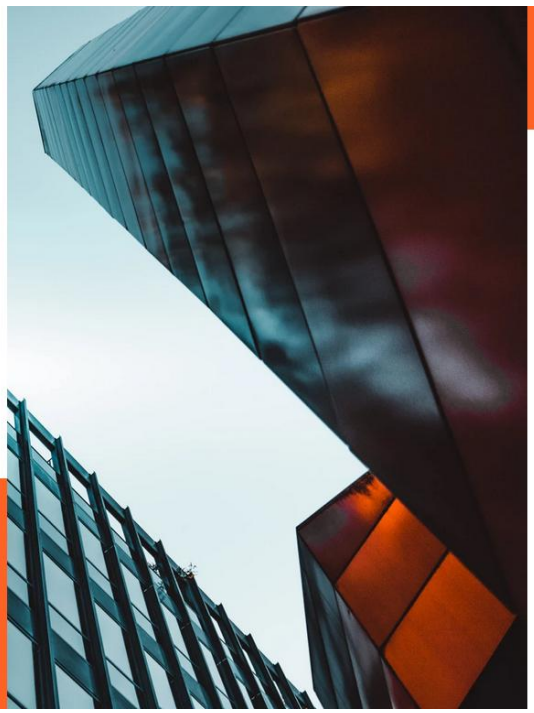
Reference Standard Document



V 1.0

Reference Standard Document for Data and Cyber Security
As maintained from time to time

Department of Information Technology

Government of Tamil Nadu

November 2021

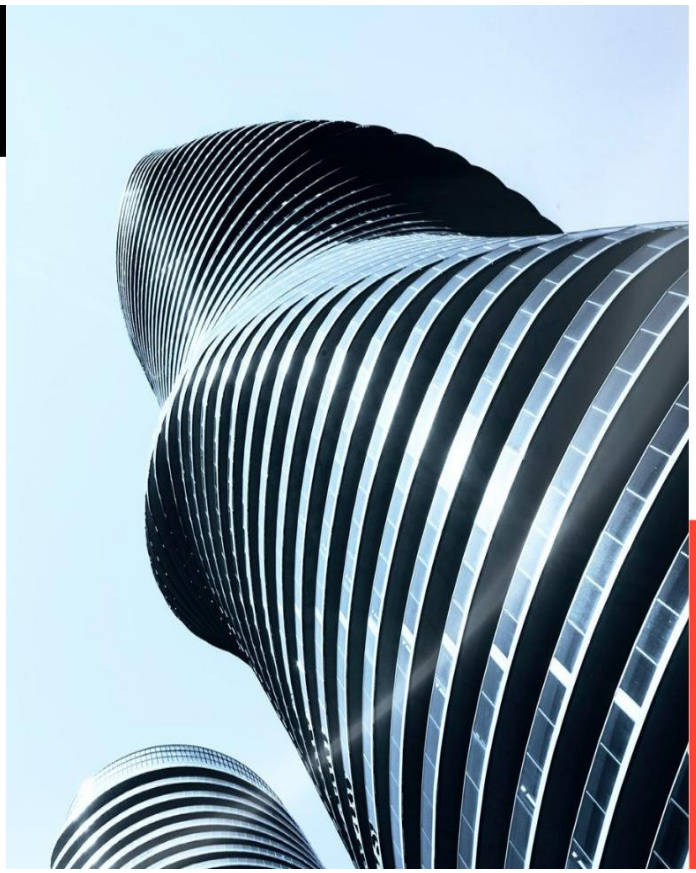
TABLE OF CONTENTS

1. Scope of the document

This document is generated as the Reference Standard Document for Data and Cyber Security in TamilNadu. This first version of the document is prepared towards adopting the standards as part of all the future governance projects. The document covers details about the Business Architecture standards, Application Architecture Standards, Interoperability Standards, Data Standards, and Cyber Security Standards.

The document is prepared with the vision to provide complete guidelines separated as Mandatory and optional for all governance projects. This document clearly explains in detail about the complete standards, benefits and references for the proposed system.

The document is prepared collaboratively by different stake holders and the document will be updated on periodic basis based on the inputs from the various sources. This document will play a major role in building up the complete standards and process of all governance projects.



Business Architecture standards

2. Business Architecture Standards

2.1 Design Thinking

Design thinking is an iterative process in which service designers seek to understand the user, challenge assumptions, and redefine problems to identify alternative strategies and solutions that might not be instantly apparent with the initial level of understanding.

Standard: Human-centered design for interactive systems (ISO 9241-210:2010) - It provides requirements and recommendations for human-centered design principles and activities throughout the life cycle of computer-based interactive systems.

Reference link : ISOStandards

2.2 Accessibility Standard

Conforming to the World Wide Web consortium's (W3C's) Web Content Accessibility Guidelines ensures that disabled people can also access services. Those with physical impairments can access specialized devices that read standards-compliant code, and those with cognitive impairments can be assured of a minimum level of access.

Standard: Web Content Accessibility Guidelines (WCAG) (Level A, AA, AAA) - The WCAG documents explain making web content more accessible to people with disabilities.

Reference link:https://www.w3.org/TR/WCAG20/

2.3 Business Process Modelling Standard

This is a standardized graphical notation for depicting business processes in a workflow. The primary goal is to provide a standard notation that is readily understandable by all business stakeholders.

Standard: Open Applications Group Integration Specification (OAGIS)**(**http://www.oagi.org. Accessed July 12, 2017 - OAGIS is an XML Interoperability standard and data model provided by the Open Access Group, supporting the electronic exchange of data, especially business documents.

Reference link:https://www.service-architecture.com/articles/xml/oagis.html

Standard: ISO/IEC/IEEE 31320-1& 2: Information technology — Modeling Languages — Part 1&2: Syntax and Semantics for IDEF0

Standard: Business Process Model and Notation (BPMN), Version 2.0 - The BPMN is a visual modeling language for business analysis applications and specifying enterprise process workflows; an open standard notation for graphical flowcharts is used to define business process workflows.

Standard: ISO 15000-5:2014 Electronic Business Extensible Markup Language (ebXML) - Part 5: Core Components Specification (CCS). Refer ISO Standard. Accessed July 12, 2017 - 2014 describes and specifies the Core Component solution as a methodology for developing a common set of semantic building blocks that represent general types of business data.

Technical Report: www.ebxml.org/specs/bpPROC.pdfCommon Business Processes v1.0.

Reference link:http://www.ebxml.org/specs/bpPROC.pdf

Standard: ebXML (2001) - The role of context in the re- usability of Core Components and Business Processes. UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business) and OASIS (Organization for the Advancement of Structured Information Standards).

Standard: NeST-GDL-OAPI.01. Version 1.0 - Implementation guidelines for Open APIs policy for e-Governance (National Data Highway).

Guidelines: Implementation guidelines for Open API policy for e-Governance NeST-GDL-OAPI.01. Version 1.0: 2020.

2.4 Business Architecture Notation

Unified Modelling Language would be used for designing systems, architecture designs and other modelling. UML is a language for specifying, constructing, visualizing, and documenting the artefacts of a software-intensive system. It is a general-purpose modelling language used with all major object methods and applied to all application domains.

Standard: Architecture Modelling Notation

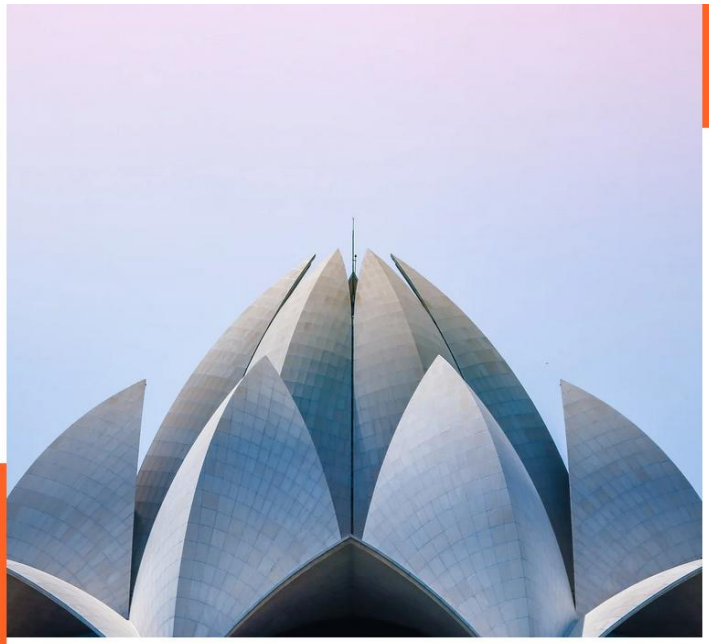
Standard: ISO 15704:2019 Enterprise modelling and architecture - Requirements for enterprise- referencing architectures and methodologies - This document specifies a reference base of concepts and principles for enterprise architectures that enable enterprise development, enterprise integration, enterprise interoperability, human understanding and computer processing.

2.5 Service Design

To ensure departments are planning delivery of e-services in a consistent way, digital service standard compliance would be mandated across the Government of TN Departments.

Standard: Digital Service Standard (DSS) Refer: NeST- GDL- IS.04 version 1.0 - is a set of over 170 National and International standards, principles and guidelines organized according to a rational taxonomy, which is easy to comprehend and implement by the Government eco-system.

Application Architecture Standards



3. Application Architecture Standards

3.1 Website Design

This standard recommends policies and guidelines for TN Government websites and portals, at any organizational level and belonging to both State Government and local Governments (including District Administrations to Village Panchayats) for making TN Government websites citizen-centric and visitor friendly. Compliance with these guidelines will ensure consistency and uniformity in the content coverage and presentation and promote excellence in TN Government Webspace.

Guidelines: Guidelines for Indian Government Websites.

References: https://web.guidelines.gov.in

Standard: Design: Cascading style sheets – CSS3, HyperText Markup Language – HTML 5.

Guidelines: NIST Special Publication 800- 37: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

References:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

3.2 Software Development Process

Business requirements should define the choice of Software Development Life Cycle (SDLC) model from either Waterfall or iterative or Agile model.

Standards

- Systems and software engineering: ISO/IEC/IEEE 24765 - Provides a common vocabulary applicable to all systems and software engineering work. It was prepared to collect and standardize terminology.

  Reference link: ISOStandards

- Software Lifecycle Process: IEEE standard 12207 - it aims to be a primary standard that defines all the processes required for developing and maintaining software systems, including the outcomes and/or activities of each process.

  Reference link:https://en.wikipedia.org/wiki/ISO/IEC_12207

- Re-use process: IEEE standard 1517 - A common framework for extending the system and software life cycle processes of IEEE Std 12207-2008 to include the systematic practice of reuse is provided. The processes, activities, and tasks to be applied during each life cycle process to enable a system and/or product to be constructed from reusable assets are specified.

  Reference link: ISO Standards

- Software Documentations: IEEE 1016 - This standard describes software designs and establishes the information content and organization of a Software Design Description (SDD).

  Reference link: ISO Standards

3.3 Software Coding

Standards/Guidelines

- Select the programming language appropriately to meet the documented requirements of the system
- Indent code for better readability
- Establish a maximum line length for comments and code to avoid horizontal scrolling of the editor window
- Use space after each comma, operators, values and arguments
- Break large, complex sections of code into smaller comprehensible modules/functions
- Arrange and separate source code between files
- Choose and stick to the naming convention
- Avoid elusive names that are open to subjective interpretation
- Do not include class names in the name of class properties
- Use the verb-noun method for naming routines
- Append computation qualifiers (Avg, Sum, Min, Max, Index) to the end of a variable name where appropriate
- Use customary opposite pairs in variable names
- Boolean variable names should contain Is, which implies Yes/No or True/False values
- Avoid using terms such as Flag when naming status variables, which differ from Boolean variables in that they may have more than two possible values
- Develop a list of standard prefixes for the project to help developers consistently name variables
- Wrap built-in functions and third-party library functions with your wrapper functions
- Constants should be all uppercase with underscores between words
- For variable names, include a notation that indicates the scope of the variable
- Provide useful error messages
- When modifying code, always keep the commenting around it up to date

- At the beginning of every routine, it is helpful to provide standard, boilerplate comments, indicating the routine's purpose, assumptions, and limitations
- To conserve resources, be selective in the choice of data type to ensure the size of a variable is not excessively large
- When writing classes, avoid the use of public variables. Instead, use procedures to provide a layer of encapsulation and also to allow an opportunity to validate value changes
- Do not open data connections using a specific user's credentials. Connections that have been opened using such credentials cannot be pooled and reused, thus losing the benefits of connection pooling

Guidelines: OWASP Secure Coding Practices: Quick Reference Guide Nov 2010 (https://owasp.org/www-pdf-archive/Owasp-171123063052.pdf)

3.4 Application Design

Standards to be implemented while designing presentation layer:

- Simple Object Access Protocol (SOAP) version 1.2 - It is a lightweight protocol for the exchange of information in a decentralized, distributed environment
- Web Service Description Language (WSDL) 2.0 – The *service* specifies a single interface that the service will support and a list of *endpoint* locations where that service can be accessed
- Web Accessibility Initiative - Accessible Rich Internet Applications (WAI-ARIA) -the Accessible Rich Internet Applications Suite defines a way to make Web content and Web applications more accessible to people with disabilities. It especially helps with dynamic content and advanced user interface controls developed with HyperText Markup Language (HTML), JavaScript, and related technologies
- Document Object Model, JavaScript Application Programming Interfaces (APIs), Mobile Web Applications, Web performance, Scalable Vector Graphics (SVG), Portable Network Graphics (PNG) Specifications, Web Computer Graphics Metafile (WebCGM), Timed Text Markup Language, - W3 Standards

Standards to be implemented while designing business-application layer:

- Web Services for Remote Portlets (WSRP) - OASIS-OPEN - Web Services for Interactive Applications (WSIA) and Web Services for Remote Portals (WSRP) aim to simplify the integration effort through a standard set of web service interfaces allowing integrating applications to quickly exploit new web services as they become available
- ISO/TC 171 - Document management applications - Standardization of technologies and processes involving capture, indexing, storage, retrieval,

distribution and communication, presentation, migration, exchange, preservation, integrity maintenance and disposal in the field of document management applications. Documents may be managed in micrographic or electronic form

- Multipurpose Internet Mail Extension (MIME) - It is an Internet standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images, and application programs
- ISO 19794 - It specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within an ISO/IEC 19785-1 data structure.
- Common Biometric Exchange Formats Framework (CBEFF) - It is a set of ISO standards defining an approach to facilitate serialisation and sharing of biometric data in an implementation agnostic manner
- Web Services Business Process Execution Language (WS - BPEL 2.0) - It is an OASIS standard for presenting activities in a business process with web services
- Unified Modeling Language (UML v2.3) - It is a language for specifying, constructing, and documenting the artifacts of software-intensive systems
- Service oriented architecture Modeling Language (SoaML) extends the UML to enable the modeling and design of services within a service-oriented design
- Business process execution language for web services – a language for the specification of business processes and business interaction protocols
- XSLT v2.0 - XSL Transformations - a language for transforming XML documents into other XML documents
- Compliance with Java Message Service (JMS) for all Java 2 Enterprise Edition J2EE), Message Oriented Middleware (MOM)
- ebXML Standard Message Service Specification Version 2.0 for security and reliability extensions to SOAP
- ISO1 5022 - XML Design rules to support the design of message types and specific information flows
- Interoperability Standards - Interoperability standards are harmonized and integrated individual standards constrained to meet healthcare and business needs for sharing information among organizations and systems for a specific scenario (use case) of health information exchanges.
- WCO Data Model Version 3.0 - The WCO Data Model is an initiative of the World Customs Organization to simplify and standardize data requirements of Cross-border regulatory agencies, including customs

- Open Office XML - ECMA-376, ISO/IEC 29500 - Information technology - Document description and processing languages - Office Open XML File Formats
- ISO 15489 International Standard for Record Management - Records management: Concepts and Principles
- ISO 9075 - Database Languages - SQL, which describe Structured Query Language
- ISO/IEC 10646 - 2017 specifies the Universal Coded Character Set (UCS). It is applicable to the representation, transmission, interchange, processing, storage, input, and presentation of the written form of the languages of the world as well as of additional symbols
- Open GIS Keyhole Markup Language (KML)

Standards to be implemented while designing Infrastructure Management and Security layer:

- ISO/ IEC 14102 - 2008 Information Technology – Guideline for the Evaluation and Selection of CASE Tools

  Reference link: ISO Standards
- ISO 16792 - 2015 specifies requirements for the preparation, revision, and presentation of digital product definition data hereafter referred to as data sets

  Reference link: : ISO Standards
- Virtualization Management (VMAN) - DMTF's Virtualization Management standard is a set of specifications that address the management lifecycle of a virtual environment

  Reference link:https://www.dmtf.org/standards/vman
- Open Virtualization Format (OVF) - An open standard for packaging and distributing virtual appliances, more generally, software to be run in virtual machines

  Reference link: https://en.wikipedia.org/wiki/Open_Virtualization_Format
- TR-069 - TR-069 enables remote and safe configuration of network devices called Customer Premises Equipment (CPE). A central server manages configuration called an Auto Configuration Server (ACS)

  Reference link:https://www.avsystem.com/crashcourse/tr069
- ISO/ IEC 27034 - ISO/IEC 27034 offers guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems, in other words, business and IT managers, developers and auditors, and ultimately the end-users of ICT

  Reference link:https://www.iso27001security.com/html/27034.html
- The Open Web Application Security Project

- CERT – Secure coding standards - CERT-In (the Indian Computer Emergency Response Team) is a government-mandated IT security organization

  Reference link:https://www.cert-in.org.in/

- ISO/IEC 24760 - 1A framework for identity management - defines terms for identity management and specifies core concepts of identity and identity management and their relationships

  Reference link: ISO Standards

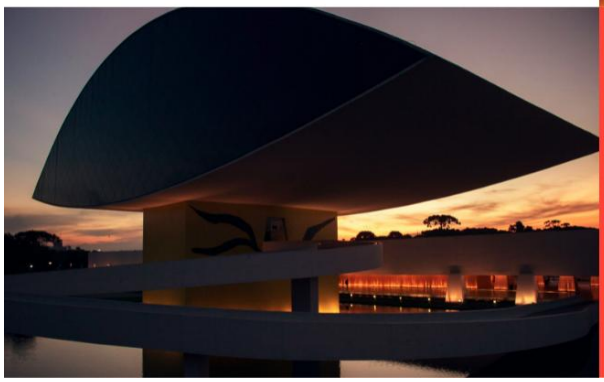
- ISO/IEC 29115 Entity Authentication Assurance - 2013 provides a framework for managing entity authentication assurance in a given context

  Reference link: ISO Standards

- ISO/IEC WD 29003 Identity Proofing and Verification - offers guidelines for the identity proofing of a person, specifies levels of identity proofing, and requirements to achieve these levels

  Reference link: ISO Standards l

InterOperability Standards



4. Interoperability Standards

4.1 Systems Interoperability

The purpose of this standard is to establish interoperability and information sharing amongst e-Governance systems using a common approach, agreed concepts and maintaining uniformity across all systems.

Mandatory Standard: Technical Standards for Interoperability Framework for E-Governance in India, IFEG version 1.0, May 2020.

Reference link: http://egovstandards.gov.in/technical-standards-ifeg

4.2 Organizational Interoperability

Organizational Interoperability enables a multilateral mechanism to ensure proper management and implementation of IFEG by identifying and addressing any possible barriers (including legal, political, managerial and economic). Multilateral mechanism means organizational structures, appropriate processes, adequate resources, facilities, autonomy and authority.

Steps for Achieving Organizational Interoperability

1. User identification standardization
2. Standardization of Processes
3. Information ownership matrix
4. Process Agreement

4.3 Semantic Interoperability

Semantic Interoperability addresses the requirement of understanding the meaning of data by different stakeholders in the same way while exchanging data.

The purpose of Semantic Interoperability is to build the capability of all stakeholders involved in the delivery of e-Services, with the following functionalities:

a. Discover information requirements for the delivery of quality e-Services
b. Explicitly describe the meaning of data to be shared multilaterally among the stakeholders
c. Process the received information in a manner consistent with its intended purpose

Steps for Achieving Semantic Interoperability

a. Semantic Interoperability Framework (SIF)
b. Domain Specific Metadata Standards

4.4 Technical Interoperability

To knit different kinds of e-Governance infrastructure and their services together through a catalogue of technical standards and specifications to achieve interoperability in e-Governance systems; this is done by exchanging information across various boundaries (applications, interfaces, libraries, levels of administration including vertical and horizontal) and storage/archival of the information.

4.5 Application Interoperability

Standards to knit different kinds of e-Governance applications and their services together:

Standards

- Use of SOAP v1.1/1.2 for web service invocation and communication
- REST (Representational State Transfer) is a simple stateless architecture that generally runs over HTTP and hence platform neutral. REST is a popular approach to development of web services and used by most popular web services around the world. When Web services use REST architecture, they are called RESTful APIs (or REST API for short).
- Description of all web services using WSDL V2.0. The web services description language describes web services in a way that other systems can consume the services
- WS-I Basic Profile 1.1 or Web Services interoperability profile is a set of non-proprietary web services specifications along with clarifications and amendments to those specifications that promote interoperability
- WS-I simple SOAP binding profile v1.0 defines the use of XML envelopes for transmitting messages and places constraints on their use
- Use of Hypertext Transfer Protocol (HTTP v1.1) and HTTPS as the application-level communications protocol for web services
- Use of SSL v3.0 for encryption / Use of TLS 1.3 or higher
- Open GIS Web Map Service Interface Standard (WMS) for GIS systems
- Extensible Stylesheet Language Transformations (XSLT v2.0) - a language for transforming XML documents into other XML documents
- XBRL Meta Model v2.1.1 - eXtensible Business Reporting Language - an XML language for business reporting
- XSL v1.0 - eXtensible Stylesheet Language - A family of recommendations for describing stylesheets for XML document transformation and presentation.
- ISO 8601 - Date and time representation standard

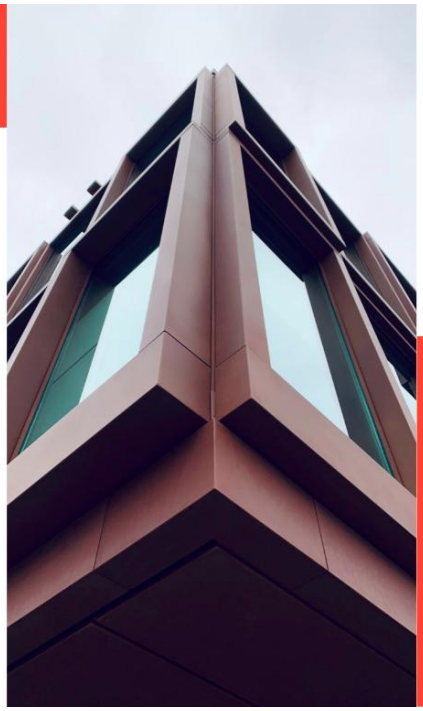
- Content Management Interoperability Services (CMIS)
- WCO Data Model Version 3.0

4.6 Data Interoperability and Data Exchange

Standards to exchange information between different kinds of applications and their services together:

Standards

- Use Extensible Markup Language (XML 1.0 or XML1.1) as a preferred data exchange standard
- JSON (JavaScript Object Notation, is an open standard file format and data interchange) format that uses human-readable text to store and transmit data objects consisting of attribute-value pairs and arrays (or other serializable values). It is a common data format with a diverse range of functionality in data interchange including communication of web applications with servers.
- Support the following standards for exchange of textual data:
  (a) Extensible Markup Language (XML 1.0 or XML 1.1) for most applications
  (b) Support Comma Separated Value (CSV) for legacy applications
- Support the following standards for the exchange of image data:
  (a) Joint Photographic Experts Group (JPEG) for photography images
  (b) Graphics Interchange Format (GIF) for internet images due to its small size and support for animation
  (c) Tagged Image File Format (TIFF) for scanned Images
  (d) Portable Network Graphic (PNG) for internet images which require increased color depth compared to GIF
- Support the following standards for the exchange of video and audio data:
  (a) Moving Pictures Expert Group (MPEG-1 to MPEG-4) for most audio and video applications
  (b) 3rd Generation Partnership Project (3GPP and 3GPP2) for audio and video over 3G mobile Networks
- Web Services Security (WS-Security, WSS) is an extension to SOAP (Simple Object Access Protocol) to apply security to Web services
- Use XML Metadata Interchange (XMI) as an XML Integration framework for defining, interchanging, manipulating and integrating XML data and objects
- Use xPath 2.0, an XML path language for selecting nodes from an XML document
- Use XQuery 1.0 to design query collections for XML data
- Use XSLT 2.0 for transforming XML documents into other XML documents.



Data Standards

5. Data Standards

5.1 Metadata and Data Standards

The adoption of Data Standards for use across e-Governance systems will enable easier, efficient data exchange and processing. It will also remove ambiguities and inconsistencies in the use of data.

Data and Metadata Standards (MDDS) provide information resources in the electronic form to communicate their existence and nature to other electronic applications (e.g., via HTML or XML) or search tools and permit the exchange of information between their applications.

Reference :http://egovstandards.gov.in/metadata-and-data-standard

Standards

- Universal Postal Union (UPU) Standards S42a-5 and S42b-5 (Postal Services)
- ISO 3166-1 alpha-3 Standard (Country Code) - Published by the International Organization for Standardization (ISO) to represent countries, dependent territories, and special areas of geographical interest

  Reference link: https://en.wikipedia.org/wiki/ISO_3166-1_alpha-3
- UNICODE It defines the way individual characters are represented in text files, web pages, and other types of documents

  Reference link:https://en.wikipedia.org/wiki/Unicode
- IETF RFC2822 (Email Address) - This standard specifies a syntax for text messages that are sent between computer users within the framework of "electronic mail" messages

  Reference link:https://datatracker.ietf.org/doc/html/rfc2822
- ISO 1000:1992 SI units and recommendations for the use of their multiples and certain other units
- ISO 369-3 (Language) Codes for the representation of names of languages.

  Reference link:https://en.wikipedia.org/wiki/ISO_639-3
- ITU-T E.164 (Country Code) - E.164 is an international standard, titled the international public telecommunication numbering plan, that defines a numbering plan for the worldwide public switched telephone network and some other data networks

  Reference link:https://en.wikipedia.org/wiki/E.164
- OASIS- CIQ-XNL version 2.0 (Full Name) - A standard for specifying person and organization names (as well as several related attributes such as former names, aliases, titles, generational identifiers. It does not provide matching rules for determining equivalence between names

  Reference link:
  https://www.immagic.com/eLibrary/ARCHIVES/TECH/OASIS/XAL_V2.PDF

- ISO/IEC 5218:2004 (Gender) - A uniform representation of human sexes to interchange information. It provides a set of numeric codes that are independent of language-derived codes and as such is intended to provide a common basis for the international exchange of information containing human sex data
- ISO 19785-1 (Common Biometric Exchange Formats Framework - CBEFF) - Structures and data elements for Biometric Information Records (BIRs)
- ISO/IEC 19794-5:2005 (E) (Face Image Data) - It specifies scene, photographic, digitization and format requirements for images of faces to be used in the context of both human verification and computer automated recognition
- ISO 19794-4:2005 (E) Finger Image Standard - It specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within an ISO/IEC 19785-1 CBEFF data structure
- ISO/IEC 19794-6:2005 (E) Iris Image Data - specifies two alternative image interchange formats for biometric authentication systems that utilize iris recognition. The first is based on a rectilinear image storage format that may be raw and the second format is based on a polar image specification that requires certain pre-processing and image segmentation
- ISO 19785-3 (Patron Format Specification) - Information technology - Common Biometric Exchange Formats Framework
- ISO-3166-1981 Standard (Country name) - Codes for the representation of names of countries
- XAL version 2 Standard of OASIS (Address) - xAL is designed to fit into other XML information structures that need the specification of an international address. The specification does allow for address specification at a multitude of detail levels, ranging from many unassigned address lines to subdividing elements such as "Street" into composing elements
- IAFIS-IC-0110 (V3) (Image Compression) - The Integrated Automated Fingerprint Identification System (IAFIS) is a computerized system maintained by the Federal Bureau of Investigation (FBI) since 1999. It is a national automated fingerprint identification and criminal history system. IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses
- ISO/IEC 19784-1 (Bio API Specifications Standards) - Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that supports the provision of that biometric system using components from multiple vendors.

5.2 Data Management

Standards to manage **data capture and storage:**

Standards

- Use of DBMS that supports JDBC latest version for java-based applications and ODBC for non-java-based system
- Support for SQL:2003 standards defined in ISO/IEC 9075. SQL:2003 is the fifth revision of SQL used by relational database
- Support for SQL:2008 standards defined in ISO/IEC 9075. SQL:2008 is the latest 2008 revision of SQL used by relational database
- Use ISO 15489-1 for records management - Information and documentation - Records management - Part 1: Concepts and principles
- Use portable document format for document - management based on ISO 32000-1
- Use ISO/TR 18492 for long-term preservation of electronic document-based information
- Establish a system for archiving information for both digitalized and physical. This framework is based on ISO 14721.

5.3 Data Design

- Use one of the following notations for data-modelling:
  a. Unified Modelling Language (UML)
  b. Barker's Notation
  c. Information Engineering
- The Unicode Standard is a character coding system designed to support the worldwide interchange, processing, and display of the written texts of the diverse languages and technical disciplines of the modern world. In addition, it seamlessly supports classical and historical texts of many written languages.

5.4 Data Security

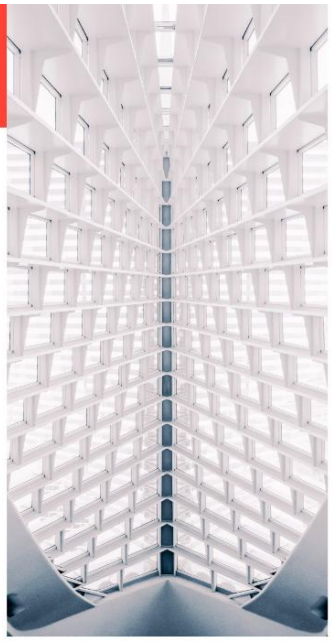
- The reference standards for cryptography include Triple Data Encryptions Standard (3DES), **Advanced Encryption Standard (AES),** and Post Quantum Cryptography (PQC)
- Security, Protection and Privacy
- Data security technologies related to access controls, authentication, back-ups and recovery, data masking, data erasure, data resilience should be considered
- Data auditing; real-time alerts; risk assessment; data minimization; purge stale data should be considered

- **Payment Card Interface (PCI), Data Security Standards (DSS**) Standard - The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

References Link :

https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

- Use RDBMS that supports the following security controls:
- Data access as an intended privilege
  - Key management and encryption
  - Integrity constraints such as domain constraints, attribute constraints, relation constraints, and database constraints
  - High availability implementation, backup, restoration and data replication
  - Database log and policy enforcement



Cyber Security Standards

6. Cyber Security Standards

6.1 Application Security

Application Security standards to be adopted during the designing, development, and implementation of application systems.

Standards

- OWASP Application Security Verification Standard (ASVS) - The Open Web Application Security Project (OWASP) is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security.
- ISO/IEC 27034 – ISO/IEC 27034 offers guidance on information security through a set of integrated processes throughout the Systems Development Life Cycle (SDLC) of an organization.

  Reference link:https://www.iso27001security.com/html/27034.html
- Common Weakness Enumeration (CWE) - The Common Weakness Enumeration is a category system for software weaknesses and vulnerabilities. It is sustained by a community project with the goals of understanding flaws in software and creating automated tools that can be used to identify, fix, and prevent those flaws.
- CERT Coding Standards - The SEI CERT Coding Standards are software coding standards developed by the CERT Coordination Center to improve the safety, reliability, and security of software systems. Individual standards are offered forC, C++, Java, Android OS, and Perl.

6.2 Information Security Management

Information Security Management covers the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

Standards

- ISO/IEC 27001 - ISO/IEC 27001 is an international standard on managing information security. The standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005 and revised in 2013. It details the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) – the aim is to help organizations make the information assets they hold more secure. **Reference link:**https://en.wikipedia.org/wiki/ISO/IEC_27001.
- **NIST Cybersecurity Framework** - NIST Cybersecurity Framework guides how organizations' internal and external stakeholders can manage and reduce cybersecurity risk. It lists organization-specific and customizable

activities associated with managing cybersecurity risk and it is based on existing standards, guidelines, and practices.

Reference link: https://www.nist.gov/cyberframework/framework

6.3 Network Security

Standards designed to ensure network security of devices, applications, services, and end-users, including security gateways and Virtual Private Networks (VPNs).

Standard: ISO/IEC 27033 - ISO/IEC 27033 provides detailed guidance on the security aspects of the management, operation and use of information system networks and their interconnections. Those individuals within an organization responsible for information security in general, and network security in particular, should adapt the material in this standard to meet their specific requirements.

Reference link: https://www.iso27001security.com/html/27033.html.

6.4 Wireless Security

Standards for design, implementation, and management of Wireless Local Area Network (WLAN) networks:

Standard: IEEE 802.11 - IEEE 802.11 is part of the IEEE 802 set of Local Area Network (LAN) technical standards and specifies the set of Media Access Control (MAC) and Physical Layer (PHY) protocols for implementing Wireless Local Area Network (WLAN) computer communication. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand and are the world's most widely used wireless computer networking standards. IEEE 802.11 is used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate and access the Internet without connecting wires.

Reference link:https://en.wikipedia.org/wiki/IEEE_802.11

Standard: WPA2/WPA3/WEP- Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are the three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). It is not recommended to use WEP

Reference link: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

6.5 Information Security Incident Management

Information Security Incident Management covers the principles of security to prevent and respond effectively to information security incidents.

Standard: ISO/IEC 27035 - The ISO/IEC 27035 Information Security Incident Management is an international standard that provides best practices and guidelines for conducting a strategic incident management plan and preparing for incident response.

Reference link:https://www.iso27001security.com/html/27035.html

6.6 Storage Security

Storage Security scope covers the security of devices and media, security of management activities related to the devices and media, applications/services, and end-users, in addition to the security of the information being transferred across the communication links associated with storage.

Standards/Guidelines

ISO/IEC 27040 - The purpose of ISO/IEC 27040 is to provide security guidance for storage systems and ecosystems and the protection of data in these systems.

IEEE P1619-2007 - Institute of Electrical and Electronics Engineers (IEEE) standardization project for encryption of stored data, but more generically refers to the Security in Storage Working Group (SISWG), which includes a family of standards for the protection of stored data and the corresponding cryptographic key management

Reference link: https://en.wikipedia.org/wiki/IEEE_P1619

IEEE P1619.1 - The P1619.1 Authenticated Encryption with Length Expansion for Storage Devices uses the following algorithms: Counter mode with CBC-MAC (CCM), Galois/Counter Mode (GCM), Cipher Block Chaining (CBC) with HMAC-Secure Hash Algorithm, XTS-HMAC-Secure Hash Algorithm

Reference Link:https://en.wikipedia.org/wiki/IEEE_P1619

IEEE P1619.2 -The P1619.2 Standard for Wide-Block Encryption for Shared Storage Media has proposed algorithms including XCB, EME2

Reference Link:https://en.wikipedia.org/wiki/IEEE_P1619

IEEE P1619.3 - The P1619.3 Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data defines a system for managing encryption data at rest security objects which includes architecture, namespaces, operations, messaging and transport

Reference Link: https://en.wikipedia.org/wiki/IEEE_P1619

6.7 Secure Design and Implementation of Virtualized Servers

Standards for secure design and implementation of virtualized servers

Standard: ISO/IEC 21878 - Information technology - Security techniques - Security guidelines for design and implementation of virtualized servers.

6.8 Cloud Security

Cloud Security Standards covers process secure design and implementation of cloud-based environments.

- The infrastructure elements including server, storage (including backup storage) and network of the Cloud should provide strong tenant isolation, provide granular identity and access management capability and encryption and be logically separate from other tenants and preferably hosted in the TNSDC (Tamil Nadu State Data Center) for reliable security.
- The entire N/W Path for each hosted government application shall be separate (logical separation & isolation) from the other clients (including other government departments).
- The cloud service offering shall support Network and Security with virtual firewall and virtual load balancer integration for auto-scale functions. It must have a separate VLAN provision with a dedicated virtual firewall between the VLANs and each client.

Standard: ISO/IEC 27017 is a security standard developed for cloud service providers and users to make a safer cloud-based environment and reduce the risk of security problems.

6.9 Privacy Information Management

The Privacy Information Management standard provides guidance on protecting privacy, managing personal information, and demonstrating compliance with major privacy regulations.

Standard/Guidelines

- ISO/IEC 27701 - The design goal is to enhance the existing Information Security Management System (ISMS) with additional requirements to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). **Reference link:** https://en.wikipedia.org/wiki/ISO/IEC_27701
- **Personal Data Protection Bill, 2019** - **Reference link:** https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
- **HIPA, FINRA, GDPR, PCI DSS** - The Health Insurance Portability and Accountability Act of 1996 is a United States federal statute enacted by the104th United States Congress and signed into law by President Bill Clinton on August 21, 1996. It was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.

The Financial Industry Regulatory Authority (FINRA) is a private American corporation that acts as Self-Regulatory (SRO), which regulates member brokerage firms and exchange markets.

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and simplify the regulatory environment for international business.

Reference links:

https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

https://en.wikipedia.org/wiki/Financial_Industry_Regulatory_Authority

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

6.10 Supply Chain Security

Private and public sector organizations increasingly rely on information and communication technology (ICT) solutions, which are produced globally, to run their operations.

Standard: The Open Trusted Technology Provider Framework (O-TTPF) is a compendium of organizational guidelines and best practices relating to the integrity of commercial off-the-shelf (COTS) information and communication technology (ICT) products and the security of the supply chain throughout the entire product life cycle. The Framework serves as the basis for the Open Trusted Technology Provider Standard (O-TTPS), which is approved as ISO/IEC 20243:2018. Reference Link: https://publications.opengroup.org/c185-1?_ga=2.135284729.910845472.1630396551-1522730350.1588184791

6.11 Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The process covers Information exchange on the Internet using a PKI, the entire lifecycle of public-key certificates used for digital signatures, authentication and the key establishment/exchange element of encryption are covered under the below standards.

7. Standards

1. ISO/IEC 27099 - Information Technology - Public key infrastructure - Practices and policy framework
2. ISO/IEC 29192 - This part of ISO/IEC 29192 specifies three lightweight mechanisms based on asymmetric cryptography. Three mechanisms are Crypto GPS, ALIKE, Identity-based signature scheme
3. Public-Key Cryptography Standards (PKCS) - These are a group of public-key cryptography standards devised and published by RSA Security LLC, starting in the early 1990s. The company published the standards to promote the use of the cryptography techniques to which they had patents, such as the RSA algorithm, the Schnorr signature algorithm and several others. Though not industry standards, some of the standards in recent years have begun to move into the "standards-track" processes of relevant standards organizations such as the IETF and the PKIX working-group
4. **CCA Guidelines conforming to IT Act 2000 and its latest amendments are given at http://cca.gov.in/guidelines.html.**
5. **Standards: PKCS Standards from PKCS#1 to PKCS#15 excluding PKCS#13** (as it is not finalized and stable). **e-Sign need to be used for digital transactions**

8. General Instructions

1. This document specifies standards which are to be complied mandatorily and the standards which are optional. However, in exceptional cases where the mandatory standards could not be complied with, the procuring entity / organization may take appropriate decisions to suit the requirements for reasons to be recorded in writing and the fact may be informed to Principal Secretary, IT and TNeGA.
2. All information on incidents be shared regularly with the Indian Computer Emergency Response Team (CERT-IN), NCIIPC (National Critical Information Infrastructure Protection Center), and CSA-TN (Cyber Security Architecture - Tamil Nadu).

9. References

- https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
- https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
- https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

10. Table of Mandatory / Optional Standards

Business Architecture Standards				
S. No.	**Standard Category**	**Suggested Standard**	**Recommendation**	**Remark**
1.1	Design Thinking	Human-centered design for interactive systems (ISO 9241-210:2010)	Optional	Holistic capacity building for departments and stakeholders will follow the standards
1.2	Accessibility Standard	Web Content Accessibility Guidelines (WCAG) (Level A, AA, AAA)	Mandatory	Mandatory as per accessibility standards for e-Governance
1.3	Business Process Modelling Standard	Open Applications Group Integration Specification (OAGIS)	Optional	Holistic capacity building for departments and stakeholders will follow the standards
1.3	Business Process Modelling Standard	ISO/IEC/IEEE 31320-1 & 2	Optional	Holistic capacity building for departments and stakeholders will follow the standards
1.3	Business Process Modelling Standard	Business Process Model and Notation (BPMN)	Optional	Holistic capacity building for departments and stakeholders will follow the standards
1.3	Business Process Modelling Standard	ISO 15000-5:2014 Electronic Business Extensible Markup Language (ebXML)	Mandatory	Mandatory as per accessibility standards for e-Governance
1.3	Business Process Modelling Standard	ebXML (2001)	Optional	Holistic capacity building for departments and stakeholders will follow the standards
1.3	Business Process Modelling Standard	NeST-GDL-OAPI.01	Optional	The departments and stakeholders will follow the standards
1.4	Business Architecture Notation	ISO 15704:2019	Optional	The departments and stakeholders will follow the standards
1.5	Service Design	Digital Service Standard (DSS) Refer: NeST-GDL-IS.04 version 1.0	Mandatory	Mandatory e-Governance standards
Application Architecture Standards				
S. No.	**Standard Category**	**Suggested Standard**	**Recommendation**	**Remark**
2.1	Website Design	Guidelines for Indian Government Websites	Mandatory	Mandatory e-Governance standards
2.1	Website Design	CSS3 + HTML5	Mandatory	Responsive and device compatibility - Latest website development

				standards

2.1	Website Design	NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations	Optional	Important Risk Management Framework for securing Government digital assets
2.2	Software Development Process	Systems and software engineering:ISO/IEC/IEEE 24765	Mandatory	Mandatory e-Governance standards
2.2	Software Development Process	Software Lifecycle Process:IEEE standard 12207	Mandatory	Software vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.2	Software Development Process	Re-use process: IEEE standard 1517	Mandatory	Software vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.2	Software Development Process	Software Documentations: IEEE 1016	Mandatory	Software vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.3	Software Coding	Guidelines listed in standards document	Mandatory	Software vendors need to self-certify code files and user departments/agencies must carry out independent code audits
2.3	Software Coding	OWASP Secure Coding Practices: Quick Reference Guide Nov 2010	Mandatory	Software vendors need to self-certify code files and user departments/agencies must carry out independent code audits
2.4	Application Design	**Presentation Layer**		
2.4	Application Design	Simple Object Access Protocol (SOAP) version 1.2	Optional	REST / SOAP is recommended
2.4	Application Design	Web Service Description Language (WSDL) 2.0	Optional	REST / WSDL is recommended
2.4	Application Design	Web Accessibility Initiative	Mandatory	Accessibility standards
2.4	Application Design	W3 Standards	Mandatory	W3 Standards should be followed for application design
2.4	Application Design	**Business application layer**		
2.4	Application Design	Web Services for Remote Portlets (WSRP) - OASIS-OPEN	Mandatory	For secure exchange of information between multiple applications

2.4	Application Design	ISO/TC 171 - Document management applications	Optional	Should be implemented by software vendors for building accessible, available and secure DMS systems
2.4	Application Design	Multipurpose Internet Mail Extension (MIME)	Mandatory	To ensure email communication sent by applications can be interpreted by all mail client
2.4	Application Design	ISO 19794	Mandatory	Should be implemented by software vendors for Secure transmission of biometric data
2.4	Application Design	Common Biometric Exchange Formats Framework (CBEFF)	Mandatory	Should be implemented by software vendors for Standardized data structures for biometric data
2.4	Application Design	Web Services Business Process Execution Language (WS - BPEL 2.0)	Optional	standard for documenting and interpreting business processes
2.4	Application Design	Unified Modeling Language (UML v2.3)	Mandatory	UML V2.3 or higher verison is mandatory
2.4	Application Design	SoaML	Optional	Capacity building needs to be done with departments and entities to implement and interpret
2.4	Application Design	Business process execution language for web services	Optional	Capacity building needs to be done with departments and entities to implement and interpret
2.4	Application Design	XSLT v2.0 - XSL Transformations	Mandatory	Should be implemented by software vendors for Standardized data structures for biometric data
2.4	Application Design	Java Message Service (JMS) for all Java 2 Enterprise Edition J2EE), Message Oriented Middleware (MOM)	Optional	Other messaging platforms can also be adopted specific to platform used for building application/ as per business use case or requirements eg. TIBCO, Apache Kafka, RabbitMQ
2.4	Application Design	ebXML Standard Message Service Specification Version 2.0	Optional	Mandatory for applications using SOAP
2.4	Application Design	ISO1 5022 - XML XML Design rules	Optional	Newer standards like ISO 20022 should be preferred
2.4	Application Design	**Interoperability Standards**		
2.4	Application Design	WCO Data Model Version 3.0 -	Optional	Version 3.9 should be adopted
2.4	Application Design	Open Office XML - ECMA-376, ISO/IEC 29500 - Information technology	Optional	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor

2.4	Application Design	ISO 15489 International Standard for Record Management	Optional	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	ISO 9075 - Database Languages - SQL	Optional	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	ISO/IEC 10646 - 2017 - Universal Coded Character Set (UCS)	Mandatory	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	Open GIS Keyhole Markup Language (KML)	Optional	OGC KML 2.3 should be adopted
2.4	Application Design			
2.4	Application Design	**Infrastructure Management and Security layer**		
2.4	Application Design	ISO/ IEC 14102 - 2008 Information Technology – Guideline for the Evaluation and Selection of CASE Tools	Mandatory	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	ISO 16792 - 2015 specifies requirements for the preparation, revision, and presentation of digital product definition data hereafter referred to as data sets	Mandatory	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	DMTF's Virtualization Management standard	Optional	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	Open Virtualization Format (OVF)	Optional	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	TR-069 - Remote and safe configuration of network devices called Customer Premises Equipment (CPE)	Mandatory	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	ISO/ IEC 27034	Mandatory	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	Secure coding standards - CERT-In	Mandatory	Should be listed as part of the coding standards section. Should be implemented wherever applicable
2.4	Application Design	ISO/IEC 24760 - 1A framework for identity management	Mandatory	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor

2.4	Application Design	ISO/IEC 29115 Entity Authentication Assurance	Optional	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
2.4	Application Design	ISO/IEC WD 29003 Identity Proofing and Verification	Mandatory	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
Interoperability Standards				
S. No.	**Standard Category**	**Suggested Standard**	**Recommendation**	**Remark**
3.1	Systems Interoperability	Interoperability Framework for E-Governance in India (IFEG)	Optional	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
3.2	Organizational Interoperability	1. User identification standardization 2. Standardization of Processes 3. Information ownership matrix 4. Process Agreement	Optional	Holistic capacity building for user departments and other stakeholders needs to be done before developing and making standards mandatory.
3.3	Semantic Interoperability	1. Semantic Interoperability Framework (SIF) 2. Domain Specific Metadata Standards	Optional	As mentioned in the reference document, the capability of all stakeholders needs to be built before developing and making standards mandatory.
3.4	Technical Interoperability	A catalogue of technical standards and specifications	Optional	Requires extensive interactions between user departments and other stakeholders for exchanging information and developing standards.
3.5	Application Interoperability	SOAP v1.1/1.2	Optional	REST should be followed
		REST API	Mandatory	Vendors need to adhere with these standards and self-certify. Could be included as part of the tender to ensure compliance of the vendor
		WSDL V2.0	Optional	REST should be followed
		WS-I Basic Profile 1.1	Mandatory	Mandatory for applications
		WS-I simple SOAP binding profile v1.0	Optional	
		HTTP v1.1 and HTTPS	Mandatory	Mandatory for applications
		SSL v3.0 / TLS 1.3 or higher	Mandatory	Mandatory for applications
		WMS (for GIS systems)	Mandatory	Mandatory for applications
		XSLT v2.0	Mandatory	Mandatory for applications

		XBRL Meta Model v2.1.1	Optional	An XML language for business reporting; Capacity building for user departments and other stakeholders needs to be done before making standards mandatory.
		XSL v1.0	Mandatory	Mandatory for applications
		ISO 8601	Mandatory	Date and time representation standard
		Content Management Interoperability Services (CMIS)	Mandatory	Mandatory for applications
		WCO Data Model Version 3.0	Mandatory	Version 3.9 should be adopted
3.6	Data Interoperability and Data Exchange	XML 1.0 or XML1.1	Mandatory	Mandatory for applications
		JSON	Mandatory	Mandatory for applications
		For text data: XML 1.0 or XML 1.1	Mandatory	Mandatory for applications
		For text data: CSV (for legacy applications)	Mandatory	Mandatory for applications
		For image data: JPEG (for photography images)	Mandatory	Mandatory for applications
		For image data: GIF (for internet images)	Mandatory	Mandatory for applications
		For image data: TIFF (for scanned Images)	Mandatory	Mandatory for applications
		For image data: PNG (for internet images which require increased color depth compared to GIF)	Mandatory	Mandatory for applications
		For video and audio data: MPEG-1 to MPEG-4 (for most audio and video applications)	Mandatory	Mandatory for applications
		For video and audio data: 3GPP and 3GPP2 (for audio and video over 3G mobile Networks)	Mandatory	Mandatory for applications
		Web Services Security (WSS) (extension to SOAP)	Optional	Applications using SOAP
		XMI: an XML Integration framework	Mandatory	Mandatory for applications
		xPath 2.0	Mandatory	Mandatory for applications
		XQuery 1.0	Mandatory	Mandatory for applications
		XSLT 2.0	Mandatory	Mandatory for applications

Data Standards

S. No.	Standard Category	Suggested Standard	Recommendation	Remark
4.1	Metadata and Data Standards	MDDS e-Governance Standards (http://egovstandards.gov.in/metadata-and-data-standard)	Mandatory	Mandatory e-governance standards
4.1	Metadata and Data Standards	Universal Postal Union (UPU) Standards S42a-5 and S42b-5	Mandatory	Universally adopted standard
4.1	Metadata and Data Standards	ISO 3166-1 alpha-3 Standard - Country Codes	Optional	Covered in e-governance MDDS standards

4.1	Metadata and Data Standards	UNICODE	Mandatory	Mandatory for applications
4.1	Metadata and Data Standards	IETF RFC2822 (Email Address)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO 1000:1992 SI units and recommendations for the use of their multiples and certain other units	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO 369-3 (Language) Codes	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ITU-T E.164 (Country Code)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	OASIS- CIQ-XNL version 2.0 (Full Name)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO/IEC 5218:2004 (Gender)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO 19785-1 (Common Biometric Exchange Formats Framework – CBEFF)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO/IEC 19794-5:2005 (E) (Face Image Data)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO/IEC 19794-4:2005 (E) (Finger Image Standard)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO/IEC 19794-6:2005 (E) (Iris Image Data)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO/IEC 19785-3 (Patron Format Specification)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO-3166-1981 Standard (Country Name)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	XAL version 2 Standard of OASIS (Address)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	IAFIS-IC-0110 (V3) (Image Compression)	Optional	Covered in e-governance MDDS standards
4.1	Metadata and Data Standards	ISO/IEC 19784-1 (Bio API Specifications Standards)	Optional	Covered in e-governance MDDS standards
4.2	Data Management	Use of DBMS that supports JDBC latest version for java-based applications and ODBC for non-java-based system	Optional	Covered in e-governance MDDS standards
4.2	Data Management	Support for SQL standards defined in ISO/IEC 9075	Mandatory	Mandatory for applications
4.2	Data Management	ISO 15489-1 for records management	Mandatory	Mandatory for applications
4.2	Data Management	Portable document format for document - management based on ISO 32000-1	Optional	Wherever applicable based on business use case and requirement
4.2	Data Management	ISO/TR 18492 for long-term preservation of electronic document-based information	Mandatory	Mandatory for applications
4.2	Data Management	ISO 14721- Open Archival Information System	Mandatory	Mandatory for applications
4.3	Data Design	Data Modelling - Unified Modelling Language (UML)	Mandatory	UML ver 2.5

4.3	Data Design	Data Modelling - Barker's Notation	Optional	UML preferred
4.3	Data Design	Data Modelling - Information Engineering	Optional	UML preferred
4.3	Data Design	Unicode - Character encoding system	Mandatory	Mandatory for applications
4.4	Data Security	Standard Encryption Algorithms- Triple Data Encryptions Standard (3DES) , Advanced Encryption Standard (AES) & Post Quantum Cryptography (PQC)	Optional	Mandatory for applications
4.4	Data Security	Data security technologies related to access controls, authentication, back-ups and recovery, data masking, data erasure, data resilience should be considered	Optional	Specific technologies should be recommended
4.4	Data Security	Data auditing; real-time alerts; risk assessment; data minimization; purge stale data should be considered	Optional	Specific technologies should be recommended
4.4	Data Security	Payment Card Interface (PCI), Data Security Standards (DSS) Standard	Mandatory	PCI compliance to be certified by the Organization
4.4	Data Security	RDBMS with below security controls ▪ Data access as an intended privilege ▪ Key management and encryption ▪ Integrity constraints such as domain constraints, attribute constraints, relation constraints, and database constraints ▪ High availability implementation, backup, restoration and data replication ▪ Database log and policy enforcement	Optional	Specific technologies should be recommended

Cyber Security Standards

S. No.	Standard Category	Suggested Standard	Recommendation	Remark
5.1	Application Security	OWASP Application Security Verification Standard (ASVS)	Mandatory	
5.1	Application Security	ISO/IEC 27034 – ISO/IEC 27034	Mandatory	The System Integrator need to follow the ISO 27001 Information Security guidelines throughout the Systems Development Life Cycle
5.1	Application Security	Common Weakness Enumeration (CWE)	Mandatory	CWE enables to stop vulnerabilities at the source

5.1	Application Security	CERT Coding Standards	Mandatory	This will improve the safety, reliability, and security of software systems
5.2	Information Security Management	ISO/IEC 27001	Mandatory	This makes the information assets more secure
5.2	Information Security Management	NIST Cybersecurity Framework	Mandatory	This helps reducing cyber risks to critical infrastructure.
5.3	Network Security	ISO/IEC 27033	Mandatory	This ensure network security of devices, applications, services, end-users, security gateways and Virtual Private Networks (VPNs).
5.4	Wireless Security	IEEE 802.11	Mandatory	This defines the processes for protecting the wireless network products using the Wi-Fi
5.4	Wireless Security	WPA2/WPA 3/WEP	Mandatory	Required to secure wireless computer networks
5.5	Information Security Incident Management	ISO/IEC 27035	Mandatory	Provides best practices and guidelines for incident management plan and preparing for incident response.
5.6	Storage Security	ISO/IEC 27040	Mandatory	This provide security guideline for protection of data in storage systems
5.6	Storage Security	IEEE P1619-2007	Mandatory	Protection of stored data, encryption of stored data, and the corresponding cryptographic key management
5.6	Storage Security	IEEE P1619.1	Mandatory	Authenticated Encryption with Length Expansion for Storage Devices using Secure Hash Algorithm
5.6	Storage Security	IEEE P1619.2	Mandatory	Standard for Wide-Block Encryption for Shared Storage Media
5.6	Storage Security	IEEE P1619.3	Mandatory	Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data
5.7	Secure Design and Implementation of Virtualized Servers	ISO/IEC 21878	Mandatory	Security guidelines for design and implementation of virtualized servers

5.8	Cloud Security	ISO/IEC 27017	Mandatory	This standard developed for cloud service providers and users to make a safer cloud-based environment
5.9	Privacy Information Management	ISO/IEC 27701	Mandatory	Enables to improve Privacy Information Management System
5.9	Privacy Information Management	Personal Data Protection Bill, 2019	Optional	Right to privacy is a fundamental right and it is necessary to protect personal data
5.9	Privacy Information Management	HIPA, FINRA, GDPR, PCI DSS	Mandatory	This enhance individuals' control and rights over their personal data and is protected from fraud and theft.
5.10	Supply Chain Security	ISO/IEC 20243:2018	Optional	The Open Trusted Technology Provider Framework (O-TTPF) is a compendium of organizational guidelines and best practices relating to the integrity of commercial off-the-shelf (COTS
5.11	Public Key Infrastructure	ISO/IEC 27099	Mandatory	Practices and policy framework
5.11	Public Key Infrastructure	ISO/IEC 29192	Mandatory	This standard specifies lightweight mechanisms based on asymmetric cryptography.
5.11	Public Key Infrastructure	Public-Key Cryptography Standards (PKCS)	Mandatory	These are a group of public-key cryptography standards to promote the use of the cryptography techniques to which they had patents,
5.11	Public Key Infrastructure	CCA Guidelines conforming to IT Act 2000	Mandatory	PKI Guidelines
5.11	Public Key Infrastructure	PKCS Standards from PKCS#1 to PKCS#15 excluding PKCS#13	Mandatory	e-Sign need to be used for digital transactions

11. Conclusion

The Standards are to be referred during the preparation of the tender by all the Tamil Nadu State Government Departments for their governance projects. As part of the tender the “Mandatory points” will be adopted as compulsory and “Optional points” will be included as per the necessity and decision of the corresponding agencies.

The Technical committee of the corresponding tenders will do the complete compliance check and if any deviation required, the committee will decide depending upon the priority and will intimate to the IT department.

The standards will be part of the vendor qualification and mandatory will be followed as compulsory basis and optional will not carry any weightage on the marks as part of the tender.