IDSO BEST PRACTICES

Personally Identifiable Information (PII)

Document # : IDSO-PII-BP-001 Version : 1.0 Effective Date : Draft

APPENDIX 3: PII DATA RISK ASSESSMENT EXAMPLE

The objective of this risk assessment is to determine the impact level of PII to identify the appropriate security controls. This exercise will also help to prioritize the data fields with the highest impact level so that the organization can prepare to put the highest required level of security controls in place. There are three impact levels based upon NIST 800-122, 800-53 and FIPS 199: low, moderate and high. Factors used to identify impact level are identifiability, quantity, sensitivity and context.[15] Table A3-1 summarizes the criteria to assign the appropriate level for each factor.

Table A3-1. Factors Used to Identify Impact Level

	LEVEL 1	LEVEL 2	LEVEL 3
IDENTIFIABILITY	PII can be used to directly identify an individual or leverage information to impersonate the individual.	PII that does not directly identify an individual but could be used to contact or impersonate an individual. This includes data that links to Level 1 data.	PII contains non-identifying information that cannot be used to identify or impersonate an individual nor provides links to Level 1 or Level 2 personal data.
DATA FIELD SENSITIVITY	PII that has a high risk of harm, embarrassment, inconvenience, or unfairness to an individual if compromised.	PII that has a moderate risk of harm, embarrassment, inconvenience, or unfairness to an individual if compromised.	PII that has a low risk of harm, embarrassment, inconvenience, or unfairness to an individual if compromised.
SPECIFIC PURPOSE	The data has a specific business purpose and needs to be stored and retained.	The data may be needed for a business purpose.	The data is not needed for a specific business purpose and can be deleted.
QUANTITY	The quantity of records with the data field is greater than 25,000.	The quantity of records with the data field is less than 25,000.	The quantity of records with the data field is less than 1000.

Table A3-2. Example Risk Assessment to Identify Impact Level

PII DATA FIELD	IDENTIFIABILITY	DATA FIELD SENSITIVITY	SPECIFIC PURPOSE	QUANTITY	SUM
FIRST NAME	2	2	3	3	10
LAST NAME	2	2	3	3	10
AGE	3	3	1	2	9
SOCIAL SECURITY	1	1	3	1	6
ZIP CODE	3	3	1	3	10

There are many ways to perform a risk assessment and the specific method used can be determined by the organization. Table A3-2 shows an example risk assessment using the factors summarized in Table A3-1. The steps for filling out this table are:

1. List all the PII data fields in the first column.
2. After all the PII data fields have been listed, assign an “identifiability” level of 1, 2, or 3.
3. Assign a level for “data field sensitivity”.
4. Assign a level for “specific purpose”.
5. Assign a level for “quantity”.
6. After the level for each factor has been assigned, sum the total for the numbers in the row in the last column.
7. Using the sum, the impact level can be assigned using Table A3-3.

Table A3-3. Impact Level

SCORE	IMPACT LEVEL
< = 6	High
BETWEEN 6 & 9	Moderate
BETWEEN 9 & 12	Low