses, Software Licenses, E-Mail (tools) and Standards of Conduct policy serves the vital purpose of protecting the integrity of Guam Power Authority (GPA's) Computer systems, application software, storage and network infrastructure, as well as sheltering the authority from potential liability resulting from misuse, disclosure of private or confidential information. Such policies also places all users on notice that GPA's Information Technology (IT) Division will at any time, monitor, track and log employee use of all technology tools and resources provided. The purpose of this standard operating procedure is to outline the "*Acceptable Use of Information Technology*" owned, leased, and operated by and within Guam Power Authority.

All hardware, software, storage media, computer and network accounts, network and information infrastructures provided and supported by GPA's IT Division are charged with and designated administrators and custodians. These assets and resources are "*For Official User Only,*" in serving the interests of the Authority. Inappropriate use may expose GPA to risks such as liability, confidential information, malware, virus attacks, and compromise.

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, sub-contractors, consultants, vendors, volunteers, temporary, and other workers of the Authority ***(hereinafter referred to as "users")***. This policy provides guidelines for acceptable and unacceptable uses of:

i. Information Technology Resources:

   a. Computer systems (Desktops, Laptops, Tablets)

   b. Network Infrastructure

   c. Peripherals

   d. And any other Electronic Data Devices

ii. Software Applications and Licenses

iii. E-mail Accounts

iv. Internet Access

v. Security and Standards of Conduct

3.0 * RESPONSIBILITIES

3.1 *Chief Information Technology Officer (CITO) or designees, and IT Division* – The IT Division is led by the CITO or a designee, and is responsible for providing oversight, guidance, monitoring and compliance with GPA's Acceptable Use of Information, Technology resources and security programs. The team is also responsible for clarifying security controls.

3.2 *GPA Managers and Supervisors* – Managers and Supervisors must ensure all employees and users are informed of appropriate uses of GPA equipment and information technology resources.

3.3 *Users* – For the purpose of this policy, *Users* are ***all*** employees, board members, contractors, sub-contractors, consultants, vendors, temporary, volunteers, third party, and other workers of GPA that will or currently uses GPA owned, or leased IT resources. Users are accountable to adhere to authority policies, guidelines, standards, local and federal laws, and regulations.

It is the responsibility of every ***user*** to adhere to authority's policies and procedures and to conduct their activities accordingly. If and when users are confronted by a situation not covered by authority policies or procedures or they do not clearly apply to a situation, users are encouraged to clarify with their respective supervisor or officials with the IT Division.

This policy will be reviewed and updated by the IT Division personnel annually to ensure standards, business process, operational functions, requirements and/or regulatory compliances (if applicable) are met.

4.0 # POLICY & GUIDELINES

4.1 General Ownership and Privacy Expectation

GPA provides IT Resources to all employees to perform their jobs and tasks. Computer user profiles/accounts, data files and structures, E-mail accounts, and software are property of GPA and shall not to be changed, modified, moved, reassigned or deleted without the prior written approval of the CITO or a designee.

While some personal use of GPA Computer systems, email and other authority owned IT resources are realistically to be expected, users have no expectation of privacy using GPA owned or leased computer systems, peripheral devices, E-mail accounts, voice mail, and any other electronic data, application software or documents produced, stored or processed. Inspections, audits, and monitoring may be warranted to ensure compliance.

4.2 Computers, Peripherals, and Other Electronic Data Device Usage

4.2.1 Users shall protect and conserve GPA property:

a) Users must take every reasonable precaution to protect such resources from loss or damage.

b) Users shall not leave their computer systems unattended and unprotected without the utilization of a manual (Ctrl-Alt-Delete) or automated password-protected screensaver.

c) Users shall not install personal equipment and unauthorized software on GPA owned, leased or rented computer systems without the written prior approval from the CITO or a designee.

d) Users shall not change any security configuration settings on their assigned computer workstation.

4.2.2 Use of GPA computers, peripherals, other electronic data devices, and associated systems shall be used for authorized activities only.

4.2.3 Users are prohibited from using computers, peripherals, and other electronic data devices and associated systems to solicit or promote commercial ventures, religious activity or political causes.

4.2.4 Computers, peripherals, other electronic data devices and associated systems shall not be used to access, create, display, send or store messages, images, or content that would reasonably be considered offensive or disruptive.

4.2.5 The list of prohibited activities include but not limited to;

a) Conducting illegal activities, harassments, threats, phishing and SPAM.

b) Copyright Infringement.

c) Engaging in political or religious activities.

d) Accessing, downloading or uploading any material containing nudity or pornographic material.

e) Gambling, wagering, betting, or selling chances.

f) Engaging in any activity for personal gain or profit.

g) Revealing or publicizing proprietary or confidential information which is not authorized.

h) Making or posting improper remarks and/or proposals (*improper remarks* include but are not limited to, those which contain defamatory, false, inaccurate, abusive, obscene, profane, racially offensive, or discriminatory statements or material).

i) Installing or using network equipment such as routers, modems, and switches without the permission of the CITO or a designee.

j) Uploading, downloading or copying commercial software, music, movies, or other creative materials in violation of copyright law.

4.2.5 Only during Authority-sponsored events are users allowed to take Authority-owned computer equipment (i.e., monitors, desktop computers, printers) out of the Authority's premise, with the prior approval and coordination of the Division Manager and CITO or a designee.

4.3 Software and License Usage

Software purchasing will be centralized and will be the responsibility of the IT Division as authorized by the CITO or an official designee. The IT Division is responsible for the review, installation, storage, and inventory maintenance of the GPA software application requirements.

The IT Division reserves the right for access to be granted for computer audit without notice to validate against an inventory of licensed software and hardware. Any unlicensed software or hardware or illicit copies of documentation will be removed by an IT Division official and offender may be subjected to progressive disciplinary and/or legal action.

The following applies to all users using GPA software and licenses:

4.3.1 All software and application programs provided and available on GPA computers, peripherals and other electronic data devices, and associated systems are *"For Official Use Only"* in serving the interests of the Authority.

4.3.2 Only approved application software will be used on GPA computer systems or networks with a valid software licensing agreement and copyright compliant. All computer software will be purchased and used in accordance with publisher licensing agreement.

4.3.3 Illegal and unauthorized duplication of software, software licenses, computer programs or other copyrighted materials on GPA computers, peripherals, and other electronic data devices and associated systems is strictly prohibited.

4.3.4 Users are prohibited from adding application software into GPA computer systems, peripherals or electronic data devices. IT Division personnel are the only authorized personnel permitted to add or remove hardware, application software, or programs unless approved in writing by GPA's CITO or designee.

4.4 Electronic Mail (E-Mail) Usage

The Electronic Mail (E-Mail) is the electronic means of communications provided by GPA to facilitate communications between computer system users. Each user is responsible for maintaining the security of their issued E-mail account and to ensure precautions are taken to prevent unauthorized usage or access to account mailbox.

GPA Management reserves the right to access and disclose partial or all messages sent over GPA's E-mail system.

The following applies to all users using GPA E-mail system:

4.4.1 E-mail shall be used for matters directly related to GPA business activities. Any personal use must not interfere with normal business activities, must not be associated with any for-profit outside business activity, and must not potentially embarrass the Authority.

4.4.2 E-mail shall not be used for mass solicitation of others for commercial ventures, religious, or political causes, outside organization, or other non-GPA or governmental matters.

4.4.3 E-mail shall not be used to promote discrimination on the basis of age, disability, gender, race, religion, national origin, sexual preference, or any other classification protected by law.

4.4.4 E-mails sent via GPA mail systems shall not contain content that is deemed to be offensive. This includes, but not limited to, the use of vulgar or harassing videos, language, or images.

4.4.5 Users are prohibited from using their E-mail accounts to access copyrighted information in a way that violates the copyright.

4.4.6 Users are prohibited from sending confidential or private information or materials, trade secrets, or proprietary information via email messages.

4.4.7 Users are prohibited from accessing the email accounts of other employees. This is a violation of the Authority's ***Password Policy and Creation Policy (SOP-163).***

4.4.8 Users are prohibited from composing and/or sending chain letters, solicitations, or advertisements not related to the Authority's business purposes or activities.

4.4.9 Users **must** avoid opening any files or other attachments, including macros on an unsolicited E-mail message. ***Unsolicited E-mail messages are defined as any E-mail message received that was sent from an unknown, suspicious, or untrustworthy source(s).***

4.4.10 All users must remain alert to malicious software often transmitted via E-mail or digital media. It is imperative that employees exercise appropriate caution with their Email Account. Users should:

a) Avoid clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.").

b) Be suspicious of ***clickbait titles*** (e.g., "You won't believe this…", This will change your life…", "How one woman made $$$ in 1 day…", "Lose 20 pounds in 1 week with this simple product.").

c) Check email and names of sender of messages to ensure they are legitimate. If you are unsure or have any questions, contact the GPAHelpdesk for clarification.

d) Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, or excessive number of exclamation marks, legitimate web sites, legitimate email account).

4.5 Internet Usage

Use of the GPA Internet Services is permitted and encouraged where such use supports the mission, vision, goals and objectives of the Authority. Access to the Internet using GPA network and systems is a privilege, therefore, all users must adhere to all policies and procedures. GPA IT monitors, tracks, records, and logs all Internet activities and data and may conduct audits to protect against unauthorized use and to ensure functionality.

The following applies to all users accessing the Internet using GPA resources.

4.5.1 Users are expected to use the Internet responsibly and productively:

a) Internet access is intended for official business and job-related activities only and personal use should be limited to break time and must not violate any policies, rules, regulations, or local or federal laws.

b) Official business and job-related activities includes research and educational tasks that may be found in the Internet that would assist in an employee's role and responsibilities.

c) Videos viewed and/or downloaded may be monitored and/or blocked by IT Division officials if they are deemed to be harmful and/or hinder productivity.

4.5.2 The following are list of activities, which is not intended to be exhaustive, that are prohibited and are unacceptable use of the Internet:

a) Using the Internet for any purpose that violates local or federal laws or GPA rules, regulations, and policies.

b) Seeking, viewing, transmitting, collecting, or storing vulgar, abusive, discriminatory, obscene (including sexually explicit or pornographic materials), harassing messages or otherwise illegal materials.

c) Slander or harass others.

d) Corrupt or destroy another user's data.

e) Using Internet resources to download, copy, or pirate software and electronic files that are copyright protected or without authorization.

f) Transmitting confidential, private material, trade secrets, or proprietary information outside of the organization.

g) Solicitations or advertisements not related to the Authority's business purposes or activities.

h) Hacking into unauthorized websites or other computer systems.

i) Sending or posting information that is defamatory to GPA, its products/services, employees, contractors, sub-contractors, vendors, and/or customers on social networking or any online publishing sites.

j) Introducing malicious software onto GPA networks and/or jeopardizing the security of the organization's electronic communication systems.

k) Representing GPA in an official capacity when not authorized to do so.

5.0 **# SECURITY & STANDARD OF CONDUCT**

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

5.1 Users are prohibited from intentionally circumventing security mechanisms such as cracking passwords, exploiting system vulnerabilities, or using systems in excess of granted privileges.

5.2 For security and network maintenance purposes, the GPA IT Division shall monitor, track, and log systems and network traffic at any time. If a user is unsure about what constitutes Acceptable Computer and Internet Usage, they should consult their supervisor/manager or the IT Division for further clarification and guidance.

6.0 # POLICY ENFORCEMENT & COMPLIANCE

Violation of this policy may result in limiting or revoking access to computer systems, associated systems, and other electronic data devices, Internet access, E-mail use, etc. in addition to other disciplinary action determined to be appropriate by management. 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 the IT Division for guidance and direction.

The IT Division will include in its Cybersecurity Trainings elements of this policy in its awareness program initiatives. Users shall also be provided and comply with the Authority ***Computer, Internet, and E-mail Usage Policy Compliance & Acknowledgment*** (Attachment 1).

6.1 Compliance Measurement

The IT Division will verify compliance to this policy through various methods, including but not limited to, IT tools; monitors, logs and tracking reports, internal and external audits, and reports of abuse or noncompliance. Employees and users are expected to report suspected violations of this policy to the Information Technology 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), and offender may be subjected to progressive disciplinary action.

6.2 Exceptions

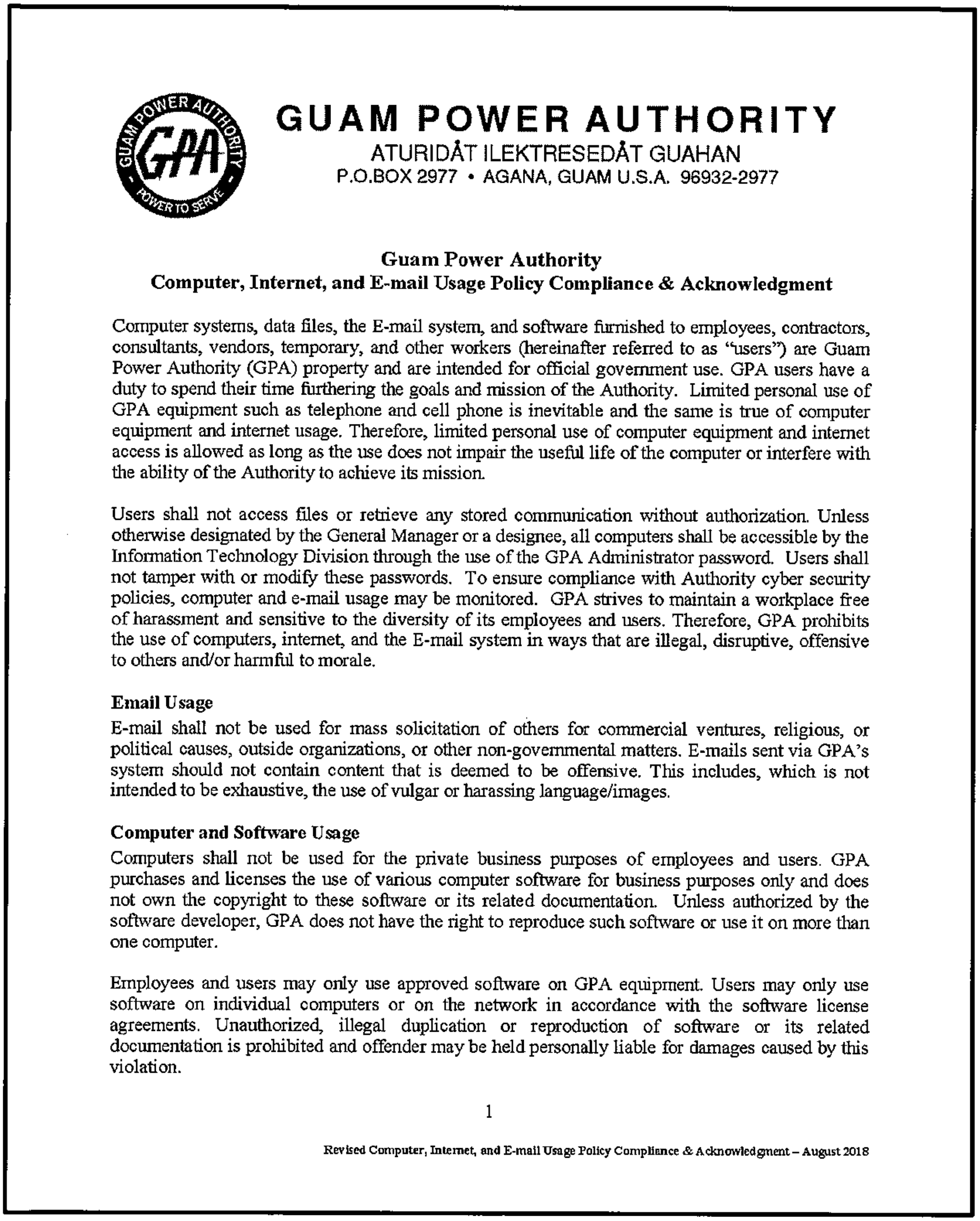
Any exception to the policy requirements must have written prior approval from the General Manager , with the concurrence of the Assistant General Manager, Engineering and Technical Services (AGMETS), and the CITO or a designee.

6.3 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 GPA Codes of Conduct depending on the severity and/or adverse effect(s) of the infraction(s) on the Authority's operation and security.

If found true, users may be held personally liable for damages caused by any violations of this policy. Users may face both civil and criminal liability from GPA or from individuals whose rights were harmed by the violation(s). For instance, penalties for copyright infringement include civil and criminal penalties. Anyone found liable for civil copyright violation may be ordered to pay either actual damages or statutory damages not less than $750 and not more than $300,000 per work infringed. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. Source: https://www.copyright.gov/title17/92chap5.html

ATTACHMENT 1: Computer, Internet, and E-mail Usage Policy Compliance & Acknowledgment Form



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

Guam Power Authority
Computer, Internet, and E-mail Usage Policy Compliance & Acknowledgment

Computer systems, data files, the E-mail system, and software furnished to employees, contractors, consultants, vendors, temporary, and other workers (hereinafter referred to as "users") are Guam Power Authority (GPA) property and are intended for official government use. GPA users have a duty to spend their time furthering the goals and mission of the Authority. Limited personal use of GPA equipment such as telephone and cell phone is inevitable and the same is true of computer equipment and internet usage. Therefore, limited personal use of computer equipment and internet access is allowed as long as the use does not impair the useful life of the computer or interfere with the ability of the Authority to achieve its mission.

Users shall not access files or retrieve any stored communication without authorization. Unless otherwise designated by the General Manager or a designee, all computers shall be accessible by the Information Technology Division through the use of the GPA Administrator password. Users shall not tamper with or modify these passwords. To ensure compliance with Authority cyber security policies, computer and e-mail usage may be monitored. GPA strives to maintain a workplace free of harassment and sensitive to the diversity of its employees and users. Therefore, GPA prohibits the use of computers, internet, and the E-mail system in ways that are illegal, disruptive, offensive to others and/or harmful to morale.

Email Usage

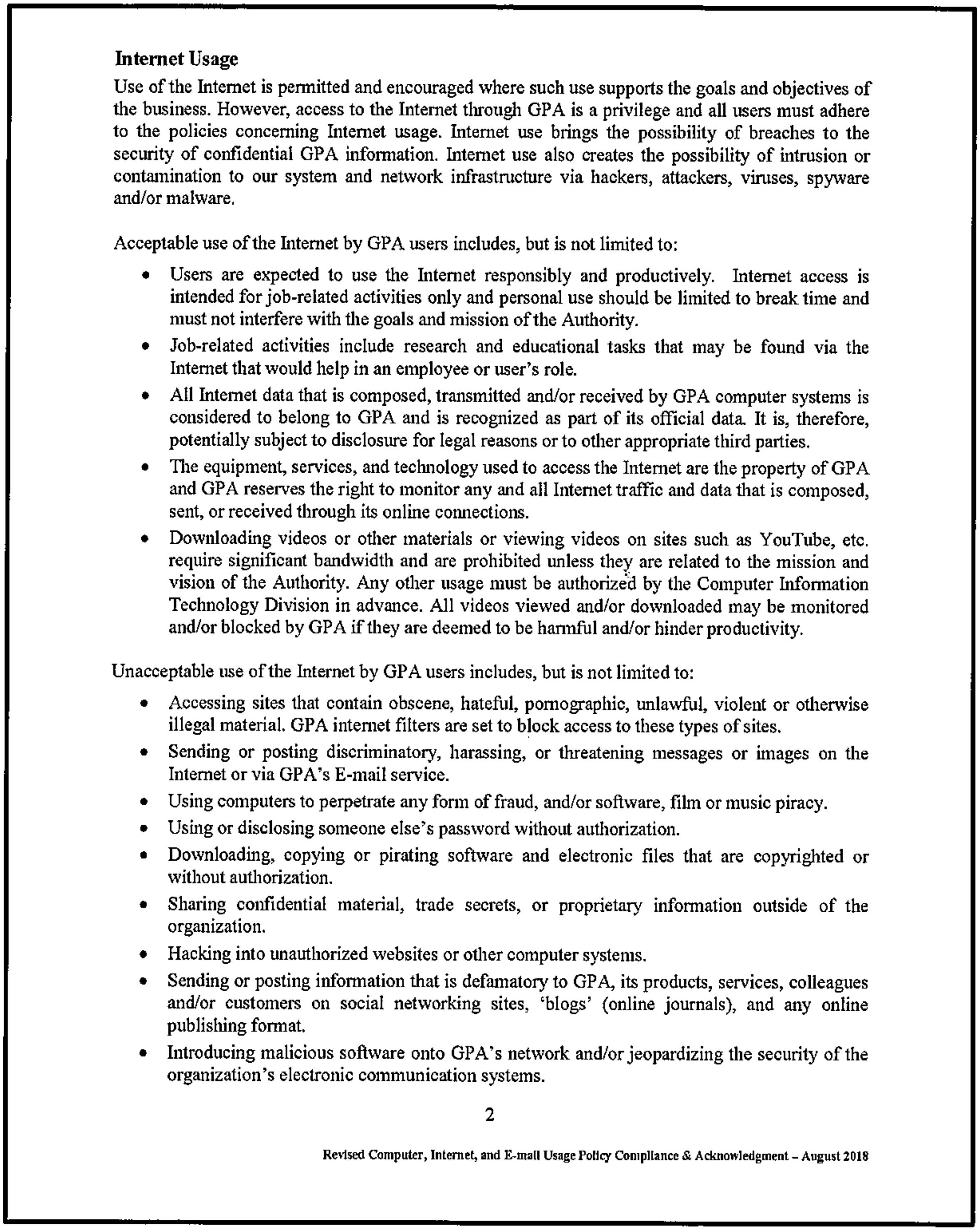
E-mail shall not be used for mass solicitation of others for commercial ventures, religious, or political causes, outside organizations, or other non-governmental matters. E-mails sent via GPA's system should not contain content that is deemed to be offensive. This includes, which is not intended to be exhaustive, the use of vulgar or harassing language/images.

Computer and Software Usage

Computers shall not be used for the private business purposes of employees and users. GPA purchases and licenses the use of various computer software for business purposes only and does not own the copyright to these software or its related documentation. Unless authorized by the software developer, GPA does not have the right to reproduce such software or use it on more than one computer.

Employees and users may only use approved software on GPA equipment. Users may only use software on individual computers or on the network in accordance with the software license agreements. Unauthorized, illegal duplication or reproduction of software or its related documentation is prohibited and offender may be held personally liable for damages caused by this violation.

ATTACHMENT 1: Computer, Internet, and E-mail Usage Policy Compliance & Acknowledgment Form



Internet Usage

Use of the Internet is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through GPA is a privilege and all users must adhere to the policies concerning Internet usage. Internet use brings the possibility of breaches to the security of confidential GPA information. Internet use also creates the possibility of intrusion or contamination to our system and network infrastructure via hackers, attackers, viruses, spyware and/or malware.

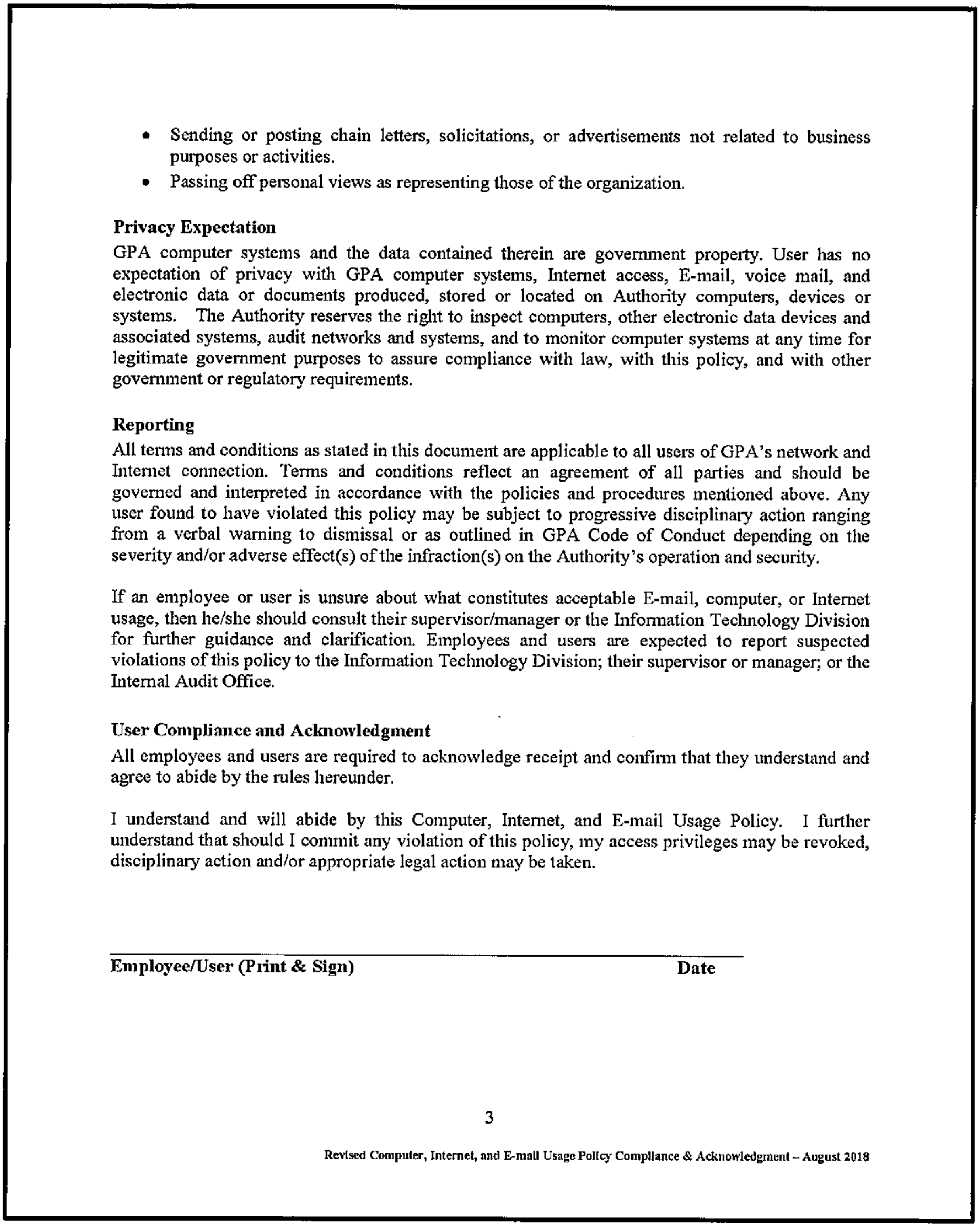
Acceptable use of the Internet by GPA users includes, but is not limited to:

- Users are expected to use the Internet responsibly and productively. Internet access is intended for job-related activities only and personal use should be limited to break time and must not interfere with the goals and mission of the Authority.
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee or user's role.
- All Internet data that is composed, transmitted and/or received by GPA computer systems is considered to belong to GPA and is recognized as part of its official data. It is, therefore, potentially subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services, and technology used to access the Internet are the property of GPA and GPA reserves the right to monitor any and all Internet traffic and data that is composed, sent, or received through its online connections.
- Downloading videos or other materials or viewing videos on sites such as YouTube, etc. require significant bandwidth and are prohibited unless they are related to the mission and vision of the Authority. Any other usage must be authorized by the Computer Information Technology Division in advance. All videos viewed and/or downloaded may be monitored and/or blocked by GPA if they are deemed to be harmful and/or hinder productivity.

Unacceptable use of the Internet by GPA users includes, but is not limited to:

- Accessing sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal material. GPA internet filters are set to block access to these types of sites.
- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via GPA's E-mail service.
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy.
- Using or disclosing someone else's password without authorization.
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.
- Sharing confidential material, trade secrets, or proprietary information outside of the organization.
- Hacking into unauthorized websites or other computer systems.
- Sending or posting information that is defamatory to GPA, its products, services, colleagues and/or customers on social networking sites, 'blogs' (online journals), and any online publishing format.
- Introducing malicious software onto GPA's network and/or jeopardizing the security of the organization's electronic communication systems.

ATTACHMENT 1: Computer, Internet, and E-mail Usage Policy Compliance & Acknowledgment Form



- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the organization.

Privacy Expectation

GPA computer systems and the data contained therein are government property. User has no expectation of privacy with GPA computer systems, Internet access, E-mail, voice mail, and electronic data or documents produced, stored or located on Authority computers, devices or systems. The Authority reserves 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.

Reporting

All terms and conditions as stated in this document are applicable to all users of GPA's network and Internet connection. Terms and conditions reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. 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 GPA Code of Conduct depending on the severity and/or adverse effect(s) of the infraction(s) on the Authority's operation and security.

If an employee or user is unsure about what constitutes acceptable E-mail, computer, or Internet usage, then he/she should consult their supervisor/manager or the Information Technology Division for further guidance and clarification. Employees and users are expected to report suspected violations of this policy to the Information Technology Division; their supervisor or manager; or the Internal Audit Office.

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 this Computer, Internet, and E-mail Usage 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.

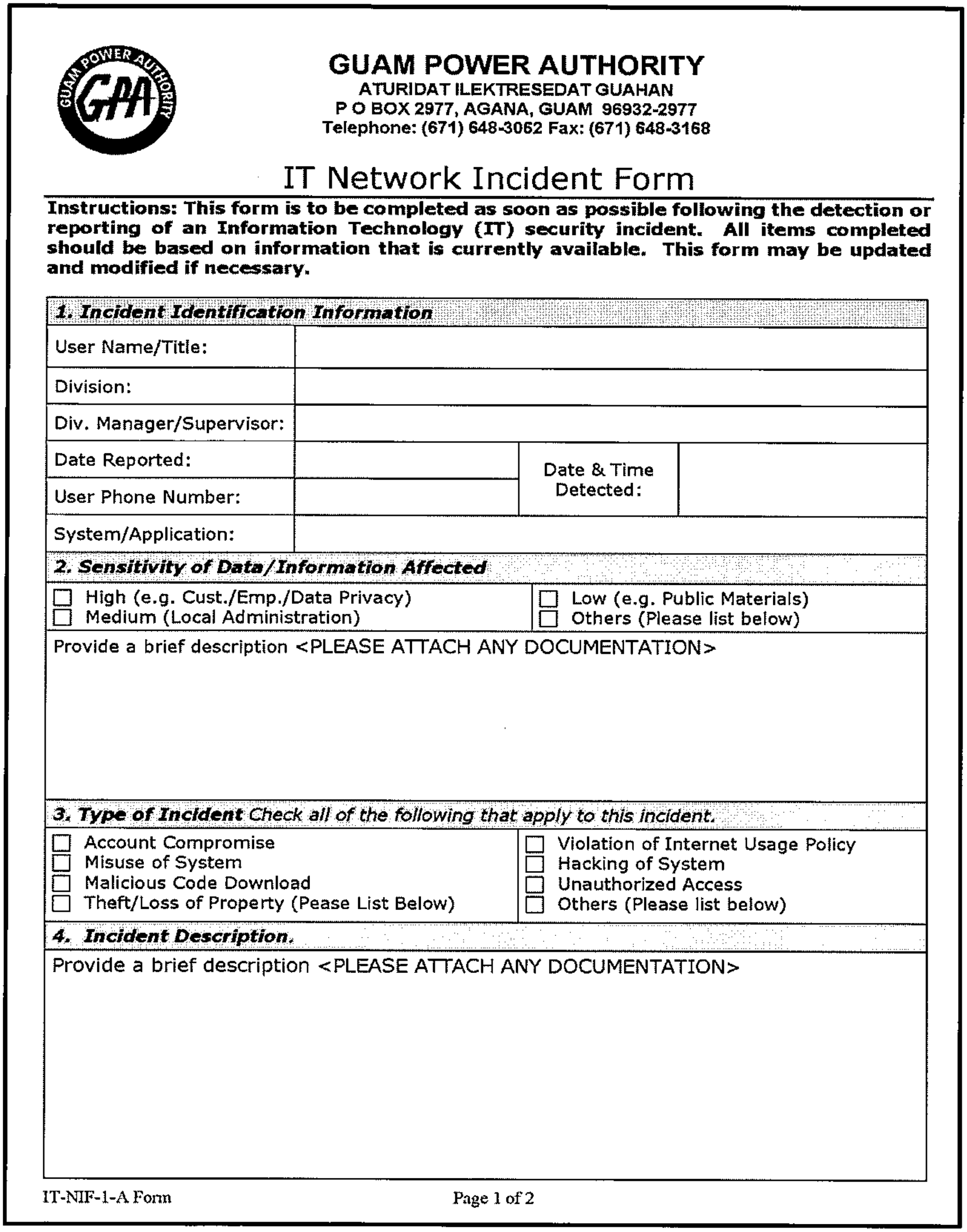
____

Employee/User (Print & Sign) **Date**

3

Revised Computer, Internet, and E-mail Usage Policy Compliance & Acknowledgment – August 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	□ Restored backup from tape
□ System Disconnected from network	□ Log files examined (saved & secured)
□ Updated virus definitions & scanned system	□ 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:________________________