भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक : पथप्रदर्शक :
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi-110002
दूरभाष Phones 2323 0131 2323 3375 2323 9402
Website : www.bis.org.in
e-mail :
तार Grams : मानकसंस्था : Manaksanstha

DRAFT IN WIDE CIRCULATION

Technical Committee: LITD 17

Document Dispatch Advice	
Ref	Date
LITD17/T- 106	04-07-2018

ADDRESSED TO:

1. All Members of Information Systems Security and Biometric Sectional Committee, LITD 17
2. All Principal Members of Electronics and Information Technology Division Council (LITDC)
3. All others interested

Dear Madam/Sir(s),

Please find enclosed the following draft Indian Standard:

DOC NO. LITD17(12162)	**Data privacy Assurance : Part 1 Engineering and Management Requirements**

Kindly examine this draft standard and forward your views stating any difficulties, which you are likely to experience in your business or profession, if this is finally adopted as National Standard.

Last Date for comments: 03-09-2018

Comments if any, may please be made in the format indicated and mailed to the undersigned. In case no comments are received or comments received are of editorial nature. You will kindly permit us to presume your approval for the above document as finalized. However, in case of comments of technical in nature are received then it may be finalized either in consultation with the Chairman, Sectional Committee or referred to the Sectional committee for further necessary action if so desired by the Chairman, Sectional Committee.
This document has been also hosted on BIS website (www.bis.gov.in).

Thanking you,

Yours faithfully,

(Reena Garg)
Head (Electronics & IT)
E-mail: litd17@bis.gov.in
hlitd@bis.gov.in
Tele: 011-23237093

Encl: As above

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक : पथप्रदर्शक :
जय हिन्द
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi-110002
दूरभाष Phones 2323 0131 2323 3375 2323 9402
Website : www.bis.org.in
e-mail :
तार : मानकसंस्था
Grams : Manaksanstha

व्यापक परिचालन मसौदा

प्रलेख प्रेक्षण संज्ञापन	
संदर्भ	दिनांक
एलआईटीडी17/टी-106	**04-07-2018**

तकनीकी समिति: एलआईटीडी17

पाने वाले का नाम:

1. सूचना प्रणाली सुरक्षा एवं बॉयोमैट्रिक विषय समिति, एलआईटीडी 17
2. इलैक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी विभाग परिषद, एलआईटीडीसी के प्रधान सदस्य
3. अन्य रुचि रखने वाले

महोदय(यों)

निम्नलिखित प्रलेख का अवलोकन करें:
एलआईटीडी17 (12162) **: डेटा गोपनीयता आश्वासन भाग 1 इंजीनियरिंग और प्रबंधन** आवश्यकताऐं

कृपया इस मसौदे का अवलोकन करें और अपनी सम्मतियाँ, यह बताते हुए कि यदि यह भारतीय मानक प्रकाशित हों तो अमल करने में आपके व्यवसाय में क्या कठिनाईयाँ आ सकती हैं, भेजें।

सम्मतियाँ भेजने की अंतिम तिथि **3-09-2018**

यदि कोई सम्मति प्राप्त नहीं होती हैं अथवा सम्मति में केवल संपादकीय संबधी त्रुटि हुई तो उपरोक्त प्रलेख को यथावत अंतिम रूप दिया जायेगा। यदि कोई सम्मति तकनीकी प्रकृति की हुई तो विषय समिति के अध्यक्ष के परामर्श से अथवा उनकी इच्छा पर आगे की कार्यवाही के लिए विषय समिति को भेजे जाने के बाद प्रलेख को अंतिम रूप दे दिया जाएगा |

यह दस्तावेज बीआईएस वेबसाइट www.bis.gov.in पर भी होस्ट किया जाता है।

धन्यवाद,

भवदीया,

(रीना गर्ग)
प्रमुख(इलैक्ट्रॉनिकी व आईटी)
ईमेल: hlitd@bis.gov.in,
litd17@bis. gov.in
टेलि: 011-23237093

संलग्नक : उपरोक्त

भारतीय मानक

डेटा गोपनीयता आश्वासन
भाग 1 इंजीनियरिंग और प्रबंधन आवश्यकताऐं

Draft Indian Standard

DATA PRIVACY ASSURANCE: Part 1

ENGINEERING AND MANAGEMENT REQUIREMENTS

ICS 35.030

BUREAU OF INDIANSTANDARDS
MANAKBHAVAN, 9 BAHADURSHAHZAFAR MARGNEW DELHI110002

FOREWORD

(Formal clauses to be added later)

This Indian Standard (Part 1) will be adopted by the Bureau of Indian Standards, after the draft finalized by Information Systems Security and Biometrics Sectional committee will be approved by the Electronics and Information Technology Divisional council.

Other parts in this series are:

Part 2 Engineering and Management guidelines

It is imperative for any organization processing personal information as part of its in-house business function, or its customer solution offering, to provide privacy assurance to those whose data it processes. The trigger for this is not only from data privacy regulations but also from market differentiation, enhanced consumer experience and employee satisfaction. This Indian standard is intended to serve as a privacy assurance framework for such organizations. Adoption of this standard will help organizations provide privacy assurance to customers and employees, and achieve & sustain privacy compliance to regulatory & contractual requirements.

This standard will help in providing data privacy assurance to individuals whose personal data the organization processes, in an environment of rapidly changing technology and regulatory landscape. It is important that the personal information management system is part of, and integrated with the organization's processes and overall management structure and that data privacy is taken into account right from the stage of design of processes, information systems, and controls, wherever personal information is involved.

The adoption of a privacy standard by an organization is a strategic decision for an organization influenced by the organization's business objectives, types of personal information processing involved, regulatory environment it is exposed to, complexity, structure and size of the organization.

Implementing this standard is not a substitute for regulatory compliance. Depending on applicable jurisdiction, nature of business and type of personal data processed, various data protection related laws may apply to an organization, which needs to be determined and complied with, by the organization. Besides providing certain level of assurance to consumers on data privacy, this standard will also help organizations in developing better understanding of such privacy requirements, embedding them into design and sustaining privacy assurance.

Contents

Draft Indian Standard

DATA PRIVACY ASSURANCE: Part 1 ENGINEERING AND MANAGEMENT REQUIREMENTS

1 SCOPE

This standard provides specific requirements – both management and engineering - for establishing, implementing, maintaining and continually improving a personal information management system. Personal information may be obtained by organizations directly from individuals either for the purpose determined by the organization or on behalf of another entity under contractual obligations. This Indian standard is applicable in both these cases, and for any industry domain such as retail, banking, logistics, entertainment, telecommunications, healthcare etc. where the individuals in business association provide their personal information, whether as a consumer, vendor, employee or prospect.

Organizations which have multiple business entities or entities located in different geographic locations may choose to adopt this standard for the organization as a whole or only for an individual entity. However, depending on the extent to which the personal data processing operations of such entity is dependent on other entities, certain parts of the standard may also apply to those entities which do not intend to adopt this standard.

The order in which requirements are presented in this standard does not reflect their importance or imply the order in which they are to be implemented.

This standard shall not apply for organizations that do not process personal data, or process personal data in non-electronic form.

This standard can be used by internal and external parties to assess the organization's ability to meet the data privacy requirements.

2 REFERENCE

The standard given below contains provisions, which through reference in this text constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed as follows:

IS No	*Title*
IS XXXXXPart 2	Data privacy assurance: part 2engineering and management guidelines
IS/ISO/IEC 27001	Information Technologies - Security Techniques - Information Security Management Systems - Requirements
IS/ISO/IEC 27000	Information Technology – Security Techniques – Information Security Management Systems-Overview and Vocabulary

3. DEFINITIONS

For the purpose of this standard, the definitions given in IS/ISO/IEC 27000 shall apply, in addition to the following:

3.1 Automated Decision Making

When a data subject is subjected to a decision solely on automated processing.

3.2 Consent

Data Subject's freely given, specific and informed agreement to the processing of their personal information.

3.3 Data controller

Any organization that determines the means and purposes of processing the personal Information.

NOTES

1. Organizations may or may not directly collect data from individuals (although that is the case most often), but at times a 3rd party organization may be entrusted to collect data, and even in such cases the organization outsourcing the collection process becomes data controller.

2. Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "PII controller" or "data exporter" can also be used in some countries instead of the term "Data controller".

3.4 Data Portability

Right to receive the personal data concerning Individual, which he or she has provided to a controller, in a structured, commonly used as machine readable format and have the right to transmit those data to another controller without any hindrance from the controller to which the personal data has been provided.

3.5 Data processor

Any organization that processes personal information on behalf of and in accordance with the instructions of a data controller.

NOTE - Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “PII processor” or “Data Importer” may also be used in some countries instead of the term “Data processor”. For an entity to become data processor, it shall also be a separate entity from Data Controller.

3.6 Data subject

Any natural person to whom the personal Information relates.

NOTE - Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “Data Subject” or “PII principal” or “Individual’ may also be used in some countries instead of the term “Data subject”.

3.7 Function

Any department, unit or formal group in an organization formed with an intent to meet certain objectives e.g human resources, accounting and finance etc.

3.8 Notice

Information regarding processing of personal information

3.9 Opt-in

Process or type of policy whereby the Individualis required to take an action to express explicit, prior consent for their personal information to be processed for a particular purpose.

3.10 Opt-out

Process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent, or oppose a specific type of processing.

Note -The use of an opt-out policy presumes that the data controller has the right to process the Personal information in the intended way. This right can be implied by some action of the Individual different from consent (e.g., placing an order in an online shop).

3.11Organization

Any organization, both for profit or otherwise, private or public, playing the role of a data controller, data processor or even both in few scenarios.

3.12 Personal Information

Any information that (a) can be used to identify the Individual to whom such information relates, or (b) is or might be directly or indirectly linked to anIndividual.

NOTES

1. Definition of personal information may vary between countries, and may include both personal data collected and generated within an organization. Examples of personal information are:
   Telephone Number (when it is allotted to a specific individual)
   Date of birth,
   Email ID
   Address Meta data such as telephone call logs, weblogs etc
   Identification numbers such as Aadhaar, PAN, and Social Security Number
2. Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “Personally Identifiable Information” or “Personal Data” or “PII” may also be used in some countries instead of the term “Personal Information”. In this standard, both the terms ‘Personal Data’ and ‘Personal Information’ have been used interchangeably.

3.13Privacy Incidents and Breaches

Any situation where personal information is processed in violation of one or more relevant requirements of data privacy regulations, privacy principles, contracts or policies is privacy incident.

When the incident pertains to a violation of personal information due to the accidental or unlawful destruction, loss, alteration, un-authorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, it also qualifies as a data privacy breach.

3.14Privacy Controls

The measures that protect personal or sensitive personal information by reducing the likelihood of occurrence of privacy risk.

NOTES

1. Privacy controls include strategic, tactical and operational measures, e.g., policies, procedures, guidelines, legal contracts, management practices or organizational structures.
2. Control is also used as a synonym for safeguard or countermeasure.

3.15Privacy risk assessment

It is the overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personal information

3.16 Processing

Any operation or set of operations performed upon personal information, whether or not by automatic means.

NOTE - Example of processing operations of personal information include, but not limited to collection, recording, organizing, analyzing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, masking, alignment or combination, blocking, erasure or destruction.

3.17 Profiling

Activity or analysis of an individual's behaviour or certain aspects based on past trends solely on automated decision making which produce legal effects concerning him or her or significantly affects him or her.

3.18Secondary use

Constitutes processing of personal information in conditions which differ from the primary use initially communicated to or agreed with the individual.

3.19 Sensitive Personal Information

A special category of personal information, either whose nature is sensitive, such as those that relate to the Individual's most intimate sphere, or that might have a significant impact on the Individual.

NOTES

1. Definition of what kind of data categories constitute Sensitive Personal Information may vary between countries as per the regulations but organizations are best placed to determine what constitute sensitive personal information depending on the nature of business, jurisdictions that apply to it, individuals etc. In context of India it shall include health records, biometrics, password, financial information, sexual orientation as per Information Technology (Amendment) Act, 2008.
2. Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "Sensitive PII" or simply "SPI" may also be used in some countries instead of the term "Sensitive Personal Information".

3.20Third Party

A natural or legal person, public authority, agency or body other than the individual, data controller, data processor and the natural persons who, are authorised to process personal information under the direct authority of the data controller or data processor.

NOTE:Third parties may include subcontractors, subsidiaries and branches of parent company.

4. PRIVACY ENGINEERING

In the development life cycle of any product, service or solution that involves processing of personal data, the organization shall introduce data privacy aspects during the design stage and it shall cover the entire personal data life cycle including data collection, processing operations, decommissioning, archival stages, etc.The need to fulfill each of the data privacy principles specified in 4.2 shall be evaluated by the organization.

4.1 Development of Privacy Requirements

The organization shall determine the requirements on data privacy that are relevant for the product, solution or service.

While determining the privacy requirements, the organization shall:

a) Determine applicable jurisdiction, both territorial and sectoral
b) Evaluate the applicability of regulations, which could be omnibus or sectoral laws
c) Identify contractual requirements pertaining to data privacy
d) Obtain inputs from Market and Consumer Expectations on data privacy
e) Factor for Design-induced requirements
f) Consider data classification criteria for the personal data that the organization is likely to process
g) Derive privacy and security controls from organizations' own privacy and security policies, processes and relevant control plans

4.2 Design considerations for Privacy

4.2.1 *Personal Data Collection*

The Organization shall determine the basis for collection & processing of personal data and shall ensure that collection of personal information is:

a) fair
b) one where the basis is legitimate
c) required for a specific and identified purpose
d) proportional to the need
e) at the right stage
f) done in lawful manner, without coercion

The basis for collection of personal data shall be relevant regulation, but in the absence of such a regulation, unless required to protect vital interest of the individual or fulfil a service or

contractwith the individual, the organizations shall obtain consent from the individual. In any case, organizations shall provide a notice to individual as in 4.2.2.

4.2.2 *Privacy Notice*

The Organization shall provide privacy notice to the individual prior to collection of personal data. When data collection is indirect or does not involve participation from the individual, the organization shall identify appropriate mechanisms to notify the individual about such collection.

While deploying Privacy notices, the organization shall take into consideration the following as per established procedure:

a) The contents of notice

b) Mode of delivery of notice

c) Timing of providing notice

d) Accessibility and comprehensibility, keeping in view diversity of individuals

e) Ease of readability

The contents of a privacy notice shall be determined by applicable regulation, but at the minimum it shall include the following:

a) Name & Address of organization collecting the personal data
b) Name & Address of organization retaining the personal data, if different from above
c) Types or categories of personal data collected
d) Purpose of collection and processing
e) Recipients of personal data, including any transfers

The key objective of providing a privacy notice to individuals is to make the data privacy practices transparent, and in order to achieve this effectively, organizations shall adopt suitable mode of communication such as privacy notices,website privacy policies, displaying privacy notices in prominent places, etc.

4.2.3 *Choice and consent*

Where consent is the basis for personal data collection, the organization shall provide individuals with privacy notice as in 4.2.2 and choice on the data intended to be collected, purpose of processing, and obtain lawful and fair consent in accordance with established policy. While

obtaining consent, the organization shall evaluate the following aspects and include them as appropriate:

a) Whether Opt-in or Opt-out

b) Default settings in case of Opt-out consent

c) Provision for individual to revoke consent

d) Timing of obtaining consent in order to give fair choice

The organization shall not use an individual's consent as a substitute for accountability.

4.2.4 *Use Limitation*

The use of personal data collected by organization shall be done only for purposes which are legitimate and agreed with individual. If personal data needs to be processed for a purpose that was not agreed or stated, the organization shall do so onlywith individual's consent.Notice will suffice if either the basis of processing does not require consentor if the new purpose is compatible with the original purpose.

The organization shall not use automated decision making alone, where the consequence of a decision causes significant harm or impact to individual. Automated decision making should be followed with manual intervention before taking the decision.

4.2.5 *Data Accuracy and Quality*

The organization shall ensure that personal information is kept accurate throughout the life cycle of personal data, and any incorrect information is promptly corrected. Provision shall be given by the organization to individuals to update their personal information when required.

4.2.6 *Security*

The organization shall adopt and implement an information security program to ensure confidentiality, integrity and availability of personal information. The degree of protection provided to various types of personal data shall be commensurate with the privacy risks, and the classification of each data type according to 4.1 (g).

The information security program shall be in compliant to industry recognized standards such as IS/ISO/IEC 27001 or any other standard prescribed by the applicable jurisdiction.

4.2.7 *Disclosure and Transfer*

Disclosure of personal data to third parties shall be only when necessary, and with consent of individual unless required by law.

The organization shall transfer personal information for further processing only if necessary and after ensuring that:

a) The vendor is evaluated to be compliant with the requirements of this standard as applicable.

b) Data privacy obligations are contractually agreed by vendor

4.2.8 *Personal Data Retention and Deletion*

The organization shall ensure that personal information is deleted when no longer required to be kept, according to a documented personal data retention policy. Deletion of personal data shall also be doneon specific request from individual unless applicable regulations do not permit. Use of irreversible de-identification techniques such as anonymization shall be adopted by the organization when data needs to be preserved for statistical, or research purpose.

4.2.9 Design Considerations to Fulfil Other Rights of Data Subjects:

The organization shall take into account design requirements emerging out of the need to fulfil any applicable rights of individuals such as the below and ensure the same are part of privacy requirements of section 4.1:

a) Right to personal data Portability

b) Right to Object to Profiling and Automated Decision Making

c) Right to Object to processing

The organization shall define circumstances under which such rights may not be fulfilled due to reasons such as disproportionate effort or cost, technological limitations, over-riding and legitimate business interests.

4.3 Verification & Testing

The organization shall ensure that the data privacy controls are verified and tested, as applicable, prior to deployment of a solution or product and at regular intervals, according to defined procedures.

While implementing verification activities, the organization shall ensure:

(a) Pre-determined privacy & security test scenarios are created for various use cases and potential threat scenarios
(b) Testing is independent
(c) Periodic compliance checks

5. PRIVACY MANAGEMENT

5.1 Privacy Objectives

The organization shall determine the applicability of this standard and define data privacy objectives. When doing so, the organization shall take into account the following but should not limit itself to the following:

a) The nature of business operations involving processing of personal information
b) The industry domain of the business and the regulatory landscape of the same
c) The type of individuals
d) The nature of personal information involved
e) Organization's business objectives
f) The geographical distribution of its operations
g) The extent to which the personal information processing is outsourced
h) Alignment with Privacy Policy

5.2 Data Privacy Function

The organization shall create a data privacy function, identify a competent and qualified person to be accountable on data privacy for the organization, its products, services or solutions. In order to enable this function the organization shall:

(a) Provide adequate resources
(b) Define structure of the function to ensure independence
(c) Define responsibilities and accountability on data privacy for the data privacy and various in-house functions involved

(d) Create a cross-functional data privacy council that helps communicating with all internal functions involved in processing or controlling personal information
(e) Ensure governance and oversight by Senior Leadership
(f) Demonstrate commitment from senior leadership in order to run a successful program.

5.3 Personal Information Management System

The organization shall establish a personal information management system (PIMS) that acts as a baseline and reference point for determining the data privacy requirements for the organization.

The organizations' PIMS shall include:

(a) Criteria for classifying personal information
(b) Inventory of personal information with level of details enough to help in determining data privacy controls
(c) Representation of personal information flow within, from and to the organization
(d) Procedure to introduce processing of new personal data element or change in any existing personal data element attribute
(e) Triggers for updating PIMS

5.4 Policies & Processes

5.4.1 *Privacy Policy*

The organization shall establish and document a privacy policy that applies to all business entities and locations of the organization as determined in the scope and shall be authorized by the senior management representative or a member of Board of Directors overseeing the data privacy function. Such policy shall be communicated to all stakeholders setting out the approach to manage the privacy objectives.

The privacy policy shall be aligned with the privacy objectives as per 5.1 apart from it, the policy shall include the following:

(a) Commitment of the top management towards fulfilment of data privacy objectives and requirements
(b) Privacy Principles that organization adopts to guide all activities related to personal information processing

5.4.2 *Processes & Guidelines*

The organization shall define,document and implement processes, procedures and guidelines on how the organization intends to achieve privacy objectives and comply with privacy policies.

While developing processes, the organization shall ensure that:

(a) The level of details and the content format is appropriate for the understanding of those functions or individuals that need to execute
(b) Responsibility is clearly defined for every activity
(c) Procedure to handle deviation and exceptions is included.

5.5 Records & Document Management

The organization shall define procedures for retaining records that demonstrate deployment of data privacy controls and for preserving various versions of policy and process documents.

While establishing such procedures, the following shall be considered:

(a) Record of logs that demonstrates affirmative action and options chosen by individual on privacy consent
(b) Evidence that captures events related to access, use, addition or change to personal information
(c) Policy on preservation of obsolete policies and process documents
(d) Retention period for the records and documents as specified in 4.2.8

5.6 Privacy Impact Assessments:

The organization shall conduct privacy impact assessment for various changes that get triggered from time to time and which may impact data privacy of individuals. In order to achieve this, the organization shall establish Data Privacy Impact Assessment methodology for ensuring consistency and rigor in carrying out data privacy impact for any change.

While defining such methodology, organization shall:

a) Define types of triggers that require such assessments e.g. new solution development, change in existing process/product.
b) Provide procedures, tools and techniques to carry our privacy impact assessments
c) Provide template for capturing the study outcome

The methodology to manage risks arising out of Privacy impact assessment shall be in accordance with 5.8.

5.7 Vendor Management

The organization shall define and document how vendors who process personal information on behalf of the organization are determined to be suitable and made accountable in the event of a data breach or privacy violation.

While establishing the mechanism, the organization shall ensure:

a) an effective process to evaluate and shortlist its vendors based on their data privacy practices and ability to meet organization's data privacy requirements.
b) data privacy obligations are reasonably transferred to the vendors contractually
c) periodic re-evaluation of their capability in ensuring data privacy

5.8 Privacy Risk Management

The organization shall establish and document privacy risk management methodology that defines how risks related to data privacy are managed and to ensure, at any time residual risks are kept at an acceptable level.

Such methodology shall include:

a. Triggers for initiating risk assessment

b. Criteria for risk evaluation

c. Privacy Risk Response Strategy

5.9 Data Privacy Incident Management:

The organization shall establish and document mechanism to manage incidents and data breaches.

Such process shall include:

(a) Breach discovery from both within the organization and from outside
(b) Investigation methodology, including root cause analysis, corrective and preventive action planning and implementation.
(c) Breach reporting process, to all relevant stakeholders including individuals and data privacy authority, where applicable.

5.10 Data Subjects' Access Management:

The organization shall establish and document mechanisms to respond to and serve access requests from an individual.

Such mechanisms shall include:

a) Providing access to one's information

b) Means to update ones' data, including deletion

c) Service level agreement including aspects on time and cost as applicable

d) Means to verify identity ofan individual

5.11 Grievance Redress:

The organization shall implement and document a grievance redress mechanism to handle grievances promptly.

Such mechanism shall include:

a) Identification & Publication of contact information of Grievance Officer
b) Channels for Receiving Complaints or requests from individuals.
c) Provision for escalation and appeal, wherever applicable.
d) Timelines for resolution of grievance as specified by applicable regulation, contract or as set by the organization

5.12 Staff Competency and Accountability

The organization shall ensure that the staff and contractors handling personal information shall be competent, kept aware and their accountability is established for any actions related to processing of personal information.

Staff handling personal information or activities related to processing personal information shall:

(a) Be trained and kept aware about developments depending on their role
(b) Be aware of their responsibility in protecting data
(c) Be traceable to their actions or inactions
(d) Subject to appropriate disciplinary actions when proved to be in violation of responsibility

The organization shall determine suitable criteria for qualification, certification and competency and evaluate staff before assigning them responsibility related to data privacy.

5.13 Ongoing Regulatory Compliance:

The organization shall put in place mechanisms that allow management to periodically monitor and review the compliance of the Privacy Information Management System with the applicable regulations and to ensure that the privacy features and controls built into solutions and products are updated based on changing privacy regulations and contracts.

5.14 Periodic Audits

The Organization shall institute periodic audits for the privacy information management system and allocate resources and authority to the audit group.

Such audits shall:

(a) Focus both on compliance organizations' practices with PIMS and effectiveness of PIMS in meeting regulatory, contractual obligations and market expectations.
(b) Include audit reports, detailing non-conformities which shall be formally reported to the auditee function and reviewed for timely closure by senior management.
(c) Be conducted by an independent group of auditors competent in data privacy, internal or external to the organization, at a periodicityappropriate for the organization.

5.15 Measurement & Continuous Improvement

The Organization shall implement a documented process for measuring and continuously improving the PIMS. Any improvements shall be based on pre-defined metrics, whether qualitative or quantitative, and appropriate initiatives may be taken up in areas that require improvement.

Metrics chosen by the organization shall be those that are most likely to reflect the effectiveness of PIMS.

6. Compliance

In order to be considered compliant with this standard, the organization shall fulfill the requirements of clause 4 & 5. Excluding any of the requirements specified in clause 4 and 5 of this standard is not acceptable when an organization claims its compliance with this standard, unless it demonstrates that certain sub clause do not apply based on an evaluation and the same shall be documented.