IDSO BEST PRACTICES

Personally Identifiable Information (PII)

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

APPENDIX 4: PII SECURITY RISK ASSESSMENT EXAMPLE

The objective of this risk assessment is to determine the security level of PII to select the appropriate security access and controls. There are three security levels: low, moderate and high. Factors used to identify impact level are access frequency, access location, number systems and number of people who have access. Table A4-1 summarizes the criteria to assign the appropriate level for each factor.

Table A4-1. Factors Used to Identify Security Level

	LEVEL 1	LEVEL 2	LEVEL 3
ACCESS FREQUENCY	Data is accessed at least once per day.	Data is accessed at least once per week.	Data is accessed at least once per month.
ACCESS LOCATION	Data is accessible by external users over the internet.	Data is accessible by portable devices through VPN or intranet.	Data is accessible through desktop computers within office premises.
NO. OF SYSTEMS PII RESIDES ON	The data is stored on more than two systems.	The data is stored on two systems.	The data is stored only on one system.
NO. OF PEOPLE WHO HAVE ACCESS TO THE SYSTEM	More than 5 people have access to the data.	Between 3 and 5 people have access to the data.	Less than 2 people have access to the data.

Table A4-2. Example Risk Assessment to Identify Security Level

PII DATA FIELD	ACCESS FREQUENCY	ACCESS LOCATION	NO. OF SYSTEMS PII RESIDES ON	NO. OF PEOPLE WHO HAVE ACCESS TO THE SYSTEM	SUM
FIRST NAME	2	2	3	2	9
LAST NAME	2	2	3	1	8
AGE	1	1	1	1	4
SOCIAL SECURITY	1	1	1	1	4
ZIP CODE	1	2	3	3	9

There are many ways to perform a risk assessment and the specific method used can be determined by the organization. Table A4-2 shows an example risk assessment using the factors summarized in Table A4-1. 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 “Access Frequency” level of 1, 2, or 3.
3. Assign a level for “Access Location”.
4. Assign a level for “No. of Systems PII Resides On”.
5. Assign a level for “No. of People Who Have Access to the System”.
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 ‘Security Level’ can be assigned using Table A4-3.

Table A4-3. Security Level

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