Digital Transformation Delivery Guardrails and Standards Agreement

A shared framework for safe, open, and decentralised digital delivery under the South African Digital Transformation Roadmap

Purpose

This document sets out the guardrails and shared standards for departments and private-sector teams implementing components of South Africa's Digital Transformation Roadmap. It ensures delivery remains consistent with DSU principles while enabling decentralised execution and rapid, secure delivery. These principles, tools, and workflows allow partners to deliver securely, openly, and collaboratively — without requiring DSU to be embedded in every project. It defines how to build within the DSU environment, not what to build.

Institutional Definition and Mandate

For the purposes of this document and all associated activities:

The Digital Services Unit (DSU) acts as the implementation arm of the Interdepartmental Working Group (IDWG) on Digital Transformation, under the authority of the Presidency.

The DSU coordinates and enables delivery across government through agile, standards-based methods, ensuring that all work aligns with the Cabinet-approved Digital Transformation Roadmap and its associated governance structures.

The DSU operates in close collaboration with:

- the Government Information Technology Officers Council (GITOC), representing departmental CIOs and digital teams;
- existing state digital units and technical capabilities within departments, entities, and agencies; and
- the Presidency Project Management Office (PMO) and Inter-Ministerial Committee (IMC) on Digital Transformation for strategic oversight and alignment.

Together, these entities form a coordinated delivery ecosystem for the modernisation of South Africa's digital government infrastructure and services.

DSU Working in the Open Principles

The Digital Services Unit (DSU) builds, delivers, and governs South Africa's next-generation government services using open, modular, and secure technology choices — aligned to global best practice, South African priorities, and principles that safeguard people and promote inclusion. These guiding principles will ensure that the development activities of teams - regardless of location - contribute to a cohesive and sovereign stack of government technology.

Adapt, Build, Buy

- Assess first: We begin by understanding the user and institutional needs, clearly defining the problem, and identifying existing demand before deciding what to create or procure.
- Adapt and reuse: Wherever possible, we adapt and reuse existing open-source, civic-tech, or government solutions that already meet part of the need.

- Build: We build new core capabilities only where sovereignty, standards, inclusion, or security require local control — or where no suitable solution exists.
- Buy: We buy solutions last, and only when they can be integrated using open standards, promote vendor diversity, and avoid lock-in. Tools like Wardley Mapping help this.
- Exception: Any deviation from this order must be justified through an assessment showing that reuse or local build is not feasible or cost-effective.
- All procurement related to DPI must comply with national procurement laws and open contracting standards (OCDS), publishing key deliverables, timelines, and IP arrangements for transparency and competition.

Open Source, Open Standards, Open Governance

- DSU-managed and government-developed code, APIs, and tools are open source by default, reusable across government and society.
- DSU curates and maintains the official repositories, reviewing contributions to ensure compliance with open standards, security, and accessibility requirements.
- We enforce open standards (OAuth2, OpenID Connect, OpenAPI, JSON Schema, and others) to ensure true interoperability.
- Our governance promotes public ownership, transparency, and collaboration in how services are built and improved.

Interoperability by Design

- Connected by default: Every product and service must work seamlessly across departments, spheres of government, and platforms.
- Common standards: APIs, data schemas, and authentication mechanisms conform to DSU's open standards.
- Composable systems: Each new component strengthens, not fragments, the shared digital ecosystem.
- No new silos: If it can't integrate, it doesn't ship.
- Ecosystem first: Interoperability extends beyond government to include private, civic, and academic partners through secure and open interfaces.
- Where appropriate, DSU standards and APIs should align with regional and international DPI reference models to enable future cross-border interoperability.

User-Centricity and Inclusion

- Start with users: Every service begins with research into real user needs, especially those of underserved communities.
- Accessible for all: Services are mobile-first, low-bandwidth, zero-rated, and available in South Africa's official languages.
- Design for context: Interfaces and processes reflect South Africa's geographic, cultural, and socio-economic diversity.
- Evidence over assumption: Continuous usability testing and feedback loops drive iteration and improvement.
- Inclusive by design: Accessibility and inclusion are non-negotiable — they are success metrics, not optional extras.
- Design, testing, and implementation must include representation across gender, disability, age, and regional diversity, ensuring no group is digitally excluded.

Modular, Scalable, and Resilient Architecture

- Build in blocks: Systems are modular, reusable, and interoperable, enabling rapid delivery and independent scaling.

- Capability-driven design and architecture: Each building block represents a distinct capability, such as authentication, data exchange, or payments, that can be reused across services. Over time, this approach will reduce or eliminate overlap between systems and ensure government invests once in shared capabilities that serve many.
- Observable and secure: All infrastructure includes monitoring, logging, and incident response by design.
- Resilience through diversity: We avoid single points of failure through decentralisation, open APIs, and technology diversity.
- Cloud-neutral and portable: Platforms can run across multiple environments without dependency on any single vendor, with portability designed to be rapid and low-effort through containerisation and infrastructure-as-code.Cloud-neutral and portable: Platforms can run on multiple environments without dependency on any single vendor and portability should be close to instantaneous.
- Iterate safely: Components (or vendors/partners) can be updated or replaced independently, without breaking the wider ecosystem.
- All omponents should adopt green computing principles, prioritising energy-efficient hosting, responsible procurement, and reuse to reduce environmental impact.

Responsible Data Stewardship and Innovation

- Ownership and Stewardship: We know who is responsible for the data collected and managed and have clear policies for data owners on data retention and secure deletion.
- Quality and Integrity: We provide robust processes to help data owners maintain the accuracy, completeness, and validity of all data in our ecosystem.
- Algorithmic Transparency and Accountability: Where AI-powered services are used to know how algorithms operate have clear lines of accountability for their outputs.
- Responsible Technology Assessment: We conduct thorough assessments of the potential societal, economic, and ethical impacts of software before its deployment.

Data Protection and Privacy by Default

- Privacy built-in: Security and data protection are embedded in every stage of design and development, not retrofitted later.
- Ongoing Security Assurance: We conduct regular security testing, vulnerability assessments, and promptly remediate identified flaws.
- User agency: People can see, manage, and consent to how their data is used, shared, and stored. Individuals have the right to know how their data is used, request correction or deletion where appropriate, and seek redress for misuse. Departments must provide transparent, accessible complaint mechanisms for digital public services.
- Compliant and ethical: All systems adhere to POPIA and global best-practice safeguards such as DPI and privacy-preserving design.
- Open, peer-reviewed security: Use open-source, verifiable tooling and cryptographic standards wherever possible.
- Secure Development Ecosystem: Our development tools, pipelines, and the entire software supply chain are secured.
- Trust through transparency: Breach handling, consent flows, and data-sharing agreements are documented and published.

Public Ownership, Transparency, and Community Collaboration

- Public code, public value: Core government platforms (MyMzansi, GOV.ZA, data exchange) are open source and publicly governed.

- Open governance: Design systems, APIs, and documentation are shared for reuse across government and society.
- Co-creation culture: Civil society, business, and academia participate in building, testing, and improving services.
- Accountable delivery: Public roadmaps, changelogs, and performance dashboards show what's being built and why.
- Shared stewardship: Ownership extends across government — the DSU convenes, coordinates, and enables, not controls.

Working in the Open

- Transparent by default: Plans, code, designs, and progress are visible internally and externally unless restricted by law or security.
- Show the work: Roadmaps, metrics, and sprint outcomes are published regularly to build public trust and learning.
- Document and reuse: Every output — from design tokens to policy templates — is reusable and documented.
- Collaborate in public: Teams share updates, user research, and post-mortems openly to invite feedback and learning.
- Open loops, not closed rooms: Delivery happens through iteration, participation, and community contribution.

We build for trust, inclusion, and resilience — together, in the open, guided by principles that promote digital rights, interoperability, and public good.

RACI Framework

The following provides an overview of the advised approach to conducting work which ensures private sector teams operate under the guidance of the department and in accordance with shared government principles. Government departments include elected representation from GITOC. Further elaboration of the RACI based on department requirements and guidelines is desirable.

Implementation Note:
The DSU requires defining clear decision gates aligned with the RACI activities above. These gates should outline:
• the **information required** for each sign-off (e.g., design review, code audit, deployment approval);
• the **responsible and accountable roles** at each gate; and
• the **timing and format** for reviews and feedback.

Documenting these gates in advance enables accountable parties to make timely, informed approvals and ensures expectations are transparent across all stakeholders. The DSU will sign off on these gates after agreement from the lead department.

Activity	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Defining Project Scope & Requirements	Digital Services Unit (DSU), Government Departments	Government Departments	Private Sector Development Teams	Digital Services Unit (DSU), Government, The Public
Developing Code	Private Sector Development Teams	Private Sector Development Teams	Digital Services Unit (DSU)	Government Departments, Government, The Public

Reviewing & Approving Code	Digital Services Unit (DSU) *Note: Approval includes conformance with DSU's interoperability, security, and API standards.*	Digital Services Unit (DSU), Government Departments	Government Departments	Private Sector Development Teams, Government, The Public
Deploying Solutions	Private Sector Development Teams, Government Departments	Government Departments	National Treasury, AGSA, Digital Services Unit (DSU)	Government, The Public
Quality Assurance (QA)	Digital Services Unit (DSU)	Private Sector Development Teams, Government Departments	Digital Services Unit (DSU)	Government, The Public
User Acceptance Testing (UAT)	Digital Services Unit (DSU), Government Departments	Government Departments	Private Sector Development Teams	Government, The Public
Training and Capacity Building	Private Sector Development Teams	Government Departments	Private Sector Development Teams, Digital Services Unit (DSU)	Government, The Public
Ongoing Maintenance & Support	Government Departments	Government Departments	Digital Services Unit (DSU)	Private Sector Development Teams. Government, The Public

All projects must complete a DPI Safeguards Checklist covering inclusion, privacy, competition, and security before public deployment. The DSU Safeguards Review will confirm compliance.

DSU Workbench and Tooling Environment

To support safe, consistent, and collaborative delivery across distributed teams, DSU provides a standardised "workbench" environment.

This enables transparency, quality assurance, and compliance with open government technology standards.

Core tools and environments include:

- **Standards:** All work delivered under this roadmap must comply with the DSU's official standards, which define how government technology is designed, built, and secured.
- **Service Manual:** The DSU Service Manual outlines the principles, playbooks, and delivery practices for designing and developing government services. It includes guidance on user research, accessibility, content design, agile delivery, cybersecurity and service assurance. All teams must follow the service phases (discovery, alpha, beta, live) and apply the DSU Service Standard in their work.
- **Version control and CI/CD:** GitLab (with DSU-approved repositories, pipelines, and security scans).
- **Design collaboration**: The MyMzansi design system (compulsory) and Figma (shared design libraries and component systems for GOV.ZA and MyMzansi).

- **Project management and agile delivery:** Asana (or equivalent as decided by DSU), using DSU sprint templates, OKR tracking, and issue boards.
- **Team communication**: Mattermost (compulsory) and, when necessary, DSU's shared workspace channels for sprint planning, stand-ups, and incident response.
- **Documentation and transparency:** DSU's public documentation hub for publishing APIs, architecture diagrams, standards, and changelogs.
- **Services:** all services will be delivered through the MyMzansi universal service channel, and not the private sector partners channels.

Safeguards in the Workbench

- Add a "Safeguards" tab in Asana/Jira sprint templates (checkboxes for inclusion, privacy, interoperability).
- GitLab repository templates to include privacy, security, and API documentation folders.
- Figma accessibility audits are crucial to design sign-off.
- Safeguards Checklist as a column in the DSU dashboard (status: pending / complete / verified).
- Frame safeguards are quality accelerators:
    - Projects with complete Safeguard Checklists move faster through DSU approval gates.
    - Departments demonstrating strong safeguard compliance get "ready-to-scale" status in the DSU portfolio dashboard.
- Every ±2 months or per use case the DSU will run a Safeguard review:
    - Run by DSU Safeguards Review Team with Department & Partner.
    - Use the checklist to validate progress and update dashboard.
    - Report summaries to IDWG once per quarter.

Core Components

All teams must design and build using DSU's shared, reusable service components, which form the backbone of South Africa's government digital ecosystem. These components ensure that services are interoperable, secure, and reusable across departments. They include, but are not limited to:

- **Forms:** A common forms framework for accessible, reusable, and schema-driven data capture across departments, ensuring consistency and integration with back-end systems.
- **Notify:** The DSU Notify component enables verified multi-channel messaging (SMS, WhatsApp, email, push notifications) through a single API, ensuring auditability, consent management, and inclusion.
- **Data Exchange (MzansiXchange):** The national data exchange platform providing real-time, API-first data sharing between departments and agencies, using DSU's open schemas, consent management, and access auditing.
- **Identity, Authentication, and Trust Ecosystem:** A federated digital identity and trust framework providing secure login (SSO), user verification, and credential issuance. This includes the national Digital ID, SSO service, Trust Framework, and Verified Credentials and Wallet ecosystem, allowing users to store and share digital documents securely.
- **Payments:** The Payments Orchestration Layer and Beneficiary Preference Mapper enable flexible, auditable government-to-person (G2P) and government-to-business (G2B) payments, integrated with Digital ID and data exchange systems.
- **Case Management and Appointments:** Shared APIs and services for tracking cases, applications, and service interactions consistently across departments.
- **CMS (Content Management System):** The GOV.ZA headless CMS provides a unified content platform for all departmental websites and citizen-facing information services, built on the DSU design system and accessible via MyMzansi.
- **Channels:** All citizen-facing services will be delivered through the MyMzansi universal service channel (web, mobile, and API gateways), ensuring a single, secure, and consistent front door for digital government services — not through private partner channels.

All private-sector and departmental teams are expected to work within this ecosystem and integrate compatible tools and components as they come online. These common components are in active development, and private-sector and departmental teams would, in the implementation of the project or use case, to contribute to their testing, validation, and improvement. Where a component is not yet released or ready for purpose, the DSU will determine the appropriate interim approach or approved alternative to ensure continuity and alignment with shared standards.

Access to the DSU environment will be granted upon project registration and adherence to security and confidentiality agreements.

DSU's standards, tools, and environments are living systems that will evolve as technology and policy advance. Private-sector partners are required to adopt updated versions within reasonable transition periods to maintain alignment with DSU's interoperability, security, and design frameworks.

Project Lifecycle Overview

Each project follows a lightweight, repeatable lifecycle aligned to agile best practices and DSU delivery standards:

- Initiation and Registration: The department, DSU and partner agree on the project scope, outcomes, and governance. The project is logged in DSU's delivery dashboard.
- Setup and Access: Teams receive onboarding to DSU tools (GitLab, Figma, Asana, Mattermost) and security guidelines.
- Design and Build: Work proceeds in short sprints, using DSU's open standards and reusable components.
- Review and Sign-off: Outputs move through pre-defined decision gates (code review, UAT, deployment).
- Publication and Reuse: Once approved, all code, APIs, and documentation are published in DSU's repositories for cross-government reuse.
- Maintenance and Handover: Departments assume ownership; DSU provides guidance and oversight.

Project delivery planning and sprint implementation should use this as a guideline.

Digital Public Infrastructure (DPI) Safeguards Compliance Checklist

This checklist operationalises the Universal DPI Safeguards (G20/DPGA 2024) across all DSU-led and departmental digital transformation initiatives.

It ensures that delivery remains inclusive, rights-based, secure, and interoperable

#	Safeguard Principle	Description / Key Requirement	Status (Y/N/In Progress)	Gaps or Risks Identified	Action / Mitigation	Verified by (DSU / Department / Partner)
1	Inclusion and Equity	Service design must address accessibility (disability, gender, language, rural/low-bandwidth users). Testing must include diverse user groups.				
2	Open Standards and Vendor Neutrality	All systems must use DSU's open standards (APIs, data schemas, OAuth2, OpenAPI) and avoid vendor lock-in.				

3	Data Protection and Privacy	Privacy-by-design implemented; data minimisation, consent, and retention policies in place; POPIA compliance verified.				
4	User Rights and Redress	Citizens can view, correct, or delete their data and lodge complaints for misuse or errors; redress procedures are public and accessible.				
5	Security and Resilience	Security testing completed; incident response plan active; cloud environment follows DSU's Cybersecurity Playbook; zero-trust principles applied.				
6	Transparency and Accountability	Delivery dashboards, changelogs, and documentation published; project ownership and decision logs transparent.				
7	Capability and Capacity-Building	Private-sector partners have implemented a skills transfer plan; departmental teams trained to maintain and extend the system independently.				
8	Open Contracting and Public Procurement Transparency	All procurement and partnership arrangements are published (OCDS format recommended); IP and cost structures transparent.				
9	Algorithmic Transparency and Human Oversight	AI or automated systems include human-in-the-loop review; algorithm documentation, logic, and datasets published where applicable.				
10	Environmental Sustainability	Energy-efficient hosting, responsible procurement, and reuse practices applied; preference for green cloud environments.				
11	Interoperability and International Alignment	APIs and data models align with DSU's standards and international DPI frameworks (MOSIP, Mojaloop, GovStack).				
12	Safeguards Audit and Review	DPI Safeguards Checklist completed, reviewed, and signed off by DSU before go-live; compliance documented in DSU dashboard.				

Refer to the Universal DPI Safeguards for more detailed information.

Completion and Sign-Off

This checklist must be completed before pilot deployment and verified by the DSU Safeguards Review Team and the Lead Department.

Capability Alignment

Every project should clearly identify the capabilities it contributes to within government across teams, skills, and the shared technology stack. DSU will maintain a capability registry to prevent duplication and ensure new components extend rather than fragment the ecosystem.

Each capability should define:

- its purpose and APIs (not just describe *what it does* (its business purpose), but also *how other systems interact with it (its APIs));*
- *the owning de*partment or lead maintainer;
- integration points with other capabilities; and
- dependencies on DPI components (ID, data exchange, payments).

Every project must also include a capacity-building plan for departmental digital teams. Private-sector and external partners are expected to work side-by-side with government counterparts, transferring knowledge, co-developing solutions, and documenting processes in line with the DSU Service Manual. The objective is that, on completion, systems are fully maintainable, extendable, and operable by government teams without ongoing vendor dependence.

Capability development will be tracked through DSU's Community of Practice and learning programmes, ensuring that institutional skills grow in tandem with the technologies delivered.

Security, Access, and Compliance

All delivery teams must adhere to DSU's secure development lifecycle and infrastructure access controls.

- Source code repositories require multi-factor authentication and role-based permissions.
- Cloud environments must comply with DSU's cybersecurity playbook.
- All deployments must pass automated vulnerability and compliance scans before production release.
- Data handling must conform to POPIA and DSU's privacy-by-design principles.
- Services: all services will be delivered through the MyMzansi universal service channel, and not the private sector partners channels.

The DSU Security Advisor provides audit and onboarding support but does not manage day-to-day delivery operations.

Reporting and Transparency

Each participating project must publish delivery metrics to the DSU dashboard, including sprint outcomes, open issues, and OKRs.

Public summaries of progress (roadmaps, changelogs, dashboards) strengthen transparency and accountability, allowing other departments to learn and reuse outputs.

DPI Safeguards Review and Audit

All projects must complete the DPI Safeguards Checklist (above) before pilot deployment. The checklist verifies compliance with inclusion, privacy, interoperability, and accountability safeguards. The DSU Safeguards Review Team validates and records compliance on the DSU dashboard.

Roles in Safeguarding:

Role / Entity	Responsibility	Stage of Check
DSU Safeguards Review Team (small cross-functional cell inside DSU)	Leads safeguard assessments; validates checklists; provides templates, training, and support.	Before and after each major delivery phase (Discovery, Alpha, Beta, Live).
Departmental Project Lead / Product Owner	Integrates safeguards into delivery plan, ensures compliance evidence (accessibility tests, privacy impact assessments, etc.).	Ongoing, during each sprint.
Private-Sector Partner / Delivery Team	Implements and documents safeguards (accessibility, inclusion, privacy, etc.) as part of development and user testing.	During design, build, and testing sprints.
GITOC or Departmental CIO	Oversees compliance with technical and data standards, ensures hosting and security policies are applied.	During setup, integration, and deployment.
IDWG (Interdepartmental Working Group)	Oversight and escalation point — reviews safeguard compliance summaries as part of portfolio governance.	End of Alpha/Beta phases or before go-live.

Acknowledgement and Commitment

We, the undersigned, commit to the principles, standards, and responsibilities outlined in this Digital Transformation Delivery Guardrails and Standards Agreement.

Our shared goal is to ensure that all digital services delivered under this framework are open, secure, interoperable, and maintainable by government.

By signing, each party confirms the following responsibilities:

Participating Department:

- Commits to co-ownership of the project, capacitation of internal digital teams, and integration of outputs into departmental systems and workflows.
- The Department remains accountable for outcomes, service sustainability, and compliance with DSU and national standards.

Private-Sector Implementation Partner:

- Commits to co-delivery under the department’s direction, adherence to DSU’s open standards and security requirements, and full transfer of knowledge, code, and documentation to government teams upon completion.
- No intellectual property or operational dependencies will be retained beyond the contract scope.

Digital Services Unit (DSU) / Interdepartmental Working Group (IDWG):

- Provides oversight, standards, and access to the DSU workbench, tools, and repositories.
- Reviews outputs for compliance with the Service Manual, interoperability, and open standards, and ensures that lessons learned are shared across government through the capability registry and Community of Practice.

This Agreement forms part of the delivery documentation for the relevant Digital Transformation Roadmap project and remains in force for the duration of project implementation and handover.

Participating Department

Name of Representative _______________________ Signature _______________________

Signed at ____________________ on this ______ day of ______________, 2025.

Private-Sector Partner

Name of Representative _______________________ Signature _______________________

Signed at ____________________ on this ______ day of ______________, 2025.

Digital Services Unit (DSU)

Name of Representative _______________________ Signature _______________________

Signed at ____________________ on this ______ day of ______________, 2025.

End of Document