भारतीय मानक
Indian Standard

IS 17428 (Part 1) : 2020

डेटा गोपनीयता आश्वासन

भाग 1 इंजीनियरिंग और प्रबंधन आवश्यकताऐं

Data Privacy Assurance

Part 1 Engineering and Management Requirements

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

ICS 35.030

© BIS 2020

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.gov.in www.standardsbis.in

December 2020 Price Group 5

Information Systems security and Privacy Sectional Committee, LITD 17

FOREWORD

This Indian Standard (Part 1) was adopted by the Bureau of Indian Standards, after the draft finalized by Information Systems Security and Privacy Sectional committee had been 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. Implementation of this standard will help organizations to provide privacy assurance to customers, employees and also to achieve and sustain privacy compliance to regulatory and 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 data privacy 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 implementation of a privacy standard by an organization is a strategic decision 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.

In the formulation of this standard, assistance has been derived from the following standards:

IS/ISO/IEC 29100 : 2011	Information Technology — Security Techniques — Privacy framework
IS/ISO/IEC 27001 : 2013	Information Technologies — Security Techniques — Information Security Management Systems — Requirements

The composition of the Committee, responsible for the formulation of this standard is given at Annex A

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

CONTENTS

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

Indian Standard

DATA PRIVACY ASSURANCE

PART 1 ENGINEERING AND MANAGEMENT REQUIREMENTS

1 SCOPE

1.1 This standard (Part 1) provides specific requirements – both management and engineering - for establishing, implementing, maintaining and continually improving a Data Privacy 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 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.

1.2 Organizations which have multiple business entities or entities located in different geographic locations may choose to implement 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 implement this standard.

1.3 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.

1.4 This standard shall apply to organizations that process personal data but shall not apply to organizations that process personal data only in non-electronic form. This standard will also exclude non - personal information.

2 REFERENCES

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*
17428 Part 2 : 2020	Data privacy assurance Part 2 Engineering and Management Guidelines
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 and the following shall apply.

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 third 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' or 'data fiduciary' can also be used in some countries instead of the term 'Data controller'.

3.4 Data Portability — The right of an individual to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine readable format and have the right to transmit those data to another controller without 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.

FOR BIS INTERNAL USE, TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

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 ‘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 for example human resources, accounting and finance etc.

3.8 Non-personal Information — Any information that is not personal information as per **3.14** is non-personal information.

3.9 Notice — Information regarding processing of personal information.

3.10 Omnibus law — Omnibus laws are overarching laws and are sector agnostic. They apply to all sectors in a country or geographical territory for example FDPA in Germany, PDPA in Singapore, GDPR in Europe, etc.

3.11 Opt-in — Process or type of policy whereby the Individual is required to take an action to express explicit, prior consent for their personal information to be processed for a particular purpose.

3.12 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 (for example, placing an order in an online shop).

3.13 Organization — 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.

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

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:

a) Telephone Number (when it is allotted to a specific individual).

b) Date of birth.

c) Email ID.

d) Address.

e) Meta data such as telephone call logs, weblogs.

f) 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’, ‘Personal Data’, ‘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.

3.15 Privacy Incidents and Breaches — Any situation or instance where personal information is processed in violation of one or more relevant requirements of data privacy regulations, privacy principles, contracts or policies, is a privacy incident.

When the incident pertains to 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 personal data breach.

3.16 Privacy 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, for example, policies, procedures, guidelines, legal contracts, management practices or organizational structures.

2 Control is also used as a synonym for safeguard or countermeasure.

3.17 Privacy Risk Assessment — It is the overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personal information.

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

NOTE — Examples 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.

3.19 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.

3.20 Sectoral law — These laws apply to a particular industry sector such as health, banking, IT and may contain specific data privacy requirements among several other requirements that may or may not be related to data privacy. Examples of such sectoral laws are: HIPAA (Health Insurance Portability and Accountability Act) in USA, GLBA (Gramm–Leach–Bliley Act) in USA and Reserve Bank of India Act in India.

FOR BIS INTERNAL USE TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

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

3.22 Sensitive Personal Information — A special category of personal information, whose nature is either 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 The kind of data categories that constitute Sensitive Personal Information may vary between countries as per the regulations but organizations are best placed to determine what constitute sensitive personal information among various data that they collect or process. In context of India it shall include health records, biometrics, password, financial information, sexual orientation as per *Information Technology Act.*

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'.

3.23 Territorial Law — These laws are applicable to geographical territory or a region, for example state laws, CCPA (California Consumer Privacy Act) applies to California, USA.

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 data privacy requirements that are relevant for the product, solution or service.

While determining the privacy requirements, the organization shall take into consideration the following:

a) Applicable jurisdiction, both territorial and sectoral;

b) Various regulatory, statutory and contractual requirements;

c) Privacy and security controls from organization's own business needs, privacy and security policies and processes.

4.2 Privacy Principles Based Design considerations

4.2.1 *Personal Data Collection and Limitation*

The organization shall determine the lawful basis for collection and processing of personal data and shall ensure that collection of such personal data is fair, intended for specific and identified purposes and is proportional to the purpose. Collection shall be done at the right stage and in lawful manner, without coercion.

The lawful basis for collection of personal data shall be one of those required by relevant regulation, including consent if permitted. Such lawful basis determined for each purpose prior to commencement of processing, shall be documented as part of data inventory. 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 at the minimum shall include the following:

1) Name and Address of entity collecting the personal data;

2) Name and Address of entity retaining the personal data, if different from above;

3) Types and categories of personal data collected;

4) Purpose of collection and processing;

5) 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, the organization shall adopt suitable modes of communicating the privacy notices, including displaying them in prominent places and websites.

4.2.3 *Choice and Consent*

When consent is the lawful basis of collection of data, 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:

FOR BIS INTERNAL USE TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

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 only with individual's consent. Notice will suffice if either the basis of processing does not require consent or if the new purpose is compatible with the original purpose.

4.2.5 *Data Accuracy*

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.

4.2.7 *Disclosure and Transfer*

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

The organization, when using services of an external party to process personal data, shall transfer such data only after fulfilling the requirements mentioned in **5.7**.

4.2.8 *Personal Data Storage Limitation*

The organization shall ensure that personal information is retained only for the duration as required by the law or business purpose according to a documented personal data retention policy. Deletion of personal data shall also be done on 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 fulfill any rights of individuals as applicable, such as those mentioned below and ensure the same are part of privacy requirements of **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 and Testing

The organization shall ensure that the applicable 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.

5 PRIVACY MANAGEMENT

5.1 Privacy Objectives

The organization shall determine and define data privacy objectives and when doing so, the organization shall at a minimum take into account the following:

a) Nature of business operations involving processing of personal information;
b) Industry domain of the business and the regulatory landscape of the same;
c) Type of individuals;
d) Nature of personal information involved;
e) Organization's business objectives;
f) Geographical distribution of its operations;
g) 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;

FOR BIS INTERNAL USE, TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

c) define responsibilities and accountability on data privacy and various in-house functions involved;

d) create a cross-functional data privacy council, as applicable, 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 Data Privacy Management System

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

The organization's DPMS 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 DPMS.

5.4 Policies and 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 and 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 and Document Management

The organization shall maintain records of processing activities that demonstrate accountability towards its data privacy compliance. In order to achieve this, the organization shall establish and implement procedures that help identify various records along with the retention period. 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 and notice;

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.

5.6 Privacy Impact Assessment

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 privacy impact assessment methodology for ensuring consistency and rigour in carrying out data privacy impact for any change.

While defining such methodology, organization shall,

a) define types of triggers that require such assessments for example 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 outcome of the assessment.

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

5.7 Data Processor Management

The organization shall define and document how data processors which process personal information on behalf of the organization are evaluated, determined to be suitable and made accountable to minimize the risk of a personal data breach or data privacy incident.

While establishing the mechanism, the organization shall ensure,

FOR BIS INTERNAL USE TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

a) an effective process to evaluate and shortlist its data processors based on their data privacy practices and ability to meet organization's data privacy requirements;

b) data privacy obligations are reasonably transferred to the data processors 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 Privacy Incident Management

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

Such process shall include:

a) Incident discovery from both within the organization and from outside;

b) Investigation methodology, including root cause analysis, corrective and preventive action planning and implementation;

c) Incident reporting process, to all relevant stakeholders including individuals and data privacy authority, where applicable.

5.10 Data Subject's Request Management

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

Such mechanisms shall include:

a) Means to verify identity of an individual;

b) Providing access to data subject's information;

c) Means to update data subject's data, including deletion;

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

5.11 Grievance Redress

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

Such mechanism shall include:

a) Identification and 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, 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 Data Privacy 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 data privacy management system and allocate resources and authority to the audit group.

Such audits shall,

a) focus on compliance of organizations' practices with DPMS, effectiveness of DPMS in meeting regulatory and contractual obligations;

b) be conducted by an independent group of auditors competent in data privacy, internal or external to the organization, at a periodicity appropriate for the organization, at least once in a year.

5.15 Measurement and Continuous Improvement

The Organization shall implement a documented process for measuring and continuously improving the DPMS. Any improvements shall be based on pre-defined metrics, whether qualitative or quantitative,

FOR BIS INTERNAL USE, TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

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 DPMS.

6 COMPLIANCE

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

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

ANNEX A

(*Foreword*)

COMMITTEE COMPOSITION

Information Systems Security and Privacy Sectional Committee, LITD 17

Organization	*Representative(s)*
Ministry of Electronics & Information Technology, New Delhi	Shri Arvind Kumar (***Chairman***)
Bharat Electronics Ltd (BEL), Bengaluru	Shrimati Sangeetha Mangal Shri Devesh Kumar Singh (*Alternate*)
Centre for Development of Advanced Computing	Dr M. Sasikumar Shrimati P. R. Lakshmi Eswari (*Alternate*)
Centre for Internet & Society	Shri Sunil Abraham Shri Amber Sinha (*Alternate* I) Shri Gurshabhad Grover (*Alternate* II)
Data Security Council of India (DSCI)	Shri Aditya
Department of Science and Technology	Shri Sujit Banerjee Dr Rajeev Sharma (*Alternate*)
HCL	Shri Sanjeev Chhabra
Indian Cellular & Electronics Association (ICEA)	Shri Bijesh Kumar Roul Shri Rajesh Sharma (*Alternate*)
Infosys Technologies Limited	Mr Srinivas Poosarla Shri Rajeev Thykatt (*Alternate* I) Ms Ashwathy Asok (*Alternate* II)
In Personal Capacity	Dr Gargi Keeni Ms Amutha Arunachalam
Indian Statistical Institute	Prof Bimal K. Roy
KCPIL	Dr V. K. Kanhere
Larsen & Toubro Limited	Shri N. Sathyan Shri Tirumala Rao K. (*Alternate*)
Ministry of Electronics & Information Technology, New Delhi	Shri Rakesh Maheshwari Shri Tarun Pandey (*Alternate* I) Shri Santosh Soni (*Alternate* II) Dr Somnath Chandra (*Alternate* III) Shri S. K. Nehra (*Alternate* IV)
Ministry of Defence (DRDO)	Ms Noopur Shrotriya Shri G Anil (*Alternate*)
National Accreditation Board for Certification Bodies	Shri A. S. Bhatnagar Ms Anajna Jain (*Alternate*)
Narnix Technolabs Pvt Ltd	Shri Narang N. Kishore
NEC India Pvt Ltd	Ms Jidnya Shah Shri Abhay Pimplikar (*Alternate*)
Oxygen Consulting Services Pvt Ltd	Shri Sanjiv Kumar Agarwala Shri Sachin Jadhav (*Alternate*)
Patanjali Associates Pvt Ltd	Shri Kanti Mohan Rustogi
Qualcomm India Pvt Ltd	Shri Vinosh Babu James
ReBIT	Shri Prashant Lotlikar Shri Deepnarayan Tiwari (*Alternate*)

FOR BIS INTERNAL USE TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

Organization	*Representative(s)*
Smart Chip Private Limited	MR DIVANSHU GUPTA MR ANKIT GUPTA (*Alternate*)
Standardisation, Testing & Quality Certification (STQC)	SHRI A. K. SHARMA SHRI A. K. UPADHAYAY (*Alternate* I) SHRI NAKUL AGGRWAL (*Alternate* II)
Tata Communications Pvt Ltd	SHRI MAHESH KALYANARAMAN
Tata Consultancy Services	SHRI SATEESH SRINIWSAIAH SHRI NATARAJAN SWAMINATHAN (*Alternate* I) SHRI ABHIK CHAUDHURI (*Alternate* II) SHRI ANUPAM AGRAWAL (*Alternate* III)
Telecommunication Engineering Centre (TEC), DOT	SHRI ARVIND CHAWLA SHRI S. SRIDHAR (*Alternate*)
THE PERSPECTIVE	SHRI RAHUL SHARMA
Unique Identification Authority of India	SHRI YASHWANT SINGH SHRI ANUP KUMAR (*Alternate*)
WYSE Biometrics Systems Pvt Ltd	SHRI Y. D. WADASKAR
BIS Directorate General	SHRIMATI REENA GARG, SCIENTIST 'F' AND HEAD (LITD) [REPRESENTING DIRECTOR GENERAL (*Ex-officio*)]

Member Secretary

SHRI KSHITIJ BATHLA
SCIENTIST 'C', BIS

Panel 3 "Privacy Information Management System" LITD 17/P-3

Organization	*Representative(s)*
Infosys Technologies Limited	SHRI SRINIVAS POOSARLA (***Convener***)
Reliance Jio	SHRI MOHIT MALIK
Centre for Internet & Society	SHRI GURSHABAD GROVER
Data Security Council of India (DSCI)	SHRI ADITYA
Genpact	SHRI SRINJOY BANERJEE
HCL	SHRI SANJEEV CHHABRA
Infosys Technologies Limited	SHRI RAJEEV THYKATT MS NEHA AGRAWAL (*Alternate*)
In Personal Capacity	MS AMUTHA ARUNACHALAM MS DIMPLE SANTWAN
KPMG	SHRI SRINIVAS POTHARAJU SHRI MERRIL CHERIAN (*Alternate*)
Larsen & Toubro Limited	SHRI TIRUMALA RAO K.
Ministry of Electronics & Information Technology, New Delhi	SHRI RAKESH MAHESHWARI SHRI PRAFUL KUMAR (*Alternate*)
Tata Consultancy Services	SHRI VIJAYANAND BANAHATTI
THE PERSPECTIVE	SHRI RAHUL SHARMA
Unique Identification Authority of India	SHRI YASHWANT KUMAR SHRI ANUP KUMAR (*Alternate*)

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reproduced in any form without the prior permission in writing of BIS. This does not preclude the free use, in the course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright be addressed to the Director (Publications), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: LITD 17 (12162).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

FOR BIS INTERNAL USE. TO BE USED FOR STANDARDS DEVELOPMENT PURPOSE ONLY

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices: *Telephones*

Central : Manak Bhavan, 9 Bahadur Shah Zafar Marg
NEW DELHI 110002
{ 2323 7617
{ 2323 3841

Eastern : 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi
KOLKATA 700054
{ 2337 8499, 2337 8561
{ 2337 8626, 2337 9120

Northern : Plot No. 4-A, Sector 27-B, Madhya Marg
CHANDIGARH 160019
{ 265 0206
{ 265 0290

Southern : C.I.T. Campus, IV Cross Road, CHENNAI 600113
{ 2254 1216, 2254 1442
{ 2254 2519, 2254 2315

Western : Manakalaya, E9 MIDC, Marol, Andheri (East)
MUMBAI 400093
{ 2832 9295, 2832 7858
{ 2832 7891, 2832 7892

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. DURGAPUR. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. JAMMU. JAMSHEDPUR. KOCHI. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAIPUR. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi