Ministry of Information Technology, Communication and Innovation

DIGITAL SERVICE FRAMEWORK

Powering Better Digital Government Services

August 2026

CONTENTS

Document Control

Version	Status	Date	Description	Author / Owner
V0.20	Draft	Dec 2025	Working draft submitted for consultation	CIB
V0.21	Draft	March 2026	Amended following inputs from DPO, ITSU and CIB	CIB
V0.22	Draft	March 2026	Amended following inputs from ITSU, AI Unit and CIB	CIB
V0.23	Draft	March 2026	Formatting and typos	CIB
V0.24	Draft	August 2026	Amendments in respect of Super App	CIB
V1.0	Release	August	First Release	CIB

1. INTRODUCTION

1.1 Purpose of the Framework

The Digital Service Framework (DSF) is the central policy enforcement mechanism through which the Government of Mauritius ensures that all digital services developed, procured or maintained by Ministries and Departments are compliant to major digital policies regulating secure government digital services.

In contrast to high-level strategies or time-bound blueprints, the DSF is designed to be permanent, prescriptive and enforceable. It is not just a set of guiding principles but also policies and standards that underpins how government digitalises services. Whether deploying a new online portal, integrating with national identity systems or upgrading legacy back-office platforms, Ministries must adhere to this framework as a prerequisite condition for project acceptance.

By establishing a clear, unified set of principles, policies and design standards, the DSF ensures that digital public services are secure, reliable, accessible and interoperable. It positions digital transformation not as a fragmented set of IT initiatives, but as a cohesive and integrated whole-of-government reform aligned with existing legislations with the right governance and operational culture.

Internationally, many governments have adopted enforceable digital service frameworks to ensure coherence, trust and quality in public sector transformation. The United Kingdom mandates its Government Service Standard for all digital projects, Estonia embeds its once-only and interoperability principles in law through the Public Information Act and X-Road, Singapore's Digital Government Blueprint makes mobile-first and reuse-first design compulsory, India enforces its Digital Service Standard for all e-Government projects and the European Union's Interoperability Framework establishes binding rules for cross-border digital services. The Mauritius DSF builds on these global precedents, positioning itself as a nationally tailored framework that ensures every service is secure, interoperable, inclusive and citizen-centric.

1.2 Role of the DSF

The Digital Transformation Blueprint (2025–2029) outlines the national vision, strategic priorities and flagship initiatives for the digital transformation of the country. It defines the "what", i.e. the services, sectors and outcomes government aspires to achieve.

The DSF defines the "how". It codifies the principles, policies and standards that must be followed to develop and deliver any digital service, whether listed in the Blueprint or not.

The Digital Transformation Blueprint is a strategic document that is periodically reviewed and updated (typically on a five-year cycle) to reflect evolving political priorities and socio-economic objectives.

The Digital Service Framework (DSF), while also subject to periodic review and updates, serves as a compliance framework that governs the design, procurement, implementation, and operation of digital services across Ministries and Departments and covers:

- Project planning
- System architecture
- Procurement of digital solutions
- Service design
- Deployment and operations
- Citizen interface and accessibility

DSF applies to all projects. However, compliance validation shall be proportionate to project risk, scope, and impact.

1.3 Why the DSF is Needed

Mauritius has made significant investments in digital infrastructure and public services. Yet, without a common enforcement framework, Ministries risk:

- Building services in silos, incompatible with shared platforms;
- Duplicating efforts, leading to higher costs and confusion;
- Delivering inconsistent user experiences, undermining public trust; and
- Violating privacy regulations due to poor identity or consent practices;
- Facing challenges in ensuring security of citizen data, which could affect overall cybersecurity resilience.

These challenges are not merely technical; they are governance gaps resulting from the absence of a unified architectural, policy and compliance framework.

The DSF addresses these structural weaknesses by:

- Establishing mandatory identity, interoperability and data-sharing standards;
- Embedding privacy, security and compliance into system design;
- Linking procurement and funding approval to technical alignment;
- Promoting reuse of shared national platforms; and
- Ensuring accountability through monitoring and audit mechanisms.

By doing so, the DSF transforms digital initiatives from isolated ICT projects into components of a coherent, secure and citizen-centric digital ecosystem.

1.4 Scope and Applicability

This framework is applicable across the public sector.

It applies to:

- All ministries and departments of the government

- Third-party vendors, contractors and integrators providing digital services to government
- All platforms, portals, apps, APIs and backend systems, whether internal or public-facing.

It covers:

- Full service lifecycle: design, development, integration, testing, deployment, maintenance and decommissioning
- All project types: citizen-facing services (G2C), business portals (G2B), internal systems (G2G) and hybrid platforms
- Any government-funded or regulated initiative with a digital component

1.5 Enforcement Through Core Policies

The DSF mandates compliance across all four pillars:

Principles (*the why*)

Values and design philosophies that underpin digital government.

Architecture Principles (*the enablers*)

Technical foundations for interoperability, cloud-readiness, reusability, and security-by-design.

Policies (the rules)

Binding requirements governing identity, data, documents, security, procurement, and audit.

Design Standards (*the how*)

Practical rules for service design, accessibility, multilingualism, mobile-first, and modular architecture.

Compliance is not optional: every digital initiative, regardless of size or origin, must adhere to these requirements as a condition of approval, funding and operational acceptance.

Summary of DSF Enforcement Mandates:

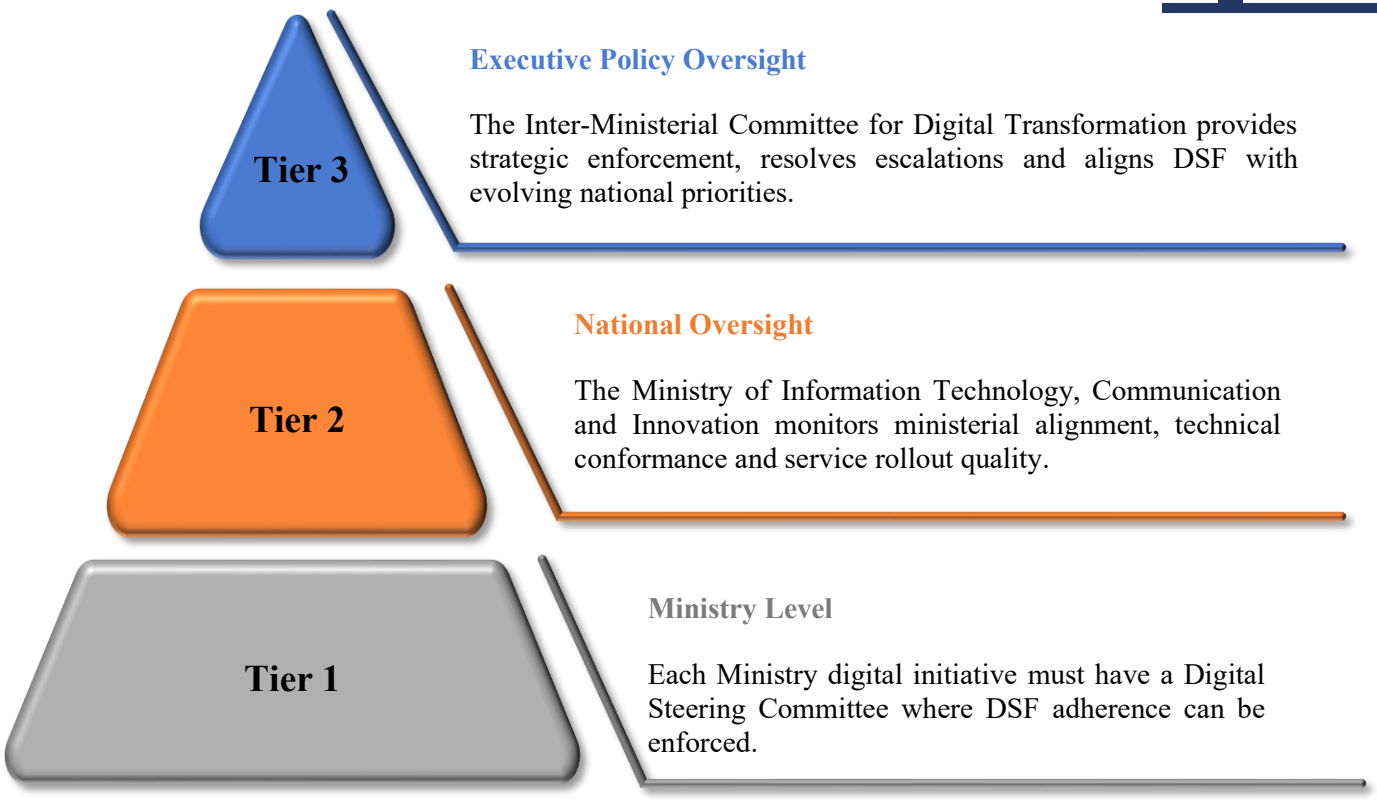
The DSF includes:

- **Guiding Principles** – Foundational rules that shape how all government digital services are designed and delivered, covering digital-by-default, mobile-first, interoperability, privacy, accessibility, security, reuse and green ICT.
- **Architecture Principles** – Technical foundations that ensure systems are modular, API-first, interoperable, secure-by-design, cloud-ready, mobile-centric, event-driven, micro-front-end enabled, resilient and integrated into the national GovStack.
- **Core Policy Mandates** – Mandatory enforcement rules governing identity, authentication, data sharing, privacy, cybersecurity, APIs, digital signing, cloud hosting, Digital Payments, monitoring, procurement, AI, digital inclusion, change management and whole-of-government reuse.
- **Design Standards** – User-facing requirements ensuring services are life-event based, accessible (WCAG 2.1 AA), multilingual, mobile-first, prefilled with authoritative data, transparent, trackable and supported by help, feedback and performance benchmarks.

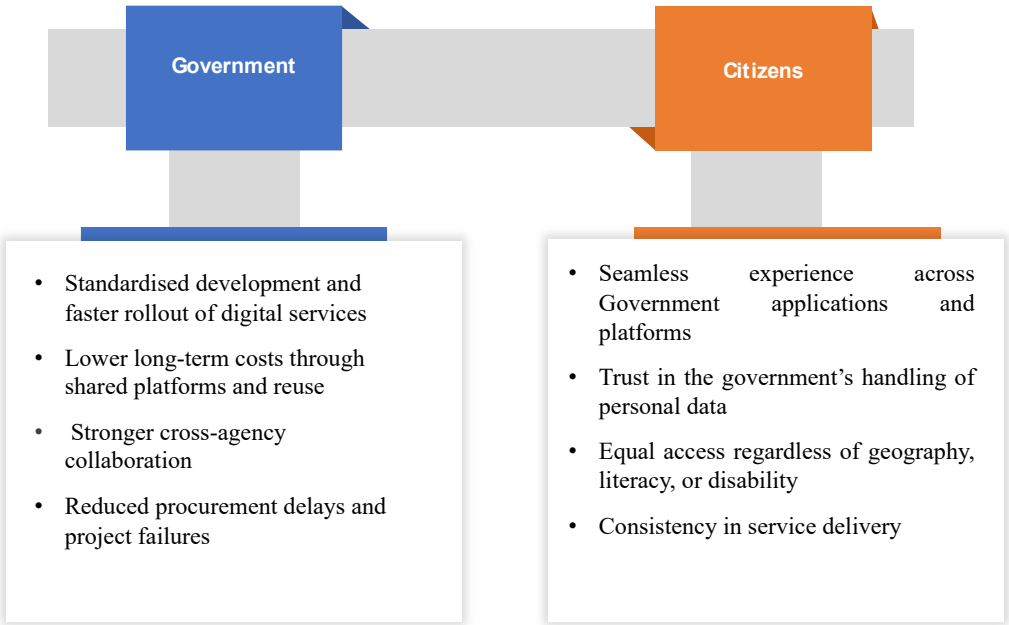
1.6 Institutional Governance of DSF

The DSF is enforced through a multi-tier governance system, aligned with the national ICT governance model setup for the monitoring of the blueprint 2025-2029.

The CIB, MDPA, GOC, METC, AI Unit and ITSU serve as the functional arms of MITCI.



1.7 Expected Outcomes



1.8 DSF as the Backbone of Trust

Trust is the foundation of digital government. Without it, citizens won't use online services. The DSF makes trust systemic through:

- Mandatory use of national identity systems for authentication
- Government-wide security protocols
- Central control over privacy frameworks
- Guaranteed service integrity, uptime and response time

Trust is not a marketing claim. It is a verifiable, auditable standard embedded in every DSF-compliant service.

1.9 DSF vs Fragmentation

The DSF is the antidote to fragmentation. It replaces:

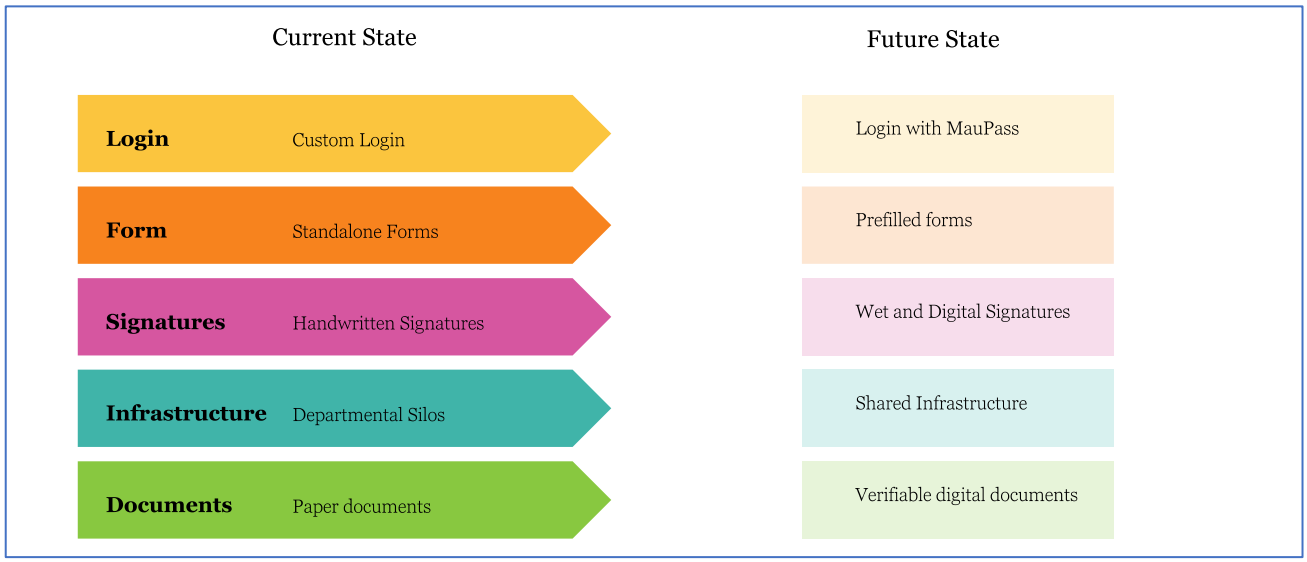


Figure 2: DSF vs Fragmentation

1.10 A Living and Evolving Framework

The DSF is versioned, reviewed and updated annually. Future updates will integrate:

- Artificial intelligence guidelines
- Blockchain-based verifiable credentials
- Expanded citizen lifecycle services

1.11 National Legal and Institutional Anchoring

While the Digital Service Framework draws on international best practices and recognised standards, its implementation is grounded in the legal, regulatory and institutional context of Mauritius.

The DSF operates in alignment with, inter alia:

- The Data Protection Act 2017
- The Electronic Transactions Act
- The Public Procurement Ac
- The National Cybersecurity Strategy
- The Mauritian Public Key Infrastructure framework

1.12 Exceptions

The DSF applies to all government digital initiatives; however, specific requirements may apply to varying degrees depending on the project's nature, scope, risk, and impact. Compliance validation shall be proportionate to project complexity and citizen impact.

1.13 Relationship with Procurement and Budgeting

The DSF is directly tied to:

- ICT project approvals
- Budget allocations
- Supplier evaluations
- System Operational Acceptance

If a digital initiative fails DSF compliance checks, it will not proceed to procurement or implementation. DSF-compliance is therefore a requirement for execution and acceptance.

1.14 Structure of the Framework

The remainder of the DSF is organised to:

1. Establish the Guiding Principles;
2. Articulate the technical architecture and integration framework;
3. Specify the binding policy requirements;
4. Detail the design and user experience standards; and
5. Define the mechanisms for monitoring, compliance and enforcement.

2. GUIDING PRINCIPLES AND FOUNDATIONS

Figure 3: List of Guiding Principles

2.1 Overview

To ensure consistency, integrity and sustainability of digital government, this Framework is grounded in a set of guiding principles that define the values, design philosophies and systemic norms that all public sector entities must embrace when implementing or managing digital services.

These principles are derived from:

- The Digital Transformation Blueprint 2025–2029 of Mauritius,
- International best practices (OECD, UN, World Bank),
- The needs of Mauritian citizens, especially in terms of trust, access and inclusivity.

They guide how services are conceived, built, deployed and improved and not just what is delivered.

2.2 Principle 1 – Digital by Default & Whole of Life

Purpose:

Citizens should be able to access public services online as the primary channel, reducing travel, paperwork and delays. Incorporating a Whole-of-Life approach ensures services are organised around major life events and end-to-end journeys, rather than ministry structures, so users do not need to understand how Government is organised to complete a service.

International Perspective:

According to the OECD Digital Government Policy Framework, a government that is digital by design establishes clear organizational leadership, paired with effective coordination and enforcement mechanisms, where "digital" is considered not only a technical topic but a mandatory transformative element to be embedded throughout policy processes. This underscores that digital services are not an optional enhancement, they must be central to policy and service delivery.

Evidence:

- Estonia: 99% of government services are online by default, cutting transaction costs significantly.
- UK GDS: Service Standard ("Digital by Default") reduced failed IT projects and simplified access.
- OECD/UN e-Government Index: Digital-first governments rank higher in citizen trust and service uptake.

Requirements:

- All new public services must be digital from the outset, not as an afterthought.
- Every eligible service must be offered online by default and promoted as the primary channel.
- Services must be designed around Whole-of-Life and Whole-of-Business journeys, ensuring users do not provide the same information multiple times.
- Forms must be prefilled using authoritative data from InfoHighway and the Citizen Data Hub. E.g., demographic data like Surname, Other Name, NIC number and date of birth from the Central Population Database may be used to prefill application forms after the identity of the applicant is verified.
- Forms may be prefilled using data from authoritative sources like the Citizen Data Hub after the applicant has been securely authenticated online or face to face using an approved identity mechanism. Verified demographic attributes such as surname, other names, NIC number and date of birth from the Central Population Database may be used to populate application fields and the prefilled information is presented to the applicant for review and confirmation prior to submission.
- Non-digital or assisted channels (e.g., kiosks, support centres) must complement but should not replace the digital version.
- Exceptions must be justified and approved by the Miinstry or Department.

***Example**:* Application to government services like social benefit applications should all be accessible via online portals or apps without requiring a physical visit.

2.3 Principle 2 – Mobile-First, Super App Enabled

Purpose:

In Mauritius, mobile is the dominant mode of internet access. Mobile-first design ensures inclusivity across socio-economic groups, by allowing everyone, regardless of their device or internet speed, to access digital government services easily. Integration into the Government Super App avoids duplication and improves convenience by bringing services together in one secure and accessible platform.

Evidence:

- India's Umang Super App: Unified access to 1000+ services improved adoption.
- Singapore GovTech: Promotes mobile-first responsive design to ensure equitable access.
- World Bank GovTech Index: Mobile-first adoption is a characteristic of mature digital government.

All services must be optimised for mobile access and eventually integrated into the government Super App ecosystem.

- Interfaces must be responsive, lightweight and work even on low-end smartphones.
- User registration and setup must be simple, requiring only essential details.
- Any mobile app developed must adopt a micro front-end model so it can be quickly and seamlessly integrated into the Government Super App for deployment.
- If the App should not be part of the Government Super App, the Central Informatics Bureau will give its clearance on same.

***Implication**:* Citizens, regardless of the device they use, will be able to access key services, from applying for a driving licence to checking social benefits or booking appointments and later all such services will be accessible seamlessly through a single, government Super App.

2.4 Principle 3 – Proof of Identity and Secure Transactions

Purpose:

Secure digital identity is the foundation of trust in government services to avoid multiple logins, fraud risk and increase confidence in online interactions. Secure digital transactions for example through the use of digital signatures protect both citizens and government entities. By adopting this principle, Mauritius can improve convenience, strengthen data security and reduce the risk of identity misuse while aligning with proven global practices in trusted digital governance.

International Perspective:

The EU eIDAS Regulation establishes a framework for digital identity and authentication. It aims to create confidence in electronic interactions and promote seamless digital services within the EU, ensuring that digital identities and electronic transactions are safeguarded against fraud and cyber threats.

Evidence:

- EU eIDAS: Established a unified legal framework for secure electronic identification and trust services across the EU.
- Estonia eID: Enabled nationwide digital identity adoption, supporting 99% online public services.
- India Aadhaar & eSign: Over 80 billion secure transactions processed, reducing fraud.
- Mauritius: MauPass and Mobile ID already exist; DSF makes them compulsory.

All services must require user login via MauPass and where relevant, Mobile ID with secure and trusted Identity proofing:

- Services must not create separate usernames/passwords or proprietary logins for citizens.
- Identity proofing must be based on authoritative identifiers: NIN for citizens, Passport or permit number for foreigners and BRN for businesses.
- All transactions must be traceable to a verified identity.
- Digital signatures must be applied to approvals, authorisations and any official digital document that requires legal validity or later verification

Benefit: Uniform, secure access improves convenience and defends against fraud.

2.5 Principle 4 – Once-Only and Data Reuse

Purpose:

Citizens should not repeatedly submit the same information to different ministries/departments. Once-only principles reduce burden, improve accuracy and save costs. By reusing data that already exists in trusted government systems, services become faster, more reliable and user-friendly. This approach also promotes efficiency across ministries, supports data integrity and builds public trust by ensuring that data sharing is done securely and with consent wherever required.

International Perspective:

The OECD recommends the adoption of the Once-Only Principle to streamline services and reduce unnecessary administrative burdens. This principle ensures that citizens and businesses provide certain standard information to public authorities only once, with data reuse enabled through interoperable systems and user consent. This approach aims to simplify procedures and enhance service delivery.

Evidence:

- Estonia's X-Road: Eliminated redundant data entry, improving efficiency.
- EU Once-Only Regulation: Legal mandate for cross-border data reuse.
- OECD: Highlights once-only as a critical driver for service efficiency and trust.

Citizens and businesses must not be asked to provide the same data more than once.

- Services must reuse authoritative data through InfoHighway like the Central Population Database/ Citizen Data Hub.
- Data-sharing agreements and data flow mappings must be in place.
- Ministries must consume APIs, not replicate data locally unless authorised.

***Application**:* If updated address data is already in the CPD, no Ministry should ask for it again.

2.6 Principle 5 – Privacy, Transparency and Ethics by Design

Purpose:

Citizens must retain control over their personal data. This principle requires that privacy, transparency and ethical safeguards are embedded into digital services from the earliest stages of design and development and maintained throughout the service lifecycle, rather than being introduced retrospectively.

Applying this principle ensures that personal data is processed lawfully, fairly and responsibly. It strengthens trust between government and citizens, reduces the risk of data breaches or misuse and ensures compliance with national and international data protection and governance frameworks.

Privacy by design ensures that privacy considerations are integrated into systems from the outset to protect personal data. In parallel, digital services must be designed to be transparent and user-centred, ensuring that individuals can easily understand how their personal data is collected, used and shared and can effectively exercise their data protection rights, including the right to withdraw consent. Ethics by design further promotes fairness, transparency and accountability across all digital services including artificial intelligence systems, strengthening confidence in government digital services.

International Perspective

The OECD Digital Government Policy Framework emphasizes that a government that is digital by design focuses on securing the assisted delivery of digital services. This includes protecting privacy, promoting transparency, and designing user experiences that help citizens understand and grant or revoke consent for their data to be used.

Reference Frameworks

- **European Union General Data Protection Regulation (EU GDPR):** Sets global benchmark for privacy by design, lawful processing, consent, purpose limitation and accountability.
- **OECD Principles on Artificial Intelligence:** Provide guidance on transparency, explainability and auditability for AI systems.

- **Mauritius Data Protection Act:** Requires compliance with data protection principles, including the conduct of Data Protection Impact Assessments (DPIAs) for high-risk processing operations.

Mandatory Requirements

All digital services must embed privacy, transparency and ethical safeguards from the design stage and throughout their lifecycle. In particular:

- All digital services must comply with the Data Protection Act and all guidance issued by the Data Protection Office.
- A Data Protection Impact Assessment (DPIA) must be conducted for high-risk processing operations using the template prescribed by the Data Protection Office.
- Where consent is relied upon as the lawful basis for processing, it must be obtained and managed in accordance with the requirements of the Data Protection Act.
- Ethical use of algorithms and AI must follow guidance issued by MITCI and international guidance ensuring explainability and auditability.

Benefit: This principle ensures that citizens maintain control over their personal data and reinforces public trust through transparent, ethical and accountable government digital services.

2.7 Principle 6 – User Centric, Accessibility and Inclusivity

Purpose:

Digital services must be designed around real user needs and life events. No citizen should be excluded due to disability, literacy level, language barriers, or geographic location. Technical compliance alone does not guarantee effective service delivery; services must be usable, understandable, and accessible to all segments of society. Inclusive, user-centred design strengthens public trust, improves adoption, and ensures equitable participation in the digital state.

International Perspective:

International best practice, including the UK Government Service Standard and the European Union's Digital Inclusion Strategy, emphasises designing services around users' needs rather than institutional structures. These frameworks combine accessibility standards with user research, usability testing, and continuous service improvement to ensure meaningful digital inclusion.

Evidence:

- The UN Convention on the Rights of Persons with Disabilities (CRPD) recognises accessible digital information and communication as a fundamental right and WCAG 2.1 is the internationally accepted technical standard for ensuring such accessibility.
- Countries such as Canada and the United Kingdom mandate accessibility compliance alongside user-centred service design practices, resulting in higher service adoption and reduced exclusion.
- Mauritius is a multilingual society where a large proportion of citizens rely primarily on Kreol and French. Ensuring multilingual interfaces is therefore essential to support adoption and reduce language-related barriers to digital access.

No citizen must be excluded from accessing digital services due to:

- Disability,
- Low digital literacy,
- Language barriers,
- Geographic remoteness.

Requirements:

- All citizen-facing services must comply with WCAG 2.1 accessibility standards.
- Ministries must conduct user research and usability validation for major citizen-facing services prior to go-live.
- Interfaces must mandatorily support English and where feasible, French and Kreol.

- Alternative access channels (e.g., assisted digital at Citizen Support Centres) must be designed into service delivery models.
- Ministries remain accountable as Service Owners for ensuring services are understandable, usable, and continuously improved based on user feedback.

***Design Mandate**:* Government digital services shall be designed around user needs first, with accessibility and inclusion embedded by design.

2.8 Principle 7 – Interoperability and Reusability and Whole-of-Government

Purpose:

Interoperability ensures that systems can communicate and work together seamlessly, while reusability prevents ministries from rebuilding similar components. Extending this to a Whole-of-Government approach ensures services operate within a unified ecosystem where common platforms, data standards and shared components reduce duplication and improve service delivery across Government.

International Perspective:

The OECD Digital Public Infrastructure guidance highlights that interoperable platforms enable collaboration across government entities. The EU Interoperability Framework identifies Whole-of-Government integration, API reuse and common standards as essential for consistency and efficiency.

Evidence:

- EU Interoperability Framework: Promotes API reuse and modular systems.
- Estonia & Singapore: Mandatory integration into national platforms reduced system silos.
- India NeGD: APIs and open standards enabled massive scalability.

Every service must be interoperable and built to reuse existing government platforms.

- Services must integrate amongst others with:
  - InfoHighway for data,
  - Physical ID, Mobile ID and MauPass for digital identity,
  - Digital Payment gateway,
  - eSign service of MauSign,
  - SMS Gateway,
  - Citizen Data Hub for citizen data
- Source code developed specifically for government must be reusable across public institutions and structured to avoid vendor lock-in. Intellectual property and licensing arrangements shall ensure government retains sufficient rights for maintenance, modification, and reuse.
- APIs must follow interoperability standards and be documented.

***Impact**:* Fragmented systems create long-term maintenance and integration costs.

2.9 Principle 8 – Open by Default

Purpose:

Transparency improves trust and reduces corruption. Open data enables innovation and better decision-making by the private sector and civil society.

International Perspective:

The International Open Data Charter, developed in 2015 through the Open Government Partnership by a coalition of governments and global open-data organisations, defines “Open by Default” as its core principle. It states that data generated by public institutions should be proactively released unless restricted by legitimate privacy, security, or confidentiality requirements. This globally recognised framework guides governments in promoting transparency, strengthening accountability and enabling innovation through accessible and reusable public data.

Evidence:

- Open Data Charter: Countries adopting open-by-default have seen improved accountability.
- UK data.gov.uk & India data.gov.in: Fuelled civic tech ecosystems.
- Mauritius open data portal: Existing foundation to be expanded.

Public-facing data and services must be transparent.

- Non-sensitive datasets must be proactively published on data.govmu.org in open, machine-readable formats.
- Service decisions, notifications and processing statuses must be visible to users to strengthen trust and accountability.
- Where feasible, the DSF encourages the use of open-source technologies to promote transparency, reuse and cost-efficiency.

***Example**:* Service dashboards showing real-time application status or waitlists.

2.10 Principle 9 – Resilience, Continuity and Security

Purpose:

Critical services must withstand outages, cyberattacks and disasters. Citizens lose trust if services fail during emergencies but also when systems become unavailable or slow during peak usage periods. For example, having backup systems and disaster recovery plans allows citizens to access emergency services even during a cyberattack or natural disaster.

International Perspective:

The National Cybersecurity Strategy 2023-2026 for Mauritius, outlines the pillar of "A Resilient Infrastructure" as essential to protecting critical information infrastructure and supporting the continuity of critical services in the face of disruptive or sophisticated attacks.

Evidence:

- NIST Cybersecurity Framework: Global model for resilience planning.
- Singapore GovCloud: Requires redundancy and DR plans for Tier 1 services.
- Estonia 2007 Cyberattacks: Led to national resilience mandates now copied worldwide.

Services must be built to withstand disruption and protect user data.

Critical services must comply with IT Security guidelines issued by MITCI.

- Services must be designed and tested for peak-demand scenarios, including load testing, concurrency management, and scalable capacity planning to ensure availability and responsiveness during high-traffic periods.

***Security Rule**:* Compliance with Government security elements/standards and IT security audits is mandatory.

2.11 Principle 10 – Value for Money and Green ICT

Purpose:

Digital government must be sustainable both financially and environmentally. Applying this principle ensures that public funds are used efficiently, avoids unnecessary duplication and reduces the environmental impact of ICT systems. For example, using shared cloud platforms instead of separate servers for each ministry saves money and energy.

International Perspective:

The OECD Digital Government Policy Framework (2020) stresses that public investments in digital transformation must ensure *value for money* by avoiding duplication, using shared

digital infrastructure and adopting scalable, interoperable systems. It highlights that fiscal sustainability and cost-efficiency are key to maintaining long-term trust in digital government programmes.

Evidence:

- EU Green Digital Principles: Require ICT energy efficiency.
- OECD on GovTech: Emphasises cost-effectiveness and modular procurement.
- India Cloud & UK G-Cloud: Demonstrated lifecycle cost savings from shared platforms.

Government must maximise return on investment and minimise environmental impact.

- Projects must demonstrate cost-efficiency and avoid duplication.
- Green coding practices and software optimisation are encouraged
- Cloud resources and devices must be used.
- Procurement must prioritise modular, scalable and low-footprint solutions.

***Sustainability Mandate**:* Digital does not mean wasteful.

2.12 Summary Table – DSF Principles

#	Principle	Enforcement
1	**Digital by Default and Whole of Life**	All new services must be digital-first
2	**Mobile-First & Super App Enabled**	Responsive design and integration All interfaces must be responsive, lightweight and compatible with low-end smartphones.

3	**Proof of Identity and Secure Transactions**	Physical ID, Digital ID (MauPass) & Mobile ID required Citizen login via MauPass and Mobile ID required; Digital signatures required for official documents requiring verification.
4	**Once-Only and Data Reuse**	Reuse from InfoHighway Services must reuse authoritative data via InfoHighway and Citizen Data Hub. Ministries must consume APIs - local replication only if legally required.
5	**Privacy, Transparency and Ethics by Design**	Mandatory DPIAs Valid consent in accordance with the Data Protection Act
6	**User -Centric, Accessibility and Inclusivity**	WCAG 2.1 & multilingual Comply with WCAG 2.1 standards. Interfaces must support Multilingual.
7	**Interoperability, Reusability and Whole of Government**	API integration Integration with InfoHighway, MauPass, Mobile ID, Digital Payment, eSign, SMS Gateway and Citizen Data Hub. APIs must follow standards and be documented.
8	**Open by Default**	Public-facing transparency Decisions, notifications and processing statuses visible to users. Encourage open-source solutions.
9	**Resilience, Continuity and Security**	Audits, uptime, DR plans

		Critical services must comply with IT security guidelines issued by the MITCI.
10	**Value for Money and Green ICT**	Reuse-first, low-carbon design Projects must demonstrate cost-efficiency. Use energy-efficient coding, cloud resources and devices. Procurement to prioritize modular, scalable and low-footprint solutions.

3. DIGITAL ARCHITECTURE PRINCIPLES AND DESIGN FOUNDATIONS

3.1 Overview

A well-governed digital government requires not only policies and processes, but also a coherent, modular and secure technology architecture. This chapter defines the national platform components, integration principles and architectural standards that all ministries and departments must align with when developing or modernising digital services.

3.2 National Digital Architecture Principles

The DSF recommends adherence to the following architectural principles, which are grouped into four key categories that define each principle's primary focus: Core Design Principles, Platform Integration Principles, Security & Resilience Principles and Emerging Digital Architecture Principles.

3.3 Core Design Principles

These principles establish the fundamental rules for how individual components and services are built and function.

#	Architecture Principle	Intent / Short Description
1	**Modular by Design**	Systems shall be developed as discrete, reusable components or services.
2	**API-First**	All systems must expose and consume services through APIs.
3	**Interoperable**	Systems must connect seamlessly through common standards and protocols.
4	**Cloud-Ready**	Systems must be deployable on the Government Cloud or approved sovereign cloud.

5	**Mobile-Centric**	Services shall be optimised for mobile access and responsiveness.
6	**Secure-by-Design**	Security controls must be embedded at every layer of the system.
7	**Zero Redundancy**	Duplicate or overlapping platforms shall not be created.

3.4 Platform Integration Principles

These principles govern how systems and data are connected and shared across the broader technology ecosystem or national platform.

#	Architecture Principle	Intent / Short Description
8	**Single Source of Truth**	Data shall originate from authoritative systems like the CDH.
9	**Reuse Before Buy**	Existing national platforms must be reused before new development.
10	**Integrated National Stack**	All systems must integrate with national platforms such as MauPass, MoKloud, etc.
11	**Data Sharing by Default**	Data shall be shared securely preferably via InfoHighway
12	**Micro Front-End by Design**	Front-end components shall be modular, reusable, and capable of integration into the Government Super App.
13	**Event Driven Architecture**	Systems must be API-first, modular, and capable of secure integration within the national digital ecosystem.

3.5 Security, Privacy & Resilience Principles

These principles focus on protecting the system, ensuring data integrity and meeting compliance requirements.

#	Architecture Principle	Intent / Short Description
14	**Zero-Trust Architecture**	Every request must be authenticated, authorised and logged.
15	**Defense-in-Depth**	Implement multiple security layers across network, application and data.
16	**Privacy-by-Design**	Privacy protections shall be embedded from inception of system design.
17	**Sovereignty-by-Design**	All critical data shall reside within national or approved sovereign infrastructure.
18	**Business Continuity-by-Design**	Systems must include redundancy, fail-over and disaster-recovery capabilities.
19	**Continuous Monitoring**	Real-time performance and security monitoring must be implemented.

3.6 Emerging Digital Architecture Principles

These principles guide the use of modern design approaches, like event-driven systems, to encourage innovation, improve flexibility and support environmental sustainability.

#	Architecture Principle	Intent / Short Description
20	**Microservice-Oriented Architecture**	Build systems as independent, reusable services communicating via APIs.

21	**Green-by-Design**	Design infrastructure and software for energy efficiency and minimal footprint.
22	**Agility and Sandbox-Driven Innovation**	Test and validate new technologies in controlled sandboxes before scale-up.

3.7 Modular by Design

Recommendation

Modular design endorsed by The Open Group TOGAF 9.2 and the OECD Digital Government Policy Framework encourages development of self-contained, reusable components that interoperate through clear interfaces.

Detailed Recommendations

- Decompose solutions into discrete, functional modules or services.
- Define boundaries following ISO 42010 Systems and Software Architecture Description.
- Enable independent deployment and maintenance.
- Register reusable modules in a shared repository to promote reuse across government.

Expected Outcome

Systems become easier to maintain, integrate and evolve, reducing cost and duplication while enabling continuous innovation.

3.8 API-First

Recommendation

An API-First approach consistent with EU European Interoperability Framework (EIF) v3.0, World Bank GovTech Maturity Index and OpenAPI 3.1 makes capabilities programmatically accessible for integration and reuse.

Detailed Recommendations

- Design APIs concurrently with business logic using RESTful or GraphQL standards.
- Document and register APIs with the MITCI/DMO.
- Secure access through OAuth 2.0 / OIDC tokens and TLS 1.3.
- Route cross-agency data exchange via the InfoHighway.

Expected Outcome

Interoperability becomes embedded in every system, accelerating integration and automation across ministries.

3.9 Interoperable

Recommendation

Interoperability is core to the European Interoperability Framework (EIF) and OECD Digital Government Model and ensures seamless exchange of information across administrative boundaries.

Detailed Recommendations

- Adopt open data formats (JSON, XML, CSV) and shared code lists.
- Align with MITCI/DMO interoperability standards.
- Connect through the InfoHighway as the integration backbone.
- Maintain standardised data definitions and metadata consistent with recognised metadata registry practices (e.g., ISO/IEC 11179).

Expected Outcome

Data flows securely between agencies, enabling coherent, citizen-centric digital services.

3.10 Cloud-Ready

Recommendation

Cloud-ready architecture is aligned with OECD Cloud Policies and ISO/IEC 17788 Cloud Computing Reference Architecture and leverages elasticity, scalability and sovereign control.

Detailed Recommendations

- Separate compute, storage and presentation layers to allow independent scaling, maintainability and modular upgrades.
- Use containerisation technologies (e.g., Docker, Kubernetes) to ensure portability across approved government hosting environments.
- Maintain geo-redundant backups within Mauritius, meeting ISO 22301 Business Continuity Management requirements.
- Ensure strict data-sovereignty compliance:

– All systems that process, store, or transmit personal data including identity, citizen, health, financial, judicial, immigration, business-registration or any data linked to an identifiable individual must be hosted exclusively within Mauritius on the Government Cloud or other MITCI-approved in-country sovereign infrastructure.

– Systems containing only public, non-personal and non-identifiable information may be considered for offshore hosting only where no personal data of any form is collected, logged, or generated, including metadata or behavioural analytics.

– Systems collecting mixed, inferred, or uncertain categories of data must be treated as handling personal data and therefore hosted in Mauritius.

This requirement applies primarily to authoritative government information systems that store or manage official records, regulated personal data, or mission-critical datasets. Enterprise productivity and collaboration tools adopted through centrally approved Government frameworks shall be subject to separate risk-based assessment and approval mechanisms.

Expected Outcome

Government services achieve agility, continuity and scalability while ensuring that any system with personal data remains fully under Mauritian jurisdiction and only purely public-information systems may be hosted offshore under strict data-classification controls.

3.11 Mobile-Centric

Recommendation

Mobile-centric design is supported by UN EGDI and WCAG 2.1 guaranteeing accessible and inclusive service delivery on all devices.

Detailed Recommendations

- Apply responsive layouts and ISO 9241-210 Human-Centred Design principles.
- Test on varied devices and bandwidths.
- Integrate MauPass for citizen authentication.
- Optimise assets for low-bandwidth environments.

Expected Outcome

Citizens enjoy consistent and inclusive digital experiences, increasing adoption of online services.

3.12 Secure-by-Design

Recommendation

Security-by-Design derived from NIST SP 800-160 and ISO 27001/27002 integrates protection throughout the system lifecycle.

Detailed Recommendations

- Conduct threat modelling and security assessments early in the design phase to identify attack surfaces, misuse cases and high-risk components.

- Implement encryption, access control and audit logging in alignment with MITCI IT Security Guidelines and national cybersecurity policies.
- Apply Zero-Trust Architecture principles from NIST SP 800-207, ensuring continuous authentication, least privilege and strict segmentation.
- Enable continuous vulnerability scanning and security monitoring, including automated patching, intrusion detection and log correlation across infrastructure components.

Expected Outcome

Systems maintain confidentiality, integrity and availability, strengthening citizen trust and national cyber resilience.

3.13 Zero Redundancy

Recommendation

Zero Redundancy is based on The Open Group's TOGAF Architecture Framework, one of the world's leading enterprise architecture standards requires government to eliminate duplication by ensuring that no parallel systems are built or maintained for the same business function. TOGAF, used internationally across governments and large enterprises, emphasises reuse of existing capabilities, consolidation of overlapping systems and strong architectural governance so that the digital environment remains coherent, cost-effective and interoperable.

Detailed Recommendations

- Perform a Reuse Assessment at project inception to identify whether an existing government platform, module, or component already provides the required capability. The assessment must review shared national platforms (e.g., MauPass, Mobile ID, MoKloud, Korek, InfoHighway, Digital Payment Gateway, MoRendezVous, SMS Gateway, etc) and confirm that duplication is avoided.
- Prioritise integration and extension of existing national systems before considering any new development, consistent with TOGAF's principles of Architecture Building Blocks (ABBs) and Solution Building Blocks (SBBs).

- Ensure new proposals align with existing standards, patterns and reusable components.
- Seek approval for any deviations only where strong justification exists such as legal constraints, technology gaps, or unavoidable functional requirements. Any approved deviation must include a roadmap to realign with national architecture in the future.

Expected Outcome

Investments are rationalised, reducing maintenance overhead and fragmentation across government.

3.14 Single Source of Truth

Recommendation

The Single Source of Truth (SSOT) principle endorsed by the OECD Data Governance Framework ensures that each core dataset within government is maintained in one authoritative system, eliminating inconsistencies and duplication. All consuming systems must rely on this authoritative source to guarantee accuracy, trust and interoperability across ministries.

Detailed Recommendations

- Identify and formalise authoritative systems for each major dataset (e.g., CPD/CDH for citizen identity and civil data; CBRD for business registration; Immigration for border and permit data).
- Access data from authoritative systems exclusively through InfoHighway or APIs, ensuring controlled, secure and auditable data exchange.
- Synchronise updates using event-driven mechanisms, enabling services to receive changes in real time and ensuring all systems reflect the latest, validated data.

Expected Outcome

Government decisions rely on accurate, consistent and verifiable data.

3.15 Reuse Before Buy

Recommendation

Reuse Before Buy is aligned with EU EIF Principle 7 ("Reuse and Share") and the World Bank GovTech Maturity Index efficiency dimension and requires ministries to leverage existing national platforms, components and services before considering new procurement or development. This promotes interoperability, reduces cost, accelerates delivery and ensures architectural consistency across government.

Detailed Recommendations

- Evaluate existing national platforms during project planning, including MauPass, Mobile ID, MoKloud, Korek, InfoHighway, Digital Payment Gateway, MoRendezVous, SMS Gateway and other shared components within the Government Stack.
- Reuse proven components wherever technically feasible, including APIs, modules, templates, shared UI/UX patterns, integration libraries and micro-front-end components already developed for other services.
- Seek authorisation for new procurement or development only when reuse is technically impossible, legally restricted, or operationally inadequate and such cases must be supported by clear justifications.

Expected Outcome

Public funds are optimised and architectural consistency is maintained across programmes.

3.16 Integrated National Stack

Recommendation

Integration with national platforms ensures a unified citizen experience.

Detailed Recommendations

- Connect systems with MauPass, Mobile ID, MoKloud, Korek, InfoHighway, Digital Payment Gateway and DIVA.
- Follow platform-specific SDK and API guidelines.
- Participate in joint interoperability testing.

Expected Outcome

Citizens interact through a seamless ecosystem of trusted government services.

3.17 Data Sharing by Default

Recommendation

Data Sharing by Default, inspired by the OECD Recommendation on Enhancing Access to and Sharing of Data (2021), encourages authorised exchange through governed interfaces.

Detailed Recommendations

- Expose and consume datasets via InfoHighway.
- Tag datasets with sensitivity levels and apply appropriate controls.
- Record metadata and usage audits for each exchange.

Expected Outcome

Data becomes a strategic asset that supports evidence-based policy and cross-agency efficiency.

3.18 Micro Front-End by Design

Recommendation

Micro front-end architecture referenced by the UK Government Digital Service Standard supports independent development and deployment of service modules.

Detailed Recommendations

- Design service interfaces as independent modules that can operate on their own but also integrate into shared platforms such as the Government Super App
- Follow DSF UX and accessibility patterns.
- Use shared libraries of the Super App.

Expected Outcome

Interfaces remain consistent while allowing agencies to innovate and release updates independently.

3.19 Event-Driven Architecture

Recommendation

Government systems should adopt an API-first and event-driven architecture to enable secure integration, orchestration, and interoperability across the national digital ecosystem. This approach supports automation, system-to-system interaction, and emerging capabilities such as AI-assisted service orchestration.

Detailed Recommendations

- Expose secure, documented machine-readable APIs for system integration.
- Where appropriate, support event-driven communication to enable asynchronous interactions and real-time processing.
- Ensure system interactions maintain traceability, auditability, and explainability, particularly where automated or AI-assisted decisions are involved.

Expected Outcome

Government systems become modular, interoperable, and capable of supporting advanced orchestration and automation across the digital ecosystem.

3.20 Zero-Trust Architecture

Recommendation

Zero-Trust Architecture defined by NIST SP 800-207 treats all connections as untrusted until verified.

Detailed Recommendations

- Enforce continuous authentication and authorisation.
- Segment networks and apply least-privilege principles.
- Monitor behaviour to detect anomalous access.

Expected Outcome

Systems achieve higher security resilience against internal and external threats.

3.21 Defense-in-Depth

Recommendation

- Layered defence endorsed by ISO 27005 Risk Management and ITU-T X.1205 combines multiple security controls to reduce single points of failure.
- Detailed Recommendations
- Deploy controls across network, application and data layers.
- Use independent monitoring and intrusion detection systems.
- Validate controls through regular penetration testing.

Expected Outcome

Breaches are contained early and service continuity is maintained under attack.

3.22 Privacy-by-Design

Recommendation

Privacy-by-Design codified in the EU GDPR Article 25 and ISO 31700 Consumer Privacy by Design integrates data-protection controls from inception.

Detailed Recommendations

- Personal data collection must be strictly limited to what is necessary in relation to the explicitly stated purpose(s).
- Ensuring consent is freely given, specific and easily withdrawable. This must be coupled with robust retention and disposal policies.
- Conduct Data Protection Impact Assessments (DPIAs) for high-risk processing operations.

Expected Outcome

Citizens' personal data remains protected by default and by design, rather than by exception. This proactive approach mitigates the risk of data breaches and reinforces public trust in digital government infrastructure.

3.23 Sovereignty-by-Design

Recommendation

Sovereignty-by-Design reflecting OECD Data Governance Principles ensures critical data and services remain under national jurisdiction.

Detailed Recommendations

- Host sensitive data within Government Cloud or approved sovereign facilities.
- Maintain contracts that preserve ownership and jurisdiction.
- Implement geographically redundant in-country backups.

Expected Outcome

National autonomy over information assets is preserved and legal risks from foreign jurisdiction are avoided.

3.24 Business Continuity-by-Design

Recommendation

Continuity-by-Design guided by ISO 22301 and ISO 27031 builds redundancy and recovery into core architecture.

Detailed Recommendations

- Implement active-active or active-standby set-ups for critical systems.
- Test fail-over and restore procedures regularly.
- Document Recovery Time (RTO) and Recovery Point (RPO) objectives.

Expected Outcome

Essential services remain available even during disruption, preserving public confidence and operational continuity.

3.25 Continuous Monitoring

Recommendation

Continuous Monitoring aligned with NIST SP 800-137 provides real-time visibility into performance and security status.

Detailed Recommendations

- Centralise logs and metrics from applications and infrastructure.
- Define thresholds and automated alerts for anomalies.
- Integrate dashboards with national SLA and cybersecurity centres.

Expected Outcome

Agencies detect and respond to issues promptly, reducing downtime and improving service quality.

3.26 Microservice-Oriented Architecture

Recommendation

Microservice architecture promoted by The Open Group and Cloud Native Computing Foundation (CNCF) structures applications as independent services with clear contracts.

Detailed Recommendations

- Structure systems into logical service components aligned with business functions.
- Expose well-documented service interfaces (e.g., APIs) to enable integration and reuse.
- Ensure service components can be updated or replaced without disrupting the entire system.
- Maintain version control and documentation for service interfaces to support governance and interoperability.

Expected Outcome

Applications become scalable and resilient, allowing agencies to innovate without impacting core operations.

3.27 Green-by-Design

Recommendation

Green-by-Design supported by ITU-T L.1470 and ISO 50001 Energy Management minimises environmental impact of digital infrastructure.

Detailed Recommendations

- Optimise server utilisation and energy efficiency.
- Employ virtualisation and resource sharing to reduce hardware footprint.
- Measure and report ICT carbon emissions.

Expected Outcome

Government ICT operations contribute to sustainability targets and lower long-term operating costs.

3.28 Agility and Sandbox-Driven Innovation

Recommendation

Agile and sandbox approaches reflected in World Bank GovTech Innovation Framework and OECD Innovation Playbook enable safe experimentation and incremental improvement.

Detailed Recommendations

- Pilot new technologies in controlled environments before scale-up.
- Apply iterative development with continuous user feedback.
- Capture and share lessons learned across ministries.

Expected Outcome

Innovation becomes systematic and low-risk, accelerating adoption of emerging technologies while maintaining governance and safety.

3.29 Summary

#	Principle	Intent / Short Description
1	**Modular by Design**	Systems shall be developed as discrete, reusable components or services.
2	**API-First**	All systems must expose and consume services through APIs.
3	**Interoperable**	Systems must connect seamlessly through common standards and protocols.
4	**Cloud-Ready**	Systems must be deployable on the Government Cloud or approved sovereign cloud.

#	Principle	Intent / Short Description
5	**Mobile-Centric**	Services shall be optimised for mobile access and responsiveness.
6	**Secure-by-Design**	Security controls must be embedded at every layer of the system.
7	**Zero Redundancy**	Duplicate or overlapping platforms shall not be created.
8	**Single Source of Truth**	Data shall originate from authoritative systems and be reused through InfoHighway / CDH.
9	**Reuse Before Buy**	Existing national platforms must be reused before new development.
10	**Integrated National Stack**	All systems must integrate with national platforms such as MauPass, MoKloud, Korek, etc.
11	**Data Sharing by Default**	Data shall be shared securely via InfoHighway and CDH.
12	**Micro Front-End by Design**	Front-end modules must be composable and reusable in the Government Super App.
13	**Event Architecture**	Systems must expose secure, documented APIs and, where appropriate, event interfaces to enable integration, automation, and orchestration across the government digital ecosystem.
14	**Zero-Trust Architecture**	Every request must be authenticated, authorised and logged.
15	**Defense-in-Depth**	Implement multiple security layers across network, application and data.

#	Principle	Intent / Short Description
16	**Privacy-by-Design**	Privacy protections shall be embedded from inception of system design.
17	**Sovereignty-by-Design**	All critical data shall reside within national or approved sovereign infrastructure.
18	**Business Continuity-by-Design**	Systems must include redundancy, fail-over and disaster-recovery capabilities.
19	**Continuous Monitoring**	Real-time performance and security monitoring must be implemented.
20	**Microservice-Oriented Architecture**	Build systems as independent, reusable services communicating via APIs.
21	**Green-by-Design**	Design infrastructure and software for energy efficiency and minimal footprint.
22	**Agility and Sandbox-Driven Innovation**	Test and validate new technologies in controlled sandboxes before scale-up.

4. CORE POLICY MANDATES

4.1 Overview

The success of digital government relies on adherence to a common set of core policies that define how services are accessed, how data is handled, how systems interact and how risks are managed.

This chapter outlines the policy areas that ministries and departments must comply with when implementing digital services. These policies ensure that every digital initiative contributes to a coherent, secure and citizen-centric ecosystem.

Each policy described below is either already in force or under finalisation through appropriate government channels. The DSF enforces them.

4.2 Digital Identity Policy

Objective:

Ensure that every digital service uses strong identity verification to prevent fraud and enable secure personalisation.

Unique Identifiers:

- Citizens: The National Identity Number (NIN), issued under the Civil Status Division and printed on National Identity Card is the authoritative unique identifier for citizens of Mauritius.
- Foreigners: For foreign residents or visitors, the Passport Number (and where applicable, residence/permit number) shall be used as the primary identifier.
- Businesses: The Business Registration Number (BRN) remains the authoritative identifier for companies and legal entities.

Mandates:

- Ministries must not create or maintain parallel identifiers. All identifiers must be validated against authoritative sources (CPD/CDH for citizens, Immigration databases for foreigners, CBRD for businesses).
- All citizen-facing digital services must integrate with MauPass for authentication, Physical ID and Mobile ID for Identity Proofing.
- Ministries may not use usernames/passwords of citizens outside MauPass or Corporate Pass for Businesses.

***Purpose**:* Protect citizen access and ensure legal validity of digital actions.

4.3 Authentication and Access Management

Objective:

All digital services must enforce secure, role-based access for both citizens in their personal capacity and government staff acting on behalf of their organisations.

Requirements:

- Citizen Access: Citizens must authenticate through MauPass or Mobile ID. Two-Factor Authentication (2FA) is mandatory for high-risk transactions and access to sensitive data.
- Staff Access: Internal users must authenticate using approved Single Sign-On (SSO). Access rights must reflect their official role within the service workflow.
- Access Logging: All access events by both citizens and staff must be recorded, encrypted and auditable.

Benefit: Clear separation of personal and organisational roles, combined with strong authentication, reduces fraud, prevents insider threats and ensures accountability.

4.4 Data Governance and Sharing Policy

Objective:

Ensure that government data is treated as a strategic asset and shared efficiently.

Mandates:

- Agencies must use authoritative sources (e.g., CPD, CDH for citizen data).
- Civil Data from the Physical ID and Mobile ID shall be read as per the card usage regulations of the National Identity Card Act.
- Data sharing must be through via InfoHighway and an API-first approach by default.
- Agencies may keep only a minimal immutable "reference snapshot" only of the data from an authoritative source necessary for their transactions and service delivery for audit and legal traceability, while minimising duplication of source data.
- All databases and data exchange must follow approved national metadata and data quality standards.

***Result**:* Reduces duplication, improves service accuracy and supports real-time integration.

4.5 Privacy and Data Protection

Objective:

Safeguard the fundamental rights of privacy of users.

Mandates:

- All digital services must comply with the Data Protection Act. Consent management, data minimisation and user rights (access, rectification, erasure, restriction, objection) must be respected.

***Governance**:* MITCI has authority to review digital service deployments for compliance.

4.6 Cybersecurity and Risk Management

Objective:

Protect government digital infrastructure and user trust against cyber threats.

Mandates:

- All systems must comply with IT Security requirements issued by MITCI. Ministries are responsible for implementing and enforcing these requirements and overseeing compliance to ensure cybersecurity resilience. Suppliers must demonstrate compliance through security documentation and adherence to required security standards (e.g., ISO/IEC 27001).
- An IT Contingency Plan (ITCP) based on international best practices should be elaborated by the provider of the solution. The ITCP should address the risks areas following relevant risk assessments and develop strategies to recover from disruptions. The ITCP should be finalised in conformity with relevant stakeholders comprising the User Representatives, CIB, ITSU, CISD, GOC Teams. Additional details may be provided at implementation stage of the solution.

***Responsibility**:* Ministries remain accountable for securing their services end-to-end.

4.7 API and Interoperability Standards

Objective:

Enable seamless data and service integration across government.

Mandates:

- All digital services must expose and consume APIs in line with interoperability standards defined by MITCI/DMO.
- RESTful APIs with common request/response formats (JSON or XML) are the default; other protocols may be used where justified.

- All APIs whether public, inter-agency, or internal must be documented and be registered with the MITCI/DMO.
- Public APIs must follow approved versioning rules and maintain backward compatibility to avoid disruption of consuming services.

***Benefit**:* Eliminates silos and accelerates inter-agency workflows.

4.8 Document Management and Digital Signing

Objective:

Ensure that documents issued or submitted through digital services are legally recognised and verifiable.

Mandates:

- Official documents wherever applicable (e.g., certificates, permits, licenses) must include a digital signature generated using the official organization digital certificate of the agency.
- The official digital document must include a verifiable 2D barcode (such as a QR code), to enable both offline and online verification in addition to the digital signature.
- Citizens must be able to access and share official digital documents through the national digital document platform (MoKloud or revamped SuperApp KOREK)

***Legal Standing**:* Digitally signed documents are equivalent to physical originals under Mauritian law.

4.9 Cloud, Hosting and Infrastructure Policy

Objective:

Standardise hosting practices to ensure resilience, cost-effectiveness and compliance.

Mandates:

- All new services must be hosted on the Government Cloud, or on an infrastructure approved by the MITCI.
- Hosting providers must be compliant with local data residency requirements, ISO 27001 and disaster recovery standards.
- Hosting arrangements should provide for uptime of 99.5% or higher.

***Efficiency**:* Reduces hosting duplication and improves energy/resource use.

4.10 Digital Payment and Financial Integration

Objective:

Facilitate secure, cashless transactions between government and users.

Mandates:

- All services involving payment must integrate with approved payment gateway.

***Citizen Benefit**:* Ensures transparent and traceable transactions.

4.11 Citizen Engagement and Transparency

Objective:

Improve transparency and two-way engagement with citizens.

Mandates:

- All services must include status tracking, acknowledgment of requests and expected turnaround times.
- Feedback and complaint channels must be built into portals or apps.

***Public Trust**:* Builds confidence in service responsiveness and fairness.

4.12 Service Monitoring and Performance

Objective:

Track service quality and inform continuous improvement.

Mandates:

- All services must include performance dashboards for internal and public use.
- Key metrics: uptime, response time, user satisfaction, usage volume.
- Ministries must submit regular Digital Service Performance Reports to the MITCI.

***Accountability**:* Creates a culture of data-driven service excellence.

4.13 Procurement and Vendor Compliance

Objective:

Ensure vendors and projects adhere to national digital policies.

Mandates:

- All ICT RFPs to include DSF clauses covering identity, APIs, hosting, security, privacy, digital signing and reuse of national platforms wherever applicable.
- Evaluation criteria can consider wherever applicable experience with MauPass, Mobile ID, InfoHighway, etc
- Suppliers must show DSF compliance evidence.
- Contracts must guarantee government ownership of all source code for all custom-developed software, software customization, data generated, processed or stored and documentation, prohibiting any form of vendor lock-in.
- Non-compliance may constitute a breach of contract, enabling rejection of deliverables, payment withholding, penalties and vendor debarment.

***Protection**:* Prevents vendor lock-in and ensures long-term system sustainability.

4.14 Responsible AI and Emerging Technologies Policy

Objective:

Ensure the ethical, transparent and accountable use of Artificial Intelligence (AI) and other emerging technologies in government services.

Mandates:

- All AI systems must undergo an Algorithmic Impact Assessment (AIA) prior to deployment.
- AI-driven decisions affecting rights or entitlements must remain explainable, auditable and contestable.
- Ministries must not deploy unverified or "black box" algorithms without oversight.
- Use of national shared AI platforms such as DIVA Digital Assistant is encouraged to avoid duplication and ensure quality.
- Any pilot of emerging technologies (e.g., blockchain, IoT, biometrics) must include a risk assessment and adhere to applicable guidelines.

Benefit: Builds citizen trust in digital services, prevents bias or misuse and ensures government remains accountable while adopting innovation.

4.15 Scheduling and Citizen Interaction Policy

Objective:

Provide citizens and businesses with a unified, transparent and fair system for managing appointments, queues and service interactions across ministries.

Mandates:

- All government entities must use the Mo RendezVous Scheduling System or other approved shared platforms.
- Appointment data must be linked with MauPass authentication to ensure identity-verified bookings.
- Citizens must be able to book, reschedule and cancel appointments through multiple channels (web, mobile, kiosks, tablets).
- Status tracking (e.g., "awaiting appointment", "in progress") must be provided to citizens in real time.
- Ministries are prohibited from building duplicate scheduling systems.

Benefit: Creates consistency across ministries, reduces waiting times, increases efficiency and gives citizens a seamless interaction experience.

4.16 Sustainability and Green ICT Policy

Objective:

Embed environmental sustainability into the design, procurement and operation of all government digital services.

Mandates:

- All ICT procurements must include lifecycle energy efficiency requirements. In addition, projects must include e-waste reduction and recycling, ICT refurbishment and reuse and compliance with green procurement standards.
- Ministries must prioritise use of the Government Cloud / GOC to consolidate infrastructure and reduce energy waste.

- Digital services must avoid duplication of platforms to minimise environmental and fiscal costs.
- Green coding practices and server optimisation must be applied for all new systems.

Benefit: Reduces carbon footprint, ensures fiscal responsibility and positions Mauritius as a leader in sustainable digital government.

4.17 Data Sovereignty and Jurisdiction Policy

Objective:

Protect national sovereignty and ensure compliance with Mauritian law by requiring that sensitive data remains within the country's jurisdiction.

Mandates:

- All critical citizen and government data must be hosted in Mauritius on Government Cloud, GOC, or other MITCI-approved sovereign infrastructure.
- Exporting or hosting data outside Mauritius requires a formal approval supported by required justifications.
- Data residency clauses must be included in ICT procurement and service contracts.

Benefit: Safeguards national security, ensures compliance with the Data Protection Act 2017 and reduces dependency on foreign jurisdictions.

4.18 Open Data and Innovation Policy

Objective:

Promote transparency, accountability and innovation by mandating the proactive release of non-sensitive government data.

Mandates:

- All ministries must publish non-sensitive datasets on the National Open Data Portal in machine-readable formats (CSV, JSON, XML).
- Where feasible, APIs must be exposed to allow reuse by businesses, researchers and civil society.
- Agencies must apply data classification to clearly mark which datasets are open, restricted, or internal.
- Ministries must publish metadata and update datasets regularly to maintain trust and utility.

Benefit: Stimulates civic innovation, supports evidence-based policymaking and strengthens public trust through transparency.

4.19 Citizen-Centric and Inclusive Service Design Policy

Objective:

Ensure that all government digital services are designed, delivered, and continuously improved based on real user needs, measurable service outcomes, and equitable access for all segments of society.

Mandates:

- Line Ministries are the designated Service Owners and remain accountable for service outcomes, adoption, usability, and user experience.
- Citizen-facing services must be designed around user journeys and life events, rather than internal institutional structures.
- Major citizen-facing services must undergo user research and usability validation.

- Measurable service performance indicators (e.g., completion rates, processing time, user satisfaction) shall be defined for high-impact services.
- All services must comply with WCAG 2.1 accessibility standards.
- Interfaces must mandatorily support English and where feasible, French and Kreol.
- Alternative access channels (e.g., assisted digital at Citizen Support Centres) must be incorporated to prevent exclusion.
- Continuous feedback mechanisms must be embedded to enable iterative improvement.

Benefit: Government digital services shall be designed around user needs first, with accessibility and inclusion embedded by design.

4.20 Change Management and Capacity Policy

Objective:

Ensure successful adoption of digital services by preparing both public sector staff and citizens for new systems and processes.

Mandates:

- Every digital service project must include a Change Management Plan covering training, awareness and communication activities for staff and citizen digital literacy initiatives. In line with the Blueprint's 'Digital Skills for All', ministries must embed outreach and assisted-digital programmes to ensure that vulnerable and digitally excluded citizens can confidently use online services.
- Ministries must designate Digital Focal Points to oversee DSF compliance and coordinate with MITCI. Each Ministry must designate a Digital Focal Point responsible for DSF compliance.
- In addition, every digital service must have a Service Owner on the business side (not IT) accountable for lifecycle management, citizen adoption and continuous

improvement. The Service Owner ensures DSF compliance is tied to business outcomes.

- Staff must be provided with role-specific training before system rollout, with refresher sessions as systems evolve.
- Ministries must regularly measure user adoption and satisfaction, adjusting outreach accordingly.

Benefit: Improves adoption rates, reduces resistance and builds a culture of continuous improvement in digital government.

4.21 Summary Table – Mandatory DSF Policies

#	Policy Area	Enforcement / Mandates
1	**Digital Identity Policy**	All services must authenticate via MauPass / Mobile ID; NIN (citizens), Passport (foreigners), BRN (businesses); no parallel logins permitted.
2	**Authentication & Access Management**	2FA for high-risk transactions; staff access via SSO; all access logged and auditable.
3	**Data Governance & Sharing Policy**	InfoHighway is mandatory; no duplication of citizen data; only authoritative sources may be used (CPD/CDH, Immigration, CBRD).
4	**Privacy & Data Protection Policy**	DPIA required; consent must be clear, informed and revocable; encryption at rest/in transit; compliance with DPA 2017.
5	**Cybersecurity & Risk Management**	Mandatory IT security audit for complex systems, penetration testing, patching, DR plans and audit trails.

#	Policy Area	Enforcement / Mandates
6	**API & Interoperability Standards**	RESTful APIs with OpenAPI specs; APIs must be registered with the MITCI/DMO; versioning and backward compatibility enforced.
7	**Document Management & Digital Signing**	All official documents must be digitally signed; QR included for verification; citizens must access/share via MoKloud or revamped platform Korek.
8	**Cloud, Hosting & Infrastructure Policy**	All services hosted on GovCloud / GOC / approved sovereign infra; 99.5% uptime; ISO 27001 compliance.
9	**Digital Payment & Financial Integration**	All payment services must use the approved Payment Gateway.
10	**Citizen Engagement & Transparency**	All services must provide status tracking, feedback and complaint channels.
11	**Service Monitoring & Performance**	Services must provide dashboards with uptime, usage, satisfaction metrics; ministries must submit regular reports to MITCI.
12	**Procurement & Vendor Compliance**	All ICT RFPs must include DSF clauses; vendors assessed on DSF readiness; government retains source code for custom software and customisation and data ownership.
13	**Responsible AI & Emerging Tech Policy**	AI systems require Algorithmic Impact Assessment; decisions must be explainable and auditable; pilots of new tech require MITCI approval.
14	**Scheduling & Citizen Interaction Policy**	All appointments must use Mo RendezVous Scheduling System; linked to MauPass; duplicate systems prohibited.

#	Policy Area	Enforcement / Mandates
15	**Sustainability & Green ICT Policy**	ICT procurement must include energy efficiency; GovCloud preferred; green coding and carbon reporting required.
16	**Data Sovereignty & Jurisdiction Policy**	All critical data must remain in Mauritius; offshore hosting only with MITCI-approved waiver.
17	**Open Data & Innovation Policy**	Non-sensitive datasets must be published on the Open Data Portal; APIs encouraged; datasets updated regularly.
18	**Digital Inclusion & Assisted Access Policy**	Assisted-digital channels (kiosks, call centres) required; digital literacy campaigns included in projects; services optimised for low-bandwidth/mobile.
19	**Change Management & Capacity Policy**	Every project must include a Change Management Plan; Digital Focal Points appointed; staff trained before rollout.

5. DIGITAL SERVICE DESIGN STANDARDS

5.1 Purpose of Design Standards

This chapter defines the mandatory design principles and technical standards that must be followed by all ministries and departments when developing or revamping digital services. These standards ensure that services:

- Are intuitive and accessible to all users,
- Work consistently across devices,
- Comply with identity, privacy and security policies,
- Allow easy integration with national platforms.

Design is not just about aesthetic. It is also about functionality, inclusiveness and trust.

#	Digital Service Design Standard	Linked Core Principle(s)	Linked Architecture Principle(s)
1.	**Accessibility Standards**	6 Accessibility & Inclusivity 7 Interoperability & Reusability	5 Mobile-Centric
2.	**Mobile-First & Responsive**	2 Mobile-First & Super App Enabled 7 Interoperability & Reusability	5 Mobile-Centric 12 Micro Front-End by Design
3.	**Service Status & Tracking**	9 Resilience & Security	19 Continuous Monitoring

5.2 Accessibility Standards (WCAG Compliance)

All digital services must comply with Web Content Accessibility Guidelines (WCAG) 2.1, Level AA or higher.

Key Features:

- Alternative text for images
- Screen reader compatibility
- Keyboard navigation for all functions
- Sufficient contrast ratios
- Text size adjustment

***Digital Inclusion**:* No one is left behind, whether visually impaired, elderly, or with limited digital literacy.

5.3 Mobile-First and Responsive Design

Citizen-facing digital services must adopt a mobile-first approach, ensuring responsive design across common device types.

Requirements:

- Fully usable on devices with screen widths of 360 CSS pixels and above..
- Optimised for 4G performance, but must remain functional and usable on 3G networks.
- Touch-friendly controls with adequate spacing.

Avoid intrusive pop-ups, oversized media, and heavy scripts.

***Reach**:* The mobile phone is the default device for digital inclusion in Mauritius.

5.4 Service Status and Tracking

All transactional services must include real-time status tracking.

Mandates:

- Show user where they are in the process (e.g., application submitted → under review → approved).
- Provide expected response time.
- Notify via email/SMS at key stages.

***Transparency**:* Builds user confidence and reduces frustration.

5.5 Summary: Design Checklist (Mandatory)

Area	Requirement
Accessibility Standards	WCAG 2.1 Level AA compliance
Mobile-First & Responsive Design	Responsive, fast, touch-optimised
Service Status & Tracking	Multi-channel notifications (SMS/email)

6. IMPLEMENTATION AND COMPLIANCE MECHANISMS

6.1 Overview

To ensure consistent adherence to the DSF, this chapter outlines the institutional, operational and technical mechanisms through which ministries and departments will:

- Implement digital services in alignment with DSF requirements,
- Undergo compliance review and approval,
- Receive capacity support and technical guidance,
- Be held accountable for non-compliance.

DSF is not optional. It is enforceable through controls, approvals, reporting and audits.

6.2 Roles and Responsibilities

A Ministries, Departments and Steering Committee

- Ensure all digital initiatives go through DSF alignment.
- Seek assistance regarding DSF from MITCI and obtain clearance from relevant bodies.
- Maintain logs of changes, updates and security assessments.

Project ownership remains with the Ministries and Departments.

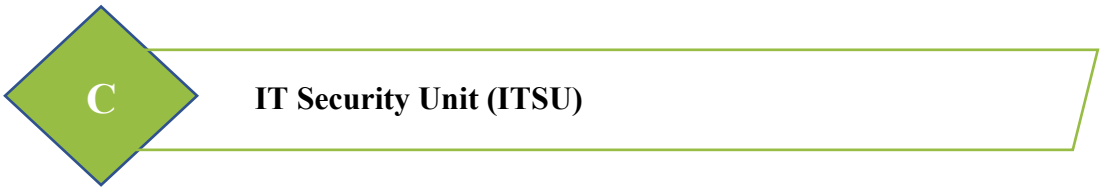
B Central Informatics Bureau (CIB)

CIB provides technical advisory and project support services to Ministries and Departments.

- Prepare or assist in preparing technical specifications aligned with the DSF
- Provide technical advice during project implementation

- Provide project management support services where mandated

CIB's involvement does not transfer project ownership from the Line Ministry.



- Provide IT security Project Management Services
- Prepare technical specifications for IT security projects aligned with DSF
- ~~Assist~~ Manage the conduct of IT Security Audit exercise.

- Ensure compliance with Data Protection Act.
- Review and provide advisory options on Data Protection Impact Assessments (DPIAs).

- Provide policy guidance and interpretation of DSF
- Review cross-ministry digital initiatives
- Grant waivers where justified

  Monitor national-level compliance
- Oversee DSF rollout across government.

F **Inter-Ministerial Committee for Digital Transformation**

- Provide top-level political support and policy direction.
- Approve strategic updates to the DSF itself.

6.3 Compliance Process

All ministries must ensure that any digital service or project complies with the Digital Service Framework (DSF) while compliance shall be proportionate and based on system relevance.

Compliance is assessed as part of the standard project lifecycle.

#	Stage	Step	Responsible Authority	Required Deliverables
1	**Funding & Initiation**	Ministry submits project request to the Ministry of Finance and notifies MITCI of planned service.	Ministry of Finance + MITCI (notification)	Project Brief, Functional Scope, Initial Budget Estimate
2	**Procurement**	DSF requirements must be reflected in tender documents so suppliers are contractually bound to deliver compliant solutions.	Line Ministry + MITCI (advisory role)	RFP with DSF clauses
3	**Implementation & Testing**	Supplier develops solution. DSF compliance is verified as part of QAT, UAT, OAT and security testing.	Line Ministry + MITCI oversight	Test Plans, Test Reports, DPIA, Security Assurance Document
4	**Deployment & Reporting**	Service goes live only after successful completion of	Line Ministry (with MITCI confirmation)	Go-Live Report, Operational Acceptance

#	Stage	Step	Responsible Authority	Required Deliverables
		testing, including DSF compliance checks.		Certificate, Post-Deployment Metrics

Note:

- DSF requirements must be written into procurement documents; otherwise, suppliers cannot be held accountable.
- DSF compliance is verified within normal testing; no separate parallel process is required. Supplier develops solution. DSF compliance is verified as part of QAT, UAT, OAT and security testing. All suppliers must explicitly demonstrate DSF compliance as part of their Quality Assurance and Testing (QAT) deliverables. Each DSF principle, policy and standard shall be mapped to test cases and suppliers shall provide verifiable evidence (e.g., API call logs, accessibility reports, signed document samples, uptime/load test results, security audit findings) in a DSF Compliance Checklist. This checklist, completed and submitted with the QAT report, will serve as the official proof of compliance. No system shall proceed to deployment or operational acceptance without a validated DSF Compliance Checklist signed off.
- MITCI retains oversight to ensure alignment with national standards.

6.4 Pre-Built Toolkits and Templates

To support rapid and compliant implementation, the government will provide:

- Technical Specifications with clauses and checklists for compliance to DSF,
- Data Protection Impact Assessment templates for faster approval,
- Design checklists for UI/UX compliance,
- API to access shared services like InfoHighway, eSign service, etc
- Sample code and integration scripts for MauPass, InfoHighway, MoKloud and Korek.

***Outcome**:* Speed without sacrificing compliance.

6.5 Technical Reviews and Audits

Every major system must go through the following testing and audits before go-live:

- UAT and OAT
- IT Security Audit
- ITCP
- DPIA Review

In addition:

- Annual revalidation for systems processing personal or financial data.

Audit Trail: All reports are stored centrally and referenced in procurement reviews.

6.6 Exceptions and Waivers

A Ministry may request temporary exemption from any DSF requirement due to:

- Legacy system constraints,
- Urgent national priorities,
- Legal or technical conflicts.

Such waivers:

- Must be endorsed by the Steering Committee.
- Are valid for a limited duration
- Must include a roadmap for eventual compliance.

Note*:* Repeated non-compliance is not encouraged.

6.7 Training and Capacity Building

To ensure adoption across all levels of government, the MITCI will offer:

- Regular awareness to Line Ministries

- Shadowing and hand-holding during implementation through the technical units
- Onboarding sessions for new suppliers or consultants,
- DSF documentation on Ministry portal.

Capacity First: Digital transformation requires human readiness, not just systems.

6.8 Monitoring, Reporting and Performance Metrics

All digital services must comply with the DSF and demonstrate performance against defined operational KPIs. Monitoring and reporting are required post-deployment to ensure transparency, accountability and audit readiness.

Core Metrics

- Service availability (uptime, response times, error rates)
- Usage (number of users, transactions, adoption trends)
- Security and privacy (incidents, breaches, attempted attacks)
- Citizen feedback (satisfaction levels, complaints, issue resolution)
- DSF compliance score (based on the official checklist)

Reporting Requirements

- Internal Auditors: Ministries must maintain and share performance records for internal audit reviews.
- External Auditors / Compliance Teams: Reports must be made available for independent verification and assurance.
- MITCI Oversight: Consolidated performance reports are submitted to MITCI for national-level monitoring.

Audit & Transparency

- Reports must be prepared in formats suitable for internal and external audit.
- Performance data may be published in national dashboards and oversight reports to ensure transparency to citizens and Parliament.

- Evidence of DSF compliance must be retained and presented during audits and reviews.

Note:

- UAT and OAT remain pre-go-live validation steps and are not part of ongoing reporting.
- Post-deployment monitoring ensures that services continue to operate securely, reliably and in alignment with DSF standards.

***Transparency**:* Performance data feeds into national dashboards and oversight reports.

6.9 Integration into Budgeting and Procurement

DSF considerations must be embedded at the time of ICT budget requests and throughout the procurement cycle.

- Ministries must explicitly address DSF compliance when preparing annual ICT budget requests.
- Projects that do not align with DSF should not be recommended for inclusion in ICT project pipelines.
- Tender specifications and evaluation criteria must exclude or downgrade bids that fail to meet DSF requirements.

***Value-for-Money**:* Integrating DSF early in budgeting and procurement ensures proper design, reduces costly rework and prevents vendor lock-in.

6.10 DSF Change Management and Versioning

The DSF will evolve through:

- Annual review cycles conducted by the MITCI,
- Public consultation and expert inputs,
- Updates to toolkits, policies and templates,
- Clear version control (e.g., DSF v1.0, v2.0).

- The DSF version in force will be the one active at the time of contract signature with a supplier.

Ministries will be notified of updates.

***Living Framework**:* The DSF adapts as the digital ecosystem matures.

7. MONITORING, AUDIT and ENFORCEMENT MECHANISMS

7.1 Overview

For the Digital Service Framework to be effective, it must be actively monitored, regularly audited and firmly enforced. This chapter defines the mechanisms that will ensure ongoing compliance, track service performance and enforce corrective measures when ministries or suppliers deviate from the framework.

Digital transformation is not just about launching services. It is about maintaining quality, trust and accountability over time.

7.2 Real-Time Service Monitoring

Digital services should be monitored by the Operations team of the respective Ministry:

Monitored Indicators:

- Uptime (monthly %, minimum 99.5%)
- API response time and failure rates
- Number of users and active sessions
- Transaction volumes
- Error codes (e.g. failed logins, submission errors)
- Notification delivery rates (SMS/email)

***Purpose**:* Allows central visibility and rapid response to outages or bottlenecks.

7.3 DSF Compliance Audits

MITCI will organize periodic audits of all digital services for DSF compliance.

Types of Audits:

- Technical Architecture Audit

- Security & Penetration Test
- Data Protection Compliance Audit
- Performance & Uptime Review
- API and Integration Audit

***Scope**:* Includes frontend, backend, data handling, authentication and API use.

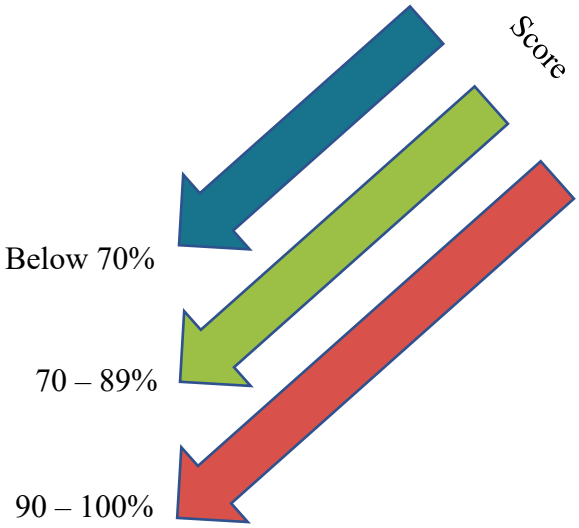
7.4 DSF Compliance Scorecard

Each digital service will receive a compliance score based on the DSF checklist.

Score Components:

- Identity integration (MauPass, Mobile ID, Physical ID)
- API integration with InfoHighway/CDH
- Accessibility and multilingual support
- Security and privacy adherence
- Use of national platforms (MoKloud, etc)
- Real-time tracking and status updates

- 90 – 100% - Fully Compliant
- 70 – 89% - Partially Compliant
- Below 70% - Non-Compliant



***Transparency**:* Scores may be published to inform users and encourage quality.

7.5 Citizen Feedback, Participation and Issue Escalation

All services must include feedback, complaint mechanisms and status tracking. In line with EGDI e-Participation indicators, ministries must also enable public consultations, e-surveys, e-petitions (where legally enabled) and publish consultation outcomes. Citizen engagement platforms must be progressively integrated with digital services to strengthen participation.

Channels:

- Integrated feedback forms and participation platforms on each portal or app
- Service ratings (1–5 stars) post-transaction
- Complaint tracking via Complaint Management System

Each Ministry must:

- Respond to complaints within 5 working days,
- Track satisfaction scores and include them in quarterly reports.

***Citizen Voice**:* Drives improvement and ensures accountability.

7.6 Supplier Accountability

Suppliers engaged to deliver digital services must be contractually bound to comply with DSF.

Procurement Controls:

- All RFPs must include DSF clauses and scoring criteria.
- Suppliers must submit DSF compliance checklists with technical proposals.
- Contract clauses must allow:
    - Government to retain full ownership of all data generated, processed, or stored under the system.
    - Government to own any custom-developed software created specifically under the contract for the project

Security and performance audits,

Remediation required

***Enforcement**:* DSF non-compliance may result in breach of contract.

7.7 Self-Assessment and Continuous Improvement

Ministries are encouraged to must conduct regular DSF self-assessments.

Checklist Includes:

- Architecture alignment
- Security posture
- Integration with core platforms
- User experience and accessibility
- Privacy and consent mechanisms

Each Ministry must:

- Maintain a record of the assessment,
- Identify areas for improvement,
- Include a compliance roadmap in its digital strategy plan.

***Culture of Learning**:* Continuous improvement, not just compliance.

8. POLICY ENFORCEMENT AND LEGAL MANDATE OF THE DSF

8.1 Overview

The DSF is not merely a set of guidelines. It is a mandatory, enforceable policy instrument backed by institutional authority. This chapter outlines the legal foundation, enforcement mechanisms and governmental obligations that ensure the DSF is upheld across all public sector digital initiatives.

Digital transformation in Mauritius must be rights-based, standards-led and binding and not subject to discretion or fragmentation.

8.2 Authority and Basis

The DSF derives its authority from:

- Cabinet approval of the Digital Transformation Blueprint,
- Cabinet approval for the DSF.
- Decisions of the IMCDT mandating compliance across ministries,
- Existing laws such as The Data Protection Act 2017, The Electronic Transactions Act, The Public Procurement Act and forthcoming reforms identified in the Blueprint including the Freedom of Information Act, revised Data Protection Act, revised ETA and enhanced Cybersecurity and Cybercrime legislation. DSF compliance will be updated to align with these reforms once enacted.

The DSF is a Cabinet-approved binding policy instrument, enforceable through procurement, funding controls and institutional oversight.

8.3 Scope of Enforcement

DSF enforcement applies to:

- All ministries and departments;
- Any vendor, consultant, or contractor developing systems for government;
- All stages of a service lifecycle: design, development, testing, deployment; and maintenance.

No digital service can be launched, procured, or funded without proof of DSF compliance.

Scope is government-wide and extends to third-party service providers.

8.4 Procurement Integration

All government ICT procurement must include DSF requirements:

- RFPs must include DSF clauses (architecture, APIs, integration),
- Evaluation must take consider DSF-readiness,

Procurement becomes a tool for enforcing interoperability and reuse.

8.5 Ministerial Accountability and Governance

Every Accounting Officer is accountable for DSF compliance and may be addressed by the Steering Committees at the level of the Ministry as an agenda item in digital projects.

Accountability rises to the top.

8.6 Sanctions and Escalation Pathways

Failure to comply with DSF policies will need to be escalated.

Additionally:

- Vendors may be debarred from future tenders,

- Ministries may face funding freeze or loss of project control.

Non-compliance has clear consequences.

8.7 Transparency and Audit Trail

The DSF mandates a clear audit trail for all major digital projects:

- Compliance checklists,
- All architecture and security reviews archived,
- DPIAs logged,
- Performance data shared with oversight committees.

Where appropriate, this information will be shared with:

- National Audit Office,
- Parliament,
- Public via dashboards and transparency reports.

Trust requires visible evidence of action.

8.8 Institutional Mandate for Updates

The MITCI is responsible for:

- Maintaining the DSF policy text and annexes,
- Issuing binding directives and FAQs,
- Convening technical committees for updates (every 12–18 months),
- Publishing official DSF versions (e.g. DSF v1.0, v2.0).

All new versions:

- Are communicated to all ministries,
- Include a compliance transition period (usually 3–6 months),
- Are archived and version-controlled for traceability.

DSF is a living instrument with legal durability.

9. FINAL RECOMMENDATIONS

9.1 DSF in Four Pillars

The DSF rests on four mutually reinforcing pillars: Principles (the why), Architecture Principles (the technical enablers), Policies (the rules) and Design Standards (the how). While the other three define the philosophy, rules and practices of digital service delivery, Architecture Principles act as the cross-cutting foundation that ensures all services are modular, interoperable, secure and built for reuse.

Pillar	Purpose	Scope	Examples (Mauritius DSF)
Principles (the *why*)	Define the values and design philosophies that underpin digital government	Long-term guiding norms (drawn from the Digital Transformation Blueprint, OECD, UN and citizen needs)	Digital by Default & Whole of Life; Mobile-First, Super App Enabled; Secure Identity; Once-Only and Data Reuse; Privacy by Design; Accessibility; Interoperability; Openness; Resilience; Value-for-Money & Green ICT
Architecture Principles (the enablers)	Establish the technical foundations that make services secure, interoperable and reusable	Modular design, API-first, cloud-ready, mobile-centric, secure-by-design, zero redundancy	Use of Government Cloud; RESTful APIs; Integration with MauPass and InfoHighway; Reuse of existing platforms; Avoidance of duplicate systems
Policies (the *rules*)	Provide binding requirements that ministries,	Identity, data, documents,	MauPass/Mobile ID required; InfoHighway mandatory; MoKloud and Revamped

	suppliers and partners must follow	security, procurement, audit	platform (Korek) for digital documents; DPIA required; Government Cloud hosting; RFPs must include DSF clauses
Design Standards (the *how*)	Translate principles and policies into practical, technical and user experience rules	Service design, accessibility, mobile-first, multilingual, testing, modular architecture	Life-event journeys; WCAG 2.1 AA accessibility; English/French/Kreol; Pre-filled forms via InfoHighway; Real-time validation; Status tracking; Privacy notices; Modular API-first architecture

This structure ensures the DSF is not abstract. It is philosophy (why), rules (what) and standards (how) combined into one enforceable framework.

9.2 Empowering Ministries, Not Adding Burden

The DSF is designed to work with existing government processes:

- Budgeting: Considered at Project Proposal stage
- Procurement: Standard DSF clauses are embedded in technical specifications.
- Testing: DSF compliance is verified within UAT and OAT, not through a separate bureaucracy.

This approach ensures coherence and accountability without slowing down delivery.

9.3 International Alignment

The DSF reflects what has worked internationally:

- Estonia: Once-Only principle and eID as backbone of citizen trust.

- UK GDS: Service Standards reduced IT project failures and improved adoption.
- India NeGD: Aadhaar, eSign, DigiLocker scaled digital services to over a billion users.
- Singapore GovTech: Mobile-first, secure hosting and reuse-first architecture.

By embedding these lessons, Mauritius positions itself as a regional leader in safe, citizen-centric digital government.

9.4 Road Ahead: Implementation Priorities

The following milestones will bring DSF from policy to practice:

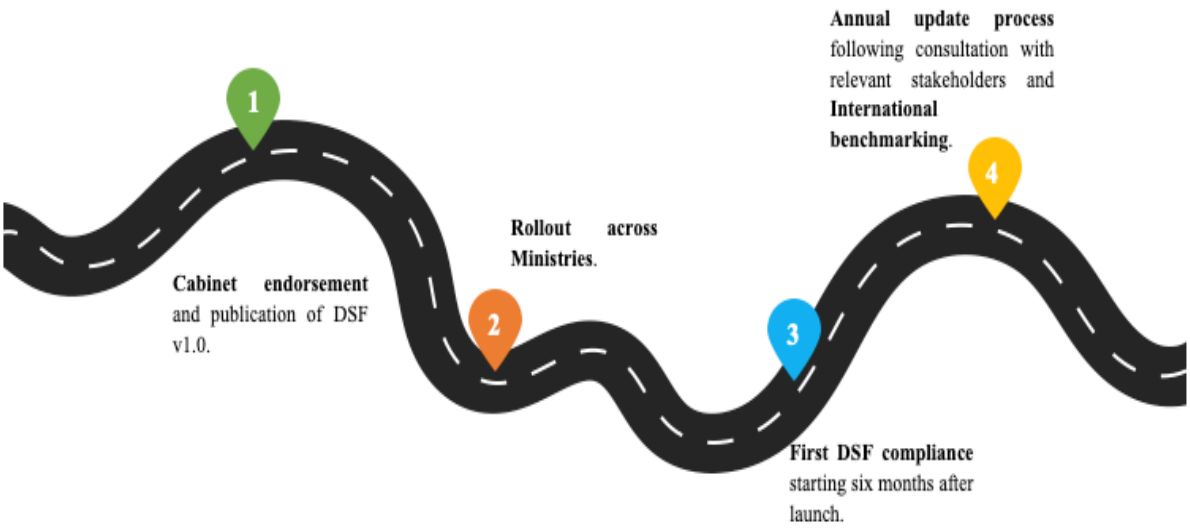


Figure 4: Roadmap

9.5 Closing Call

The DSF is a digital social contract:

- It empowers ministries to innovate while ensuring coherence.
- It protects citizens by embedding privacy, security and trust.
- It strengthens accountability by linking compliance to funding, procurement and audits.

By adopting DSF, every Ministry, supplier and official becomes a guardian of digital trust. Together we can digitise with dignity, build with responsibility and govern with purpose.

10. ANNEX 1 – ACRONYMS

Acronym	Full Form	Description
AI Unit	Artificial Intelligence Unit	The AI Unit is responsible for implementing the national Artificial Intelligence Strategy and coordinating the adoption of AI across government.
API	Application Programming Interface	A standard method for systems to communicate and exchange data.
BRN	Business Registration Number	The unique identifier assigned to companies and legal entities in Mauritius.
CDH	Citizen Data Hub	The authoritative hub aggregating citizen records from CPD, Civil Status and National ID systems.
CIB	Central Informatics Bureau	Government unit providing project management, technical specifications and oversight for ICT projects.
CPD	Central Population Database	The authoritative population register containing civil and identity data of citizens, keyed on the NIN.
DPIA	Data Protection Impact Assessment	A risk assessment required under the Data Protection Act to ensure privacy-by-design in digital services.

Acronym	Full Form	Description
DSF	Digital Service Framework	The mandatory compliance framework for all government digital services.
GovCloud	Government Cloud	Sovereign cloud infrastructure approved for hosting government services and data.
Government Stack	Government National Stack	Refers to the structured set of foundational digital building blocks, shared platforms, identity systems, interoperability layers and infrastructure components adopted by the Government of Mauritius to enable secure, interoperable and scalable digital service delivery.
ICT	Information and Communication Technology	Refers broadly to digital systems, platforms and services.
IMCDT	Inter-Ministerial Committee for Digital Transformation	High-level committee providing strategic enforcement and direction for DSF.
ITSU	IT Security Unit	Government unit responsible for IT security, aspects, IT security audits and cybersecurity enforcement.
KOREK	Government Digital Document platform with unified front end	Platform that allows citizens to access Government services, store and share digital documents.

Acronym	Full Form	Description
DPO	Data Protection Office	National authority enforcing compliance with the Data Protection Act.
METC	Mauritius Emerging Technology Council	A governmental advisory body that formulates policies and strategies to promote the adoption of emerging technologies for national economic growth.
MITCI	Ministry of Information Technology, Communication and Innovation	The lead Ministry responsible for digital transformation and DSF oversight.
MoKloud	Government Digital Document platform	Platform that allows citizens to receive, store and share digitally signed documents.
Mobile ID	Mobile Identity	National mobile-based digital identity enabling secure authentication and digital signatures.
NIN	National Identity Number	The unique lifelong identifier assigned to Mauritian citizens under the Civil Status Division.
RFP	Request for Proposals	Standard procurement process document used to solicit bids for ICT projects.
SSO	Single Sign-On	Authentication mechanism allowing users to log in once and access multiple services securely.

Acronym	Full Form	Description
VDS	Visible Digital Seal	ICAO-standard 2D barcode (e.g., QR code) used to enable offline verification of documents.
WCAG	Web Content Accessibility Guidelines	International standards ensuring websites and apps are accessible to all, including persons with disabilities.

11. ANNEX 2 – REFERENCES

11.1 National Legislation and Policies

- Government of Mauritius (2017). Data Protection Act 2017. https://dataprotection.govmu.org
- Government of Mauritius (2000 – revised). Electronic Transactions Act. https://mauritiusassembly.govmu.org
- Government of Mauritius (2006 – revised). Public Procurement Act. https://ppo.govmu.org
- Ministry of Information Technology, Communication and Innovation (2025). Digital Transformation Blueprint 2025–2029. https://mitci.govmu.org
- Government of Mauritius (2023). Government Cloud Policy. Ministry of Information Technology, Communication and Innovation. https://govmu.org

11.2 Guiding Principles

- Organisation for Economic Co-operation and Development (OECD) (2020). *The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government* (07 October 2020). https://www.oecd.org/en/publications/the-oecd-digital-government-policy-framework_f64fed2a-en.html
- World Bank GovTech Maturity Index (GTMI). https://www.worldbank.org/en/programs/govtech/gtmi
- European Union eIDAS Regulation. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

- OECD (27 November 2024). *Once-Only Principle: Streaming and Improving Services.* https://ec.europa.eu/digital-building-blocks/sites/spaces/OOTS/pages/840269998/OECD%2Brecommends%2Bstreamlining%2Band%2Bimproving%2Bservices%2Bthrough%2BOnce-Only

- European Union Digital Inclusion Strategy. https://digital-strategy.ec.europa.eu/en/policies/digital-inclusion

- OECD (2024). *Digital Public Infrastructure for Digital Governments.* https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf

- Open Data Charter (2015). *Principles.* https://opendatacharter.org/principles/

- Government of Mauritius (2023). *National Cybersecurity Strategy 2023–2026.* https://cert-mu.govmu.org/cert-mu/wp-content/uploads/2023/11/Policies-and-Legislation.pdf

11.3 International Standards and Best Practices

- International Civil Aviation Organization (ICAO) (2021). *Document 9303: Machine Readable Travel Documents.* Montréal: ICAO. https://www.icao.int/publications

- International Organization for Standardization (ISO) (2019). *ISO/IEC 18013-5: Personal Identification — Mobile Driver Licence (mDL) — Part 5: Application.* Geneva: ISO. https://www.iso.org

- European Union (2014). *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services (eIDAS Regulation).* Official Journal of the European Union, L257/73. https://eur-lex.europa.eu

- European Union (2016). *General Data Protection Regulation (GDPR) (EU 2016/679).* Official Journal of the European Union, L119. https://eur-lex.europa.eu

- Organisation for Economic Co-operation and Development (OECD) (2014). *Recommendation of the Council on Digital Government Strategies.* Paris: OECD. https://www.oecd.org/gov/digital-government

- United Nations (2022). *United Nations E-Government Survey 2022.* New York: Department of Economic and Social Affairs. https://publicadministration.un.org/egovkb

- World Wide Web Consortium (W3C) (2018). *Web Content Accessibility Guidelines (WCAG) 2.1.* W3C Recommendation. https://www.w3.org/TR/WCAG21

- National Institute of Standards and Technology (NIST) (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).* Gaithersburg: NIST. https://www.nist.gov/cyberframework

11.4 Regional and Comparative Case Studies

- Government of Estonia (2020). *X-Road: Interoperability Services for Digital Government.* Tallinn: Information System Authority. https://x-road.global

- Government of India (2018). *Aadhaar, eSign and DigiLocker – India Stack Overview.* New Delhi: Ministry of Electronics and Information Technology (MeitY). https://www.meity.gov.in

- GovTech Singapore (2021). *Digital Government Blueprint.* Singapore: Government Technology Agency. https://www.tech.gov.sg

- Government Digital Service (GDS) (2019). *Service Standard.* London: UK Cabinet Office. https://www.gov.uk/service-manual/service-standard

11.5 Additional International Frameworks and Standards

- The Open Group (2018). *TOGAF® Standard, Version 9.2.* Reading, UK: The Open Group. https://www.opengroup.org/togaf

- European Commission (2017). *European Interoperability Framework (EU EIF v3.0).* Brussels: European Commission. https://ec.europa.eu/isa2/eif_en
- International Organization for Standardization (ISO) (2011). *ISO/IEC 42010: Systems and Software Engineering — Architecture Description.* Geneva: ISO. https://www.iso.org
- International Organization for Standardization (ISO) (2011). *ISO/IEC 27031: Information Technology — Security Techniques — Guidelines for ICT Readiness for Business Continuity.* Geneva: ISO. https://www.iso.org
- International Organization for Standardization (ISO) (2019). *ISO/IEC 22301: Security and Resilience — Business Continuity Management Systems — Requirements.* Geneva: ISO. https://www.iso.org
- International Organization for Standardization (ISO) (2023). *ISO/IEC 31700: Consumer Protection — Privacy by Design for Consumer Goods and Services.* Geneva: ISO. https://www.iso.org
- National Institute of Standards and Technology (NIST) (2020). *Special Publication 800-207: Zero Trust Architecture.* Gaithersburg: NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final
- Organisation for Economic Co-operation and Development (OECD) (2014). *Recommendation on Digital Government Strategies.* Paris: OECD. https://www.oecd.org/gov/digital-government
- World Bank Group (2021). *Digital Government Readiness Assessment Framework.* Washington DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099720006292139780

- International Telecommunication Union (ITU) (2008). *ITU-T Recommendation X.1205 — Overview of Cybersecurity.* Geneva: ITU. https://www.itu.int

12. ANNEX 3 – GOVERNMENT STACK

Rather than build in silos, public agencies must plug into a shared ecosystem powered by reusable platforms such as MauPass, Mobile ID, Physical ID, InfoHighway, Citizen Data Hub, MoKloud, Digital Payment, Mo RendezVous, DIVA and the Super App. Together, these constitute the Government Stack/ Digital Public Infrastructure (DPI), a layered national stack ensuring interoperability, reusability to support secure digital services.

Every service must integrate with these core national platforms:

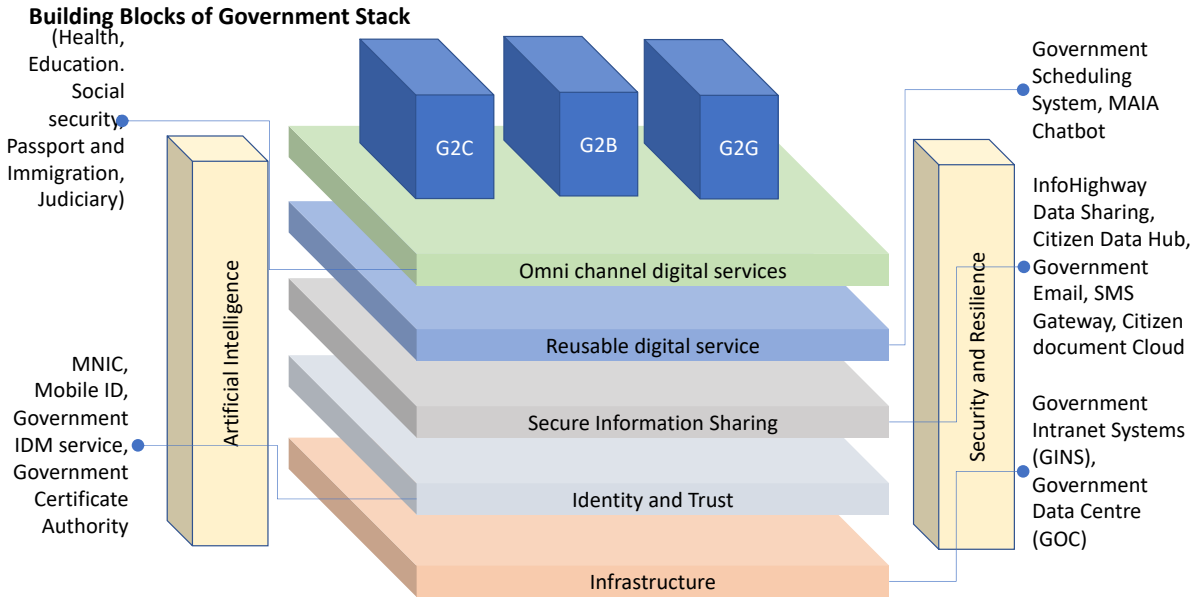


Figure 5: Building Blocks of Government Stack

A. MauPass (Authentication Gateway)

- Single sign-on (SSO) for all services.
- Supports 1FA, 2FA and integration with Mobile ID.
- Identity Provider for Government and managed by the MITCI.

B. **Mobile ID (Identity Proofing, Digital Signature and Online Authentication)**

- The National Identity Card remains the foundational and legally recognised proof of identity in Mauritius. It is primarily used for physical, face-to-face identity verification in the real-world environment. When a citizen is required to present proof of identity in person, the physical National Identity Card serves as the authoritative credential. Mobile ID can also be used in these face to face scenarios.
- The Mobile ID provides to digital signing of digital documents.

When required to authenticate with MauPass, the Mobile ID can be used.

C. InfoHighway (Data Sharing Platform)

- Enables real-time exchange of data between ministries.
- Publisher-subscriber model with approval workflows.
- Enforces role-based access, encryption and usage logs.

D. Citizen Data Hub (CDH)

- Aggregates authoritative citizen records (Civil Data, identity, address, status).
- Synchronised with Civil Status and National ID databases.
- Acts as a trusted data source to prefill forms and validate submissions.

E. MoKloud (Document Wallet)

Allows citizens to store digital documents.

- The existing Super App will be enhanced through the revamping of MoKloud.

The Super App Korek provide unified access to digital services and government-issued documents.

F. Super App (Unified Mobile Platform)

- Hosts service modules from various ministries.
- Follows micro front-end architecture for modular deployment.
- Provides a unified UX and common notification inbox.
- See MoKloud

G. Digital Payment Gateway

- Standard platform for online payments to government.
- Integrates with local banks and mobile money.

H. Mo RendezVous Scheduling System

- The Government Scheduling System serves as a reusable building block to support appointments and bookings across ministries and departments. It provides citizens and businesses with a unified interface to request services, while allowing agencies to optimise resource allocation and reduce administrative overhead. Integration with MauPass ensures identity-verified access and consistent user experience.

I. DIVA Chatbot / Digital Assistant

- DIVA acts as the national multilingual AI assistant, providing citizens with conversational access to government information and services through web, mobile and messaging platforms. As a shared service, DIVA reduces duplication of effort across agencies while improving accessibility and responsiveness in citizen engagement.

J. Government Intranet Systems (GINS)

- The Government Intranet Systems constitute the secure backbone for internal communications, collaboration and knowledge-sharing among ministries. They complement the Citizen-facing channels by ensuring that government officers can exchange information, manage workflows and coordinate securely across organisational boundaries.

K. Government Online Centre (GOC) / Data Centre

- The Government Online Centre provides centralised hosting and resilience for mission-critical applications. It ensures high availability, continuity and disaster recovery for national platforms, while serving as the foundation for hybrid and government-cloud strategies. Its role is central to safeguarding uptime, security and data sovereignty.

L. MauSign

- MauSign is the national Certificate Authority (CA) established under the Mauritian Public Key Infrastructure (PKI) framework to issue digital certificates used for authentication, encryption and digital signing. It ensures confidentiality, integrity, authentication and non-repudiation in electronic transactions and communications providing trusted digital signatures for individuals, organisations and government officers.

- MauSign is managed by the MDPA and operates under the oversight of the ICTA, the Controller of Certification Authorities. MauSign supports the issuance of digital certificates for individuals , organisations, Servers and Application Service Providers (ASPs) certificates which allows a citizens to use his/her MauPass 2FA account to digitally sign a digital documents using the e-Sign service of MauSign.