IDSO BEST PRACTICES

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Alternative Data Standards

IDSO INVESTMENT DATA Standards Organization

Document# IDSO-PII-BP-001

IDSO BEST PRACTICES
Personally Identifiable Information (PII)

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

1. PURPOSE

The purpose of this document is to provide guidance, processes, and risk management practices when working with personally identifiable information (PII) associated with Alternative Data. This document explains the importance of protecting the confidentiality of the PII and provides guidance in its use, access, and disclosure, including operational best practices, regulatory requirements, and other considerations when exploring or accumulating Alternative Data.

2. SCOPE

This document covers identification, categorization, risk assessment, and management of personally identifiable information (PII) when exploring or accumulating Alternative Data.

3. AUDIENCE

The primary target audience of this document are managers and compliance teams interested in regulatory guidance and process management of personally identifiable information (PII). This document is applicable to teams within the following company profiles that participate in the Alternative Data ecosystem.

3.1 **Raw Data Originators:** Companies that collect the data. Originators can collect data for the sole purpose of selling or generating data as part of their core business.

3.2 **Research Providers:** Companies that use raw data to produce original research and derived signals. Occasionally, Research Providers also generate data through surveys, measurements, and other means.

3.3 **Aggregators:** Companies that aggregate and enrich data with the intent to sell, license or distribute data to the investment community.

3.4 **Investors:** Investment companies & professionals that use data to add value to their investment process.

4. TABLE OF CONTENTS

Section ***Page***

5. BACKGROUND

5.1 RESPONSIBILITY

Safeguarding sensitive information is a responsibility of all entities that work with Alternative Data. The loss of Personally Identifiable Information (PII) can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. The treatment of PII is different than other data because it not only needs to be protected but secured and maintained in accordance with Federal law.

5.2 STATISTICS

According to the 2017 Data Breach Investigations Report issued by Verizon, 61% of the data breach victims are businesses with under 1,000 employees and 62% of breaches involved hacking.[1] Approximately 73% of the breaches were financially motivated and 24% of breaches affected financial organizations. The Online Trust Alliance (OTA) revealed in its 2015 Data Protection Best Practices and Assessment Guides that more than 90% of the 2014 data breaches could have been prevented by adhering to basic procedures and using available security technologies.[2]

5.3 COSTS OF DATA BREACH

Per the 2017 Ponemon Cost of Data Breach Study, the global average cost of a data breach is $3.62 million with an average size data breach of only 24,000 records.[3] Visible PII incident costs may include customer breach notifications, attorney fees and litigation, technical investigations, public relations, and security improvements. Less visible costs include disruption of operations, insurance premium increases, loss of customer relationships, devalued reputation, and lost revenue. Well-known data breaches that have occurred in recent years include:

5.3.1 **Adobe:** Approximately 38 million records containing PII were stolen, including encrypted debit & credit cards, expiration dates, and other sensitive data. After many lawsuits, Adobe agreed to pay $1.1 million in fees.

---

[1] 2017 Data Breach Investigations Report, 10th edition. Verizon. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ Last Accessed June 27, 2017.

[2] Security & Privacy Best Practices. Online Trust Alliance (OTA). https://otalliance.org/resources/security-privacy-best-practices Last Accessed June 27, 2017.

[3] 2017 Ponemon Cost of Data Breach Study. Ponemon Institute and IBM. https://www.ibm.com/security/data-breach/ Last Accessed June 27, 2017.

5.3.2 **Anthem:** In 2015, 80 million patient records were compromised, exposing name, social security numbers, email addresses and employment information. The data breach is expected to cost Anthem well over $100 million.

5.3.3 **JPMorgan Chase:** In 2014, personal information of 76 million households and 7 million small businesses were affected. The estimated cost of recovery will be approximately $1 billion.

5.4 COMPANY SIZE

Adobe, Anthem, and JPMorgan Chase are examples of larger companies; however, most data breaches occur with small to medium-sized companies and never make national headlines. Those who work with Alternative Data must understand the risks and responsibilities associated with data containing PII.

5.5 INTERNAL PROCEDURES

Internal procedures should capture business risks in conjunction with the appropriate legal and compliance counsel. To effectively manage PII, each organization must consider its contractual obligations and internal procedures. There are extensive regulations that exist to properly handle PII, however, not all are applicable to organizations that use Alternative Data within the institutional investment process.

5.6 BEST PRACTICES FOR PII

The purpose of this document is to provide guidance in the identification, categorization, risk management, procedures, and training of personally identifiable information (PII) in the Alternative Data industry. Each section provides guidance and best practices for handling, managing, and storing PII. The appendices provide checklists, processes, classifications, and other utilities for assessing and managing. By using these guidelines, organizations who use Alternative Data will be prepared to handle PII misuse or breaches and avoid losses resulting from inadequate PII procedures and security.

6. PERSONALLY IDENTIFIABLE INFORMATION (PII)

6.1 DEFINITION

A commonly used term to describe personal information is PII (Personally Identifiable Information). PII is “information about an individual” maintained or controlled by an organization, including those who use Alternative Data. Unauthorized use of PII has the potential to seriously harm individuals and organizations.

6.2 COMMON TERMS

Terms that are commonly used when discussing PII are “distinguish,” “trace” or “link”. PII can be used to distinguish or trace an individual’s identity, such as name, social security number,

driver's license number, taxpayer identification number, financial accounts, date of birth, physical address, email address, mother's maiden name, or biometric records.[4]

6.3 DATA CATEGORIES & EXAMPLES

PII also covers information that can be linked to an individual, such as medical, educational, financial, employment information or identifying characteristics such as handwriting, fingerprints, retina scan, voice signature, and facial features.[2] Table 6-1 details common PII data categories and examples. Table 6-1 is a non-exhaustive list and each organization should determine if the data can be used to distinguish, trace, or link to an individual.

Table 6-1. PII Data Categories and Examples[5]

PII EXAMPLE CATEGORY	SPECIFIC EXAMPLES
NAMES	Full name, maiden name or alias
ADDRESS INFORMATION	Street address, email address
TELEPHONE NUMBERS	Mobile, business, and personal numbers
IDENTIFICATION NUMBERS	Social security number (SSN), passport number, driver's license number, taxpayer identification number
ACCOUNT INFORMATION	Financial account, patient account, credit card numbers
PERSONAL CHARACTERISTICS	Photographic image, x-rays, fingerprints, biometric images, voice signature, facial geometry
PERSONAL PROPERTY	Vehicle registration, title information
INFORMATION LINKED TO AN INDIVIDUAL	Date of birth, place of birth, race, religion, weight, employment information, medical information, education information, financial information

6.4 PII IDENTIFIABILITY LEVEL

Each PII field should be rated on an identifiability scale. For example, SSN or driver's license number can directly identify an individual. However, data composed of 'area codes' or 'gender' could not lead to the direct identification of an individual. PII that can uniquely identify an

[4] Definition from National Institute of Standards and Technology Special Publication 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010.

[5] Data categories are based upon information from National Institute of Standards and Technology Special Publication 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010.

individual will have a higher identifiability level than PII that cannot identify an individual. Table 6-2 introduces this categorization.

Table 6-2. PII Identifiability Level

IDENTIFIABILITY LEVEL	DESCRIPTION	EXAMPLES
LEVEL 1	PII can be used to directly identify an individual or leverage information to impersonate the individual.	Full name, social security number (SSN), passport number, driver's license number, bank account number, user name & password to bank account, health records
LEVEL 2	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.	Phone number, email, home address
LEVEL 3	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.	Non-financial account numbers, invoice numbers, confirmation numbers

6.5 OTHER PII CLASSIFICATIONS

The PII identifiability level is an important categorization for helping to identify the risk associated with PII. There are also several other classifications for identifying the PII risk. Appendix 2 provides categorical levels for PII sensitivity level and Appendix 3 introduces two other groupings. The union of these PII categories to assess PII will be discussed in detail in Section 9 *Risk Management Process*.

7. REGULATIONS ON PII AND FAIR INFORMATION PRACTICES

7.1 PRIVACY LAWS

There are many relevant U.S. and international privacy laws, such as the widely-recognized U.S. Fair Information Practices and the Privacy Act, the Gramm-Leach Bliley Act (GLBA), and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA).

7.2 OECD PRIVACY GUIDELINES

The Organization for Economic Co-Operation and Development (OECD) Privacy Guidelines are the most widely-accepted privacy principles and organizations should establish policies and procedures that address all the Fair Information Practices. The OECD identified the following Fair Information Practices listed in the Table 7-1 below.

Table 7-1. Fair Information Practices Identified by OECD[6]

FAIR INFORMATION PRACTICE	DESCRIPTION
COLLECTION LIMITATION	There should be limits to the collection of personal data. The data should be obtained by lawful and fair means, and with the consent of the data subject.
DATA QUALITY	Data should be pertinent for the purpose for which it will be used.
PURPOSE SPECIFICATION	The purpose of the data collection should be specified for a use and only be used for that purpose.
USE LIMITATION	Personal data should not be disclosed or used for purposes other than those specified.
SECURITY SAFEGUARDS	Personal data should be protected by security safeguards against unauthorized access, use, modification or disclosure of data.
OPENNESS	There should be a general policy of openness about developments, systems, and policies relating to personal data.
INDIVIDUAL PARTICIPATION	An individual should have the right to obtain confirmation and data from a data controller if they have data relating to him. If the request is denied, the individual should be able to challenge the data controller and then have data erased, rectified, completed or amended.

[6] Summary of Fair Information Practices are from National Institute of Standards and Technology Special Publication 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010.

ACCOUNTABILITY	A data controller should be accountable for complying with all the above measures.

7.3 GRAMM-LEACH BLILEY ACT (GLBA)

Organizations engaging in financial activities are subject to the Gramm-Leach Bliley Act (GLBA). The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

7.4 CIPSEA

Businesses that collect PII for statistical purposes are subject to strict confidentiality requirements of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA). Violations of these laws can result in civil or criminal penalties.

7.5 COMPLIANCE WORKING GROUP

Each organization should create a compliance working group to manage PII within the organization. The compliance working group should insure that the compliance strategy conforms to the appropriate statutes and laws.

7.6 GENERAL DATA PROTECTION REGULATION (GDPR)

Any organization that collects or processes data from EU residents should implement measures, which meet the principles of data protection by design and data protection by default. If the organization is collecting consumer information, it must receive opt-in from the users and disclose intended data uses. For organization which processes data, a data protection officer (DPO) who is a person with expert knowledge of data protection law and practices should assist the organization to monitor internal compliance with GDPR.

7.7 LEGAL OBLIGATIONS

An organization should consider its legal obligations to protect PII when determining its PII risk level in consultation with the appropriate counsel or compliance personnel. Decisions about a law or regulation require consultation as applicable laws, regulations, and other mandates change over time. Protecting the confidentiality of PII requires knowledge of information security, privacy, and legal obligations.

8. IDENTIFICATION AND REMEDIATION

8.1 UN-EVALUATED PII

When Alternative Data is purchased or collected, all uncategorized data should be segregated from use until it has been properly assessed. All data should be obtained by legal means and should be stored in a designated area or database until it has been evaluated for PII content.

Only authorized individuals or approved third party contractors should have access to data that has not been properly evaluated for PII content.

8.2 IDENTIFY PII

PII should be identified immediately upon procurement of the data. PII can be identified by conducting interviews and/or completing a questionnaire with the data originator. Appendix 1 has an example PII questionnaire based upon The Privacy Impact Assessment Guide by the U.S. Securities and Exchange Commission.[7] PII can also be identified by reviewing associated documentation or reviewing the actual data fields.

8.3 DELETING UNNECESSARY PII

Each PII field that has been identified in a dataset must have a specific purpose. If no specific purpose has been identified for each PII field, then that specific PII field should be disposed of in the appropriate manner. Storing minimal PII required for a specific purpose is the best method of minimizing security efforts and reducing the risk of PII-related incidents or breaches.

PII printed on hard copy printouts can easily be disposed of by shredding, pulverizing or incinerating. The deletion of a digital file is insufficient in disposing of the PII because a digital back-up file or other "fingerprint" file may be retained in the computer system. The method of disposal must not only include the deletion of the original fields or files, but also deletion of any files that are automatically created by the computer system. The sanitation method chosen must be based upon the storage device and the impact level of PII. There are many types of sanitization methods and many of these are detailed in the NIST Guideline for Media Sanitization.[8]

8.4 DE-IDENTIFICATION & ANONYMIZATION OF PII

Storage and access to complete data records may not be necessary. After PII has been identified in a dataset, and an impact level has been assigned, one method of reducing impact level of a dataset is "de-identification" or "anonymization" of PII. Certain resources separate these two categories, and others use these terms interchangeably.

8.4.1 **De-identification** means that certain parts of the dataset of data fields have been obscured or removed. The information has been removed so that an individual cannot be identified.

8.4.2 **Anonymization** of information is "previously identifiable information that has been de-identified and for which the transformation back no longer exists." By anonymizing the dataset, it will cease to be classified as PII.

[7] The Privacy Impact Assessment (PIA) Guide. U.S. Securities and Exchange Commission, Privacy Office. Office of Information Technology, January 2007.

[8] National Institute of Standards and Technology Publication Special Publication 800-88 Guidelines for Media Sanitization. December 2014.

8.5 METHODS

An algorithm may be used to "de-identify" the information. Impact levels can be reduced if the algorithm or re-identification information is stored separately with limited access or the dataset cannot be re-linked through publicly available information. Examples of de-identification and anonymization include:

8.5.1 **Pseudonymization:** The fields that identify an individual are replaced with pseudonyms. The pseudonyms are used to link personal information across multiple data records.

8.5.2 **Hashing:** The fields are hashed (encrypted) into a unique key value. For example, changing an email address "someone@email.com" to "6cdf45c160".

8.5.3 **Suppression:** The fields are removed. For example, changing an email address "someone@email.com" to "null".

8.5.4 **Masking:** The fields are masked using a special character. For example, changing an email address "someone@email.com" to "$$$$$$$".

8.5.5 **Aggregation:** The data is aggregated or made less precise. This is often conducted for statistical analysis to analyze trends and patterns.

8.5.6 **Substitution:** The data is replaced by substitute data. The data type and character length may or may not be preserved. The substituted characters are randomly generated using an algorithm.

8.5.7 **Shuffling:** The rearrangement of data within the same data field. For example, if an account number is "60014592", then the shuffled data will be "60914025".

8.5.8 **Swapping:** Exchanging data fields of one record with the same data fields of another record. For example, the zip codes of two records can be swapped or the first and last name field can be swapped to increase security and reduce impact level.

8.5.9 **Noising:** Adding small amounts of noise or variation into the dataset. For example, adding a fixed percentage to the numbers in a data field.

8.6 METHODS & IMPACT LEVEL

Many other methods can be used to anonymize or de-identify information.[9] The particular method can be determined by R&D or management to reduce the PII impact level. Appendix 3 provides a method for assessing impact level of a dataset. The team can evaluate the impact of the dataset before and after anonymization/de-identification to determine if the PII impact level has been successfully reduced.

8.7 BEST PRACTICES

Although anonymization and de-identification techniques decrease the impact level, these methods must not be exclusively relied upon to secure the PII. An algorithm or methodology could potentially be unencrypted. The best practice involves either:

8.7.1 Deletion and sanitization of the PII; or

[9] National Institute of Standards and Technology Publication NISTIR 8053, De-Identification of Personal Information, October 2015.

8.7.2 Anonymization or de-identification combined with the appropriate security controls to ensure complete PII security.

9. RISK MANAGEMENT

9.1 RISK MANAGEMENT PROCESS

The risk management process outlined in Table 9-1 provides a structured process for PII security and compliance. Organizations who work with Alternative Data should perform risk assessments for all data to determine the appropriate PII impact levels.

9.1.1 **Definition:** Risk assessment is the process of identifying risks to individuals and organizational operations and may include the mission, purpose, reputation, organizational assets, employees, and customers.

9.1.2 **System Boundaries:** An important part of the risk management process is creating the appropriate system boundaries. Well-defined system boundaries establish the scope of protection for organizational information systems and include people, processes, and information technologies.

9.1.3 **Risk Assessment Policy:** The risk assessment should provide a policy for handling each level of PII and should be incorporated into the internal compliance procedure(s). New data should not be exposed or used by any individual in an organization until a risk assessment has been conducted and the data has been approved.

9.1.4 **Approach:** A risk assessment approach may include, depending on the PII utilized, assessment of the potential damage to individuals from leakage, ease of individual identification, the aggregate number of individuals identified, ease of extraction and retrieval of PII from the dataset, and the percent of the dataset that contains PII.

Table 9-1. Risk Management Process for Companies Who Use Alternative Data[10]

STEP	DESCRIPTION
CATEGORIZATION	This step of the risk management process involves categorizing PII and the information systems used to store PII.
SELECTION	This step involves the selection of security controls to protect PII based upon security categorization.
IMPLEMENTATION	This step involves employment of security controls for protecting PII within the information system.
ASSESSMENT & MONITORING	The security controls must be assessed to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome. The security controls should be monitored continuously to protect PII. When necessary, documentation should be updated with changes to the system or its environment.

9.2 IMPACT LEVEL

'Impact' can be defined as the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, misuse or breach of PII. The impact level is based on PII levels and directs the security safeguards which need to be implemented. PII should be identified and classified into three categories[11] based on the potential impact of a security breach in a system as shown in Table 9-2.

[10] Definition and Risk Management steps are detailed in National Institute of Standards and Technology Special Publication 800-30 Guide to Conducting Risk Assessments, September 2012 and National Institute of Standards and Technology Special Publication 800-37 Applying the Risk Management Framework to Federal Information Systems, February 2010.

[11] Defined in National Institute of Standards and Technology Special Publication 800-60 *Guide to Mapping Types of Information Systems to Security Categories,* August 2008 and Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Table 9-2. PII Confidentiality Impact Level[4]

IMPACT LEVEL	DESCRIPTION	EXAMPLES
HIGH	Loss of confidentiality, integrity or availability could have a severe or catastrophic effect on an organization or individuals.	The organization may not be able to perform one or more of its primary functions. There will be damage to organizational assets. There will be harm done to individuals resulting in loss of life or serious life-threatening injuries.
MODERATE	Loss of confidentiality, integrity or availability could have a severe adverse effect on an organization or individuals.	The organization may experience a significant degradation in mission capability to a certain extent and duration. There may be significant damage to organizational assets. There may be significant financial loss. This may result in harm done to individuals that does not result in loss of life or serious, life-threatening injuries.
LOW	Loss of confidentiality, integrity or availability could have a limited adverse effect on an organization or individuals.	The organization may experience a degradation in mission capability to a certain extent and duration. The effectiveness of the organization's functions may be noticeably reduced. There may be minor damage to organizational assets. There may be minor financial loss. This may result in minor harm to individuals

9.3 PII IMPACT LEVEL CATEGORIZATION

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, context, and confidentiality.[15] Table 9-3 provides a description of these factors. To determine PII impact level, all factors should be included so that the 'impact level' is a composite score. Therefore, a higher impact rating of one factor may over-ride lower impact ratings for the other factors.

Table 9-3. Factors Used to Determine PII Impact Levels[12]

FACTOR	DESCRIPTION
IDENTIFIABILITY	Organizations should evaluate how easily PII can be used to identify specific individuals. For example, SSN or driver's license number can directly identify an individual. However, data composed "area codes" or "gender" could not lead to the direct identification of an individual. PII that can uniquely identify an individual will have a higher impact level than PII that cannot identify an individual.
QUANTITY OF PII	Organizations may want to consider how many individual data fields have been identified. For example, a breach of 1,000,000 records would have a higher impact than ten records. A greater number of records has the potential of greater harm to an organization's reputation. For these reasons, organizations may choose to set a higher impact level for large datasets.
DATA FIELD SENSITIVITY	Organizations should evaluate the sensitivity of each PII data field, as well as many data fields together. Many organizations often choose to set a field to at least moderate if a data field such as an SSN is present.
CONTEXT OF USE	Context of use is the purpose for which PII is collected, stored, used, processed disclosed, or disseminated. Organizations should consider the specific use because it is unnecessary to store and secure PII information that does not have a specific purpose.
OBLIGATION TO PROTECT CONFIDENTIALITY	The organization should consider legal obligations when determining PII confidentiality impact level. Many organizations are subject to laws and regulations to protect personal information.

10. SECURITY CONTROLS

10.1 SECURITY CLASSIFICATION

There are many types of security controls that are available to safeguard data processes, storage, and transmission and comply with the relevant regulations for PII. Controls selected and implemented by an organization depends upon the PII security categorization, which can be classified as low, moderate, or high impact level. Controls should be selected based on factors such as access frequency, access locations, number of systems, and number of people. An example of using this methodology is in Appendix 3[13].

[12] Factors are from National Institute of Standards and Technology Special Publication 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010.

[13] Based upon "The Complete Book of Data Anonymization: From Planning to Implementation" by Balaji Raghunathan. CRC Press, 2013.

10.2 SECURITY CONTROL CATEGORY

Each organization should determine the appropriate method of selecting security control levels. The security control category should ideally consider both the 'impact level' and 'security level' as demonstrated in Appendices 3 and 4 respectively.

10.2.1 The first step is to determine the 'PII impact level," which will be high, moderate, or low (see Appendix 3).

10.2.2 The next step is to determine the 'PII security level,' which is also categorized as high, moderate, or low (see Appendix 4).

10.2.3 The final step is to take the highest level of the two measures (impact level, security level) and use that level for the security control category.

10.3 EXAMPLE

For example, if the impact level is "high" and the security level is "high," then assign the PII to the category of "security controls for high-impact systems." If the impact level is "low" and the security level is "low," then assign the PII to the category of "security controls for low-impact systems. If one level is high and the other is low, the organization should assign the upper level as the security control category.

10.4 BEST PRACTICES FOR SECURITY CONTROLS

Table 10-1 summarizes the best practices for the PII security control level for low-impact systems. This category provides the minimum requirements for PII security controls. Tables 10-2 and 10-3 show the best practices for a moderate and high-impact security control level, respectively. The security controls for a moderate-impact level should use all the controls for the low-impact level plus the additional moderate-impact level recommendations. The security controls for the high-impact level employs all the controls for the low plus moderate-impact levels with additional recommendations.

Table 10-1. Security Controls for Low-Impact Systems[14]

SECURITY CONTROL	DESCRIPTION
SYSTEM SECURITY	The organization should have an overall system security plan. The plan may include an overview of the security requirements, the security categorization of the system, and how security fits with the mission of the organization.
ACCESS ENFORCEMENT	Organizations should control access to PII through access control policies. The access control policy addresses responsibilities, management commitment, laws and policies, implementation, and access controls. The access control policy can be incorporated into the Information Technology (IT) procedure or similar SOP.
AUDIT POLICY & PROCEDURES	The organization should develop a policy of auditing systems that contain PII. The policy can be part of the Information Technology (IT) or similar SOP. Organizations should regularly audit Information Security Systems or review audit records for inappropriate or unusual activity affecting PII. The audits can involve account usage, remote access, configuration settings, equipment removal, etc.
SECURITY ASSESSMENT	The organization's security controls should be periodically assessed. PII stored on systems connected to other information systems, internal or external networks, should be secure. Continuous monitoring enables ongoing awareness of threats and vulnerabilities.
CONFIGURATION MANAGEMENT	Baseline configurations should be documented and serve as a basis for future changes to the information system. The baseline configuration includes information about software packages, computers, servers and operating systems along with current version numbers and patches. Automated tools can help to maintain consistent baseline configurations. The organization should evaluate changes to the information system to determine potential security impacts prior to change implementation.
CONTINGENCY PLAN	Contingency plans to maintain operations should be created for cyber-attacks, misuse of PII, and failure to comply with laws and regulations. The organization should provide contingency training to information systems users.
IDENTIFICATION AND AUTHENTICATION	Users should be uniquely identified and authenticated before accessing PII.

[14] Security Controls are from National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

IDSO BEST PRACTICES

Personally Identifiable Information (PII)

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

SECURITY CONTROL	DESCRIPTION
INCIDENT RESPONSE TRACKING	The organization should document and track security incidents. The organization may use automated tools for tracking and collecting information about security incidents.
MAINTENANCE	Organizations should keep records of maintenance of any component of the information system that is connected to the database or other device that stores PII.
MEDIA ACCESS	Organizations can restrict access to media containing PII, including portable digital media (USB flash drives) and non-digital media.
PHYSICAL ACCESS & PROTECTION	The organization should monitor the physical access to where the PII resides. Visitors should be required to sign in and out of an area that stores PII.
PERSONNEL SECURITY	Individuals that have access to PII should be (1) authorized for access by the company, and (2) have read, understood, and signed a non-disclosure or similar agreement(s). The organization should establish security roles and responsibilities for third-party providers.
INFORMATION SYSTEM MONITORING	Organizations should monitor the information system to detect potential attacks and unauthorized remote or local connections. Monitoring can be used to track additional information through the information system if necessary. The monitoring system can be setup to automatically provide security alerts and notifications. The organization should employ vulnerability scanning tools to identify and eliminate vulnerabilities in the information system.

Table 10-2. Security Controls for Medium-Impact Systems[15]

SECURITY CONTROL	DESCRIPTION
SECURITY AWARENESS & TRAINING	The organization should provide security awareness training on insider threat. Insider threats includes current or previous employees with long-term job dissatisfaction, bullying, workplace violence or other serious violations of organizational policies.
AUDIT POLICY & PROCEDURES	The organization may employ automated mechanisms to integrate audit review, analysis, and reporting. The audit records can be correlated across the organization to gain awareness.
SECURITY ASSESSMENT	The organization should use assessors or assessment teams to conduct impartial security control assessments and monitor security controls.
CONFIGURATION MANAGEMENT	The organization should retain previous versions of baseline configurations to support rollback if needed. There should be configuration change control, which includes review, documentation, implementation, testing and audits. The organization should keep an inventory of information system components for system maintenance.
PHYSICAL ACCESS & PROTECTION	The organization should monitor physical intrusion using alarms and surveillance equipment.
SECURITY PLANNING	The organization should not allow employees to post public information on public websites.
VULNERABILITY SCANNING	The organization should employ vulnerability scanning tools that are readily updated as new vulnerabilities are discovered.
INFORMATION SYSTEM MONITORING	The organization should monitor the information system using automated tools to detect unusual or unauthorized activities. The monitoring system should also automatically provide security alerts, notifications, and records. Security checks are performed at start-up restart, shutdown, and during software installation.

[15] Security Controls are from National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Table 10-3. Security Controls for High-Impact Systems[16]

SECURITY CONTROL	DESCRIPTION
AUDIT POLICY & PROCEDURES	The analysis of the audit records is combined with performance data, monitoring data, and physical access monitoring to better understand risks.
SECURITY ASSESSMENT	The organization uses in-depth monitoring, vulnerability scanning, insider threat assessment and malicious user testing to improve security. Penetration testing (i.e. cyber-attacks) is also used to assess information systems to identify vulnerabilities.
CONFIGURATION MANAGEMENT	The organization uses automated mechanisms to maintain baseline configurations and document changes to the information system.
CONTINGENCY PLAN	The organization uses simulated events to help train personnel in crisis situations.
INCIDENT RESPONSE TRAINING	The organization incorporates simulated events for training purposes. The organization uses automated mechanisms to track, collect data and analyze security incidents.
INFORMATION SYSTEM MONITORING	The organization should use automated mechanisms to make security alerts available throughout the organization. The system will automatically shut the information system down and restart it if integrity violations are discovered.

10.5 INCIDENT RESPONSE

Incidents and breaches involving PII have the potential to damage an organization's reputation and incur substantial costs and time. Organizations which use Alternative Data should develop policies that describe when and how individuals should be notified, when and if a breach should be reported publicly, whether to provide remedial services to individuals affected.

Organizations should integrate such policies into their existing compliance procedures. Table 10-4 describes the four phases for handling security incidents: preparation, detection and analysis, containment, eradication, and post-incident recovery.

[16] Security Controls are from National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Table 10-4. Phases for Handling Security Incidents[17]

SECURITY INCIDENT PHASE	DESCRIPTION
PREPARATION	Organizations should create response plans for breaches involving PII and incorporate the plans into their existing procedures. The policies and procedures should be conveyed to the organization's staff through training and awareness programs.
DETECTION AND ANALYSIS	Organizations may continue to use their current detection and analysis technologies for managing PII.
CONTAINMENT, ERADICATION, AND RECOVERY	Technologies and systems for control, suppression, and retrieval may be useful for breaches involving PII. However, additional procedures for incident handling may be necessary to insure successful containment, eradication, and recovery.
POST-INCIDENT ACTIVITY	Information obtained through detection, analysis, containment, and recovery should be collected for sharing within the organization to help protect against future incidents.

11. PII POLICIES & MANAGEMENT

11.1 PII POLICIES

PII operational safeguards and security controls should to be clearly documented in explicit policies and communicated through training and awareness. After PII policies and procedures have been created, one or more designated individuals should be accountable for implementation, maintenance, functioning, and compliance of the appropriate controls in the organization.

11.2 PROCEDURE TOPICS

Table 11-1 lists topics that should be included in procedural document(s) for identification, categorization, control, storage, and incident response of PII for companies which use Alternative Data. The document(s) should be reviewed annually and should include senior management which is ultimately responsible for managing PII.

[17] Security Controls are from National Institute of Standards and Technology Special Publication 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010.

Table 11-1. Topics to Include for Written PII Policies

DOCUMENT SECTION	DESCRIPTION
DEFINITION	A formal definition of PII should be included in the procedure.
APPLICABLE PRIVACY LAWS, REGULATIONS, AND POLICIES	A synopsis of all relevant privacy laws, regulations, and policies should be included in the procedure.
LOCATION	The location and storage of PII should be carefully considered. For each database or data storage medium that contains PII, a documented intent of use for the database or storage medium should be created and maintained. Additional security controls may need to be implemented depending upon the PII sensitivity and data accessibility.
ROLES AND RESPONSIBILITIES	The departments and/or individual roles and responsibilities for using and protecting PII should be defined. The roles and responsibilities in responding to PII-related incidents and reporting should also be defined.
ACCESS RULES	The access rules for PII must be carefully considered. The more often PII is accessed by people and systems, the greater the number of opportunities for PII to be compromised. The organization should conduct a periodic review of personnel permitted access to PII.
RISK ASSESSMENT	The organization should assess risk associated with PII impact level and unauthorized access and disruption of the information system that stores PII. The risk assessment process should be reviewed at least annually, and include senior management responsible for managing PII.
SECURITY CONTROLS	The security controls used to secure PII should be detailed in the procedure(s).
RETENTION SCHEDULES AND PROCEDURES	The length of time that data is stored and maintained must be considered. Limiting the amount of PII in an organization reduces the potential negative consequences in the case of a data breach. Organizational steakholders should meet at least annually to ensure that PII still has a specific use.
INCIDENT RESPONSE AND DATA BREACH	A response plan to handle data breaches should be detailed in the procedures. The response plan should address

DOCUMENT SECTION	DESCRIPTION
	communications with all relevant individuals and government agencies and include remedial policies for breaches.
RESTRICTIONS ON DATA COLLECTION, STORAGE, DISCLOSURE AND USE	Guidance should be provided on restrictions of data collection, disclosure, sharing, storage and use of PII within the organization.
APPROPRIATE DISPOSAL	An organization should regularly review its holdings of PII to determine whether the PII is relevant and necessary for meeting the organization's business purpose and mission. If PII is no longer necessary, it should be properly destroyed. The procedure for the appropriate disposal of data should be documented.
FAILURE TO FOLLOW PRIVACY RULES	Remedies should be written detailing the consequences for failure to follow the privacy rules.
MISUSE OF PII	The procedure should include instructions for handling a security or privacy breach involving PII.
AUDITS	The organization should develop a policy of auditing systems that contain PII. Organizations should regularly review audit records of inappropriate or unusual activity affecting PII.

11.3 COOPERATION & COLLABORATION

Organizations who use Alternative Data should promote close cooperation among senior management and legal counsel when addressing issues related to PII. Cooperation and collaboration of the relevant internal and external experts help to prevent incidents that could result in the misuse of PII by strictly adhering to internal policies and procedures and adequately training staff to oblige by these systems and procedures.

12. EDUCATION, TRAINING, AWARENESS

12.1 TRAINING

After policies and procedures have been formalized, training and education is essential to a successful PII program for Alternative Data. Laws and regulations may specifically require training for staff, managers, and contractors. An organization should have a training plan and implementation approach, and an organization's leadership should communicate the seriousness of protecting PII to its staff. All individuals who have access to systems containing PII should be trained on the internal PII policies. The goal of training is to build knowledge and skills that will enable staff to protect PII for companies that use Alternative Data.

12.2 TRAINING FOR SECURITY CONTROLS

Table 12-1 describes best practices for training of access enforcement, security awareness, contingency plan, and incident response. For additional information on developing a training program, refer to NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.[18]

Table 12-1. Training for Security Controls

SECURITY CONTROL	DESCRIPTION
ACCESS ENFORCEMENT	The organization should provide training on access control policies including responsibilities, implementation, and access controls. The access to databases containing PII should be limited to individuals trained on appropriate PII acquisition and retention procedures.
SECURITY AWARENESS & TRAINING	The organization should provide security awareness training to system users as (1) part of the initial training and (2) procedures are updated. The training should include (1) the need for information security, and (2) how to respond to security-related incidents. The initial training should be conducted prior to authorization of access to the IT system. The organization should document training activities and retain individual training records.
CONTINGENCY PLAN	The organization should provide contingency training to information systems users that are involved with systems that store PII.
INCIDENT RESPONSE TRAINING	The organization should provide incident response training for users that access information systems with PII storage.

13. AUTHORIZED SOFTWARE

Software can be used to determine if a dataset complies with IDSO standards. To satisfy requirements specified in this standard with software, the software must be assessed by IDSO prior to use to determine its proper use of IDSO standards. The approved software can be used to complement an examiner's assessment of a dataset against the standards. Software can provide rapid adoption of PII data standardization to reduce compliance risks associated with national

[18] National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.

privacy and data security laws. The use of a PII compliance software requires prior authorization from IDSO; otherwise, the software output cannot comply with the requirements of this standard.

14. REFERENCES/RELATED PROCEDURES

National Institute of Standards and Technology Special Publication 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010.

National Institute of Standards and Technology Special Publication 800-39 *Guide to Managing Information Security Risk,* March 2011.

National Institute of Standards and Technology Special Publication 800-30 *Guide to Conducting Risk Assessments,* September 2012.

National Institute of Standards and Technology Special Publication 800-37 *Applying the Risk Management Framework to Federal Information Systems,* February 2010.

National Institute of Standards and Technology Special Publication 800-60 *Guide to Mapping Types of Information Systems to Security Categories,* August 2008.

Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.

National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013.

National Institute of Standards and Technology Publication NISTIR 8053, De-Identification of Personal Information, October 2015.

2017 Data Breach Investigations Report, 10th edition. Verizon. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ Last Accessed June 27, 2017.

Security & Privacy Best Practices. Online Trust Alliance (OTA). https://otalliance.org/resources/security-privacy-best-practices Last Accessed June 27, 2017.

2017 Ponemon Cost of Data Breach Study. Ponemon Institute and IBM. https://www.ibm.com/security/data-breach/ Last Accessed June 27, 2017.

The Privacy Impact Assessment (PIA) Guide. U.S. Securities and Exchange Commission, Privacy Office. Office of Information Technology, January 2007.

National Institute of Standards and Technology Publication Special Publication 800-88 Guidelines for Media Sanitization. December 2014.

Raghunathan, Balaji. The Complete Book of Data Anonymization: From Planning to Implementation" CRC Press, 2013.

15. APPENDICES

14.1 Appendix 1: Example PII Questionnaire.

14.2 Appendix 2: PII Sensitivity Level.

14.3 Appendix 3: PII Data Risk Assessment Example.

14.4 Appendix 4: PII Security Risk Assessment Example.

14.5 Appendix 5: Checklist for Assessing the Risk & Compliance of PII for Alternative Data Use.

16. REVISION HISTORY

The following revision history contains the changes since the last revision of the document.

Version Number	***Change Description***	***Revised By***	***Date of Revision***
1.0	New procedure		

IDSO BEST PRACTICES

Personally Identifiable Information (PII)

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

Signature Page

Document Author:	**IDSO Designee:**
Written By:	
Date:	
Document Approver:	**IDSO Management:**
Approved By:	
Date:	

IDSO BEST PRACTICES

Personally Identifiable Information (PII)

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

APPENDIX 1: EXAMPLE PII QUESTIONNAIRE

Project Name: _____
Project Description: _____
Purpose: _____

Contact Name: _____ Title: _____
Organization: _____ Email: _____ Phone: _____

What data is to be collected? _____
_____

Describe data to be collected: _____
_____

What specific legal authorities, arrangements or agreements were defined during the collection of data?
_____

What are the sources of the data? _____
_____

Why is the data being collected? _____
_____

Will the data be shared internally, externally or both? _____

Does the project use PII that can be used to directly identify an individual?
☐ Yes. Please fill out the remaining questions. ☐ No. Please skip the remaining questions.
Field: _____ Description: _____Purpose: _____
Field: _____ Description: _____Purpose: _____
Field: _____ Description: _____Purpose: _____
Field: _____ Description: _____Purpose: _____
Field: _____ Description: _____Purpose: _____
Field: _____ Description: _____Purpose: _____
Please list additional items separately and attach as an appendix.

Signature: _____ Date: _____
Company Management or Designee: _____

Signature: _____ Date: _____
System Owner: _____ Title: _____
Company: _____ Phone: _____

APPENDIX 2: PII SENSITIVITY LEVEL.

Per the Department of Homeland Security,[19] "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 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.

[19] Handbook for Safeguarding Sensitive Personally Identifiable Information. Homeland Security. March 2012.

IDSO BEST PRACTICES

Personally Identifiable Information (PII)

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

SENSITIVITY LEVEL	STAND-ALONE	PAIRED WITH ANOTHER IDENTIFIER
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 included law enforcement personnel then the sensitivity would be high (Level 1) because the data could cause harm, embarrassment, inconvenience, or unfairness to an individual. The sensitivity of data depends upon its context of use. The same data field can have a different sensitivity depending upon its context.

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 will help 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 between 25,000 and 1,000	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

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 computer 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.	At most 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

IDSO BEST PRACTICES
Personally Identifiable Information (PII)

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

APPENDIX 5: CHECKLIST FOR ASSESSING RISK & COMPLIANCE OF PII

IDENTIFICATION & REMEDIATION		SECTION
1	All datasets should be obtained by legal means.	8.1
2	Alternative Data purchased or owned by the organization should be assessed for PII.	8.1
3	PII that has not been assessed should be segregated.	8.1
4	A risk assessment should be performed to identify PII impact level.	8.6, 9.1, 9.2, 9.3
5	PII without a specific business purpose should be disposed of in the appropriate manner.	8.3
6	PII should be de-identified or anonymized to reduce PII impact level where appropriate.	8.4, 8.5

REGULATIONS ON PII AND FAIR INFORMATION PRACTICES		SECTION
7	The organization should create a compliance working group to manage PII within the organization.	7.5
8	The compliance working group should insure that the compliance strategy conforms to the appropriate statutes and laws.	7.5

RISK MANAGEMENT		SECTION
9	The organization should have a risk assessment process to identify the impact level of PII and the security level to protect PII.	9

PII STORAGE		SECTION
10	PII should be strategically located and stored to maximize security.	11.2
11	There should be a documented intent of use for each database or data storage medium that contains PII.	11.2
12	The access to databases containing PII should be limited to individuals trained on appropriate PII acquisition and retention procedures.	11.2

SECURITY CONTROLS		SECTION
13	The organization should have an overall system security plan.	10.4
14	A restricted access system should be established for sequestered data that has not been properly assessed for PII.	8.1, 10.4
15	The appropriate security controls should be selected based upon impact level (security level).	10.2 - 10.4

IDSO BEST PRACTICES

Personally Identifiable Information (PII)

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

SECURITY CONTROLS		SECTION
16	Organizations should control PII access through access control policies.	10.4, 11.2
17	The organization should develop a policy of auditing systems that contain PII.	10.4, 11.2
18	Users should be uniquely identified and authenticated before accessing PII.	10.4
19	The organization's security controls should be periodically assessed.	11.2
20	Baseline configurations should be documented and serve as a basis for future changes to the information system.	10.4
21	Contingency plans to maintain operations should be created for cyber-attacks, misuse of PII, and failure to comply with laws and regulations.	10.4
22	The organization should document and track security incidents.	10.4
23	Organizations should keep records of maintenance of any component of the information system that is connected to the database or other device that stores PII.	10.4
24	Organizations should implement a restrictive set of rights/privileges or accesses so that users have access to the least amount of information required to perform their job duties	10.4
25	Organizations should prohibit or strictly limit remote access to PII. The data must be encrypted if it is accessed remotely.	10.4
26	The organization should monitor the physical access to where the PII resides.	10.4
27	Individuals that have access to PII should be authorized for access by the company, and have read, understood, and signed a non-disclosure or similar agreement(s).	10.4
28	Organizations should monitor the information system to detect potential attacks and unauthorized remote or local connections.	10.4

PII POLICIES & MANAGEMENT		SECTION
29	The organization should create at least one written procedure for PII handling and management.	11
30	The definition of PII should be defined in the procedure.	6.1
31	A synopsis of all relevant privacy laws, regulations, and policies should be included in the procedure.	7
32	The procedure should strategically consider the location and storage of PII to minimize security or privacy incidents.	11.2
33	The departments and individual roles and responsibilities for using and protecting PII should be defined.	11.2

IDSO BEST PRACTICES
Personally Identifiable Information (PII)

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

PII POLICIES & MANAGEMENT		SECTION
34	The roles, responsibilities, and response for PII-related incidents should be defined.	11.2
35	The procedure should clearly define the accessibility of PII by individual and system to minimize the opportunity for PII to be compromised.	10.4, 11.2
36	The length of time that PII is stored and maintained should be defined.	11.2
37	The organization should assess risk associated with PII impact level.	9, 11.2
38	Guidance should be provided on restrictions of data collection, disclosure, sharing, storage and use of PII within the organization.	10.4, 11.2
39	The procedure should specify an interval for review of PII holdings to determine whether the PII is relevant and necessary.	11.2
40	The procedure should provide instructions for the proper disposal of PII.	8.3, 11.2
41	Rules should be written detailing the consequences for failure to follow privacy rules.	7, 11.2
42	The procedure should include instructions for handling a security or privacy breach involving PII.	10.5, 11.2

PII REVIEW AT REGULAR INTERVALS AND AT LEAST ANNUALLY		SECTION
43	The organization should conduct a periodic review of personnel permitted access to PII.	11.2
44	The organization should review their active data holdings for PII to assure that PII is properly sequestered, relevant and meets specific business criteria.	11.2
45	The organization should update their Risk Assessment document at least annually.	9, 11.2
46	Organizations should regularly review audit records of inappropriate or unusual activity affecting PII.	10.4, 11.2
47	The PII procedure should be updated at least annually.	11.2

BREACHES INVOLVING PII		SECTION
48	A response plan to handle PII breaches should be detailed in the PII procedure.	10.4, 10.5, 11.2
49	Technologies and systems for control, suppression, and retrieval may be useful for breaches involving PII.	10.4

50	Information obtained through detection, analysis, containment, and recovery should be collected to help protect against future incidents.	10.4

TRAINING		**SECTION**
51	The organization should provide training on access control policies including responsibilities, implementation, and access controls.	12.2
52	The organization should provide security awareness training to system users as part of the initial training and as procedures are updated.	12.2
53	The organization should provide contingency training to information systems users that are involved with systems that store PII.	12.2
54	The organization should provide incident response training for users that access information systems with PII storage.	12.2

COMPLIANCE REPORT

To: IDSO Membership

From: IDSO Review Committee

Report on the Statements

We have compiled the accompanying draft IDSO Standards which comprise the personally identifiable information (PII) best practices and standards as of January 31, 2018, including selected United States code and associated regulations relevant to the publication.

Responsibility for the Standards

The IDSO Review Committee is responsible for the review of the standards and best practices in accordance with applicable regulation and industry practices. Such materials are in compliance with U.S. regulation and industry best practices per the committee's best judgment and evaluation.

Our examination obtains evidence about content in the standards. The evidence selected depends on the examiners judgment, including the assessment of the risks of misstatement, whether due to fraud or error. In making those assessments, the examiner considers U.S. code and regulations in order to design procedures that are appropriate in the circumstances. These assessments are not for the purpose of expressing an opinion on the effectiveness of the best practices or standards.

Signature

Anthony Dykes, Attorney at Law
IDSO Counsel