

# Investment Data Standards Organization Best Practices

## IDSO BEST PRACTICES Personally Identifiable Information (PII)

Document # : IDSO-PII-BP-001

Version : 1.0

Effective Date : Draft

### APPENDIX 2: PII SENSITIVITY LEVEL.

Per the Department of Homeland Security,<sup>19</sup> “Sensitive PII” is Personally Identifiable Information that could result in harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stringent handling guidelines due to the increased risk to an individual if the data was compromised. Table A2-1 shows categorization for PII Sensitivity Levels.

**Table A2-1. PII Sensitivity Level**

SENSITIVITY LEVEL	STAND-ALONE	PAIRED WITH ANOTHER IDENTIFIER
LEVEL 1	Social security Level Driver’s license or state identification Passport number Alien registration number Identification number that can identify an individual in another country Biometric identifiers	Citizenship or immigration status Medical Information Consumer report information Religious affiliation Sexual orientation Account passwords Last 4 digits of SSN Police & criminal investigation or history Employee performance ratings & disciplinary Actions Mother’s maiden name Employee grievances Financial & banking information Pre-award contract or grant information Financial disclosure forms Patient records Genome sequence & study data Information collected about children under the age of 13.

<sup>19</sup> Handbook for Safeguarding Sensitive Personally Identifiable Information. Homeland Security. March 2012.  
*Confidential and Proprietary Information – Investment Data Standards Organization Best Practices  
 Not to be Disclosed or Reproduced Without Prior Written Approval*

# Investment Data Standards Organization Best Practices

## **IDSO BEST PRACTICES** **Personally Identifiable Information (PII)**

Document # : IDSO-PII-BP-001

Version : 1.0

Effective Date : Draft

---

<b>SENSITIVITY LEVEL</b>	<b>STAND-ALONE</b>	<b>PAIRED WITH ANOTHER IDENTIFIER</b>
LEVEL 2	PII that has a moderate risk of harm, embarrassment, inconvenience, or unfairness to an individual if compromised.	
LEVEL 3	PII that has a low risk of harm, embarrassment, inconvenience, or unfairness to an individual if compromised.	

For quantifying PII sensitivity, the context matters. For example, if the dataset consists of a list of names that attended a public meeting, then the collection of names would have a low sensitivity level (Level 3). However, if the list of names was law enforcement personnel or immigrants waiting for deportation procedures, then the sensitivity would be high (Level 1) because the data could cause harm, embarrassment, inconvenience, or unfairness to an individual. Therefore, the sensitivity of data depends upon its context of use. The same data field can have a different sensitivity depending upon its context.