# Nepal Enterprise Architecture (NEA) Framework

## Consultative Documents

First Draft Date: 17th Bhadra 2083

Drafted By:

Office of the Prime Minister and Council of Ministers (OPMCM)

**Information Technology Development and Governance Office (ITDGO), Kathmandu**

## Preface

The Government of Nepal (GoN) is advancing its digital transformation to improve public service delivery, strengthen governance, and support sustainable socio-economic development. As digital technologies have become an essential part of government operations today, there is a growing need for a common enterprise architecture to ensure interoperability, consistency, security, and efficient use of public resources. The Nepal Enterprise Architecture (NEA) Framework has been developed to provide this common foundation for planning, developing, implementing, and governing digital government initiatives across all levels of government.

The NEA Framework provides a shared architectural vision for building integrated, citizen-centric, secure, and resilient digital services. It promotes the reuse of common digital capabilities, adoption of open standards, interoperability through shared platforms, effective data governance, and the development and use of Digital Public Infrastructure (DPI). It also places strong emphasis on privacy, cybersecurity, transparency, accountability, and digital sovereignty throughout the lifecycle of government information systems.

The framework brings together guiding principles, the NEA Stack, implementation approaches, governance mechanisms, data governance and architecture governance arrangements. Together, these provide a common direction for building an integrated digital government ecosystem. The framework encourages government entities to move from isolated, agency-centric systems towards a collaborative and connected architecture based on shared services, authoritative data sources, standardized interfaces, and reusable digital building blocks.

The NEA Framework is intended to be a living document. Technology, public policies, legal and regulatory requirements, and citizens' expectations continue to evolve. The framework should therefore be reviewed and updated periodically to reflect emerging technologies, international good practices, and lessons learned from implementation.

Through continuous improvement and collective commitment, the NEA Framework will contribute to building a modern, secure, interoperable, and citizen-centric digital government and support Nepal's long-term digital transformation agenda.

## List of Abbreviations

| | |
|---|---|
| ARB | Architecture Review Board |
| DPI | Digital Public Infrastructure |
| ITDGO | Information Technology and Digital Governance Office |
| KYC | Know Your Customer |
| mTLS | mutual Transport Layer Security |
| NDXP | National Data Exchange Platform |
| NEA | National Enterprise Architecture |
| NeGIF | Nepal Government Interoperability Framework |
| NFC | Near Field Communication |
| NID | National Identity (card / system) |
| NIN | National Identity Number |
| NISDC | National Information Systems & Data Catalogue (the register of registers) |
| OPMCM | Office of Prime Minister and Council of Ministers |
| PKI | Public Key Infrastructure |
| PPID | Pairwise Pseudonymous Identifier |
| QR | Quick Response |
| RPO / RTO | Recovery Point Objective / Recovery Time Objective |
| SIM | Subscriber Identity Module |
| SLA | Service Level Agreement / Objective / Indicator |
| UI/UX | User Interface / User Experience |
| USSD | Unstructured Supplementary Service Data (feature-phone channel) |
| WCAG | Web Content Accessibility Guidelines |

# Table of Contents

# 1. Background

Nepal has made significant investments in digital technologies over the past decade to modernize government operations and improve public service delivery. As a result, various digital systems have been developed across different levels of government. However, many of these systems were built independently, using different standards, technologies, and architectures. This has created a fragmented digital landscape characterized by duplicated investments, limited interoperability, inconsistent service delivery, and a complex user experience for citizens and businesses.

Government Enterprise Architecture (GEA), the Nepal Government Interoperability Framework (NeGIF), and several domain-specific standards have already provided an important foundation for digital transformation. However, these initiatives have been implemented unevenly across government, and many information systems continue to evolve independently rather than as part of a single enterprise architecture in recent years as well.

To address these challenges and meet the growing demand for seamless, secure, and integrated public services, Nepal needs a unified digital government approach rather than a collection of fragmented automation moves. This framework provides a common blueprint for digital transformation by establishing shared principles, common standards, reusable digital infrastructure, and robust security and governance practices. It enables government agencies to develop interoperable, efficient, and citizen-centric digital services while reducing duplication, improving collaboration, and maximizing the value of public investment in digital technologies.

# 2. About This Document:

Nepal Enterprise Architecture (NEA) framework defines how every component - business processes, data, applications, and technology - relates to and evolves within a unified ecosystem. It ensures that every new system or service aligns with common principles, standards, and target architectures so that it integrates seamlessly with existing capabilities rather than creating new silos. This framework organizes the government's digital ecosystem into four core architecture domains. Each domain contains a single authoritative set of architecture artifacts that collectively provide the foundation for planning, designing, implementing, and governing digital government as follow:

### A. Business Architecture

The Business Architecture defines what government does and how public services are delivered. It identifies business capabilities, business processes, organizational responsibilities, and service models. The Service and Capability Model maps each public service to the reusable business capabilities that support it, enabling agencies to adopt a "build once, reuse many times" approach at the business level.

### B. Data Architecture

The Data Architecture defines what information government manages and how it is governed. It establishes authoritative data ownership, common data models, metadata standards, data quality requirements, interoperability rules, and the legal basis for collecting, sharing, and protecting data across government.

### C. Application Architecture

The Application Architecture defines which digital applications and platforms support government services and how they interact. It describes the application portfolio, baseline and target architectures, transition roadmaps, shared digital platforms, reusable services, APIs, and digital service channels that enable integrated and efficient service delivery.

### D. Technology Architecture

The Technology Architecture defines the underlying technology foundation required to operate digital government securely and reliably. It establishes technology standards, infrastructure platforms, communication protocols, security controls, cloud and data center strategies, operational requirements, and technology lifecycle management.

These four architecture domains form the four spines of the NEA. Each domain maintains one authoritative set of architecture artifacts, ensuring that government agencies work from a common source of truth. Every digital initiative, application, platform, and technology investment should align with these authoritative artifacts to achieve interoperability, consistency, reuse, and sustainable digital transformation.

| Domain | What it answers | Primary authoritative artifacts |
|---|---|---|
| Business | What services do we deliver, and which capabilities does each reuse? | Service & capability model |
| Data | Who owns which fact, in what schema, on what lawful basis? | Register of registers (NISDC) |
| Application | What's in the application portfolio, and what shared blocks does each compose? | Ministry portfolio + building-block catalogue |
| Technology | What contracts, protocols and foundations do everything run on? | National API standard + ratified profiles |

## 3. Vision

A modern, dynamic, secure, and interoperable digital government that delivers seamless, efficient, and inclusive public services through enterprise architecture, shared digital infrastructure, and value networking.

# 4. Mission

Enable one identity, one government front door, shared digital rails, reusable capabilities, and once-only data- governed by consent, lawful authority, transparency, and accountability.

# 5. Guiding Principles

## A. Foundation Principles

### 5.1. Common Architecture and Design

All public and private entities delivering public services shall conform to the NEA and applicable national reference architectures, standards, design systems, and governance mechanisms, ensuring consistency, interoperability, reuse, security, and value for public investment.

### 5.2. Digital Public Infrastructure First

Public service providers shall reuse common national digital platforms and shared services before developing new agency-specific solutions. Shared infrastructure shall include digital identity, payment gateway, notification service, National Data Exchange Platform (NDXP) and public key infrastructure (PKI).

### 5.3. Building Block approach, Reuse before buy

Public service providers shall architect applications as composition of modular building blocks, comprising core, common, and reference building blocks. Common and reference building blocks shall be developed, governed, and maintained centrally wherever appropriate and made available for reuse across government.

Entities shall reuse existing business capabilities, authoritative data, platforms, applications, software components, and shared digital services before procuring or developing new solutions. New building blocks shall be created only where an existing capability cannot adequately meet the required business or service needs.

Legacy systems shall be assessed for their alignment with the NEA principles, standards, and target architecture and shall be progressively modernized, integrated, enhanced, replaced, or retired as appropriate.

### 5.4. Compliance to Open Standards

Government digital solutions shall adopt open standards, interoperable technologies, standard APIs, and open data formats to promote interoperability, portability, innovation, competition, and long-term sustainability while minimizing vendor lock-in. The Government shall retain ownership, lawful access, control, portability, and the unrestricted ability to retrieve, migrate, and reuse its data, independent of any technology vendor, platform, or service provider.

### 5.5. Vendor Neutrality and Portability

Government systems shall be designed and procured to minimize vendor lock-in through open standards, documented data models, interoperable interfaces, and clear contractual exit and transition provisions. Government data shall be exportable and migratable in open, machine-readable formats, and reusable software components shall be portable where technically and operationally feasible.

Where proprietary data formats are unavoidable, an equivalent copy shall be maintained in an open, documented, and machine-readable format to ensure continued access, portability, and future migration.

## B. Citizen Experience and Service Delivery Principles

### 5.6. Citizen-Centricity and Inclusion

Government services shall be designed around the needs of citizens, businesses, and public institutions ensuring that services are simple, accessible, inclusive, trusted, and easy to use. Business processes shall be reviewed, simplified, and redesigned to eliminate unnecessary steps, duplication, and pain points before they are digitized or automated. Service design shall be measured by its ability to reduce the time, cost, effort, and complexity experienced by service users while improving the overall quality and satisfaction of service delivery.

Digital services shall follow common design and accessibility standards, including multilingual interfaces, consistent and reusable UI/UX patterns, accessibility for persons with disabilities, mobile-first design, and support for low-bandwidth and diverse-device environment.

#### Mobile-first design:

Digital services shall adopt a mobile-first approach while ensuring that essential services remain accessible through web, feature-phone/USSD, assisted service centres, and other appropriate channels. However, the digital transformation shall not exclude citizens who lack smartphones, reliable connectivity, digital skills, or access to digital services.

#### Accessibility and multilinguality

All digital services shall provide accessible interfaces conforming to applicable WCAG requirements and shall support Nepali and English from the first release, where applicable. Architecture, content management, and support mechanisms shall enable additional languages to be introduced without fundamental redevelopment of the service.

#### Single uniform national design system:

Government digital services shall follow a single national UI/UX design system comprising common design principles, interaction patterns, accessibility requirements, components, and content guidelines. Reusable design components shall be centrally governed and maintained so that citizens experience government digital services as one coherent and consistent digital government, rather than as a collection of unrelated applications.

### Continuous user-centred improvement:

Service performance shall be continuously evaluated using user feedback, service-delivery data, accessibility assessments, and measurable outcomes. Services shall be improved iteratively based on evidence of user needs and service performance.

## 5.7. One Door Citizen Services

Government shall provide a unified and consistent digital experience, enabling citizens and businesses to access services, information, and grievance mechanisms through common entry points regardless of the responsible agency.

**Examples:**

**Nagarik App** shall serve as the primary reference channel for integrated digital public services. Web, subnational, assisted, and future conformant channels shall use the same authoritative service catalogue, identity, interoperability mechanisms, and shared digital rails, ensuring consistent service information, processes, and status across channels.

**Hello Sarkar** shall serve as the primary reference channel for grievances and case routing. Other conformant grievance-intake channels shall feed into the same case-management contract, workflow, and status view rather than creating separate and fragmented complaint repositories. Citizens shall be able to submit, track, and receive updates on grievances through their channel of choice.

However, life-safety and emergency services shall remain accessible through dedicated emergency channels and shall not depend on the normal government digital-service stack where doing so could delay or compromise emergency response.

## 5.8. Business Before Technology

The digital initiatives in public service providers shall be driven by public policy objectives, business capabilities, service needs, and measurable outcomes rather than by technology choices. Business processes shall be reviewed, simplified, and redesigned through Business Process Reengineering (BPR) before digitization or automation, wherever appropriate. Technology shall be selected to support the redesigned business process and achieve the intended service outcomes.

### Value driven investment

Each investment needs to have its connection to a citizen or government outcome. For any proposal for a new technology or service there needs to be a definition of the outcome the investment will deliver, metrics for measuring the outcomes, and a description of what capability it replaces or expands on. Technology deliverables shall not be treated as service outcomes. For example, launching a portal is a delivery output, not an outcome in itself. Budget approval shall therefore consider the expected business and service outcomes, benefits, and

value of the investment rather than relying solely on its technical specifications or proposed technology.

### Service outcome shall be measured

Every service has a published owner, baseline, target, and a small set of citizen and operational measures: completion, elapsed time, assisted-channel success, accessibility, error/correction rate, availability, and cost where measurable. A digital service shall be considered successful only when evidence demonstrates that it has achieved the intended service and business outcomes. Going live is an implementation milestone; delivering the intended improvement in service outcomes is the measure of success.

## 5.9. Digital by Default

Government services shall be digital by default with digital channels serving as the primary means of service delivery. However, it will ensure that assisted and non-digital channels remain available for people who need them. Services shall be designed for appropriate access through web, mobile applications, USSD or other low-bandwidth channels, contact and call centres, assisted digital service centres, and physical service points as appropriate to the nature of the service.

No person shall be excluded from essential public services solely because they lack access to digital devices, connectivity, digital skills, or the ability to use digital channels independently. Assisted channels shall provide equivalent access to the service and, wherever practicable, use the same service processes, identity, data, and status mechanisms as digital channels.

Digital credentials, electronic records, and digital signatures shall have the same legal effect as their applicable physical or paper-based instruments, where recognized by applicable law.

# C. Data and Interoperability Principles

## 5.10. Data as a National Asset

Government data shall be managed as a valuable national asset throughout its lifecycle to support evidence-based policymaking, efficient service delivery, transparency, and innovation while protecting privacy and security. This includes data governance, metadata management, stewardship, and data quality management.

Government data shall be managed as a strategic national asset throughout its lifecycle to support evidence-based policymaking, efficient and integrated service delivery, transparency, accountability, and responsible innovation while protecting privacy, confidentiality, security, and other lawful interests. Data shall be governed through clear ownership and stewardship, authoritative sources, common data standards, metadata management, data quality management, lifecycle management, and appropriate access and sharing mechanisms.

### 5.11. Once-Only Data Collection

Citizens and businesses shall not be required to provide information that is already lawfully held by government and available through an authoritative source. Government entities shall reuse trusted and authoritative data through secure and interoperable mechanisms, subject to applicable law, purpose limitation, consent requirements, and appropriate access controls.

Each core government dataset shall have a clearly designated data owner and steward, with an authoritative source or authoritative registry established and maintained for that dataset. Other systems shall consume and reuse authoritative data rather than creating competing master records, except where a legitimate business, legal, or operational requirement requires otherwise. A governed multi-tenant platform may host data from multiple agencies, provided that each agency's data remains logically and, where required, physically segregated.

### 5.12. Data Sharing and Interoperability by Design

Government agencies shall securely exchange data through standardized APIs, common data models, metadata standards, and interoperability platforms instead of creating isolated data silos. Agencies should publish service and API catalogues to enable secure data discovery and reuse. National Data Exchange Platform (NDXP) and related shared platforms shall be the controlled integration backbone among different systems.

### 5.13. Common Interoperable Payment Standard

Government digital services shall adopt common, open, and interoperable payment standards and interfaces to enable citizens and businesses to make and receive payments through their preferred banks, wallets, payment instruments, and channels without being locked into a particular provider, scheme, application, or device.

Payment interoperability shall be technology-neutral and function-driven. Technologies and payment methods including account-to-account transfers, cards, QR code, NFC, contactless, mobile wallets, and future mechanisms shall interoperate through the common standards where applicable. Thus, the digital government services shall be interoperable by default and shall avoid unnecessary closed payment loops, proprietary dependencies, and provider lock-in.

## D. Identity and Trust Principles

### 5.14. National ID for Digital Verification and Authentication

National ID shall be the primary foundation for digital identity and authentication of individuals. Government shall use trusted digital identity and trust services, including electronic authentication, digital signatures, digital seals, and digitally verifiable credentials—to enable secure, trusted, and legally recognized digital transactions while minimizing paper-based verification wherever legally permissible. Alternative identity mechanisms shall be provided for individuals and populations not covered by the National ID system or who cannot reasonably access or use it. Such mechanisms shall meet defined assurance, security, privacy,

and interoperability requirements and shall not create unnecessary barriers to access essential public services.

**Agencies don't store the NIN**: Service-delivery agencies shall not store the National Identity Number (NIN) as their routine service identifier. Each agency shall receive a unique, opaque, non-derivable Pairwise Pseudonymous Identifier (PPID) scoped to that agency. The PPID shall be generated or issued through the authorized digital identity infrastructure and shall not enable one service provider to correlate an individual across other services. Where a service requires identity verification, the authorized identity service shall perform the necessary mapping between the NIN and the relying party's PPID. Where recovery or audit requires a PPID-to-NIN mapping, such mapping shall be maintained within a separately governed identity domain with appropriate legal authority, access controls, auditability, and privacy safeguards. Service-delivery agencies shall not independently maintain or reconstruct NIN-to-PPID mappings.

**A Mobile Number Is Not an Identity:** A mobile number shall not be treated as a person's identity or as a high-assurance credential by itself. Digital services shall accommodate lawful number portability, reassignment, and changes of mobile number and shall use authorized signals or verification mechanisms to identify relevant risks. Users shall have secure mechanisms for correcting identity information, updating contact details, and recovering access. High-assurance authentication shall not rely solely on possession of a SIM card. The required level of identity assurance shall be determined by the risk and legal requirements of the transaction.

### 5.15. Prioritize Digital Verifiable Credentials

Digital credentials and signatures shall be legal equivalent to existing credentials issued by different public entities. A national framework and verification system shall be developed for implementation of Digital Credentials. Physical credentials are issued on special request and may incur additional charges.

## E. Security, Resilience and Sovereignty Principles

### 5.16. Secure, Resilient and Sovereign by Design

Security, resilience, privacy, and digital sovereignty shall be integrated throughout the lifecycle of government digital systems and infrastructure. Systems shall adopt risk-based security management, business continuity, disaster recovery, resilience, and applicable national and international best practices.

The critical government data and infrastructure shall remain under national governance and control within specialized Governance Framework. Secure and privacy-preserving defaults shall be enabled by design. Systems shall, by default, use strong authentication, least-privilege access, appropriate encryption, security logging and audit trails, and privacy-protective

settings. Any relaxation of these controls shall require a documented risk assessment, explicit justification, appropriate authorization, and periodic review.

**Resilient Digital Public Infrastructure**: Shared digital infrastructure including digital identity, payments, and data exchange shall be designed to remain available even when an individual agency system is unavailable. A slow, unavailable, or failed dependency shall return a defined status, preserve submitted work where possible, and provide a documented assisted or manual fallback. Failures shall not occur silently.

**Zero Trust, Least Privilege:** All system-to-system and user access shall follow zero-trust and least-privilege principles. Systems shall authenticate to each other using appropriate mechanisms such as mutual TLS (mTLS). Access shall be limited to the minimum privileges required for the authorized role, purpose, and duration, and all privileged and sensitive access shall be logged and auditable.

**Encryption at rest and in transit:** Citizen and other sensitive government data shall be protected using strong encryption both in transit and at rest. Encryption keys shall be securely managed, with appropriate key rotation, access controls, and lifecycle management. Any justified exception shall require documented risk assessment, explicit authorization, and compensating controls.

## 5.17. Privacy by Design and Citizen Data Rights

Privacy shall be embedded by design and by default throughout the lifecycle of digital systems, rather than addressed as a post-implementation control. Systems shall collect and process only the verified claims and minimum data necessary for a defined purpose, use data only for the lawful and declared purpose, minimize retention, and apply appropriate consent, access, security, and accountability controls.

Citizens shall have appropriate control and visibility over the use of their personal data. Applications requiring personal data shall obtain authorization through a shared consent mechanism using conformant citizen-controlled, assisted, or delegated channels. Data exchanges authorized by law without consent including those required for court orders, tax administration, law enforcement, or other lawful purposes shall be supported by a recorded legal basis and appropriate safeguards.

**Accountable and Transparent Access to Personal Data**: The access to personal data shall be lawful, accountable, and traceable. Every access to personal data shall be logged at the time of access, including the identity of the person or system accessing the data, the purpose of access, the legal or administrative authority, and the date and time of access with right to review records of access by citizens.

## F. Governance and Accountability Principles

### 5.18. Human Accountability and Decision Transparency

Automated systems shall support, but not replace, accountable decision-making unless otherwise authorized by law. Entities shall ensure that automated decisions are transparent, auditable, and explainable where appropriate, and remain subject to clear human oversight and accountability. This shall be supported through appropriate governance mechanisms such as audit trails, policies, documented processes, and record-keeping.

### 5.19. Strong Governance Capabilities

Government shall establish clear, accountable, transparent, and effective governance mechanisms for enterprise architecture, data, technology, security, and digital services. Governance shall define decision rights, responsibilities, standards, oversight, compliance, and accountability across national, sectoral, and agency level. Establish accountable transparent and effective mechanisms for Data Governance, IT Governance and Architectural Governance. Government shall continuously develop institutional and technical capacity for architecture, data, cybersecurity, technology, procurement, service management, and other relevant governance domains to ensure that NEA can be effectively implemented, operated, monitored, and evolved.

## 6. The NEA Stack

The NEA Stack is organized into five responsibility levels from Level 0 (Foundation) to Level 4 (Applications and Tools). Each level defines a distinct architectural responsibility and set of reusable capabilities; it does not prescribe a mandatory processing sequence. A service may use only the levels and components necessary to fulfil its requirements and may interact directly with an appropriate shared capability or trusted service. Government shall retain policy, contractual, operational, and sovereign control over critical digital capabilities and trust assets. Each component shall have clearly defined ownership, stewardship, operator, service-level, security, and accountability arrangements.

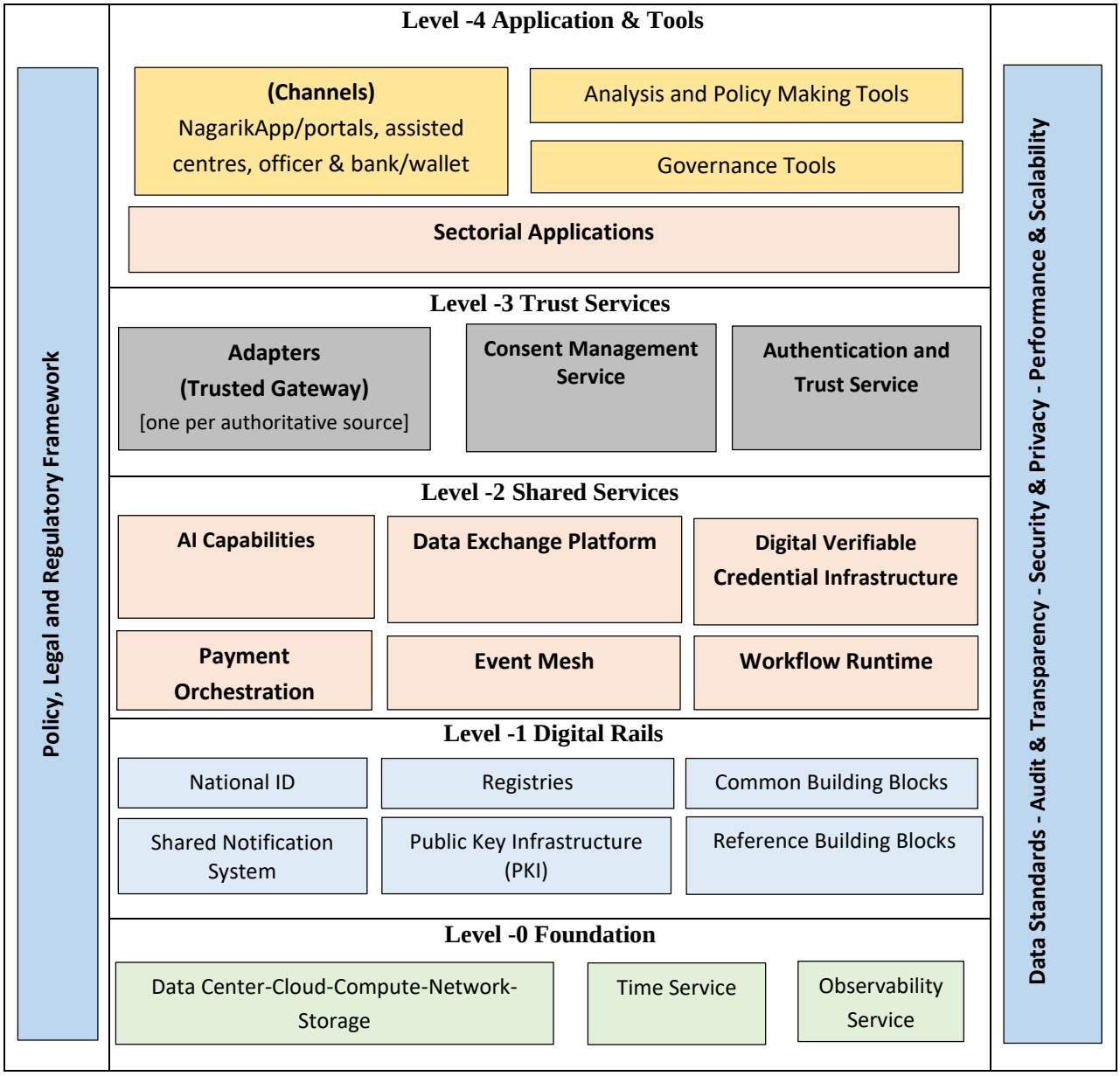



FIGURE 1: THE NEA STACK

### Level 0 – Foundation

The foundation layer provides the core ICT infrastructure components such as compute, network, storage, messaging, workload connectivity, secure authoritative time, resilient name

resolution, trust-anchor distribution, secrets, observability, backup/recovery and delivery pipelines on which the entire platform operates. This layer ensures that all higher-level services operate on a secure, scalable, resilient, and highly available infrastructure.

### Level 1 – Digital Rails

This layer provides the nationally governed shared digital assets and common capabilities: National ID, Registries (Business Registries, Address Registries, Civil Registries, etc.), Reference and Common Building Blocks, Shared Notification System and Public Key Infrastructure (PKI). These digital rails form the common foundation upon which all government applications are built.

### Level 2 Shared Services

This layer provides reusable and shared platform services: Data Exchange Platform, Digital Verifiable Credential Infrastructure, Workflow Runtime, Event Mesh, Payments and Audit & Transparency. These services support multiple government systems which are implemented once and shared across the digital ecosystem. In combination these services reduce duplication, improve interoperability, and accelerate digital service delivery.

### Level 3 Trust Services

This layer ensures that data sharing is secure, privacy is preserved and aligned with applicable legal and regulatory requirements. It includes Adapters, Consent Management Service, Authentication & Trust Service and AI capabilities. One controlled adapter per authoritative source wraps supported commands, queries and events into the national contract and maps fields to national schemas which connect authoritative source systems such as civil registration, tax, immigration, banking, or health databases to the common platform. The adapter never becomes the source of record. The Authentication and Trust Service verifies the identity of users, applications and organizations before granting access to digital services between users, government agencies, and digital systems. Consent Management Service enables citizens to control how their personal information is shared between organizations and records explicit consent for data access.

### Level 4 Application & Tools

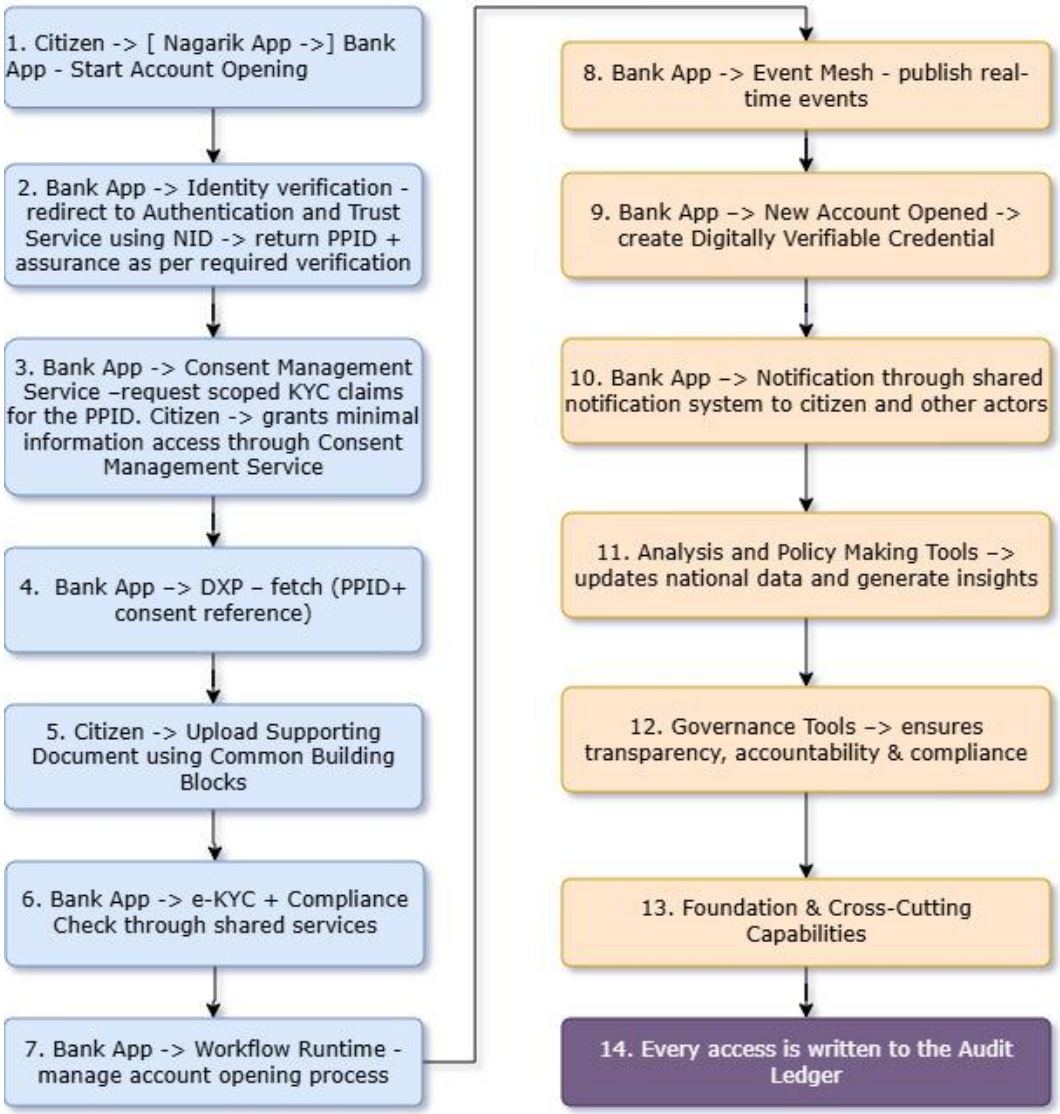
This top layer contains the channels through which the citizens or officers access government services. The government web portals or citizen mobile applications such as Nagarik App call lower layer services through the contract and never reach a source directly. Emergencies sit outside the stack: a citizen in danger reaches a responder directly. In addition the Analysis and Policy-Making Tools use aggregated platform data to support evidence-based policymaking, planning and strategic decision-making and Governance Tools support operational management, monitoring, compliance, reporting and administration of the national digital platform. This layer represents the interface between the digital government platform and its users.

### Cross-Cutting Capabilities

The cross-cutting capabilities span every layer of the architecture and ensure consistent implementation across the platform.

- **Policy, Legal and Regulatory Framework**- It provides the legislative and governance foundation required for digital government. It includes laws, regulations, policies, standards, institutional governance and compliance mechanisms governing digital identity, privacy, cybersecurity, data sharing and electronic transactions.
- **Security and Privacy**- It ensures confidentiality, integrity, availability, authentication, authorization, encryption, identity protection, cyber resilience and compliance with privacy requirements across all platform components.
- **Performance and Scalability**- It ensures the platform can support increasing numbers of users, transactions and digital services without degradation in performance. It encompasses high availability, elasticity, resilience, disaster recovery, capacity planning and performance optimization.
- **Data Standards-** It establishes common data models, metadata standards, schemas, classifications, APIs, and interoperability standards. Frameworks such as NeGIF and GDS ensure that data exchanged across government agencies is consistent, accurate, and interoperable.
- **Audit and Transparency-** It ensures that all significant digital activities are securely logged, traceable, and auditable to provide appropriate transparency into government operations, data access, and service delivery. Audit records support compliance, oversight, fraud detection, forensic investigation, and continuous improvement and transparency strengthens public trust and institutional accountability.

## 6.1. Showcase (opening a bank account) using the NEA Stack




### 1. Citizen Accesses the Service (Level-4 – Channels)

A citizen who wants to apply for a new bank account, he/she opens the Nagarik App on his mobile phone and selects "Open New Bank Account". The Nagarik App forwards the request to the respective Banking System which initiates application for a new bank account. Alternatively, the user can use the mobile banking application, internet banking portal or physically visit the bank branch for new account opening process.

### 2. Citizen Authentication (Level-3 – Authentication & Trust Service)

The citizen must verify his/her identity before opening the account. The respective bank account opening system redirects the citizen to the Government Authentication and Trust Service, which then authenticates the citizen using the PPID (authentication token generated using National ID). After successful authentication, the bank account opening system receives a secure authentication token and allows the citizen to continue the process.

### 3. Citizen Consent (Level-3 – Consent Management Service)

The bank account opening system requests permission to access the citizen's identity and Know Your Customer (KYC) information from government registries. The user reviews the requested information through the Consent Management Service and electronically grants consent for the requested information, its purpose, the receiving organization and the duration of access.

### 4. Retrieve Verified KYC Information (Level-2 – National Data Exchange Platform, Level-1 – Registries)

Once consent is granted, the bank account opening system sends secure API requests through the NDXP. The NDXP validates the authentication token, consent reference and access authorization before retrieving verified information from authoritative registries, such as the National ID, Civil Registration System and Address Registry. Only the minimum required verified information is returned that automatically populates the bank account application form.

### 5. Upload Supporting Documents (Level-1 – Common Building Blocks)

If additional supporting documents are required (such as a recent photograph, income source declaration, or proof of address), the citizen uploads them through the bank application. The Common Building Blocks, including file upload, OCR, image validation and document verification services validate the uploaded documents before they are attached to the application.

### 6. Perform KYC and Compliance Checks (Level-2 – Digital Verifiable Credential Infrastructure)

The bank account opening system performs electronic Know Your Customer (e-KYC) verification using the verified government data. The additional compliance checks such as sanctions screening, politically exposed person screening, anti-money laundering (AML) and customer risk assessment are carried out in accordance with Nepal Rastra Bank (NRB) regulations and directives before the account is approved.

### 7. Process the Account Opening (Level-2 – Workflow Runtime)

The bank account opening system submits the application to the Workflow Runtime, which manages the account opening process. The workflow automatically routes the application through identity verification, KYC review, compliance verification, account approval, account number generation and customer onboarding. The bank officers perform only the tasks assigned to them based on their authorized roles.

### 8. Publish Real-Time Events (Level-2 – Event Mesh)

The important events such as Identity Verified, KYC Completed, Account Approved and Account Activated are published through the Event Mesh as the account opening process progresses. The

authorized banking systems and other subscribed services receive these events in real time without requiring direct system-to-system integration.

### 9. Issue a Digital Customer Credential (Level-2 – Digital Verifiable Credential Infrastructure)

The bank may issue a digitally verifiable customer credential such as a verified KYC credential or account ownership credential after the account is successfully opened. The credential shall be digitally signed using the Digital Verifiable Credential Infrastructure and Public Key Infrastructure (PKI). Authorized organizations can then verify the credential electronically, subject to the citizen's consent and applicable regulations.

### 10. Notify the Citizen (Level-1 – Shared Notification System)

The bank account opening system sends notifications through the Shared Notification System or the bank's notification service for the activation status of the account. The citizen receives an SMS, email or mobile application notification confirming successful account opening together with the account number and further steps.

### 11. Generate Insights (Level-4 – Analysis & Policy Making Tools)

The operational data generated during the account opening process is collected and analyzed. The authorized officials of the bank and relevant regulators use Analysis and Policy Making Tools to monitor account opening volumes, processing times, customer onboarding performance, digital adoption and service quality to support operational improvements and evidence-based decision-making.

### 12. Monitor Governance and Compliance (Level-4 – Governance Tools)

The Governance Tools continuously monitor service performance, cybersecurity events, audit logs, regulatory compliance and service-level agreements (SLAs). These tools help ensure transparency, accountability, compliance with Nepal Rastra Bank regulations and continuous improvement of digital banking services.

### 13. Foundation and Cross-Cutting Capabilities (Level-0 and Cross-cutting Layers)

All shared government services operate on the Government's Foundation Infrastructure throughout the entire process: including cloud, compute, storage, networking, observability, and time synchronization services. Every transaction complies with the cross-cutting principles of security, privacy, interoperability, data standards, auditability, transparency, performance, scalability, and the legal and regulatory framework. The bank integrates with these shared services through secure, standards-based interfaces while maintaining its own internal banking systems.

# 7. NEA Stack Implementation

The NEA Stack shall follow a common set of architectural and governance principles to ensure consistency, interoperability, reuse, security, and long-term sustainability across government digital systems. The following implementation principles shall apply to all government agencies and ICT initiatives:

## 7.1. Layered Implementation

The NEA stack shall be implemented as a layered architecture in which each layer provides reusable capabilities and services to the layers above it. The implementation of government digital services shall follow the principle of reuse, composability, interoperability, and clear separation of responsibilities across the layers.

Government agencies shall reuse capabilities available through the NEA Stack, including national DPI, shared government services, and sectoral capabilities, wherever applicable. Agencies shall not independently develop or operate capabilities that are already available as reusable services in lower layers unless a justified functional, legal, security, or operational requirement exists.

Each layer shall:

- perform only the responsibilities assigned to it;
- consume capabilities and services from lower layers through standardized interfaces;
- expose appropriate reusable capabilities to higher layers;
- avoid unnecessary duplication of capabilities provided by other layers; and
- comply with applicable national standards, security, privacy, interoperability, and governance requirements.

Digital solutions shall be designed as composable services, allowing capabilities from multiple layers to be combined to deliver end-to-end government services. Changes to shared capabilities shall be managed through established architecture governance, standards, versioning, and change-control mechanisms to prevent disruption to dependent services.

Sectoral DPI shall be established where multiple organizations within a sector require common capabilities. It shall be built upon national DPI and shared government services and shall not duplicate capabilities already available within the NEA Stack.

## 7.2. Standards Compliance

Government agencies shall implement digital systems in accordance with the applicable NEA principles, standards, reference architectures, technical specifications, and implementation guidelines issued under the NEA. All ICT projects shall comply with the approved standards applicable to their scope, including architecture, interoperability, data, APIs, security, digital identity, infrastructure, and other relevant technical domains.

Where compliance with an applicable standard is not feasible, the implementing agency shall obtain an approved architecture exception in accordance with the NEA Framework and implement a roadmap to achieve compliance where appropriate.

### 7.3. Service and Capability Catalogue

The government shall maintain a centralized service and capability catalogue to provide a common view of government digital services, reusable capabilities, responsible organizations, authoritative data sources, and service dependencies. All new government digital services and significant new digital capabilities shall be registered in the catalogue as part of the architecture review and project onboarding process. The catalogue shall be used to identify existing capabilities for reuse and to support assessment of dependencies, ownership, interoperability, and architectural compliance.

The catalogue shall be maintained by the ITDGO and shall be integrated, where appropriate, with the National Information System and Data Catalogue (NISDC) and other relevant government registries.

### 7.4. Reuse Before Build

Before developing or procuring any new digital capability, agencies shall assess whether an equivalent or suitable reusable capability is already available through the NEA Stack, national DPI, shared government services, or relevant sectorial DPI. The agencies shall reuse or integrate with the existing capability rather than develop a duplicate implementation where a suitable reusable capability exists, unless an approved architectural exception has been granted.

New capabilities shall be designed for reuse and interoperability where they are likely to serve multiple agencies or government services. The duplicate implementations of common capabilities such as authentication, notification, payment, consent management, document verification, data exchange, and digital signatures shall be avoided.

Architectural exceptions shall be justified based on functional, legal, security, privacy, performance, availability, sovereignty, or other material requirements and shall be subject to the NEA architecture governance and approval process.

### 7.5. Contract-First Integration

All shared services and reusable digital capabilities shall be defined through standardized service contracts before implementation. The service contract shall serve as the authoritative interface between service providers and consumers. The published service contracts shall specify the service interfaces, data models and schemas, security and authorization requirements, authentication mechanisms, request and response formats, error handling, service-level requirements, and versioning rules as applicable.

Service providers shall maintain and publish the approved contracts through the designated government service/API registry or repository and shall manage changes through defined versioning and change-control processes.

Government agencies shall ensure that their solutions conform to applicable published service contracts, standards, and security requirements. Agencies may use different programming

languages, technology platforms, or implementation approaches, provided that their solutions conform to the applicable contracts and standards.

### 7.6. Legacy System Modernization

Existing government systems that cannot immediately comply with applicable NEA standards may continue to operate through controlled integration mechanisms or approved adapters, provided that they meet applicable security, privacy, interoperability and operational requirements. Legacy integration shall be treated as a transitional arrangement and shall not be used as a basis for perpetuating non-compliant architectures or creating new dependencies on legacy systems.

Each legacy system requiring continued operation shall have an approved modernization roadmap that identifies the target architecture, required standards and capabilities, key dependencies, implementation priorities, and indicative timelines for progressive alignment with the NEA. Legacy systems that are no longer required or cannot be economically modernized should be planned for decommissioning or replacement.

### 7.7. Incremental Adoption

The NEA stack shall be implemented incrementally and progressively. Existing systems shall not be required to be replaced immediately solely to achieve NEA compliance. Instead, they shall progressively align with applicable NEA standards and architectural requirements through planned enhancement, modernization, integration, or replacement initiatives as appropriate.

All new digital projects and major system enhancements shall comply with applicable NEA standards and architectural requirements from inception. An approved architectural exception and a defined transition plan shall be required where immediate compliance is not feasible.

### 7.8. Resilience and Business Continuity

Shared digital services and critical government systems shall be designed and implemented to maintain availability, integrity, and recoverability in the event of system failures, infrastructure disruptions, cyber incidents, natural disasters, or other major operational disruptions.

Before implementing or procuring a critical shared digital service, the responsible agency shall assess its business continuity and recovery requirements and define appropriate Recovery Time Objective (RTO), Recovery Point Objective (RPO), backup, failover, disaster recovery, and service restoration arrangements based on the criticality of the service.

Critical shared services shall avoid single points of failure and shall have appropriate redundancy, geographically separated recovery capabilities, secure backup, and tested recovery procedures, commensurate with their service criticality and risk.

Business continuity and disaster recovery arrangements shall be periodically tested and reviewed. The results of recovery exercises shall be documented and corrective actions shall be tracked through the established governance process.

## 7.9. Governance

The implementation of the NEA shall be governed through architecture review, conformance assessment, approved technical standards, and defined governance and change-control processes in accordance with this framework.

Major ICT projects shall undergo architecture review and NEA conformance assessment at appropriate stages of the project lifecycle, including, where applicable, before approval, procurement, major enhancement, and deployment. Project proposals, procurement specifications, solution designs, and implemented solutions shall demonstrate compliance with applicable NEA principles, standards, and architectural requirements.

The ITDGO shall facilitate and coordinate the architecture review and conformance assessment process, provide technical guidance to implementing agencies, and monitor compliance with the NEA framework.

An agency may request a time-bound architecture exception through the established NEA governance process where immediate compliance is temporarily impractical. The exception request shall include the justification, associated risks, compensating controls, validity period and a migration or remediation plan for achieving compliance

## 7.10. Continuous Improvement

The NEA stack shall be continuously reviewed and evolved to respond to changes in government priorities, legislation, public service needs, emerging technologies, cybersecurity risks and international best practices. The government of Nepal shall periodically review and update the NEA through ITDGO including its shared capabilities, standards, reference architectures, implementation guidance and governance processes in accordance with the NEA framework.

Any changes to NEA shall be managed through the established architecture governance and change-control processes. The updates shall maintain backward compatibility and minimize disruption to existing implementations while enabling the progressive adoption of improved capabilities and standards wherever practical.

# 8. Data Governance

Government data shall be governed in accordance with the Constitution of Nepal, applicable laws and regulations, government policies, and approved national standards. Detailed technical and operational requirements shall be defined through applicable data, security, privacy, interoperability, and records-management standards and guidelines.

## 8.1. Data Ownership and Custodianship

Every authoritative government dataset shall have a designated data owner and data custodian. The data owner shall be the government entity or competent authority having the legal mandate and business responsibility for the subject matter represented by the data. Data ownership shall be determined based on the constitution, applicable law, regulation, government decision or formally delegated authority. The data owner shall be accountable for the lawful purpose, use, sharing, classification, quality requirements, retention and overall governance of the data.

The data custodian shall be the organization responsible for the operational management of the authoritative data on behalf of the data owner, including its availability, integrity, security, quality, maintenance and implementation of approved data governance requirements. The data owner and data custodian may be the same organization.

The roles of data owner, data custodian, data producer and data consumer shall be explicitly defined where multiple organizations contribute to an authoritative register or dataset. The data producers shall be authorized to create or update data while data consumers shall access data only for authorized purposes. The data owner, data custodian, authoritative source, authorized producers and applicable governance information shall be recorded in the NISDC.

Any dispute regarding data ownership or custodianship shall be resolved by the competent authority in accordance with applicable laws and governance arrangements. The final decision shall be recorded in the NISDC.

## 8.2. Data Classification

Government data shall be classified according to its sensitivity and purpose to ensure appropriate protection, access, use, sharing, retention and disclosure.

**Sensitivity Classification**

Government data shall be classified according to its sensitivity based on the potential impact of unauthorized access, disclosure, modification, loss, or misuse. The data owner shall propose the sensitivity classification of a dataset and the designated competent authority shall approve it in accordance with applicable national data classification and security standards. At a minimum, government data shall be classified as follows:

- Public – data approved for public access and reuse;
- Internal – data intended for authorized government use;
- Confidential – data requiring restricted access and enhanced protection; and

- Restricted – highly sensitive data requiring the highest level of protection and access control.

**Purpose Classification**

Government data shall also be categorized according to its primary purpose or role, such as:

- Identity and personal data;
- Reference and public data;
- Transactional and event data;
- Records and evidence; and
- Audit data.

The sensitivity and purpose classifications of authoritative datasets shall be recorded in the NISDC and be reviewed when the nature, use, legal status or risk associated with the data changes. The detailed classification criteria, handling requirements, access controls, protection measures, and review procedures shall be defined through applicable national data, privacy, security, and records-management standards.

## 8.3. Authoritative Sources and Once-Only Principle

Each authoritative government data element, dataset, or register shall have a designated authoritative source responsible for maintaining the current and authoritative record. Government agencies shall follow the Once-Only Principle, whereby information already held by an authorized government source shall not be unnecessarily collected again from citizens, businesses, or other government organizations.

Where legally and operationally permitted, government services shall obtain required information from the authoritative source through approved interoperability mechanisms and shall use the minimum data necessary for the intended purpose.

Consumer systems may maintain derived, cached, analytical, archival, evidentiary, or operational copies where necessary and authorized. Such copies shall:

- have a defined purpose and applicable legal basis;
- retain provenance and reference to the authoritative source;
- have appropriate freshness and retention requirements;
- not be treated as an authoritative source; and
- not be used to override or independently alter the authoritative source.

Government agencies shall not establish a competing authoritative source for an already registered data element, dataset, or register unless explicitly authorized by law or through the established data governance process.

Authoritative sources, ownership, custodianship, data domains, and interfaces shall be registered in the NISDC

## 8.4. Data Quality

The Data Owner remains accountable for data quality, while the Data Custodian is responsible for implementing the controls and processes necessary to maintain that quality. Appropriate data quality requirements shall be established for authoritative data, including:

- accuracy;
- completeness;
- consistency;
- currency and timeliness;
- validity;
- uniqueness;
- provenance; and
- integrity.

Data Custodians shall establish processes for identifying, reporting, correcting, and monitoring data quality issues. Data quality requirements shall be proportionate to the importance, sensitivity, and intended use of the data. Data Consumers shall not independently alter authoritative data. Corrections to authoritative records shall be made only through the designated authoritative source and approved correction procedures.

## 8.5. Data Sharing and Access

Government data shall be accessed and shared only for an authorized purpose and on a lawful basis, in accordance with applicable data classification, privacy, and security requirements. Data Consumers shall obtain data from the designated authoritative source through approved interoperability mechanisms and shall use only the minimum data required for the authorized purpose.

Government status alone shall not constitute a basis for access. Access shall be determined by the applicable legal authority, role, purpose, and authorization requirements.

Direct database-to-database integration between independent government systems shall not be used for routine data sharing. Data exchange shall use approved APIs, events or other standardized interoperability mechanisms unless an exception is approved for a justified requirement.

Where ongoing or significant data sharing occurs between organizations, the applicable governance arrangement shall define the purpose, participating organizations, data to be shared, responsibilities, access conditions, and accountability requirements.

Data access and sharing shall be appropriately logged and auditable in accordance with applicable legal, security, privacy, and governance requirements.

## 8.6. Metadata and NISDC

The NISDC shall serve as the government-wide metadata catalogue for government information assets including datasets, registers, information systems, digital services, APIs,

and associated governance information. It shall provide a common mechanism for registering, discovering, and governing these information assets. The NISDC shall maintain, as applicable, the following metadata:

- description and data definitions;
- Data Owner and Data Custodian;
- authoritative source;
- applicable classification and legal authority;
- interfaces and exchange mechanisms;
- data quality and lifecycle information; and
- relevant dependencies and lineage.

No new authoritative register or authoritative data source shall be designated without identification and registration of its legal authority, Data Owner, Data Custodian, and authoritative source in the NISDC.

NISDC shall maintain appropriate lifecycle status for registered information assets, such as proposed, active, deprecated, retired, and withdrawn.

## 8.7. Data Lifecycle, Retention and Disposal

Government data shall be managed throughout its lifecycle:
*creation/collection → validation → use → sharing → retention → archival → disposal.*

Data shall be collected and used only for specified and authorized purposes. It shall be retained only for the period required by applicable laws, records management requirements, and operational needs. Data retention requirements shall consider the following, as applicable:

- legal and regulatory obligations;
- public records and archival requirements;
- business and operational needs;
- audit requirements;
- privacy and data minimization requirements; and
- legal holds or litigation requirements, where applicable.

Disposal of government data shall be authorized, documented, and carried out using appropriate controls to prevent unauthorized recovery or disclosure.

Authoritative data shall not be deleted, retired, or replaced without an approved transition, archival, or disposal decision and appropriate consideration of dependent services. Detailed data retention periods, archival requirements, disposal procedures, and related controls shall be defined through applicable national standards, norms, and guidelines.

Applicable lifecycle and retention information for significant datasets and registers shall be recorded in the NISDC.

## 8.8. Federated Data Governance

Data governance shall operate consistently across federal, provincial, and local governments, while respecting constitutional responsibilities, statutory authority, and formally delegated functions. However, federalism shall not result in incompatible data models, interoperability mechanisms, or governance requirements. Government entities shall conform to applicable national data, interoperability, security, and service standards. Where a register or dataset involves multiple levels of government:

- the Data Owner and Data Custodian shall be designated in accordance with applicable legal authority;
- legally authorized organizations may act as Data Producers or Contributors;
- the respective roles, responsibilities, and authorities shall be documented;
- data provenance shall be maintained where records are produced or updated by multiple organizations; and
- applicable data models, schemas, and exchange mechanisms shall support national interoperability.

Where responsibilities are shared across levels of government, the applicable law, delegation, or intergovernmental agreement shall define the arrangements for data ownership, custodianship, production, access, quality, and dispute resolution.

## 8.9. Data Governance Compliance and Monitoring

Government agencies shall comply with applicable NEA data governance requirements, national data standards, privacy and security requirements, records-management requirements, and applicable laws and policies.

Data Owners and Data Custodians shall periodically review the governance status of significant datasets and registers, including ownership, classification, authoritative source, data quality, access arrangements, lifecycle status, and applicable compliance requirements.

The NISDC shall support data governance monitoring by maintaining relevant metadata and governance status of registered information assets.

Non-compliance shall be identified through appropriate data governance, architecture, audit, security, privacy, or other authorized assessment mechanisms and shall be subject to corrective action. Where immediate compliance is not feasible, the responsible organization shall follow the established governance and exception process and shall maintain an approved, time-bound remediation or transition plan.

# 9. Architecture Governance

Architecture Governance establishes the institutional authority, decision-making processes, responsibilities, and controls for governing the architecture of government IT systems in accordance with the NEA framework, applicable laws, government policies, and approved national standards. It shall ensure that government ICT investments and digital systems are interoperable, secure, reusable, citizen-centric, sustainable, aligned with national priorities and consistent with the approved target architecture. Architecture Governance shall apply to ministries, departments, constitutional and statutory bodies, federal agencies, provincial governments, local governments, and other public entities within the scope of the NEA framework as applicable.

## 9.1. Information Technology and Digital Governance Office

The ITDGO under the Office of Prime Minister and Council of Ministers (OPMCM) shall serve as the central government authority for enterprise architecture governance and coordination of government-wide digital architecture. ITDGO shall establish and maintain the governance mechanisms required for implementation of the NEA framework and shall coordinate with relevant government institutions responsible for digital infrastructure, cyber security, software development and operation, data governance, identity, privacy, records management, and other related functions. ITDGO shall perform the following principal functions regarding the architecture governance.

**A. Enterprise Architecture Governance**

ITDGO shall

- maintain and periodically update the NEA framework;
- establish and operate the architecture governance process;
- maintain the national architecture repository;
- facilitate the Architecture Review Board (ARB);
- conduct architecture conformance assessments;
- maintain architecture maturity and compliance information; and
- provide architecture guidance and advisory support to government entities.

**B. Standards and Reference Architecture**

ITDGO shall coordinate the development, approval, publication, and maintenance of applicable national standards and reference architectures, including, as appropriate:

- API and interoperability standards;
- data and information standards;
- identity and trust standards;
- cybersecurity and security architecture standards;
- cloud and infrastructure standards;
- accessibility standards;

- user interface and design standards, and
- other standards necessary to implement the NEA framework.

The standards shall be developed and maintained through an established version-controlled governance process and shall be reviewed periodically.

#### C. Architecture Conformance and Compliance

To ensure architecture conformance and compliance, ITDGO shall

- establish architecture review and conformance criteria;
- review architecture received from government entities;
- maintain conformance and exception records;
- coordinate architecture audits and assessments;
- monitor compliance with approved architecture and standards; and
- report significant compliance issues to the competent authority.

#### D. Coordination with Shared Digital Infrastructure

ITDGO shall coordinate architecture decisions with the agencies responsible for DPI and shared digital services to ensure that government entities reuse approved shared capabilities and do not unnecessarily establish duplicate national or cross-government capabilities.

### 9.2. Roles of Government Institutions Responsible for DPI and Shared Services

Government agencies that are legally or administratively responsible for DPI and shared services shall perform their respective functions in accordance with their mandates and the NEA framework. Such institutions shall:

- design, develop, operate, and maintain the digital infrastructure or shared services under their respective mandates;
- comply with applicable national standards, security and data governance requirements, and the NEA framework;
- provide reusable and interoperable capabilities where their mandate requires provision of shared government services;
- provide relevant architecture, service, dependency, and technical information for inclusion in the government architecture repository and NISDC, as applicable; and
- cooperate with other government institutions to avoid unnecessary duplication of infrastructure, platforms, and digital capabilities.

The specific responsibilities of each institution shall be determined by its legal mandate, government decisions, approved organizational arrangements, and applicable policies, and shall not be inferred solely from the NEA framework.

## 9.3. Architecture Review Board

The Architecture Review Board (ARB) shall serve as the principal cross-government architecture decision-making and competent authority. The composition of the ARB shall include:

1. Secretary, ITDGO – Chairman;
2. Joint Secretary, OPMCM – Member;
3. Joint Secretary, IT Governance and Standardization Division, ITDGO – Member;
4. Joint Secretary, Public IT Infrastructure Division, ITDGO – Member;
5. Chief, National Cyber Security Centre – Member;
6. Executive Director, Software Development and Operation Center – Member;
7. Representatives, Experts nominated by OPMCM – 2 Members;
8. IT Director, IT Standardization and Architecture Section, ITDGO – Member Secretary

The ARB shall:

- oversee implementation of the NEA framework;
- approve government-wide reference architectures and major architecture standards within its delegated authority;
- approve architecture conformance decisions;
- approve or recommend architecture exceptions and waivers;
- resolve significant architecture conflicts between government entities;
- promote reuse of shared digital infrastructure and common capabilities;
- provide guidance on strategic adoption of emerging technologies;
- review architecture maturity, compliance, and implementation progress; and
- recommend amendments and improvements to the NEA framework to the Government of Nepal for approval.

The ARB shall define its own working procedures. All architecture decisions shall be formally documented and, where applicable, shall specify the approval status, associated conditions, required actions, and responsible parties.

## 9.4. Responsibilities of Public Agencies

Each public entity implementing or operating an ICT or digital system shall be responsible for ensuring that its architecture conforms to the NEA framework and applicable national standards. The concerned government entity shall:

- designate an accountable business owner and technical/architecture focal point;
- prepare and maintain the required architecture documentation;
- identify applicable NEA principles, standards, reference architectures, and shared platforms;
- conduct architecture assessment before major procurement or implementation;
- submit projects requiring central architecture review to ITDGO;
- implement approved architecture decisions and conditions;

- maintain system, application, data, integration, security, and infrastructure architecture information;
- register applicable information assets and dependencies in the NISDC and architecture repository;
- maintain evidence of architecture compliance; and
- address identified non-conformities within the approved timeframe.

## 9.5. Architecture Change Control

Any amendments to the NEA framework, mandatory architecture standards, reference architectures, common patterns, or government-wide architecture requirements shall be managed through a formal change-control process.

A change proposal shall identify:

- reason and objective of the change;
- affected architecture components;
- business, legal, technical, security, data, and interoperability impacts;
- dependencies and affected entities;
- transition and implementation requirements; and
- proposed effective date.

ITDGO shall coordinate the assessment and approval of changes according to their significance. Major changes shall be approved by ARB, as applicable. Approved changes shall be version-controlled, published through the appropriate government mechanism, and communicated to affected entities. An appropriate transition period or migration arrangement shall be established wherever existing systems are affected.

## 9.6. Monitoring and Reporting

ITDGO shall establish mechanisms to monitor implementation and effectiveness of the NEA implementation. Monitoring shall include, as appropriate:

- compliance with architecture requirements;
- architecture conformance status;
- outstanding non-conformities;
- approved exceptions and their status;
- adoption of national standards;
- reuse of shared digital capabilities;
- interoperability and NDXP adoption;
- duplication of digital capabilities;
- significant architecture risks; and
- implementation of major architecture decisions.

ITDGO shall maintain appropriate architecture governance information and periodically report significant findings to the ARB. The ARB shall periodically review architecture governance performance and recommend corrective actions, priorities, or improvements to the NEA framework.