ABSTRACT

Information Technology Department – Data/Security Governance – Departments to obtain mandatory compliance from Standards Compliance Technical Committee (SCTC) for any e-governance/hardware prior to procurement for ensuring data interoperability and security - “Reference Standards” – Approved – Orders- Issued.

INFORMATION TECHNOLOGY (E2) DEPARTMENT

G.O.(Ms.) No.3 **Dated: 20.01.2022**
பிலவ, தை – 07
திருவள்ளுவர்ஆண்டு–2053
Read:

1. G.O.(D) No.25, Information Technology (B4) Department, dated 02.11.2016.
2. Minutes of 10th meeting of High-Level Security Governance Committee held on 17.11.2021.

******

ORDER:

The Government of Tamil Nadu has been working to improve the delivery of services to citizens through information and communication technology. Government departments are offering their G2B, G2C and G2G services through online and mobile applications. Over time, departmental IT systems have grown independent of each other without reaping the benefits of sharing large collection of data across their applications, which is critical for decision making process.

2. As several citizen-centric services from Government Departments are offered online and through mobile apps, the security of data maintained by these applications has to be ensured in order to protect them from data breach or other cyber threats. In this context, the data security of the Government applications has assumed increasing importance.

3. In the G.O. 1st read above, a High-Level Security Governance Committee (HLSGC) for Security Governance has been constituted under Information Technology Department to give necessary guidance to Cyber Security Incidence Response Team – Tamil Nadu (CSIRT-TN) as and when required.

4. In order to lay down the standards for security and data for all Government Applications, a “Data/Security Advisory Team” was constituted under the High Level Security Governance Committee with the following composition:

..2

1)	Thiru.G. Venkataraman, Additional Director-General of Police / Officer-on-Special Duty, Information Technology Department	Chairman
2)	Thiru.K.Srinivasa Raghavan, State Informatics Officer, National Informatics Centre, Chennai – 600 090.	Members
3)	The Chief Executive Officer, Tamil Nadu e-Governance Agency, Chennai – 600 002.	
4)	Dr.R.Gunasekaran, Head, Department of Computer Technology, Anna University, Chennai – 600 025.,	
5)	Cdr. L.R. Prakash (Retd), Senior Director, Centre for Development of Advanced Computing (CDAC), Chennai.	
6)	Dr.R.Muthukumar, Director, Standardisation Testing and Quality Certification (STQC), Chennai.	
7)	The General Manager (Technical, IT Infra), Electronics Corporation of Tamil Nadu (ELCOT), Chennai.	Member-Secretary

The Data/Security Advisory Team was asked to examine the standards related to Security and Data for e-Governance applications and to submit their recommendations to the HLSGC.

5. Accordingly, the Data/Security Advisory Team prepared the first version of Reference Standards and placed it before the HLSGC. The HLSGC, in its 10th meeting held on 17.11.2021, had approved the reference Standards.

The Government has accepted the reference standard for adherence by all departments.

6. The salient features are as follows:

- These are called “Reference Standards” for data and Cyber Security version 1.0 and will be updated regularly.
- Provides standards relevant to e-governance projects to ensure compliance to requirements which are Business Architecture Standards, Application Architecture Standards, Interoperability Standards, Data Standards and Cyber Security Standards.

- The standards are classified in section 7 of policy as Mandatory (coded in red) and Recommended (coded in green) for purposes of e-governance and electronic hardware procurement.
- The Mandatory standards are to be followed for all e-government systems/application /hardware procurements/purchase/development by all departments.
- SCTC is constituted to ensure compliance to standards. It shall be chaired by the Chief Executive Officer, Tamil Nadu e-Governance Agency (TNeGA) with members such as Managing Director, ELCOT, State Informatics Officer, NIC-TN State Unit, Director, CDAC-Chennai, Director, Society for Electronic Transaction and Security (SETS), Director STQC and academic representative from IIT-Madras/Anna University or their representatives. The Joint Chief Executive Officer, TNeGA shall be the Member-Secretary of the Committee. The Committee can co-opt 2 persons from private sector based on any specialized need/sector.
- The functions of SCTC shall include:
  - It shall provide all departments compulsory approval of compliance of the tender documents to mandatory standards including provision for data sharing for data purity project with Tamil Nadu e-Governance Agency (TNeGA) prior to tendering for purchase/development of any e-governance application/software/electronic hardware. The full compliance review will happen in stages through the tendering to implementation and finally at time of go-live of the projects. It shall issue detailed guidelines for compliance certification process.
  - Issuing binding directions on adherence to standards to the user departments for both existing and future e-Gov systems.
  - Approving any deviation/exemption for not adopting specific mandatory standards.
  - Directing departments to adopt certain standards even if they are not part of this document.

7. The Government, after careful examination has approved the "Reference Standards" for strict adherence by all departments.

8. The Information Technology department will be authorized to issue any clarifications/amendments/updates to these standards from time to time.

(By Order of the Governor)

NEERAJ MITTAL
PRINCIPAL SECRETARY TO GOVERNMENT

To:
All Departments of Secretariat, Secretariat, Chennai – 600 009.
All District Collectors, Government of Tamil Nadu.
The Managing Director,
Electronics Corporation of Tamil Nadu Limited (ELCOT),
692, MHU Complex, Anna Salai, Nandanam, Chennai –600 035.
The Director of e-Governance / Chief Executive Officer,
Directorate of e-Governance / Tamil Nadu e-Governance Agency,
2nd & 7th Floor, P.T.LEE Chengalvaraya Naicker Building,
Anna Salai, Chennai - 600 002.

The State Informatics Officer,
National Informatics Centre,
Rajaji Bhavan Complex, 3rd Ave, Tiruvalluvar Nagar, Besant Nagar,
Chennai - 600 090.
The Additional Director General of Police,
Cyber Crime Wing, Mylapore, Chennai – 600 004.
The Director,
Society for Electronic Transactions and Security (SETS),
MGR Film City Road, CIT Campus, Tharamani, Chennai – 600 113.
The Director,
Centre for Development of Advanced Computing (CDAC),
8th Floor, D Block, Tidel Park, Tharamani, Chennai – 600 113.
The Director,
Standardisation, Testing and Quality Certification (STQC) Directorate,
VSI Estate, Near Lattice Bridge, Thiruvanmiyur, Chennai – 600 041.
The Director,
National Critical Information Infrastructure Protection Centre (NCIIPC) (South),
P.B No. 1343, Jalahalli H.P.O, Bengaluru – 560 013.
The Director of Information and Public Relations, Secretariat, Chennai – 600 009.

Copy To:

O/o. Hon'ble Chief Minister, Secretariat, Chennai – 600 009.
The Personal Assistant to Hon'ble Minister (Information Technology),
Secretariat, Chennai – 600 009.
The Principal Private Secretary to Chief Secretary to Government,
Secretariat, Chennai – 600 009.
The Private Secretary to the Principal Secretary to Government,
Information Technology Department, Secretariat, Chennai – 600 009.
Sf/Sc.

// Forwarded / By Order //

21/01/2022

Section Officer.

21/1/2022

Reference Standards

Information Technology Department

Government of Tamil Nadu

January 2022

TABLE OF CONTENTS

Message

Information Technology will be key to achieving the $ 1 Trillion GDP goal by 2030. Tamil Nadu Government has committed to provide Swift, Measurable, Accessible, Responsive and Transparent (SMART) Governance by deploying information technology across all departments. I congratulate the Information Technology department in its maiden effort to publish Reference Standards for all e-Government systems that will enable implementation of the whole of Government approach.

Thiru. M.K.Stalin
Hon’ble Chief Minister
Government of Tamil Nadu

Message

The Government is working towards a citizen-friendly Governance driven by Information Technology. Unfortunately, departmental IT systems have grown independently of each other, which is posing challenges in getting benefits of large data across various systems due to lack of standardization.

The Reference Standard is an attempt to achieve interoperability of e-Governance systems and secure digital assets of the Government of Tamil Nadu. I am confident that this effort will lead to better governance for citizens.

Thiru. T. Mano Thangaraj
Hon'ble Minister for Information Technology
Government of Tamil Nadu

Message

Information technology has the capability to provide good governance, simplify the life of citizens and ensure that the poorest citizens are taken care of by providing wider access to social welfare schemes. This requires that G2B and G2C processes are e-enabled and service delivery mechanisms meet the myriad needs of the citizens.

As technology has evolved, various departments have followed different paths to e-Governance and this has led to siloed development. This has not only prevented innovation in governance but also led to inefficiencies. Cyber Security has become an additional challenge as the pace of digitalization has picked up. Standardization of systems can help us in building robust solutions and solve these challenges. I am happy that the Reference Standards document is being published for adoption by the Government of Tamil Nadu IT systems that will help us achieve these goals.

Dr. V. Irai Anbu IAS
Chief Secretary
Government of Tamil Nadu

Foreword

Tamil Nadu is giving high priority to deploy e-Governance to improve the lives of citizens. This requires that all departments must work in a coordinated manner. But with increased IT penetration cyber-attacks are becoming a real threat. These Reference Standards have thus been collated for adoption in all government IT systems so that the IT systems can operate in a secure, interoperable and efficient manner. I would like to thank the Hon'ble Finance Minister who envisioned the need for creation of such a standards document in the first place.

A high-level advisory committee of experts was constituted to arrive at these standards. These were then examined and approved by the High-Level Security Governance Committee (HLSGC). Public consultation was undertaken by hosting it on websites (IT Department at https://it.tn.gov.in/, ELCOT at https://elcot.in/ and TNeGA at https://tnega.tn.gov.in/) and by sharing the document for comments with 100+ industry vendors for feedback.

"Reference Standards" is a result of this exercise and covers relevant standards and also classifies them as mandatory and recommended standards. It shall be applicable to all IT systems of Government of Tamil Nadu.

I thank all the contributors, organizations, both private and public who have contributed to this maiden effort including Thiru. K. Vijayendra Pandian, IAS., CEO, TNeGA, Thiru. Ajay Yadav, IAS., MD ELCOT, Thiru. S. Balachander IAS., Jt. CEO, TNeGA , Thiru. Amresh Pujari, IPS, ADGP, Thiru. G.Venkataraman, IPS, ADGP, Thiru. K.Srinivasa Raghavan, SIO, NIC, Dr.R.Gunasekaran, HOD, Computer Science, Anna University, CDR L.R. Prakash(Retd), Senior Director, C-DAC, Dr. R. Muthukumar, Director, STQC, Dr. S. Velmourougan, Scientist D, STQC, Dr.N.Sarat Chandra Babu, Executive Director, SETS, Dr.Reshmi TR, Scientist, SETS, Thiru. Sarath Rudh, Director, NCIIPC, Thiru.M.Kannan, GM ELCOT, Thiru Venkatesh, Joint Director, TNeGA, Dr.D.Ethirajan, Joint Director CDAC, Thiru.Prasanna, Joint Director, CDAC, Thirumathi S.P. Shri Jayanthi, DM-ELCOT and Thiru. Pallab Saha,The Open Group.

This is a living document and will be updated regularly. We, therefore, request feedback and suggestions from all stakeholders on a continuous basis. Any feedback/suggestions can be sent to secyit.tn@nic.in.

(Dr. NEERAJ MITTAL, IAS)
Principal Secretary
Information Technology
Government of Tamil Nadu

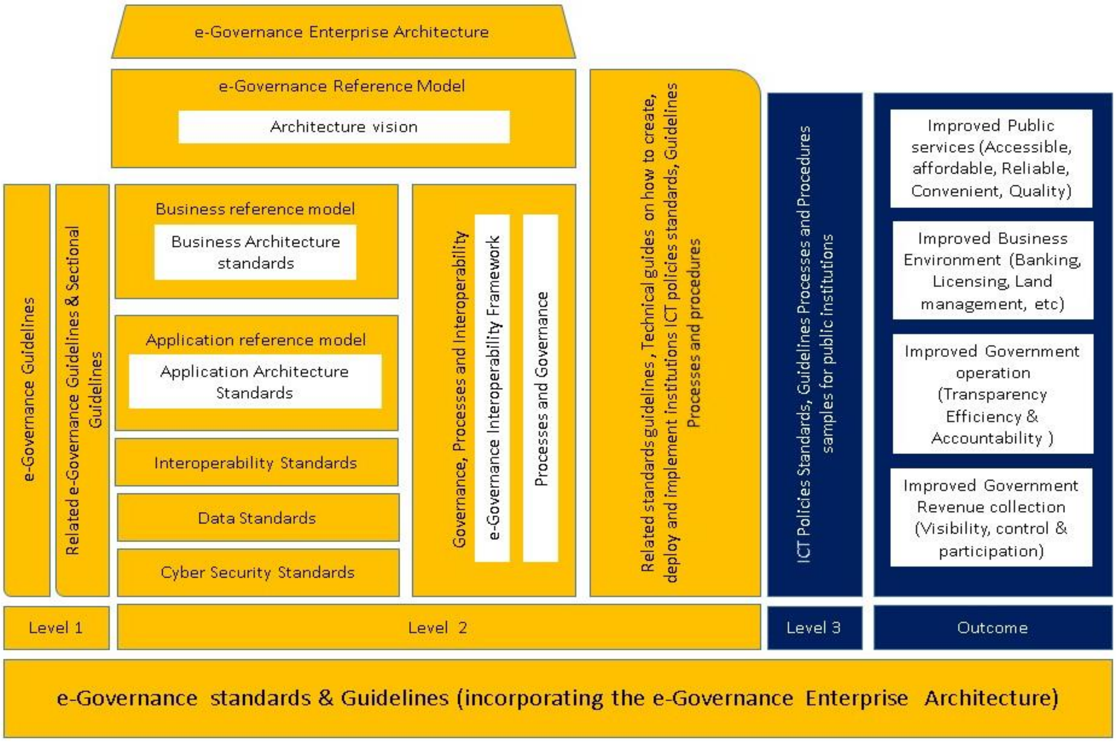
1. Introduction

1.1. Background

Electronic governance or e-Governance is the application of Information Technology for delivering government services, exchange of information, communication, transactions and integration of various stand-alone systems between Government-to-Government(G2G), Government-to-Citizen (G2C), Government-to-Business(G2B), Government-to-Employees (G2E), as well as back-office processes and interactions within the entire Government framework. Through e-Governance, Government services are made available to citizens in a convenient, efficient and transparent manner. Data Integrity and Cyber security is essential for IT infrastructure in order to deliver convenient, efficient and transparent services. Each e-Governance project should have a highly secure layer to protect data processed and delivered through it.

The 'Reference Standards' aim is to assist in the delivery of more consistent and cohesive service to citizens and support the more cost-effective delivery of ICT services by Government. A worldwide practice for conducting Government wide e-Government analysis, design, planning and implementation, using a holistic approach at all times, for the successful development and execution of e-Government Strategy is known as "e-Government Enterprise Architecture". The e-Governance Reference Standards are designed to cover most requirements of e-Government Enterprise Architecture. There are five categories/areas covering all aspects of e-Government.

These are Business architecture, Application architecture, Interoperability, Data standardization, preservation of Data and Cyber Security Standards for e-Governance projects planned and implemented in Tamil Nadu to inculcate confidentiality, integrity and availability throughout its life cycle. This document collates the various standards and guidelines that are relevant to e-Governance projects and provides guidance to select appropriate standards and best practices to meet its requirements.


e-Governance Enterprise Architecture
e-Governance Reference Model
Architecture vision
e-Governance Guidelines
Related e-Governance Guidelines & Sectional Guidelines
Business reference model
Business Architecture standards
Application reference model
Application Architecture Standards
Interoperability Standards
Data Standards
Cyber Security Standards
Governance, Processes and Interoperability
e-Governance Interoperability Framework
Processes and Governance
Related standards guidelines , Technical guides on how to create, deploy and implement institutions ICT policies standards, Guidelines Processes and procedures
ICT Policies Standards, Guidelines Processes and Procedures samples for public institutions
Improved Public services (Accessible, affordable, Reliable, Convenient, Quality)
Improved Business Environment (Banking, Licensing, Land management, etc)
Improved Government operation (Transparency Efficiency & Accountability)
Improved Government Revenue collection (Visibility, control & participation)
Level 1
Level 2
Level 3
Outcome
e-Governance standards & Guidelines (incorporating the e-Governance Enterprise Architecture)

The above e-Governance Enterprise Architecture provides a holistic view of the various standards and guidelines to be considered for the whole of e-Governance. The portions marked in yellow above are covered in this document.

1.2. Scope of Reference Standards

This document recommends standards and guidelines for e-Governance projects throughout its life cycle to plan, develop, test, execute and monitor. The Reference Standards document can be used internally in the department as a pre-compliance checklist to self-assess or self-certify or by a third-party consultant/auditor. It can also be used 'in part', as a procurement mechanism to help specify requirements of a supplier contract.

The International/ National standards and guidelines are clustered into five sections namely

1. Business Architecture Standards
2. Application Architecture Standards
3. Interoperability Standards
4. Data Standards
5. Cyber Security Standards

The document describes the purpose of standards, its benefits and references. Further, it provides guidance to all department users on mandatory and recommended (but not mandatory) standards. These are color coded as red and green respectively at the end of this document.

Reference Standards Document for Data and Cyber Security proposed by Information Technology Department, Government of Tamil Nadu shall help in:

- Identifying software and system requirements;
- Validating the comprehensiveness of a requirements definition;
- Identifying software and system design objectives;
- Identifying software and system testing objectives;
- Identifying quality control criteria as part of quality assurance;
- Identifying acceptance criteria for a software product and/or software-intensive computer system;
- Establishing measures of quality characteristics in support of these activities.

The document has been prepared collaboratively with experts and different stakeholders. We hope that this document will evolve based on feedback from different stakeholders over time and lead to interoperable, secure IT systems for the Government.

Business Architecture standards

2. Business Architecture Standards

The Business Architecture is defined based on the Business Reference Model (BRM). The Business Reference Model is a functional framework focusing on providing an organized, tiered hierarchical construct representing the business functions of the e-Governance services. It aims to provide a functional view identifying common business capabilities across Public Institutions required to provide services to citizens, business and other institutions. The BRM can be viewed as the generic business architecture requirement that will drive and shape the subsequent data, application and technology architectures of the Public Institution.

This section helps the departments in the following aspects;

- To define the target business architecture that defines how e-Governance services need to operate to achieve their goals and respond to the strategic objectives set out in the Architecture Vision Standards and Technical Guidelines.
- To describe the product and/or the service strategy, the organization, function, process and information.

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:

ISO 9241-210:2019: Human-centered design for interactive systems - It provides requirements and recommendations for human-centered design principles and activities throughout the life cycle of computer-based interactive systems. It is intended to be used by those managing design processes and is concerned with ways in which both hardware and software components of interactive systems can enhance human system interaction.

2.2. Accessibility

Web Content Accessibility Guidelines (WCAG) ensure that people with physical impairments can access specialized devices and those with cognitive impairments can be assured of a minimum level of access.

Standard:

WCAG: Web Content Accessibility Guidelines (Level A, AA, AAA) explains how to make web content more accessible to people with disabilities. WCAG covers websites, applications and other digital content.

Hyperlink:

https://www.w3.org/TR/WCAG

2.3. Business Process Modeling

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. It comprises six standards and one guideline.

Standard:

- *OAGIS:* Open Applications Group Integration Specification is an Extensible Markup *Language* (XML). Interoperability standard and data model provided by the Open Access Group, which supports the electronic exchange of data, especially business documents.

Hyperlink:

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

- *ISO/IEC/IEEE 31320-1&2:* Information technology — Modeling Languages — Part 1&2: Syntax and Semantics for IDEF0. This standard identifies the basic components of Integration Definition 0 (IDEF0) syntax. IDEF0 stands for Integration Definition for Process Modeling, a public-domain methodology used to model businesses and their processes so they can be understood and improved. It is a type of flowchart diagram. BPMN: Business Process Model and Notation, Version 2.0 - It is a visual modeling language for business analysis applications and specifying enterprise process workflows.
- *ISO 15000-5:2014*: Electronic Business Extensible Markup Language (ebXML) - Part 5: Core Components Specification (CCS). It can be employed wherever business information is being shared or exchanged amongst and between enterprises, *governmental* agencies and/or other organizations in an open and worldwide environment. The Core Components user community consists of business and governmental users, business document modelers and business data modelers, Business Process modelers and application developers of different organizations that require interoperability of business information. This interoperability covers both interactive and batch exchanges of business data between applications through the use of internet and web-based information exchanges, as well as traditional Electronic Data Interchange (EDI) systems.

- *ebXML (2001)*: It provides an open, XML-based infrastructure that enables the global use of electronic business information in an interoperable, secure and consistent manner by all trading partners.

Guideline:

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

Hyperlink:

http://www.egovstandards.gov.in/sites/default/files/Implementation%20Guidelines%20for%20Open%20API%20Policy%20for%20e-Governance%20%20%28National%20Data%20Highway%29%20V1.0_0.pdf

2.4. Business Architecture Notation

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

Standard:

ISO 15704:2019 Enterprise modeling and architecture - Requirements for enterprise-referencing architectures and methodologies - It specifies a reference base of concepts and principles for enterprise architectures which enables enterprise development, enterprise integration, enterprise interoperability, human understanding and computer processing.

2.5. Service Design

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

Standard:

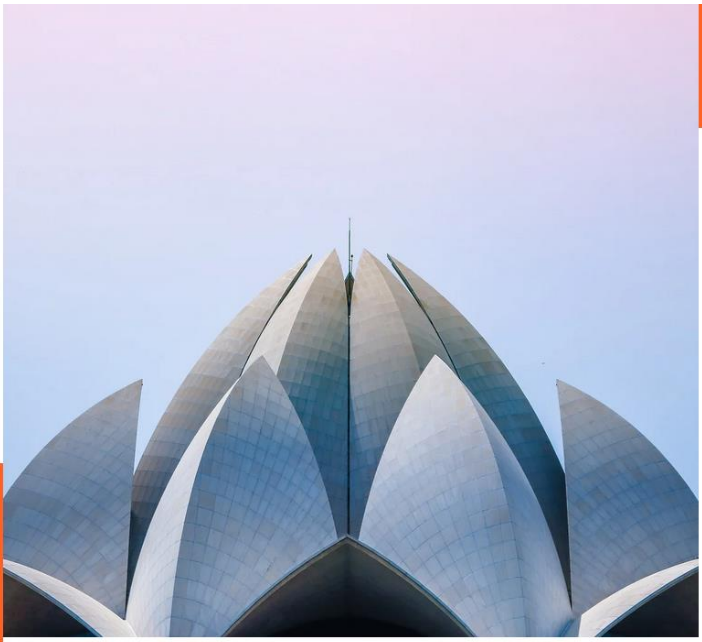
Digital Service Standard (DSS)

To protect the personal information and the privacy of individuals in their interactions with the digital systems, it is a set of principles for protection of privacy and the personal information of individuals.

Hyperlink:

http://www.egovstandards.gov.in/sites/default/files/Digital%20Service%20Standard%20Version%201.0.pdf

Application Architecture Standards



3. Application Architecture Standards

Application Architecture standards aim to reduce complexity and promote reusability, flexibility and extensibility, simplicity and ease of use, adherence to open standards, service oriented technology and vendor independence such that maximum value is extracted from ICT investments. This will minimize the time, cost and complexity of developing, deploying, maintaining and enhancing the applications.

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 the TN Government Webspace.

Guidelines:

- Guidelines for Indian Government Websites.

Hyperlink:

https://cdnbbsr.s3waas.gov.in/s3c92a10324374fac681719d63979d00fe/uploads/2020/03/2020032611.pdf

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

Hyperlink:

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

Standard:

Design: Cascading style sheets – CSS3, Hyper Text Markup Language – HTML 5.

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 models.

Standard:

- *ISO/IEC/IEEE 24765:2017:* Systems and software engineering - Provides a common vocabulary applicable to all systems and software engineering work.
- *ISO/IEC/IEEE 12207:2017:* Software life cycle Process - Applies to the acquisition of systems and software products and services, to the supply, development,

operation, maintenance and disposal of software products and the software portion of a system, whether performed internally or externally to an organization. It also provides a process that can be employed for defining, controlling and improving software life cycle processes. The processes, activities and tasks of this standard, either alone or in conjunction with ISO/IEC 15288, may also be applied during the acquisition of a system that contains software.

- *IEEE 1016-2009:* Software Design Descriptions - This describes software designs and establishes the information content and organization of a Software Design Description (SDD). An SDD is a representation of a software design to be used for recording design information and communicating it to key stakeholders.

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 name the variables consistently

- 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 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

Guideline:

OWASP Secure Coding Practices: Quick Reference Guide Nov 2020

Hyperlink:

https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.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) version 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) -It 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 Hyper Text 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 (Web CGM), Timed Text Markup Language, W3C Standards

Standards to be implemented while designing the **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.
- *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 19794-5:2011* - 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 serialization 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 (Simple Object Access Protocol)

- *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.
- *Open Office XML - ECMA-376, ISO/IEC 29500* - Information technology - Document description and processing languages - Office Open XML File Formats
- *ISO 15489-1:2016* International Standard for Record Management - Records management: Concepts and Principles
- *ISO 9075-1:2016* - Database Languages - SQL, which describe Structured Query Language. Specifies the grammar of SQL and the result of processing statements in that language by an SQL-implementation.
- *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. Computer-Aided Software Engineering (CASE) tools represent a major part of the supporting technologies used to develop and maintain information technology systems.
- *Virtualization Management (VMAN)* - DMTF's (Distributed Management Task Force) Virtualization Management standard is a set of specifications that address the management life cycle of a virtual environment

Hyperlink:

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.

Hyperlink:

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

- *ISO/ IEC 27034* - Provides guidance to assist organizations in integrating security into the processes used for managing their applications.

- *CERT – Secure coding standards* - CERT-In (the Indian Computer Emergency Response Team) is a government-mandated IT security organization.
- *ISO/IEC 24760-1:2019 framework for identity management* - defines terms for identity management and specifies core concepts of identity and identity management and their relationships.
- *ISO/IEC 29115:2013* Entity Authentication Assurance - provides a framework for managing entity authentication assurance in a given context.
- *ISO/IEC TS 29003:2018* Identity Proofing and Verification - offers guidelines for the identity proofing of a person, specifies levels of identity proofing and requirements to achieve these levels.

InterOperability Standards

4. Interoperability Standards

Interoperability Standards provide the know-how to achieve interoperability of data and information within and outside the government. It enables any Public Institution to provide and receive information and integrate its processes with other Public Institutions using predetermined 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.

Standard:

Technical Standards for Interoperability Framework for e-Governance in India, IFEG version 1.0, May 2012.

Hyper link:

http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf

4.2. Organizational Interoperability

Organizational Interoperability enables a multilateral mechanism to ensure proper management and implementation of IFEG (Interoperability Framework for e-Governance (IFEG) in India) 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 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

Standards / Framework:

- *Semantic Interoperability Framework (SIF)*: Semantic interoperability is the ability of computer systems to exchange data with unambiguous and shared meaning. Semantic interoperability is a requirement to enable machine computable logic, inferencing, knowledge discovery and data federation between information systems.

Hyperlink:

http://egovstandards.gov.in/sites/default/files/Interoperability%20Framework%20For%20e-Governance%20(IFEG)%20Ver.1.0.pdf

- *Domain Specific Metadata Standards*: A key component of metadata is the schema. Metadata schemas are the overall structure for the metadata. It describes how the metadata is set up and usually addresses standards for common components of metadata like dates, names and places. There are also discipline-specific schemas used to address specific elements needed by a discipline.

Hyperlink:

http://egovstandards.gov.in/sites/default/files/Institutional_Mechanism_for_Domain_MDDS.pdf

4.4. Technical Interoperability

To knit different kinds of e-Governance infrastructure and their services together through a catalog 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. Protocols, Schemas and Services for Interoperability

The following can be used to knit different kinds of e-Governance applications together to establish interoperability:

- Use of Simple Object Access Protocol (*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 is platform neutral. Web services with REST architecture 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)* - It is an open standard that allows different content management systems to inter-operate over the Internet.

4.6. Data Interoperability and Data Exchange

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

Standard:

- 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. 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

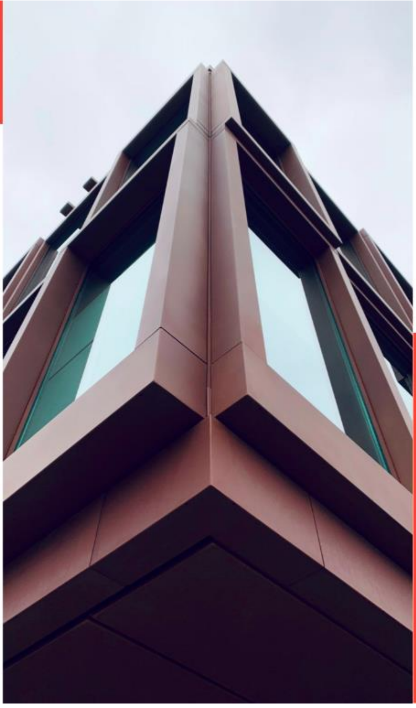
(d) Portable Network Graphic (PNG) for internet images which require increased color depth compared to GIF

- 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

Data Standards enables easier, more efficient exchanging and processing of information. It also removes ambiguities and inconsistencies in the use of data across Public Institutions.

5.1. Metadata and Data Standards

Data Standard is a technical specification that describes how data should be stored or exchanged for the consistent collection and interoperability of that data across different systems, sources and users. The adoption of Data Standards will enable easier, efficient data exchange and processing. It will also remove ambiguities and inconsistencies in the use of data.

Metadata standards are the requirements which are intended to establish a common understanding of the meaning or semantics of the data, to ensure correct and proper use and interpretation of the data by its owners and users. To achieve this common understanding, several characteristics, or attributes of the data need to be defined

Hyperlink:

http://en.wikipedia.org/wiki/Metadata_standards

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. The government notified standards for various domains are available; the departments may refer to the corresponding MDDS standard.

Hyperlink:

http://egovstandards.gov.in/sites/default/files/MDDS%20Demographic%20Ver%201.1.pdf - *It describes the nomenclature of Generic data elements and their business formats and the Metadata for each of these elements has been specified.*

http://www.ndpp.in/download/standard/eGOV-PID-Standard-Preservation-Metadata-Schema-Version1.0.pdf - *It provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record.*

http://egovstandards.gov.in/xml-schema-for-generic-data-elements-cd - *XML Schema for Generic Data Elements, common Across All the Domains.*

Standard:

- *Universal Postal Union (UPU) Standards S42a-5 and S42b-5* (Postal Services)

Hyperlink:

http://egovstandards.gov.in/postal-index-number-pin

- *ISO 3166-1:2020* alpha-3 Standard (Country Code) - Published by the International Organization for Standardization (ISO) to represent countries, dependent territories and special areas of geographical interest
- *UNICODE* - It defines the way individual characters are represented in text files, web pages and other types of documents

Hyperlink:

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

Hyperlink:

https://datatracker.ietf.org/doc/html/rfc2822

- *ISO 80000-1:2009* - standard information and definitions concerning quantities, systems of quantities, units, quantity and unit symbols and coherent unit systems, especially the International System of Quantities, ISQ and the International System of Units, SI.
- *ISO 369-3* (Language) Codes for the representation of names of languages.

Hyperlink:

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

Hyperlink:

https://en.wikipedia.org/wiki/E.164

- *OASIS* – CIQ - XML 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.
- *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 19785-1:2020* (Common Biometric Exchange Formats Framework - CBEFF) - Structures and data elements for Biometric Information Records (BIRs)

- *ISO/IEC 19794-5:2011*-Biometric data interchange formats-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 19794-4:2011*-Biometric data interchange formats-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 19794-6:2011*-Biometric data interchange formats-Iris Image Data - specifies two alternative image interchange formats for biometric authentication systems that utilize iris recognition.
- *ISO 19785-3:2020* - Information technology - Common Biometric Exchange Formats Framework - Patron Format Specification. *ISO-3166-2020* Standard (Country name) - Codes for the representation of names of countries and their subdivisions
- *XAL version 2 Standard of OASIS* (Address) - It 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
- *ISO/IEC 19784-1:2018* (Bio API Specifications Standards) - defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors.

5.2. Data Management

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

Standard:

- Support for SQL: 2008 standards defined in ISO/IEC 9075-1:2016. SQL:2008 is the sixth revision of SQL used by relational database
- Support for SQL: 2016 standards defined in ISO/IEC 9075-1:2016. SQL:2016 is the latest revision of SQL used by relational database
- Use ISO 15489-*1:2016* for records management - Information and documentation - applies to the creation, capture and management of records regardless of structure or form, in all types of business and technological environments, over time

- Use Portable Document Format (*PDF*) for document - management based on *ISO 32000-2:2020*. This standard specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents. Use *ISO/TR 18492* for long-term preservation of electronic document-based information. It provides practical methodological guidance for the long-term preservation and retrieval of authentic electronic document-based information.
- Establish a system for archiving information for both digital and physical. This framework is based on *ISO 14721*. It defines the reference model for an open archival information system (OAIS).

5.3. Data Design

- Use anyone of the following notations for data-modeling:
  a. Unified Modeling 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.

5.4. Data Security

- The reference standards for cryptography include Triple Data Encryptions Standard (3DES), Advanced Encryption Standard (AES) and Post Quantum Cryptographic (PQC) Algorithms
- 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 Industry Data Security Standards (PCIDSS)* - 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.

Hyperlink:

https://www.pcisecuritystandards.org/document_library?document=pci_dss

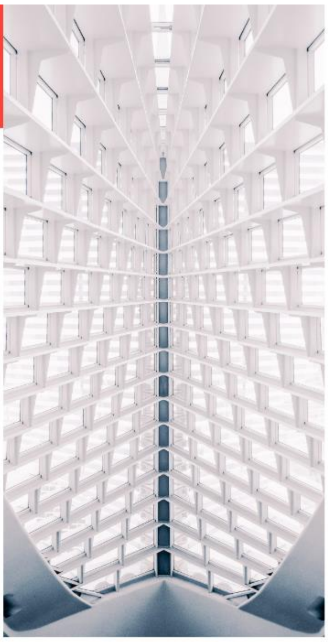
- Use RDBMS that supports the following security controls:
  a. Data access as an intended privilege

b. Key management and encryption

c. Integrity constraints such as domain constraints, attribute constraints, relation constraints and database constraints

d. High availability implementation, backup, restoration and data replication

e. Database log and policy enforcement



Cyber Security Standards

6. Cyber Security Standards

Security Architecture defines how the Public Institutions will securely and economically protect their business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing statutes pertaining to integrity, confidentiality, accountability, availability and assurance.

6.1. Application Security

Application Security standards to be adopted during the design, development and implementation of applications.

- The *Open Web Application Security Project (OWASP)* is a foundation that works to improve the security of software. It defines a set of general software security coding practices that can be integrated into the software development life cycle. Implementation of these practices will mitigate most common software vulnerabilities

Hyperlink:

https://github.com/OWASP/ASVS/raw/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf

Standard:

- *ISO/IEC 27034* – ISO/IEC 27034 offers guidance to assist organizations in integrating security into the processes used for managing their applications. It introduces definitions, concepts, principles and processes involved in application security.
- Common Weakness Enumeration (CWE) - The Common Weakness Enumeration is a category system for software weaknesses and vulnerabilities.

Hyperlink:

https://cwe.mitre.org/

- *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.

6.2. Information Security Management

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

Standard:

- *ISO/IEC 27001* - ISO/IEC 27001 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.

- *NIST Cyber security Framework* - NIST Cyber security Framework guides how organizations' internal and external stakeholders can manage and reduce cyber security risk. It lists organization-specific and customizable activities associated with managing cyber security risk and it is based on existing standards, guidelines and practices.

Hyperlink:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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.

6.4. Wireless Security

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

Standard:

- *IEEE 802.11* – It 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.
- *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 standards developed by the Wi-Fi Alliance to secure wireless computer networks.

Hyperlink:

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.

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.

Standard/Guidelines:

- *ISO/IEC 27040:2015 - Storage Security* - The purpose of ISO/IEC 27040 is to provide security guidance for storage systems and ecosystems and the protection of data in these systems. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services and security relevant to end-users during the lifetime of devices and media and after end of use
- *IEEE P1619-2007* - This standard specifies cryptographic transform and key archival methods for protection of data in sector-level storage devices.
- *IEEE P1619.1* - This standard specifies cryptographic and data authentication procedures for storage devices that support length-expansion, such as tape drives.
- *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

6.7. Secure Design and Implementation of Virtualized Servers

Standards for secure design and implementation of virtualized servers

Standard:

ISO/IEC 21878:2018 - Information technology - Security techniques - Security guidelines for design and implementation of Virtualization Servers (VSs). It specifies security guidelines for the design and implementation of VSs. Design considerations focusing on identifying and mitigating risks and implementation recommendations with respect to typical VSs are covered in this document.

6.8. Cloud Computing Services Security

Cloud computing services Security Standards cover 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 Network 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).
- Personal Data Protection – In compliance with Government of India Norms.

6.10. 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 life cycle of public-key certificates used for digital signatures, authentication and the key establishment/exchange element of encryption are covered under the below standards.

Standard:

- *ISO/IEC 27099* - Information Technology - Public key infrastructure - Practices and policy framework. The standard will support the full life cycle of public key certificates used for digital signatures, authentication and the key establishment/exchange element of encryption.
- *ISO/IEC 29192-4:2013* - This part of ISO/IEC 29192 is based on asymmetric cryptography.
- *Public-Key Cryptography Standards (PKCS)* - The Public-Key Cryptography Standards (PKCS) comprise a group of cryptographic standards that provide guidelines and application programming interfaces (APIs) for the usage of cryptographic methods.
- *CCA* (Controller of Certifying Authority) guidelines provide a legal framework for electronic governance by giving recognition to electronic records and digital signatures.

Hyperlink:

http://cca.gov.in/guidelines.html

6.11. General Instructions

1. All information on cyber intrusion incidents must be shared regularly with the Indian Computer Emergency Response Team (CERT-IN), National Critical Information Infrastructure Protection Center (NCIIPC) and Cyber Security Architecture - Tamil Nadu (CSA-TN).
2. As part of the CSA-TN, it is mandated to install the monitoring agents (provided by CSA-TN) for the applications hosted by the departments. The Managed-SOC in TNSDC as part of the CSA-TN framework helps in continuous monitoring of the servers to prevent attacks.

Hyperlink:

- https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf
- CERT-In Guidelines from https://www.cert-in.org.in/

7. Mandatory and Recommended Standards

This document so far covers a compilation of standards that are relevant to e-Governance systems. But all these standards are not mandatory to be followed. The table below specifies mandatory and recommended standards. However, in exceptional cases where the mandatory standards cannot be complied with, the procuring entity / organization may seek exemption from Standards Compliance Technical Committee (SCTC) (defined later).

Mandatory (Red) **Recommended (Green)**

Business Architecture Standards				
S. No.	**Standard Category**	**Standard / Guidelines**	**Recommendation**	**Remarks**
2.1	Design Thinking	Human-centered design for interactive systems (ISO 9241-210:2019)	Recommended	The Standard provides requirements and recommendations for human-centered design principles and activities throughout the life cycle of computer-based interactive systems
2.2	Accessibility Standard	Web Content Accessibility Guidelines (WCAG) (Level A, AA, AAA)	Mandatory	The WCAG Guidelines explain making web content more accessible to people with disabilities.
2.3	Business Process Modeling Standard	Open Applications Group Integration Specification (OAGIS)	Recommended	Interoperability standard and data model provided by the Open Access Group, supporting the electronic exchange of data, especially business documents.
	Business Process Modeling Standard	ISO/IEC/IEEE 31320-1 & 2	Recommended	The Standard identifies the basic components of Integration of drawn visual elements of the language and how they may be used together.
	Business Process Modeling Standard	Business Process Model and Notation (BPMN)	Recommended	The standard provides a visual modeling language for business analysis applications and specifying enterprise process workflows.
	Business Process Modeling Standard	ISO 15000-5:2014	Recommended	The Standard 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.
	Business Process Modeling Standard	ebXML (2001)	Recommended	The standard focused on the role of context in the reusability of Core Components and Business Processes.

	Business Process Modeling Standard	NeST-GDL-OAPI.01	Recommended	Implementation guidelines for Open APIs policy for e-Governance (National Data Highway)
2.4	Business Architecture Notation	ISO 15704:2019	Recommended	The standard 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	Digital Service Standard (DSS) Refer: NeST-GDL-IS.04 version 1.0	Recommended	The Standard describes the implementation of guidelines for Open API Policy for e-governance.
		Application Architecture Standards		
S. No.	**Standard Category**	**Standard / Guidelines**	**Recommendation**	**Remarks**
3.1	Website Design	Guidelines for Indian Government Websites	Mandatory	The standard recommends policies and guidelines for TN Government websites and portals
	Website Design	CSS3 + HTML5	Mandatory	The websites should comply with W3C Standards.
	Website Design	NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations	Recommended	The framework focused on System Life Cycle Approach for Security and Privacy
3.2	Software Development Process	Systems and software engineering's/IEC/ IEEE 24765 :2017	Mandatory	The Standard Provides a common vocabulary applicable to all systems and software engineering work. It was prepared to collect and standardize terminology.
	Software Development Process	Software life cycle Process : IEEE standard 12207:2017	Mandatory	The process 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.
	Software Development Process	Software Design Descriptions IEEE 1016:2009	Mandatory	The standard describes software designs and establishes the information content and organization of a Software Design Description (SDD)
3.3	Software Coding	Guidelines listed in standards document	Mandatory	The Guidelines listed below should be followed as part of the coding practices.

	Software Coding	OWASP Secure Coding Practices: Quick Reference Guide Nov 2020	Mandatory	The OWASP defines a set of general software security coding practices, in a checklist format, that can be integrated into the software development life cycle.
3.4	Application Design	**Presentation Layer**		
	Application Design	Simple Object Access Protocol (SOAP) version 1.2	Recommended	The SOAP provides a simple and lightweight mechanism for exchanging structured and typed information between peers in a decentralized, distributed environment
	Application Design	Web Service Description Language (WSDL) 2.0	Recommended	REST is recommended and WSDL provides a model and an XML format for describing Web services.
	Application Design	Web Accessibility Initiative	Mandatory	The WAI provides accessible Rich Internet Applications Suite defines a way to make Web content and Web applications more accessible to people with disabilities.
	Application Design	W3 Standards	Mandatory	W3 Standards should be followed for application design.
	Application Design	**Business application layer**		
	Application Design	Web Services for Remote Portlets (WSRP) - OASIS-OPEN	Mandatory	The WSRP aims 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.
	Application Design	ISO/TC 171 - Document management applications	Recommended	The Standardization of technologies and processes involving capture, indexing, storage, retrieval, distribution and communication, presentation, migration, exchange, preservation, of document management applications
	Application Design	Multipurpose Internet Mail Extension (MIME)	Mandatory	The MIME is an Internet standard that extends the format of email messages to support text in character sets.
	Application Design	ISO 19794-5:2011	Mandatory	The Standard specifies a data record interchange format for storing, recording and transmitting the information from one or more finger or palm image areas.
	Application Design	Common Biometric Exchange Formats Framework (CBEFF)	Mandatory	The standards defining an approach to facilitate serialization and sharing of biometric data in an implementation agnostic manner

	Application Design	Web Services Business Process Execution Language (WS - BPEL 2.0)	Recommended	The OASIS standard for presenting activities in a business process with web services
	Application Design	Unified Modeling Language (UML v2.3)	Mandatory	A language for specifying, constructing and documenting the artifacts of software-intensive systems.
	Application Design	SoaML	Recommended	The SoaML extends the UML to enable the modeling and design of services within a service-oriented design.
	Application Design	Business process execution language for web services	Recommended	A language for the specification of business processes and business interaction protocols.
	Application Design	XSLT v2.0 - XSL Transformations	Recommended	A language for transforming XML documents into other XML documents.
	Application Design	Java Message Service (JMS) for all Java 2 Enterprise Edition J2EE), Message Oriented Middleware (MOM)	Recommended	The 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
	Application Design	ebXML Standard Message Service Specification Version 2.0	Recommended	The role of context in the reusability of Core Components and Business Processes.
	Application Design	**Interoperability Standards**		
	Application Design	Open Office XML - ECMA-376, ISO/IEC 29500 - Information technology	Recommended	The Document description and processing languages - Office Open XML File Formats
	Application Design	ISO 15489 -1:2016 International Standard for Record Management	Recommended	The Standard defines the concepts and principles from which approaches to the creation, capture and management of records are developed.
	Application Design	ISO 9075-1:2016 Database Languages – SQL	Recommended	The Standard defines the Information technology - Database languages - SQL", which describes Structured Query Language.
	Application Design	ISO/IEC 10646 - 2017 - Universal Coded Character Set (UCS)	Mandatory	The Standard 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.

	Application Design	Open GIS Keyhole Markup Language (KML)	Recommended	The KML to be implemented while designing the Infrastructure Management and Security layer.
	Application Design	**Infrastructure Management and Security layer**		
	Application Design	ISO/ IEC 14102 - 2008 Information Technology	Mandatory	Guideline for the Evaluation and Selection of CASE Tools
	Application Design	ISO 16792 - 2021-Technical product documentation — Digital product definition data practices	Mandatory	This Standard specifies requirements for the preparation, revision and presentation of digital product definition data, hereafter referred to as data sets.
	Application Design	DMTF's Virtualization Management standard	Recommended	DMTF's Virtualization Management standard is a set of specifications that address the management life cycle of a virtual environment.
	Application Design	Open Virtualization Format (OVF)	Recommended	An open standard for packaging and distributing virtual appliances, more generally, software to be run in virtual machines.
	Application Design	ISO/ IEC 27034	Mandatory	The Standards offers guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems.
	Application Design	Coding standards - CERT-In	Mandatory	The Secure coding standards provided by CERT-IN should be strictly followed.
	Application Design	ISO/IEC 24760-1:2019 framework for identity management	Mandatory	The framework for identity management - defines terms for identity management and specifies core concepts of identity and identity management and their relationships.
	Application Design	ISO/IEC 29115:2013 Entity Authentication Assurance	Recommended	The Standards provides a framework for managing entity authentication assurance in a given context.
	Application Design	ISO/IEC TS 29003:2018 Identity Proofing and Verification	Mandatory	The Standards offers guidelines for the identity proofing of a person, specifies levels of identity proofing and requirements to achieve these levels.

Interoperability Standards				
S. No.	**Standard Category**	**Standard / Guidelines**	**Recommendation**	**Remarks**
4.1	Systems Interoperability	IFEG	Recommended	Technical Standards for Interoperability Framework for E-Governance in India,
4.2	Organizational Interoperability	1. User identification standardization 2. Standardization of Processes 3. Information ownership matrix 4. Process Agreement	Recommended	Organizational Interoperability enables a multilateral mechanism to ensure proper management and implementation of IFEG by identifying and addressing any possible barriers.
4.3	Semantic Interoperability	1. Semantic Interoperability Framework (SIF) 2. Domain Specific Metadata Standards	Recommended	Semantic Interoperability addresses the requirement of understanding the meaning of data by different stakeholders in the same way while exchanging data.
4.4	Technical Interoperability	A catalog of technical standards and specifications	Recommended	Technical Interoperability 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	SOAP v1.1/1.2	Recommended	Web service invocation and communication to achieve the Application Interoperability.
	Application Interoperability	REST API	Recommended	REST is a simple stateless architecture that generally runs over HTTP and hence platform neutral
	Application Interoperability	WSDL V2.0	Recommended	The web services description language describes web services in a way that other systems can consume the services.
	Application Interoperability	WS-I Basic Profile 1.1	Mandatory	Web Services interoperability profile is a set of non-proprietary web services specifications along with clarifications and amendments to those specifications that promote interoperability
	Application Interoperability	WS-I simple SOAP binding profile v1.0	Recommended	WS-I defines the use of XML envelopes for transmitting messages and placing constraints.

	Application Interoperability	HTTP v1.1 and HTTPS	Mandatory	The Hypertext Transfer Protocol (HTTP v1.1) and HTTPS as the application-level communications protocol for web services should be followed.
	Application Interoperability	SSL v3.0 / TLS 1.3 or higher	Mandatory	The SSL V3.0 and TLS 1.3 should be adopted as part of the application hosting.
	Application Interoperability	WMS (for GIS systems)	Mandatory	A Web Map Service is a standard protocol developed by the Open Geospatial Consortium and should be adopted for GIS Systems
	Application Interoperability	XSLT v2.0	Recommended	A language for transforming XML documents into other XML documents.
	Application Interoperability	XBRL Meta Model v2.1.1	Recommended	A extensible Business Reporting Language - an XML language for business reporting.
	Application Interoperability	XSL v1.0	Recommended	A language for transforming XML documents into other XML documents.
	Application Interoperability	ISO 8601	Mandatory	Date and time representation standard
	Application Interoperability	Content Management Interoperability Services (CMIS)	Mandatory	Content Management Interoperability Services (CMIS) is an open standard that allows different content management systems to interoperate over the Internet.
4.6	Data Interoperability and Data Exchange	XML 1.0 or XML1.1	Recommended	Use Extensible Markup Language (XML 1.0 or XML1.1) as a data exchange standard should be adopted.
	Data Interoperability and Data Exchange	JSON	Mandatory	The 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) should be adopted.
	Data Interoperability and Data Exchange	For text data: CSV (for legacy applications)	Mandatory	The format should be supported by the applications wherever necessary.
	Data Interoperability and Data Exchange	For image data: JPEG (for photography images)	Mandatory	The format should be supported by the applications wherever necessary.

	Data Interoperability and Data Exchange	For image data: GIF (for internet images)	Mandatory	The format should be supported by the applications wherever necessary.
	Data Interoperability and Data Exchange	For image data: TIFF (for scanned Images)	Mandatory	The format should be supported by the applications wherever necessary.
	Data Interoperability and Data Exchange	For image data: PNG (for internet images which require increased color depth compared to GIF)	Mandatory	The format should be supported by the applications wherever necessary.
	Data Interoperability and Data Exchange	For video and audio data: MPEG-1 to MPEG-4 (for most audio and video applications)	Mandatory	The format should be supported by the applications wherever necessary.
	Data Interoperability and Data Exchange	For video and audio data: 3GPP and 3GPP2 (for audio and video over 3G mobile Networks)	Mandatory	The format should be supported by the applications wherever necessary.
	Data Interoperability and Data Exchange	Web Services Security (WSS) (extension to SOAP)	Recommended	WSS is an extension to SOAP (Simple Object Access Protocol) to apply security to Web services.
	Data Interoperability and Data Exchange	XMI: an XML Integration framework	Recommended	XMI as an XML Integration framework for defining, interchanging, manipulating and integrating XML data and objects
	Data Interoperability and Data Exchange	xPath 2.0	Recommended	XML path language for selecting nodes from an XML document.
	Data Interoperability and Data Exchange	XQuery 1.0	Recommended	To design query collections for XML data.
	Data Interoperability and Data Exchange	XSLT 2.0	Recommended	Transforming XML documents into other XML documents.

Data Standards

S. No.	Standard Category	Standard / Guidelines	Recommendation	Remarks
5.1	Metadata and Data Standards	MDDS Standards	Mandatory	Metadata and Data Notified standards for specific domains (Health Domain, Panchayati Raj, Rural Drinking Water and Sanitation, MDDS-Demographic)
	Metadata and Data Standards	Universal Postal Union (UPU) Standards S42a-5 and S42b-5	Recommended	Standard defines International Postal Address Components and Templates.
	Metadata and Data Standards	ISO 3166-1:2020 alpha-3 Standard - Country Codes	Recommended	The International Standard for country codes and codes for their subdivisions.
	Metadata and Data Standards	UNICODE	Mandatory	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.

	Metadata and Data Standards	IETF RFC2822 (Email Address)	Recommended	Standard for the Format of ARPA Internet Text Messages.
	Metadata and Data Standards	ISO 80000-1:2009 Quantities and units	Recommended	Standard defines general information and definitions concerning quantities, systems of quantities, units, quantity and unit symbols and coherent unit systems, especially the International System of Quantities, ISQ and the International System of Units, SI.
	Metadata and Data Standards	ISO 369-3 (Language) Codes	Recommended	International standard Code for the representation of names of languages.
	Metadata and Data Standards	ITU-T E.164 (Country Code)	Recommended	This standard defines a numbering plan for the worldwide public switched telephone network and some other data networks.
	Metadata and Data Standards	OASIS- CIQ-XNL version 2.0 (Full Name)	Recommended	Extensible Name Language (xNL) Standard Description for W3C DTD/Schema.
	Metadata and Data Standards	ISO/IEC 5218:2004 (Gender)	Recommended	This standard specifies a uniform representation of human sexes for the interchange of information.
	Metadata and Data Standards	ISO 19785-1:2020 (Common Biometric Exchange Formats Framework – CBEFF)	Recommended	This standard specifies the use of CBEFF data elements by a CBEFF patron to define the content and encoding of a standard biometric header (SBH) to be included in a biometric information record.
	Metadata and Data Standards	ISO/IEC 19794-5:2011- Biometric data interchange formats-Face Image Data	Recommended	Standard for Biometric data interchange formats — Face Image Data
	Metadata and Data Standards	ISO/IEC 19794-4:2011- Biometric data interchange formats- (Finger Image Standard)	Recommended	Standard for Biometric data interchange formats — Finger image data
	Metadata and Data Standards	ISO/IEC 19794-6:2011- Biometric data interchange formats- (Iris Image Data)	Recommended	This standard specifies iris image interchange formats for biometric enrolment, verification and identification systems.
	Metadata and Data Standards	ISO/IEC 19785-3:2020 (Patron Format Specification)	Recommended	Standard for Common Biometric Exchange Formats Framework - Patron Format Specification.

	Metadata and Data Standards	ISO-3166-1:2020 Standard (Country Name)	Recommended	Codes for the representation of names of countries. This code is intended for use in any application requiring the expression of current country names in coded form.
	Metadata and Data Standards	XAL version 2 Standard of OASIS (Address)	Recommended	Extensible Address Language (xAL) Standard Description.
	Metadata and Data Standards	ISO/IEC 19784-1:2018 (Bio API Specifications Standards)	Recommended	Standard for Biometric application programming interface.
5.2	Data Management	Use of DBMS that supports JDBC latest version for java-based applications and ODBC for non-java-based system	Recommended	Use latest versions of JDBC, ODBC
	Data Management	Support for SQL standards defined in ISO/IEC 9075-1:2016	Mandatory	This standard describes the conceptual framework to specify the grammar of SQL and the result of processing statements in that language by an SQL-implementation
	Data Management	ISO 15489-1:2016 for records management	Mandatory	Standard for Information and documentation — Record management.
	Data Management	Portable document format for document - management based on ISO 32000-2:2020	Recommended	Standard for Document management — Portable document format.
	Data Management	ISO/TR 18492 for long-term preservation of electronic document-based information	Mandatory	Standard for long-term preservation of electronic document-based information.
	Data Management	ISO 14721:2012- Open Archival Information System	Mandatory	ISO 14721 defines the reference model for an open archival information system.
5.3	Data Design	Data Modeling - Unified Modeling Language (UML)	Mandatory	UML is a standard language for specifying, visualizing, constructing and documenting the artifacts of software systems.
	Data Design	Data Modeling - Barker's Notation	Recommended	The notation has features that represent the properties of relationships including cardinality and optionality, exclusion, recursion and use of abstraction.
	Data Design	Data Modeling - Information Engineering	Recommended	Data modeling is the process used to structure how data is stored, as well as modeling relationships within the data.

	Data Design	Unicode - Character encoding system	Mandatory	Unicode standards should be followed.
5.4	Data Security	Standard Encryption Algorithms- Triple Data Encryptions Standard (3DES) , Advanced Encryption Standard (AES) & Post Quantum Cryptographic (PQC) Algorithms	Recommended	Securing data by encrypting it using standard encryption algorithms.
	Data Security	Data security technologies	Recommended	Data security technologies related to access controls, authentication, back-ups and recovery, data masking, data erasure, data resilience should be considered.
	Data Security	Data auditing; real-time alerts; risk assessment; data minimization; purge stale data should be considered	Recommended	Auditing of data and real time alerts to be provided.
	Data Security	Payment Card Industry Data Security Standards (PCIDSS)	Recommended	The PCI DSS provides guidelines for securely processing, storing or transmitting payment card data.
	Data Security	RDBMS security controls	Recommended	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.

Cyber Security Standards

S. No.	Standard Category	Standard / Guidelines	Recommendation	Remarks
6.1	Application Security	OWASP Application Security Verification Standard (ASVS)	Mandatory	ASVS provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.
	Application Security	ISO/IEC 27034	Recommended	This standard provides guidance to assist organizations in integrating security into the processes used for managing their applications.

	Application Security	Common Weakness Enumeration (CWE)	Recommended	CWE is a community developed list of common software security weaknesses.
	Application Security	CERT Coding Standards	Recommended	Coding standards improve the safety, reliability and security of software systems.
6.2	Information Security Management	ISO/IEC 27001	Mandatory	Standards on Information security management
	Information Security Management	NIST Cyber security Framework	Recommended	The NIST Framework consists of standards, guidelines and best practices to manage *cyber security* risk.
6.3	Network Security	ISO/IEC 27033	Recommended	This standard describes the threats, security requirements, security control and design techniques associated with Network Security.
6.4	Wireless Security	IEEE 802.11	Recommended	The IEEE Standard for WLAN.
	Wireless Security	WPA2/WPA3/WEP	Recommended	Security certification programs to secure wireless computer networks.
6.5	Information Security Incident Management	ISO/IEC 27035	Mandatory	This standard deals with Information security incident management.
6.6	Storage Security	ISO/IEC 27040:2015	Recommended	The purpose of this standard is to provide security guidance for storage systems and ecosystems as well as for protection of data in these systems.
	Storage Security	IEEE P1619-2007	Recommended	IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices.
	Storage Security	IEEE P1619.1	Recommended	This is Standard for Authenticated Encryption with Length Expansion for Storage Devices.
	Storage Security	IEEE P1619.2	Recommended	Standard for Wide-Block Encryption for Shared Storage Media.
	Storage Security	IEEE P1619.3	Recommended	This is Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data.
6.7	Secure Design and Implementation of Virtualized Servers	ISO/IEC 21878:2018	Recommended	This standard specifies Security guidelines for design and implementation of virtualized servers

6.8	Cloud Security	ISO/IEC 27017	Mandatory	This 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	ISO/IEC 27701	Recommended	This standard specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System
6.10	Public Key Infrastructure	ISO/IEC 27099	Recommended	This standard specifies the Public key infrastructure — Practices and policy framework
	Public Key Infrastructure	ISO/IEC 29192-4:2013	Recommended	International Standard that specifies lightweight cryptography for the purposes of data confidentiality, authentication, identification, non-repudiation and key exchange.
	Public Key Infrastructure	Public-Key Cryptography Standards (PKCS)	Recommended	The public-key cryptography standards are to promote the use of the cryptography techniques.
	Public Key Infrastructure	CCA Guidelines conforming to IT Act 2000	Recommended	The CCA guidelines provide a legal framework for electronic governance by giving recognition to electronic records and digital signatures.

Note: Departments and government Users who require a copy of any standards mentioned above in this document may contact TNeGA for the same.

8. Implementation Mechanism

All departments shall take mandatory approval of compliance from **Standards Compliance Technical Committee (SCTC)** to the mandatory standards including provisions for data sharing with TNeGA for data purity prior to tendering/purchase/development of any e-governance/software/electronic hardware procurement. SCTC shall approve compliance of e-governance/software/ electronic hardware procurement (tender documents) to the mandatory standards and data sharing. The compliance review will happen in stages through the tendering/purchase to implementation and finally at time of go-live of the projects. It shall also be competent to issue mandatory directions to departments for compliance to these standards in existing e-governance systems and issue detailed guidelines for the process of compliance certification.

Composition of SCTC:

The committee shall be chaired by CEO TNeGA with members as MD ELCOT, SIO NIC, Director CDAC, Director SETS, Director STQC and academic representative from IITM/Anna University/or their representatives. The departmental representative whose compliance approval is sought for from SCTC shall be an invitee. JCEO TNeGA shall be the member secretary of the committee. The committee can co-opt 2 persons from private sector based on any specialized need for the sector.

Functions of the SCTC:

- Issue "compliance to standards" including provision for data sharing with TNeGA for all e-governance/ software/ electronic hardware prior to purchase/tenders/development for all TN government departments.
- Make recommendations on adherence to standards that shall be binding on the user departments for both existing and future e-governance systems.
- Give approval for any deviation/exemption is required not to adopt mandatory standards.
- Direct departments to adopt certain IT standards even if they are not part of this document.
- Responsible for the adoption of these standards from time to time.

Role of TNeGA and other departments:

- Standards that are categorized as “Mandatory” must compulsorily be included for compliance in the development/ in tender documents by all departments. Departments shall be required to incorporate mandatory standards specified in this document and on data sharing in their e-Governance/software/electronic hardware applications prior to development/tendering and get prior “compliance to standards” clearance from SCTC. Standards that are categorized as “Recommended” may be included in addition to mandatory standards based on the context after a careful risk assessment on the project under implementation.
- TNeGA/ELCOT/all departments will adhere to the mandatory standards for their e-Governance projects that comprise IT systems, web-based applications and mobile-based applications for various departments in Tamil Nadu.
- For purposes such as hardware procurement by ELCOT/user departments, the necessary mandatory sections applicable (for example: WiFi standard) in the standards should also be incorporated as updated and published from time to time.

The Information Technology department will be empowered to issue clarifications/amendments/updates from time to time to this document.

Acronyms and Abbreviations

S.No	Acronym	Abbreviation
1	AES	Advanced Encryption Standard
2	API	Application Programming Interface
3	ASCII	American Standard Code for Information Interchange
4	ASVS	Application Security Verification Standard
5	BPMN	Business Process Model and Notation
6	CAD	Computer-Aided Design
7	CASE	Computer-Aided Software Engineering
8	CBC	Cipher Block Chaining
9	CBEFF	Common Biometric Exchange Formats Framework
10	CCA	Controller of Certifying Authorities
11	CCS	Core Components Specification
12	CERT-In	Indian Computer Emergency Response Team
13	CMIS	Content Management Interoperability Services
14	CMMI	Capability Maturity Model Integration
15	COTS	Commercial Off-The-Shelf
16	CSA-TN	Cyber Security Architecture-Tamil Nadu
17	CSS	Cascading style sheets
18	CSV	Comma Separated Value
19	CWE	Common Weakness Enumeration
20	Data Purity	Data sharing as per Government Order vide G.O.(Ms) No.17 Information Technology (E1) department dated 23.09.2021
21	DBMS	Database Management System
22	DDOS	Distributed Denial of Service
23	DMTF	Distributed Management Task Force
24	DSS	Digital Service Standard
25	ebXML	Electronic Business Extensible Markup Language
26	ECMA	European Computer Manufacturers Association
27	EDI	Electronic Data Interchange

28	E-Governance	E Governance systems including G2C, G2B, G2G software, software applications used in for various purposes, electronic workflow applications, IT systems, web-based applications and mobile-based applications for various departments in Tamil Nadu, whether developed in-house or out-sourced.
29	FIPS	Federal Information Processing Standards
30	G2B	Government to Business
31	G2C	Government to Citizen
32	GCM	Galois/Counter Mode
33	GDP	Gross Domestic Product
34	GDL	Geometric Description Language
35	GIF	Graphics Interchange Format
36	GIS	Geographic Information System
37	GSM	Global System for Mobile Communications
38	HLSGC	High-Level Security Governance Committee
39	HTML	Hyper Text Markup Language
40	HTTP	HyperText Transfer protocol
41	HTTPS	HyperText Transfer Protocol Secure
42	ICT	Information and Communication Technology
43	IDEF0	Integration Definition 0
44	IEC	International Electro technical Commission
45	IEEE	Institute of Electrical and Electronics Engineers
46	IETF	Internet Engineering Task Force
47	IFEG	Interoperability Framework for e-Governance
48	ISMS	Information Security Management System
49	ISO	International Organization for Standardization
50	ISQ	International System of Quantities
51	IT	Information Technology
52	J2EE	Java 2 Enterprise Edition
53	JDBC	Java Database Connectivity
54	JMS	Java Message Service
55	JPEG	Joint Photographic Experts Group

56	JSON	JavaScript Object Notation
57	KML	Keyhole Markup Language
58	MDDS	Data and Metadata Standards
59	MIME	Multipurpose Internet Mail Extension
60	MOM	Message Oriented Middleware
61	MPEG	Moving Pictures Expert Group
62	NCIIPC	National Critical Information Infrastructure Protection Centre
63	NIST	National Institute of Standards and Technology
64	O-TTPF	Open Trusted Technology Provider Framework
65	OAGIS	Open Applications Group Integration Specification
66	OAIS	open archival information system
67	OAPI	Open Application Programming Interface
68	OASIS	Organization for the Advancement of Structured Information Standards
69	OS	Operating System
70	OVF	Open Virtualization Format
71	OWASP	Open Web Application Security Project
72	PCIDSS	Payment Card Industry Data Security Standards
73	PDF	Portable Document Format
74	PERL	practical extraction and report language
75	PIMS	Privacy Information Management System
76	PKCS	Public-Key Cryptography Standards
77	PKI	Public Key Infrastructure
78	PNG	Portable Network Graphics
79	REST	Representational State Transfer
80	RSA	Rivest-Shamir-Adleman
81	SDD	Software Design Description
82	SDLC	Systems Development Life Cycle
83	SI	International System of Units
84	SISWG	Security in Storage Working Group
85	SoaML	Service oriented architecture Modeling Language

86	SOAP	Simple Object Access Protocol
87	SOC	Security Operations Center
88	SPI	Service Provider Interface
89	SQL	Structured Query Language
90	SSL	Secure Sockets Layer
91	SVG	Scalable Vector Graphics
92	TIFF	Tagged Image File Format
93	TLS	Transport Layer Security
94	TN	Tamil Nadu
95	TNeGA	Tamil Nadu e-Governance Agency
96	TNSDC	Tamil Nadu State Data Center
97	TPM	Trusted Platform Module
98	UCS	Universal Coded Character Set
99	UML	Unified modeling Language
100	UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
101	UPU	Universal Postal Union
102	VLAN	Virtual local area networks
103	VMAN	Virtualization Management
104	VPNs	Virtual Private Networks
105	VSs	Virtualized Servers
106	W3C's	World Wide Web consortium's
107	WAI-ARIA	Web Accessibility Initiative - Accessible Rich Internet Applications
108	WCAG	Web Content Accessibility Guidelines
109	WCO	World Customs Organization
110	Web CGM	Web Computer Graphics Metafile
111	WLAN	Wireless Local Area Network
112	WMS	Web Map Service Interface Standard
113	WPA	Wi-Fi Protected Access
114	WS - BPEL	Web Services Business Process Execution Language

115	WS-I	Web Services interoperability
116	WSDL	Web Service Description Language
117	WSIA	Web Services for Interactive Applications
118	WSRP	Web Services for Remote Portlets
119	WSS	Web Services Security
120	XAL	Extensible Address Language
121	XBRL	eXtensible Business Reporting Language
122	XCB	X protocol C-language Binding
123	XMI	XML Metadata Interchange
124	xPath	XML path
125	XQuery	XML Query
126	XSL	eXtensible Stylesheet Language
127	XSLT	Extensible Stylesheet Language Transformations