


**JUDICIARY OF GUAM
POLICY AND PROCEDURES
ADMINISTRATIVE POLICY NO. UJ 22-04**

 Judiciary of Guam	Division: ADMINISTRATIVE OFFICE OF THE COURTS
TITLE: Personal Identifiable Information Policy	EFFECTIVE DATE: February 15, 2022
REVISED DATE:	APPROVED BY: <i>Kristina L. Baird</i> Kristina L. Baird, Administrator of the Courts

I. PURPOSE

The Judiciary of Guam (“Judiciary”) recognizes the need to maintain the confidentiality of Personally Identifiable Information and understands that such information is unique to each individual. This Policy provides internal guidance only and does not create any rights enforceable in law or otherwise.

II. SCOPE

This policy applies to all employees who (1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of Personally Identifiable Information (as defined below) in connection with their job duties at the Judiciary. This policy does not protect the privacy or confidentiality of any information that is required by law or court order to be public or otherwise distributed.

III. DEFINITIONS

- A. Personally Identifiable Information (“PII”):** PII means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational

credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual. *See* 2 CFR § 200.79.

B. Protected PII: An individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed. *See* 2 CFR § 200.82.

C. Federal Information System: An information system used or operated by a federal agency or by a contractor of a federal agency or by another organization on behalf of a federal agency. *See* OMB Circular A-130.

D. Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. *See* OMB Memorandum M-17-12.

E. Data Access: The Judiciary maintains multiple systems where PII data may reside; thus, user access to such systems is the responsibility of the Judiciary's Management Information Systems ("MIS") division. MIS has created internal controls for such systems to establish legitimate access for users of data, and access shall be limited to those approved by MIS. Any change in vendor status or the termination of an employee or independent contractor with access will result in the termination of the user's access to all systems where the PII may reside.

IV. POLICY

Disseminating non-public, sensitive information about Judiciary matters could violate federal and/or local laws and individual privacy rights; put a witness or law enforcement officer in danger; prejudice the rights of a litigant; or unfairly damage the reputation of a person.

Judiciary personnel should presume that non-public, sensitive information obtained in connection with work is protected from disclosure, except as needed to fulfill official duties of Judiciary personnel, and as allowed by court order, statutory or regulatory prescription, or case law and rules governing criminal and civil discovery. Other than as necessary to fulfill Judiciary official duties, disclosure of such information to anyone, including to family members, friends,

or even colleagues, is prohibited and could lead to disciplinary action. Unauthorized disclosures of sensitive personal or proprietary information could lead to criminal prosecution or administrative action.

V. DATA TRANSMISSION AND TRANSPORTATION

- A. Judiciary Premises Access to PII:** The specific Judiciary divisions which obtain PII shall identify their particular responsibilities for on-site access of data that may include access to PII; MIS has the oversight responsibility for all electronic records and data access capabilities. Individual divisions have the operational responsibility for designating initial access and termination of access for individual users within their divisions and providing timely notice to MIS.

- B. Vendors:** The Judiciary may share data with vendors who have a business need to have PII data. Where such inter-organization sharing of data is required, MIS is responsible for creating and maintaining data encryption and protection standards to safeguard all PII data that resides in the databases provided to vendors. Approved vendor lists will be maintained by the Judiciary's Procurement division, which has the responsibility to notify MIS of any changes to vendor status with the Judiciary.

- C. Portable Storage Devices:** The Judiciary reserves the right to restrict PII data it maintains in the workplace. In the course of doing business, PII data may also be downloaded to laptops or other computing storage devices to facilitate Judiciary business. To protect such data, the Judiciary will also require that any such devices use MIS-approved encryption and security protection software while such devices are in use on or off Judiciary premises. MIS has the responsibility for maintaining data encryption and data protection standards to safeguard PII data that resides on these portable storage devices.

- D. Off-Site Access to PII:** The Judiciary understands that employees may need to access PII while off-site or on business travel, and access to such data shall not be prohibited, subject to the provision that the data to be accessed is minimized to the degree possible to meet business needs.

VI. RESPONSIBILITIES

Judiciary employees are regularly required to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII in order to execute their job duties. It is the responsibility of individual divisions within the Judiciary to evaluate and determine the confidentiality requirements of the various data handled by that division's employees. The confidentiality requirements of various PII is based on its level of sensitivity and the impact on the Judiciary should that information be disclosed, altered, or destroyed without authorization. The

confidentiality of information may also be affected by relevant laws which may explicitly require certain information to be either confidential or public.

All electronic files that contain Protected PII will reside within a protected information system location, as approved by MIS. All physical files that contain Protected PII will reside within a locked/secured/monitored location when not being actively viewed or modified. PII will also not be sent through any form of insecure electronic communication e.g. e-mail or instant messaging systems. Significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded, securely deleted, or disposed of by a means that renders the information unrecognizable and beyond reconstruction.

VII. BREACH RESPONSE

Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, the MIS Administrator or his/her designee will complete the Reporting Form on Actual or Imminent Breach of PII or PPII (Attachment A). The Judiciary will transmit this form to a Program Manager at the Office of Justice Programs no later than twenty-four (24) hours after an occurrence of an actual breach or the detection of an imminent breach. Additionally, the Judiciary shall provide notice as required by 9 GCA § 48.30 in the event of a breach as defined under that law.

The Judiciary Staff Attorneys will handle breach notifications(s) to all governmental agencies to whom such notice must be provided in accordance with time frames specified under applicable law.

VIII. REGULATORY REQUIREMENTS

It is the policy of the Judiciary to comply with any international, federal or local statute and reporting regulations, particularly 9 GCA Chapter 38, Notification of Breaches of Personal Information. The Judiciary has delegated the responsibility for maintaining PII security provisions to the divisions noted in this policy. The Judiciary's Staff Attorneys shall be responsible for overseeing all regulatory reporting compliance issues. If any provision of this policy conflicts with a statutory requirement of international, federal or local law governing PII, the policy provision(s) that conflict shall be superseded.

IX. INTERNAL REPORTING

If an employee has reason to believe that PII data security has been breached or that Judiciary employees and/or representative(s) are not adhering to the provisions of this policy, an employee should contact MIS, the Human Resources Administrator, and/or the Administrator of the Courts.

X. CONFIRMATION OF CONFIDENTIALITY

All Judiciary employees must maintain the confidentiality of PII as well as Judiciary proprietary data to which they may have access and understand that such PII is to be restricted to only those with a need to know. Employees with ongoing access to such data will sign acknowledgement reminders annually attesting to their understanding of this requirement.

XI. VIOLATIONS OF PII POLICIES AND PROCEDURES

The Judiciary views the protection of PII data to be of the utmost importance. Infractions of this policy or its procedures will result in disciplinary actions under the Judiciary's Personnel Rules and/or Code of Conduct and may include suspension or termination in the case of severe or repeat violations.

XII. REFERENCES

- A. 9 GCA Chapter 48 – Notification of Breaches of Personal Information
- B. 5 GCA Chapter 32, Article 7 - Social Security Number Confidentiality
- C. Judiciary Policy Governing Computing and Technology Resources
- D. Judiciary Password Management Policy
- E. Judiciary Laptop and Mobile Device Interim Policy and Procedures
- F. Judiciary Court Property Policy
- G. 2 CFR § 200.79
- H. 2 CFR § 200.82
- I. Office of Management and Budget (OMB) Circular A-130
- J. Office of Management and Budget (OMB) Memorandum M-17-12



JUDICIARY OF GUAM

Administrative Office of the Courts
COURT PROGRAMS OFFICE



HON. F. PHILIP CARBULLIDO

Guam Judicial Center, 120 West O'Brien Drive

KRISTINA L. BAIRD

Administrator of the Courts

Chief Justice of Guam

M. GRACE LAPID ROSADINO

Court Programs Acting Administrator

ATTACHMENT A

Reporting Form on Actual or Imminent Breach of PII or PPII

1. Breach Reported by:			
Division:			
Name:		Supervisor:	
Email:		Email:	
Phone:		Phone:	
2. Breach Response Team:			
Name:		Name:	
Email:		Email:	
Phone:		Phone:	
Name:		Name:	
Email:		Email:	
Phone:		Phone:	
Name:		Name:	
Email:		Email:	
Phone:		Phone:	
3. Breach Summary:			
Date and time of breach:			
Location of breach:			

Do not include PII or classified information. Summarize the facts of circumstances of the theft, loss, or compromise of PII or PPII as currently known, including:

- a. A description of the parties involved in the breach;

b. The physical or electronic storage location of the information at risk;

c. If steps were immediately taken to contain the breach;

d. Whether the breach is an isolated occurrence or a systematic problem;

e. Who conducted the investigations of the breach, if applicable; and

f. Any other pertinent information.

4. Type of Breach:			
Lost Information or Equipment	<input type="checkbox"/>	Unauthorized Disclosure	<input type="checkbox"/>
Stolen Information or Equipment	<input type="checkbox"/>	Unauthorized Access	<input type="checkbox"/>
Unauthorized Equipment <small>(e.g., using an unauthorized personal device, server, or email account to store PII)</small>	<input type="checkbox"/>	Unauthorized Use <small>(e.g., employee with agency-authorized access to database or file accesses and uses information for personal purposes rather than for official purposes)</small>	<input type="checkbox"/>
5. Storage Medium:			
Laptop or Tablet	<input type="checkbox"/>	Smartphone	<input type="checkbox"/>
Desktop	<input type="checkbox"/>	Paper files	<input type="checkbox"/>
External Storage Device	<input type="checkbox"/>	External Storage Device <small>(e.g., CD, DVD, USB Drive, etc.)</small>	<input type="checkbox"/>
IT System (Intranet/Shared Drive)	<input type="checkbox"/>	Oral Disclosure	<input type="checkbox"/>
Email:			
Type of Breached Personal Information:			
6. Reported to			
1. Name:			
Name:			
Title:			
Email:			
Phone:			
Date and time of the report:			
2. Name:			
Name:			
Title:			
Email:			
Phone:			
Date and time of the report:			
3. Name:			
Name:			
Title:			
Email:			
Phone:			
Date and time of the report:			

7. Data Elements and Information Types (select all that apply)		
Stand Alone Identifying Numbers (A)		
<input type="checkbox"/> Social Security number	<input type="checkbox"/> Driver's license, state ID numbers	
<input type="checkbox"/> Passport numbers	<input type="checkbox"/> Alien Registration numbers	
<input type="checkbox"/> Financial account numbers	<input type="checkbox"/> Biometric identifiers	
When Stand Alone information is used in combination with any of the following:		
Biographical Information (B)		
<input type="checkbox"/> Name (including nicknames)	<input type="checkbox"/> Gender	<input type="checkbox"/> Race
<input type="checkbox"/> Date of birth (Day, Month, Year)	<input type="checkbox"/> Ethnicity	<input type="checkbox"/> Nationality
<input type="checkbox"/> Country of birth	<input type="checkbox"/> City or county of birth	<input type="checkbox"/> Marital status
<input type="checkbox"/> Citizenship	<input type="checkbox"/> Immigration status	<input type="checkbox"/> Religion/religious preference
<input type="checkbox"/> Home address	<input type="checkbox"/> Zip code	<input type="checkbox"/> Home phone or fax number
<input type="checkbox"/> Spouse information	<input type="checkbox"/> Sexual orientation	<input type="checkbox"/> Children information
<input type="checkbox"/> Group/organization Membership	<input type="checkbox"/> Military service information	<input type="checkbox"/> Mother's maiden name
<input type="checkbox"/> Business mailing address (sole proprietor)	<input type="checkbox"/> Business phone or fax number (sole proprietor)	<input type="checkbox"/> Global positioning system (GPS)/location data
<input type="checkbox"/> Personal e-mail address	<input type="checkbox"/> Business e-mail address	<input type="checkbox"/> Employment information
<input type="checkbox"/> Education information	<input type="checkbox"/> Resume or curriculum vitae	<input type="checkbox"/> Professional/personal references
Biometrics/Distinguishing Features/Characteristics (C)		
<input type="checkbox"/> Fingerprints	<input type="checkbox"/> Palm prints	<input type="checkbox"/> Vascular scans
<input type="checkbox"/> Retina/iris scans	<input type="checkbox"/> Dental profile	<input type="checkbox"/> Scars, marks, tattoos
<input type="checkbox"/> Hair color	<input type="checkbox"/> Eye color	<input type="checkbox"/> Height
<input type="checkbox"/> Video recording	<input type="checkbox"/> Photos	<input type="checkbox"/> Voice/audio recording
<input type="checkbox"/> DNA sample or profile	<input type="checkbox"/> Signatures	<input type="checkbox"/> Weight
Medical/Emergency Information (D)		
<input type="checkbox"/> Medical/health information	<input type="checkbox"/> Mental health information	<input type="checkbox"/> Disability information
<input type="checkbox"/> Workers' compensation information	<input type="checkbox"/> Patient ID number	<input type="checkbox"/> Emergency contact information
Device Information (E)		
<input type="checkbox"/> Device settings or preferences (e.g., security level, sharing options, ringtones)	<input type="checkbox"/> Cell tower records (e.g., logs, user location, time, etc.)	<input type="checkbox"/> Network communications data
Specific Information / File Types (F)		
<input type="checkbox"/> Taxpayer information/tax return information	<input type="checkbox"/> Law enforcement information	<input type="checkbox"/> Security clearance/background check information
<input type="checkbox"/> Civil/criminal history information/police record	<input type="checkbox"/> Academic and professional background information.	<input type="checkbox"/> Health information
<input type="checkbox"/> Case files	<input type="checkbox"/> Personnel files	<input type="checkbox"/> Credit history information.

NOTE: Data elements and information types indicated above should not be regarded as an all-inclusive list of PII, PPII or sensitive data elements.

8. SUBGRANTEE CERTIFICATION

Certification (Signature options: A. Wet or B. Electronic/digital)

I certify under penalty of perjury to the U.S. Department of Justice and the Laws of Guam, that the information provided here is true and correct to the best of my knowledge.

A.		B.	
----	--	----	--

9. GCO-FPO USE ONLY

Report to Grantor

1. Name:			
Email:			
Phone:			
Date, time and method report sent:			
2. Name:			
Email:			
Phone:			
Date, time and method report sent:			
3. Name:			
Email:			
Phone:			
Date, time and method report sent:			

Comments/information reported:

Recommended actions:

10. GCO-FPO USE ONLY (continued)			
Staff			
Name:			
Email:			
Phone:			
Date, time and method report			
Date, time and method report made to administrator:			
Comments:			
<p>Certification (Signature options: A. Wet or B. Electronic/digital) <i>I certify under penalty of perjury to the U.S. Department of Justice and the Laws of Guam, that the information provided here is true and correct to the best of my knowledge.</i></p>			
A.		B.	
11. Administrator			
Name:			
Email:			
Phone:			
Date, time and method report			
Date, time and method report made to grantor:			
Comments:			
<p>Certification (Signature options: A. Wet or B. Electronic/digital) <i>I certify under penalty of perjury to the U.S. Department of Justice and the Laws of Guam, that the information provided here is true and correct to the best of my knowledge.</i></p>			
A.		B.	
12. Miscellaneous			
<input type="checkbox"/> Grantor Receipt acknowledgement		<input type="checkbox"/> Grantor closed (Date of closure: _____)	
<input type="checkbox"/> Subgrantee notified of closure		<input type="checkbox"/> Filed (mother)	<input type="checkbox"/> Filed (subgrantee folder)
Date:			