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