Department of Housing and Urban Development

PII Confidentiality Impact Level (PCIL) Categorization Template

HUD System Name

HUD System Acronym and CSAM ID

Rev.1.2

Overview

Identifying the system's Personally Identifiable Information (PII) Confidentiality Impact Level (PCIL) pronounced like ***"pickle"*** value is a follow-on step to the information system provisional security and privacy categorization step.

The security objectives of integrity and availability are equally important for PII, and organizations should use the NIST Risk Management Framework to determine the appropriate integrity and availability impact levels. Organizations may also need to consider PII-specific enhancements to the integrity or availability impact levels. Accuracy is a required Fair Information Practice for most PII, and the security objective of integrity helps to ensure accuracy. Integrity is also important for preventing harm to the individual and the organization. For example, unauthorized alterations of medical records could endanger individuals' lives and medical mistakes based on inaccurate information can result in liability to the organization and harm to its reputation.

The confidentiality of PII should be protected based on its impact level. This template outlines factors for determining the PCIL for a particular instance of PII, which is distinct from the confidentiality impact level described in Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. The PII Confidentiality Impact Level takes into account additional PII considerations and should be used to determine if additional protections should be implemented. The PCIL ***low, moderate,*** or ***high*** indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. Once the PCIL is selected, it will be annotated on the HUD Form 1113, Privacy Impact Assessment (PIA) and selected in ***"Agency Defined Data Items"*** section in CSAM. Both the PCIL template and PIA must be sent to HUD Privacy mailbox at *privacy@hud.gov* for review/completion.

Determining the PCIL is most effective when completed in collaboration with System Owner / System Manager, Information System Security Owner and Privacy Liaison Officer.

In order to determine the PII Confidentiality Impact Level, impact levels should be used together using a ***"Balanced Approach"***. The ***"Balanced Approach"*** considers all inputs as an average. It is a best judgment standard where the analyst considers the values and various weights of the individual components. This ***"Balanced Approach"*** takes all factors into consideration to determine the PII Confidentiality Impact Level.

STEP 1. Review the FIPS 199 impact value for each of the six factors.

- Carefully read the definitions of each impact value in ***Table 1 (below)***. Use these definitions, as tailored below in Step 2, to determine the impact value for each of the six factors from NIST SP 800-122*.*

Table 1: FIPS 199 Potential Impact Values as Incorporated in NIST SP 800-122

Potential Impact Value	Type of adverse effect on organizational operations, organizational assets, or <u>individuals</u>	Expected adverse effect of the loss of confidentiality, integrity, or availability on organizational operations, organizational assets, or individuals
LOW	Limited	1. cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 2. result in minor damage to organizational assets; 3. result in minor financial loss; or 4. result in minor harm to individuals.
MODERATE	Serious	1. cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2. result in significant damage to organizational assets; 3. result in significant financial loss; or 4. result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
HIGH	Severe or catastrophic	1. cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; 2. result in major damage to organizational assets; 3. result in major financial loss; or 4. result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

STEP 2. Using the guidance provided below, determine the impact value for each of the six factors from NIST SP 800-122.
* NIST SP 800-122 gives examples for each factor linked ***HERE*****.**

FACTOR 1 -- IDENTIFIABILITY

NIST SP 800-122	NIST SP 800-122 PII Confidentiality Impact Levels

Factors	Low	Moderate	High
Identifiability	Data elements are not directly identifiable alone but may indirectly identify individuals or significantly narrow large datasets.	Combined data elements uniquely and directly identify individuals.	Individual data elements directly identifying unique individuals.

Factor 1. <u>Select</u> Identifiability impact value:

□ LOW □ MODERATE □ HIGH

(Provide justification for the impact value selected.)

FACTOR 2 -- QUANTITY OF PII (Number of Individuals)

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact Levels		
	Low	Moderate	High
Quantity of PII	A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in ad dressing a breach. (0-4999 Individuals)	A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. (5000-49,999 Individuals)	A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. "Big Data" (50,000+ Individuals)

Factor 2. <u>Select</u> Quantity of PII impact value:

□ LOW □ MODERATE □ HIGH

(Provide justification for the impact value selected.)

FACTOR 3 -- DATA FIELD SENSITIVITY

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact Levels		
	Low	Moderate	High
Data Field Sensitivity	Data fields, alone or in combination, have little relevance outside the context.	Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.	Data fields, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.

Factor 3. Select Data Field Sensitivity impact value:

□ LOW □ MODERATE □ HIGH

(Provide justification for the impact value selected.)

FACTOR 4 -- OBLIGATION TO PROTECT CONFIDENTIALITY

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact Levels		
	Low	Moderate	High
Obligation to Protect Confidentiality	Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.	Role-specific privacy laws, regulations or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide requirements. Violations may result in serious civil or criminal penalties.	Organization or Mission-specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government-wide or industry-specific requirements. Violations may result in severe civil or criminal penalties.

Factor 4. Select Obligation to Protect Confidentiality impact value:

□ LOW □ MODERATE □ HIGH

(Provide justification for the impact value selected.)

FACTOR 5 -- ACCESS TO AND LOCATION OF PII

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact Levels		
	Low	Moderate	High
Access to and Location of PII	Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities. PII is not stored or transported off-site by employees or contractors.	Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization's workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization-owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)). Backups are stored at contractor-owned facilities.	Located on computers and other devices on a network not controlled by the organization or on mobile devices or storage media. Access open to the organization's entire workforce. Remote access allowed by equipment owned by others (e.g., personal mobile devices). Information can be stored on equipment owned by others (e.g., personal USB drive).

Factor 5. Select Access to and Location of PII impact value:

□ LOW □ MODERATE □ HIGH

(Provide justification for the impact value selected.)

FACTOR 6 -- CONTEXT OF USE

NIST SP 800-122 Factors	NIST SP 800-122 PII Confidentiality Impact levels		
	Low	Moderate	High
Context of Use	Disclosure of the act of collecting, and using the PII, or the PII itself is unlikely to result in limited harm to the individual or organization such as name, address, and phone numbers of a list of people who subscribe to a general-interest newsletter.	Disclosure of the act of collecting, and using the PII, or the PII itself may result in serious harm to the individual or organization such as name, address, and phone numbers of a list of people who have filed for retirement benefits.	Disclosure of the act of collecting, and using the PII, or the PII itself is likely to result in severe or catastrophic harm to the individual or organization such as name, address, and phone numbers of a list of people who work undercover in law enforcement.

Factor 6. Select Context of Use impact value:

□ LOW □ MODERATE □ HIGH

(Provide justification for the impact value selected.)

STEP 3. Determine the PII Confidentiality Impact Level (PCIL) value.

- Use the following table to roll up the previous answers from Factors 1 through 6***.*** Enter an ***"X"*** in the ***Low, Moderate,*** or ***High*** column for each row. Use these values to determine the ***PII Confidentiality Impact Level (PCIL)*** value.

Factor	Impact Value
Identifiability	Select
Quantity of PII	Select

Data Field Sensitivity	Select
Obligation to Protect Confidentiality	Select
Access to and Location of PII	Select
Context of Use	Select

STEP 4. Select the PII Confidentiality Impact Level (PCIL) value:

OVERALL PCIL VALUE **SELECT**

- Justify your selection of the overall ***PII Confidentiality Impact Level (PCIL)*** value. Take into consideration the FIPS 199 impact values from **Table 1 (above)** and the six factors from NIST SP 800-122. Use the ***"Balanced Approach"*** described on page 3.

(Provide justification for the PCIL value selected.)

Signatures: *** Program Office System Manager(s) only sign for Shared Drives and SharePoint**

System Owner / System Manager

Print name, title, and office of signatory.

Information System Security Officer

Print name, title, and office of signatory.

Privacy Liaison Officer

Print name, title, and office of signatory.

Privacy Office SME

Print name and title of signatory.