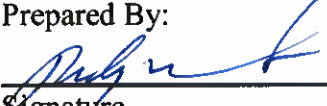

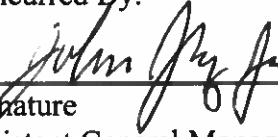



<p align="center">GUAM POWER AUTHORITY</p> <p align="center">STANDARD OPERATING PROCEDURE</p>	<p>Prepared By: _____</p> <p> /Rudy Manibusan</p> <p>Signature _____ Print _____</p> <p>Computer Technician Supervisor</p>
<p>TITLE: Information/Data Classification, Impacts, and Responsibilities</p>	<p>Reviewed By: _____</p> <p> /Melvyn Kwek</p> <p>Signature _____ Print _____</p> <p>Chief Information Technology Officer</p>
<p>NO: <u>SOP-142</u></p> <p>Supersedes: _____ Dated _____</p>	<p>Concurred By: _____</p> <p> /John J. Cruz, Jr., P.E.</p> <p>Signature _____ Print _____</p> <p>Assistant General Manager, Engineering & Technical Services</p>
<p>Page <u>1</u> of <u>8</u></p>	<p>Approved By: _____</p> <p> / 8/28/19</p> <p>John M. Benavente, P.E. DATED</p> <p>General Manager</p>

1.0 PURPOSE OVERVIEW

The purpose of this policy is to address the securing of the production, processing, storage, and transmission of information regardless of media type, (Hard Disk, USB device or paper, aka Hard Copy), and or electronic data (soft copy), (transmitted/transferred over the Internet or E-Mail) and the disposal of the hard copy or soft copy of the Guam Power Authority (GPA or Authority).

The policy defines the hierarchical classification of data classification, guide to identify sensitive information, information protection measures, potential risks and impact, information assets responsibilities, and limitations on rights to inspect public records. The policy also provides guidance to GPA management, security and compliance personnel responsible for handling sensitive information.

2.0 SCOPE & REGULAR POLICY REVIEW

This policy applies to **all** employees, board members, contractors, consultants, vendors, volunteers, temporary, and other workers of the Authority. This policy establishes a framework and basis as it applies to making information available to others within our organization as well as those outside our organization, to include those who handle sensitive information given to them from other government agencies, companies or individuals. The policy shall be applied to all

CODES:

* REVISED

ADDED

information or data that is created, collected, stored or processed by GPA either in electronic form (soft copy) or non-electronic format (hard copy).

It is important for all to keep this Information/Data Classification Policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues, technologies and regulations. This policy is a living document that will be reviewed annually and/or updated as needed. The Chief Information Technology Officer (CITO) or a designee, together with Internal Auditor shall regularly review, at least once a year, this policy to ensure that the policy is up to par with regulatory requirements, applicable laws, and the Authority's operations.

3.0 DEFINITIONS

Information may appear in many forms, including reports, brochures and other promotional materials, Internet web sites, on-line documents, automated information, and public records. GPA has proprietary information which it deems sensitive in nature and requires levels of protection from inappropriate or inadvertent disclosure.

- 3.1 Sensitive Information – Refers to any data or information that could be used by those intending to target either electric, water or waste water sector critical infrastructure, damage facilities, disrupt operations, or harm individuals.
- 3.2 Critical Infrastructure – Provides the essential services that serve as the backbone of the island's economy, security, and health. We know it as the electricity we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family.

4.0 GUIDE TO IDENTIFY SENSITIVE INFORMATION

As a business process, it is important for the Authority to evaluate and identify information as sensitive as it relates to the production, processing, storage, transmission, and disposal, as well as the conditions for permitted disclosures. The following questions will help identify potentially Sensitive Information:

- 4.1 As it relates to GPA critical assets, key facilities, or systems, does the information contain operational procedures, lists relating to critical assets and identified critical cyber assets, network topology or similar diagrams, floor plans of computing centers that contain critical cyber assets, equipment layouts of critical cyber assets, disaster recovery plans, incident response plans, and security configuration information?
- 4.2 What will be the impact on critical assets, key facilities, IT and Operational systems will the information have if it inadvertently reached an unintended audience?

- 4.3 Does the information contain personal details of key operating personnel such as biographical data, contact information, names, addresses, telephone numbers, etc.?
- 4.4 Could someone intent on causing harm to personnel or critical assets, key facilities, and systems use the information to his or her advantage?

5.0 **INFORMATION PROTECTION MEASURES**

Information protection goals can be obtained from various sources. For example, an organization's security policy, organizational structure, and informal data segregation approaches. This information may also come from technical support teams, information owners, information custodians, module owners and managers. There may also be regulatory and legal requirements to consider.

- 5.1 **Authentication** – The most common safeguard for confidentiality is the requirement for authentication. Authentication helps to ensure that an individual authorized is identified. Authentication usually requires that an individual provide a UserID and password. More sophisticated authentication technologies are available such as Two Factor Authentication or Eye Retina or Finger Print Scans or Facial Recognition.
- 5.2 **Role Based** – Another common information safeguard is based on business and job function. This approach implies that access is defined by roles and privileges. Information owner, custodian or manager, validates and authorizes business need.
- 5.3 **Encryption** – Encryption formats information so that it cannot be inappropriately viewed or altered without detection. Login processes and most financial transactions are commonly encrypted. This mechanism can be used to ensure privacy of sensitive or personal information as well. Creative deployment of encryption technology may help to ensure confidential information in various formats is consistently protected.
- 5.4 **Technological Control** – There are technology specific controls like virus protection; disk, system and application redundancy; and network segregation.
- 5.5 **Assurance** – Validating that systems are safeguarded are also a level of protection. Examples are policy compliance monitoring, code walkthroughs, intrusion detection, system performance monitoring, transactional monitoring, administrative monitoring, and file access monitoring.

6.0 **INFORMATION/DATA CLASSIFICATION GUIDELINES**

All information processed, stored, transmitted and or transferred within GPA shall be assigned one of the following classifications. Collections of diverse

information shall be classified as to the most secure classification level for information component.

6.1 **RESTRICTED (Confidential)**

GPA information or Data regarding critical assets, key facilities, and systems maintaining the reliability and security of GPA may require secure restrictions in its access, production, processing, sharing, handling, storage, transmission and distribution, replication, and destruction procedures and is not shared with other entities or affiliates. Inadvertent or unauthorized disclosure or modification could severely impact GPA's infrastructure. For example, results of engineering studies showing system weakness or vulnerabilities within the electrical or power generation systems; or information or data protected by local or federal privacy regulations and confidentiality agreements.

Restricted: The unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to GPA and or its affiliates: employees (permanent, temporary, unclassified), customers, vendors, contractors, sub-contractors, and visitors.

The highest level of security controls shall be applied to Restricted data.

6.2 **COMPANY (Internal Use, Private)**

Data or information regarding critical assets, key facilities, and systems maintaining the reliability and security of GPA may require protective measures in its access, production, processing, sharing, handling, storage, replication or destruction of information. Inadvertent or unauthorized disclosure or modification could adversely impact GPA's infrastructure. For example, detailed drawings of electrical power and distribution system, detailed drawings of building facilities or detailed drawings of network layout and critical network devices.

Private: The unauthorized disclosure, alteration or destruction of information or data could result in a moderate level of risk to GPA or its affiliates: employees (permanent, temporary, unclassified), customers, vendors, contractors, sub-contractors, and visitors.

By default, all GPA information or data that is not explicitly classified as Restricted or Public data shall be treated as Private, Internal User Information or data only.

6.3 **PUBLIC**

Information or data lawfully, properly and regularly disclosed broadly to the public requiring no restrictions in producing, processing, handling, storing,

distributing, replicating or destroying information. Disclosure will not adversely impact GPA and or the critical infrastructure. For example, the physical location of a critical asset without any designation of criticality i.e., address of the building of a new substation, marketing brochures, and public and customer notices and updates

Public: The disclosure, alteration or destruction of data that results in little or no risk to the Authority and its affiliates: employees (permanent, temporary, unclassified), customers, vendors, contractors, sub-contractors, and visitors.

7.0 DATA DEFINITION AND RISK OF POTENTIAL IMPACT LEVELS

7.1 Below are data definitions over the Authority's information assets.

- a) Confidentiality – Preserving authorized restriction of information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of **confidentiality** is the unauthorized disclosure of information.
- b) Integrity – Guard against improper information modifications or destruction and includes ensuring information non-repudiation and authenticity. A loss of **integrity** is the unauthorized modification or destruction of information.
- c) Availability – Ensuring timely and reliable access to and use of information. A loss of **availability** is the disruption of access to or use of information or an information system.

7.2 Below presents potential risk and impacts if data are compromised based on data definition.

- a) High – The potential impact is **high** if the loss of confidentiality, integrity, or availability has and could have a severe or catastrophic adverse effect on the Authority's operations, assets, personnel and or individuals.

Example: The loss of confidentiality, integrity, or availability might: cause a severe degradation in or loss of mission capability to an extent and duration that GPA is not able to perform one or more of its primary functions; result in major damage to organizational assets; result in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

- b) Moderate – The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on the Authority's operations, assets, personnel and or individuals.

Example: The loss of confidentiality, integrity, or availability might: cause a significant degradation in operational capability to an extent and

duration that GPA is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; result in significant damage to the authority's assets; result in significant financial loss; or result in significant harm to personnel and or individuals that does not involve loss of life or serious life threatening injuries.

- c) Low – The potential impact is *low* if confidentiality, integrity and availability have limited adverse effect on the authority's operations, assets, personnel and or individuals.

Example: The loss of confidentiality, integrity and availability might: cause a degradation in operational capacity to an extent and duration that GPA is able to perform its primary functions. But the effectiveness of the function is noticeably reduced, result in minor damage to the authority's assets, result in minor financial loss, result in minor harm to personnel or individuals.

8.0 INFORMATION ASSETS RESPONSIBILITIES

All existing GPA information shall belong to one of the classifications outlined in Sections 6.1 – 6.3 of this policy.

- 8.1 Information is classified, and may be reclassified, by the information owner and/or appropriate division manager.
- 8.2 Information owners are responsible for appropriately classifying the information. They are also responsible for ensuring compliance to this policy within their area of responsibility.
- 8.3 Information custodians are responsible for labeling information with the appropriate classification and application of required safeguards.
- 8.4 Information users or individual staff members are responsible for complying with the information requirements and ensuring sensitive information appropriately protected and labeled with appropriate classifications.
- 8.5 Particular care should be exercised when using mobile devices, such as laptops, tablets, USB keys, and mobile phones to access/store confidential information. The size, and ease with which such devices can be transported, increases the potential risk of data disclosure/loss. Such a loss can potentially have a severe or catastrophic adverse effect on GPA's operations, assets, or on individuals.
- 8.6 For guidance and procedures relative to the release and dissemination of information to various media, the general public, and outside individuals or groups, please refer to SOP-054 relative to *Release of Information to Media and General Public*.

9.0 FREEDOM OF INFORMATION ACT

All GPA information and or records are subject to the *Freedom of Information Act* (FOIA) or Sunshine Reform Act of 1999, codified at Title 5 Guam Code Annotated Chapter 10. The FOIA provides that every person has the right to inspect and take a copy of any public document on Guam, except as otherwise expressly prohibited in law.

- 9.1 Upon request of copy of public records, agencies shall comply with the request within four (4) working days from receipt of the request if the records are disclosable public records in the possession of the agency.
- 9.2 In unusual circumstances, the time limit may be extended up to ten (10) calendar days, including Saturdays, Sundays and legal holidays, by written notice by the director of the agency or the director's designee to the person making the request.
- 9.3 Below are limitations on the right to inspect pursuant to the FOIA law:
 - a) Records pertaining to pending litigation to which the agency is a party, until the pending litigation has been finally adjudicated or settled.
 - a) Records of complaints to, or investigations conducted by, or records of intelligence information, or security procedures or information, of an agency or its personnel.
 - b) Personnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy. All information regarding salary, and the name, and worksite mailing address of each employee and public official shall be public record.
 - c) Test questions, scoring keys and other examination data used to administer a licensing examination, examination for employment, or academic examination.
 - d) The home address and telephone number of any person whose occupation is subject to regulation or licensure by the government of Guam, or of any public official or government employee, or of any member of a government board, commission, or council, unless such person gives express permission to disclose such information.
 - e) All existing privileges or confidential records or other information expressly protected under the law.
 - f) Records specifically pertaining to security procedures, passwords, combinations, access codes, electronic or computer user I.D.s, policies or procedures on security.
- 9.4 Below are records exempted from FOIA as established by the United States Congress. Details on these nine exceptions can be found at <https://www.foia.gov>.
 - a) Exemption 1: Information that is classified to protect national security

- b) Exemption 2: Information related solely to the internal personnel rules and practices of an agency.
- c) Exemption 3: Information that is prohibited from disclosure by another federal law.
- d) Exemption 4: Trade secrets or commercial or financial information that is confidential or privileged.
- e) Exemption 5: Protects the integrity of the deliberative or policy-making processes within the agency by exempting from mandatory disclosure opinion, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. Examples are attorney-work product privilege and attorney-client privilege.
- f) Exemption 6: Information that, if disclosed, would invade another individual's personal privacy.
- g) Exemption 7: Information compiled for law enforcement purposes that could: (1) reasonably be expected to interfere with enforcement proceedings; (2) deprive a person of a right to a fair trial or an impartial adjudication; (3) reasonably be expected to constitute an unwarranted invasion of personal privacy; (4) reasonably be expected to disclose the identity of a confidential source; or (5) reasonably be expected to endanger the life or physical safety of any individual.
- h) Exemption 8: Information that concerns the supervision of financial institutions.
- i) Exemption 9: Geological information on wells.

10.0 **COMPLIANCE AND REPORTING**

Where guidance or interpretation of this policy is needed, employees are advised to discuss the situation with their immediate supervisor/manager, the Public Information Office, or Legal Counsel for proper guidance and direction prior to release of any requested information.

Anyone who has reason to suspect a deliberate and/or willful violation of this policy must promptly report it to their immediate supervisor, manager, CITO, or the Internal Audit Office. Policy violations will be assessed and action taken to remediate the violation accordingly. Any employee found to have willfully violated this policy 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.