



NATIONAL DIGITAL IDENTIFICATION POLICY



Government of Samoa

Samoa Bureau of Statistics

Table of Contents

FOREWORD	iv
ACRONYMS & ABBREVIATIONS.....	v
DEFINITIONS	vi
1. EXECUTIVE SUMMARY	1
2. INTRODUCTION/PREAMBLE.....	2
3. PURPOSE AND OBJECTIVES.....	4
Purpose	4
Vision.....	4
Mission.....	4
Objectives	4
Values and Guiding Principles	4
4. MANDATE / LEGAL FRAMEWORK	6
National Policies, Strategies and Plans	6
Laws and Regulations	6
Regional Agreements	7
International Agreements	7
5. SCOPE OF APPLICATION	9
6. FOUNDATIONAL FEATURES OF THE NDID SYSTEM.....	13
7. POLICY STATEMENTS.....	15
8. MEANS OF IDENTITY (CREDENTIALS)	19
4 means of Identity Credentials.....	19
9. CONSENT AND CONTROL.....	21
9.1. Principle of Consent.....	21
9.2. Informed and Granular Consent	21
9.3. Consent Management and Record	21
9.4. Right to Withdraw and Limit Access to an Individuals Identity Records.....	22
9.5. Exceptional Circumstances.....	22
9.6. Accountability and Oversight	22
10. REGISTRATION PROCESS	23
10.1. Eligible Persons.....	23
10.2. Biographical Data Collected (Core Identity Fields)	23
10.3. Mass Registration.....	23
10.4. Registration at Birth (Post-Mass Registration).....	24
10.5. Continuous Registration	25
10.6. Registration of Children and Persons Requiring Assistance	25

10.7.	Implementation Responsibility.....	25
10.8.	Data Integrity and Reporting	26
10.9.	Coordination and Support	26
11.	BIOMETRIC ENROLMENT & VERIFICATION	28
11.1.	Age-Based Enrolment Rules.....	28
11.2.	Deduplication and Biometric Verification.....	28
11.3.	Quality Assurance and System Standards	29
11.4.	Data Protection and Privacy Safeguards	30
11.5.	Special Measures for Inclusion and Accessibility	31
12.	DIGITAL AUTHENTICATION	32
12.1.	Core Functions.....	32
12.2.	Methods of Authentication.....	32
12.3.	Use of NDID Authentication by Relying Parties.....	33
12.4.	Verification and Compliance Framework.....	34
12.5.	Consent and Transparency in Authentication.....	34
12.6.	Security, Oversight and Audit	35
12.7.	Fallback Procedures and Accessibility	35
13.	DIGITAL IDENTITY ASSURANCE LEVELS	37
13.1.	Level of Assurance Categories.....	37
13.2.	Application of Levels of Assurance by Sector	37
13.3.	Governance and Use of Levels of Assurance	38
13.4.	Relationship to Authentication Methods	38
13.5.	Review and Adaptation.....	38
14.	GRIEVANCE REDRESS AND ACCOUNTABILITY	39
14.1.	Access Channels.....	39
14.2.	Mandatory Public Communication	40
14.3.	Grievance Handling Process and Timelines	40
14.4.	Scope of Complaints	43
14.5.	Transparency, Awareness, and Feedback	43
15.	FEES AND CHARGES.....	44
15.1.	Initial Registration	44
15.2.	Replacement and Reissuance.....	44
15.3.	Updates and Corrections.....	44
16.	APPROVAL AND REVIEW	44
17.	IMPLEMENTATION PLAN.....	46
	PURPOSE.....	46
	GUIDING PRINCIPLES:.....	46
	POLICY MEASURES, TIMEFRAME AND IMPLEMENTING PARTNERS.....	49
	CROSS-CUTTING TRACKS (APPLIED ACROSS ALL PHASES)	57

TOP RISKS AND MITIGATIONS	58
MONITORING AND EVALUATION.....	59
Annex A – Tier Framework.....	62
Annex B – Relevant International Standards for NDID Implementation	63
Annex C – Grievance Registration Form	65



FOREWORD



I am honored to introduce the National Digital Identification (NDID) Policy for Samoa.

As Samoa advance into an increasingly connected world, building a resilient inclusive and modern digital economy requires a foundational of trust. This transformation is every Samoan's right to be legally recognised, included and protected. The National Digital Identification System is anchored by the SDIN - *Samoa Digital Identification Number*. The SDIN establishes the foundational layer of our Digital Public Infrastructure (DPI).

Over the years, access to public and private services has been constrained by paper-based processes, geographical isolation and fragmented systems. This Policy sets out a clear roadmap to make things easier. By replacing traditional barriers to verify and secure citizens digital identity, we ensure every individual in both urban and rural area, remote communities and people with disabilities can easily be verified and authenticated. This will improve how we access health care, education, financial services, social protection and disaster response support.

Crucially, this policy is built on the principle of **inclusion, consent** and **user protection**. We recognised that technology must serve humanity, not the other way around. To that end, the NDIDs systems embeds strong data privacy safeguards, biometric protection, rights-based governance and an Accessible Grievances Redress Mechanism, that ensures transparency and accountability at every stage. Special enrolment pathway has been specifically designed so that **no-one** is left behind.

The implementation of this policy aligns directly with our national vision under the Pathway for the Development of Samoa FY2026/27 – FY2030/31 and our broader digital and economic strategies. It reflects our commitment to honoring regional frameworks, while adhering to international standards for identity and data protection.

I extend my sincere gratitude to the Samoa Bureau of Statistics (SBS), government ministries, civil society organisations, Pulega mamalu i nuu ma afioaga, and our international development partners, and the World Bank for their unwavering commitment to bringing this vision to life.

I invite public institutions and private sector partners and all Samoans to embrace this Policy as we build a safer, more inclusive, and prosperous digital identification future together.

(Hon. Moefa'auvao Julius Ah Kui Tafuna'i.)

Minister for the Samoa Bureau of Statistics.

ACRONYMS & ABBREVIATIONS

National Institutions & Systems

- CBS – Central Bank of Samoa
- MOF – Ministry of Finance
- NDID – National Digital Identification
- NDIDS – National Digital Identification System
- OEC – Office of the Electoral Commissioner
- SBS – Samoa Bureau of Statistics
- SDIN – Samoa Digital Identification Number
- SOE – State-Owned Enterprise

International Development Partners

- UNDP – United Nations Development Programme
- WB – World Bank

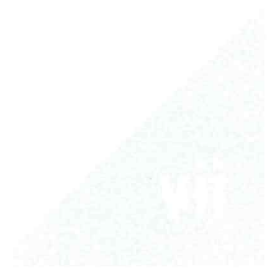
Digital Identity Standards & Frameworks

- ABIS – Automated Biometric Identification System
- API – Application Programming Interface
- CRVS – Civil Registration and Vital Statistics
- DFS – Digital Financial Services
- e-KYC – Electronic Know Your Customer
- ICAO – International Civil Aviation Organization (e-passport & biometric standards)
- ICT – Information and Communication Technology
- ID – Identification
- ISO – International Organization for Standardization
- KYC – Know Your Customer
- MFA – Multi-Factor Authentication
- MTTD – Mean Time to Detect
- MTTR – Mean Time to Respond
- NIST – National Institute of Standards and Technology (biometrics & cybersecurity benchmarks)
- OTP – One-Time Password
- OWASP – Open Web Application Security Project (web security standards)
- PKI – Public Key Infrastructure
- SSL/TLS – Secure Sockets Layer / Transport Layer Security
- ToR – Terms of Reference
- WCAG – Web Content Accessibility Guidelines (digital accessibility standards)

DEFINITIONS

- **Assisted Registration** - the registration process whereby an eligible person who requires support due to disability, age, literacy limitations, geographic isolation, or other barriers receives authorised assistance from a designated registration officer or approved official to complete enrolment in the NDID system.
- **Authentication** – The process of confirming the identity of a registered person using biographic, biometric, or digital credentials.
- **Automated Biometric Identification System (ABIS)** – The central biometric deduplication mechanism of the NDID system, used to compare biometric data (such as fingerprints or facial images) against the national database to detect and prevent duplicate registrations, thereby ensuring the uniqueness and integrity of each registered identity.
- **Biometric Data** – Personal characteristics used for identification, including facial images, fingerprints, and specimen signatures (as defined in the NDID Act 2024).
- **Civil Registration System** – The official system responsible for the continuous and permanent recording of vital events, including births, deaths, and marriages, in accordance with the Births, Deaths and Marriages Registration Act.
- **Civil Registration and Vital Statistics (CRVS)** – The national framework comprising the Civil Registration System (CRS), which records vital events such as births, deaths, and marriages, and the statistical processes that generate official vital statistics from those records. CRVS provides the legal foundation for identity in Samoa.
- **Continuous Registration** - the ongoing enrolment of eligible persons into the NDID system following the completion of the Mass Registration phase, including new residents, late applicants, and individuals updating or correcting their registration information.
- **Credential** – A physical or digital proof of identity issued under the NDID system, including the Samoa Digital Identification Number (SDIN), tokens, physical ID card, and digital ID.
- **Data Processor** – Data Processor means any public or private entity that processes National Digital Identification (NDID) data solely on behalf of and under the documented instructions of the Registrar General or designated authority, and which does not determine the purposes or means of such processing.
- **Digital Identity (NDID)** – A secure, technology-enabled identity issued under the National Digital Identification System (NDIDS) to each registered person in Samoa, consisting of a unique Samoa Digital Identification Number (SDIN) and associated digital or physical credentials used for identity verification and authentication.
- **Inclusion** – Ensuring that all eligible persons, including women, youth, people with disabilities, and those in rural and remote communities, can register and use the NDID system.
- **Level of Assurance (LoA)** – A measure of the degree of confidence that the person claiming an identity is the rightful holder of that identity, defined by the strength of registration and authentication processes.
- **Mass Registration:** means the one-time, nationwide registration campaign conducted at the commencement of NDID implementation to establish the foundational Identity Database, during which eligible persons are enrolled, verified, and assigned a Samoa Digital Identification Number (SDIN)
- **National Digital Identification System (NDIDS)** – is a secure, government system for uniquely identifying and authenticating individuals to access services, based on consent, privacy, and legal protection.
- **National Digital Identification Advisory Board** – The oversight body established under the NDID Act 2024 to provide strategic guidance and accountability for the NDID system.
- **Relying Party** – Any government ministry, state-owned enterprise, statutory body, regulated private sector organisation, or other entity formally authorised under the NDID Act and Regulations to use the National Digital Identification (NDID) system for identity verification and authentication. This may include designated government service points at district level, such as District Council Offices (Fono Fa'avae), where formally authorised under applicable protocols.

- **Registrar General** – The statutory authority responsible for administering the NDID system, as designated under the NDID Act 2024.
- **Samoa Digital Identification Number (SDIN)** – The unique, lifelong number assigned to each registered person under the NDID system.
- **Token** – A privacy-enhancing substitute for the SDIN that can be used in transactions to protect the underlying identifier from unnecessary exposure.



1. EXECUTIVE SUMMARY

This Policy provides a roadmap for the national adoption of the SDIN — guiding the process from system establishment and legal alignment to population registration, issuance of credentials, and long-term institutional governance.

The Policy sets out an implementation framework structured around the national mass registration process. Short-term priorities focus on readiness and preparatory measures prior to mass registration; medium-term priorities guide implementation during the mass registration phase; and long-term and ongoing measures ensure system consolidation, continuous registration, and sustainable governance beyond mass enrolment.

The Policy is structured around six core pillars:

- 1) Legal, Regulatory and Governance – clarity of roles, accountability, and oversight.
- 2) Verification and Compliance – robust assurance levels, credential standards, and audits.
- 3) Inclusive and Equitable Access – inclusive and continuous registration and outreach to women, youth, persons with disabilities, and rural communities.
- 4) Security, Privacy and User Protection – protection of data, user consent, and grievance mechanisms.
- 5) Interoperability, Standards and Infrastructure – interoperability across public and private systems, supported by resilient digital infrastructure.
- 6) Capacity, Monitoring and Sustainability – building institutional capability, financing, and monitoring frameworks.

Through these pillars, the Policy provides an implementation roadmap:

- Target 1 – Institutional setup and legal alignment.
- Target 2 – Mass registration and credential issuance.
- Target 3 – continuous registration through CRVS.
- Target 4 – rollout in priority services (health, finance, social protection, taxation, passports, licensing).
- Target 5 – cross-sector interoperability with ministries, SOEs, and private sector.
- Target 6 – consolidation, monitoring, and regional/global interoperability.

The NDID is a cornerstone of Samoa's digital transformation, enabling secure access to healthcare, education, financial services, and social protection. By embedding inclusion, privacy, security, and resilience into its design, the Policy ensures that no one is left behind from participating in Samoa's digital future and the wider digital economy.

2. INTRODUCTION/PREAMBLE

The National Digital Identification (NDID) Policy sets Samoa's strategic direction for building a trusted and inclusive national identity system. It represents a shift from traditional paper-based identification toward a secure, technology-enabled platform designed to serve people wherever they live — from urban centres to rural and remote communities.

NDID ensures that every eligible Samoan citizen and resident can obtain a verifiable identity that is recognised across government and private sector services. By strengthening how identity is confirmed and protected, the system aims to make everyday interactions — such as accessing healthcare, education, financial services, and social support — simpler, safer, and more reliable for individuals, families, and communities.

WHAT?

What is a National Digital Identification System?

Globally, the World Bank's Identification for Development (ID4D) defines a digital ID system as “a foundational system that provides proof of identity to all residents, uniquely identifying individuals and enabling them to access services and exercise rights.”

In Samoa, the NDID system embodies this principle by assigning every registered person a SDIN. The system is made up of four integrated components:

- Civil Registration and Vital Statistics (CRVS) – the legal foundation for identity through births, deaths, and marriages.
- Identity Database – storing biographic data and issuing SDINs.
- Biometric Database – for adults 18 years and above, ensuring uniqueness and preventing fraud through fingerprints, facial images, and specimen signatures.
- Authentication Services – allowing individuals to securely prove their identity across services, both online and offline.

This architecture ensures that NDID is inclusive, continuous, and permanent, and that it serves as a trusted backbone for service delivery, statistics, and governance.

WHY?

Why have a National Digital Identification Policy?

While the Act and Regulations provide the legal foundation, the Policy is the mechanism for action. It translates law into coordinated strategies by:

- Establishing procedures for continuous registration and outreach, particularly to vulnerable groups.
- Setting standards for authentication and service interoperability across government and private sectors.
- Embedding safeguards for data protection, consent, and grievance redress.
- Defining clear roles and responsibilities for institutions and stakeholders.
- Ensuring coherence by linking NDID to broader national priorities in digital transformation, financial inclusion, and social protection.

In short, the Policy ensures that NDID does not remain a legal framework on paper, but becomes a living system adopted and trusted by all Samoans.

WHY NOW?

As Samoa advances its digital transformation and strengthens resilience to climate and economic shocks, a trusted digital identity system is emerging as a foundational element of national Digital Public Infrastructure (DPI).

Digital Public Infrastructure refers to the core digital systems that enable secure, inclusive, and efficient service delivery on a national scale. Just as roads and electricity underpin physical development, digital identity underpins participation in the digital economy, access to services, and national resilience.

Without a unified digital identity system:

- Government services remain fragmented and difficult to integrate.
- Individuals face repeated identity checks across agencies.
- Social protection and disaster response delivery can be delayed.
- Financial inclusion and digital service uptake are constrained.
- Cybersecurity and data governance risks increase.

NDID establishes a secure, verifiable identity layer for Samoa — forming the identity foundation of the country's digital public infrastructure ecosystem.

Its implementation is timely due to:

1. **Legislative framework and readiness** – The enactment of the National Digital Identification Act (2024) and accompanying Regulations (2025) establishes a comprehensive legal foundation for immediate implementation.
2. **Disaster and Social Protection Resilience** – A robust NDID system will enable rapid, verified identification of individuals and households affected by disasters, supporting timely delivery of emergency assistance, social protection benefits, and recovery services. This includes the ability to operate in low-connectivity environments and maintain continuity of identity services during disruptions.
3. **Digital transformation momentum** – Alignment with Samoa's ICT Sector Plan 2022/23–2026/27 ensures NDID is central to e-government, digital economy and cyber resilience priorities.
4. **Financial and Institutional Support** – The Samoa Finance Sector Resilience and Development Project (SFSRDP), financed by the World Bank, allocates US\$12 million to support NDID development and integration with Civil Registration and Vital Statistics (CRVS) systems.
5. **Infrastructure readiness** – Investments in submarine cable connectivity, data centre upgrades, and high mobile penetration provide the necessary infrastructure for secure, nationwide digital services.
6. **Regional leadership and Inclusivity** – Samoa has the opportunity to lead the Pacific in implementing a rights-based digital ID system, setting a benchmark for inclusivity, governance, and trust.

The NDID system will operate as part of Samoa's broader digital ecosystem, aligned with national strategies on cybersecurity, digital infrastructure, and ICT development, ensuring coherence across government systems and long-term sustainability.

3. PURPOSE AND OBJECTIVES

Purpose

To provide a national framework for establishing, managing, and sustaining a trusted and inclusive digital identity system that underpins secure service delivery, supports private sector innovation, and ensures equitable participation in Samoa's digital economy.

Vision

"A Samoa where everyone can be seen, served, and supported through a secure digital identity that protects rights and connects people to the services they need."

Mission

To deliver a rights-based National Digital Identification system by:

- Ensuring a unique and reliable identity for every citizen and resident.
- Embedding privacy, security, and consent in all processes.
- Promoting equitable access, with a focus on women, youth, people with disabilities, and rural communities.
- Enabling seamless and secure interoperability across government services, civil registration systems, and regulated private sector platforms to improve everyday access to essential services.
- Strengthening institutional capacity, local expertise, and technical resilience, while promoting public awareness and education on the value and responsible use of National Digital Identification, to ensure long-term sustainability, trust, and meaningful participation.

Objectives

1. Strengthen Samoa's legal and governance framework to ensure accountability, transparency, and effective oversight of the NDID system.
2. Establish a secure, consent-based identity verification ecosystem that enhances trust and protects user rights.
3. Promote equitable access and ensure no one is excluded from registration or use of NDID.
4. Guarantee data privacy, cybersecurity, and user protection through robust technical and legal safeguards.
5. Enable interoperability and integration across civil registration, government services, health, education, finance, and private sector systems.
6. Build institutional readiness, technical capacity, and sustainable governance structures to ensure long-term system resilience, including continuity of identity services during disasters, emergencies, and climate-related events.
7. Support national disaster preparedness and response by enabling rapid, trusted identification for emergency assistance, social protection and recovery services.

Values and Guiding Principles

The NDID system will be implemented in line with the following values and guiding principles:

1. **Universality and Inclusivity** – registration is compulsory, continuous, and permanent, ensuring every person is covered, with special focus on women, youth, persons with disabilities, and rural communities.
2. **Trust, Confidentiality, and Human Rights** – protection of personal data, respect for privacy, and upholding human rights are non-negotiable foundations of the system.
3. **Accuracy and Integrity** – uniqueness of identity will be guaranteed through deduplication, verification, and authentication mechanisms.
4. **Transparency and Accountability** – governance of the NDID system will be open, accountable, and responsive to citizens, including accessible grievance mechanisms.

5. **Integration** - The NDIDS is structurally integrated with the Civil Registration System and associated national databases (health and passport), ensuring a unified and legally grounded identity architecture.
6. **Interoperability** – The NDIDS enables secure, standards-based data exchange and authentication across authorised government entities, state-owned enterprises, and accredited relying parties, through regulated interfaces and verification services in accordance with the Act and Regulations.
7. **Resilience and Sustainability** – the system will be designed to withstand natural disasters, technological changes, and evolving national needs.
8. **Innovation and Digital Transformation** – The NDID serves as a core pillar of Samoa's Digital Public Infrastructure (DPI), providing the trusted identity layer that enables secure e-government services, digital payments, interoperable data exchange, and innovation across the digital economy.

This includes the responsible and governed use of emerging technologies to support system efficiency while protecting user rights

This Policy does not create new legal obligations beyond those established under the National Digital Identification Act 2024 and supporting Regulations. Rather, it provides a strategic and operational framework to guide implementation, ensuring that existing legal provisions are applied in a coordinated, consistent, and effective manner across all participating entities.

4. MANDATE / LEGAL FRAMEWORK

This policy derives its authority from the National Digital Identification Act 2024, which:

- Establishes the NDID system and its components (Civil Registration, Identity Database, Biometric Database, Authentication).
- Assigns functions to the Registrar General and creates the National Identification Advisory Board.
- Mandates inclusive and continuous registration, user rights, data protection, and penalties for misuse.

The National Digital Identification Regulations 2025 further operationalise the Act by setting out:

- Registration procedures (SDIN issuance, tokens, and physical ID cards).
- Authentication standards for relying parties, including online services.
- Data protection obligations, with specific measures for the Biometric Database and the Registrar General's role in safeguarding confidentiality.
- Grievance processes to ensure citizens can challenge errors or misuse.
- Offences and penalties for fraud, unauthorised disclosure, or breaches of security.

Together, the Act and Regulations ensure the NDID system is legally grounded, operationally enforceable, and rights-protective.

National Policies, Strategies and Plans

The NDID Policy is anchored within Samoa's broader national development and digital transformation agenda. Several key policy instruments provide the strategic context:

- **Pathway for the Development of Samoa 2021/22-2025/26** - outlines Samoa's long-term development trajectory, emphasising inclusive growth, good governance, and resilience. The NDID supports this by ensuring all citizens have a secure identity to access services and participate fully in national development.
- **Samoa's Digital Pathway 2023-2030** - positions digital transformation as a national priority, highlighting the role of secure digital identity in enabling e-government, e-commerce, and innovation.
- **Samoa ICT Sector Plan 2022/23-2026/27** - identifies digital ID as a foundational enabler of ICT-driven service delivery, interoperability of government platforms, and private sector development.
- **National Social Protection Policy Framework 2023** - strengthens the use of NDID as a trusted mechanism for identifying and verifying beneficiaries, improving the targeting, delivery, and monitoring of social assistance programmes, including during disasters and emergency response.
- **Samoa National Cybersecurity Strategy (2025/26 – 2030/31)** - establishes the national framework for protecting digital systems and critical information infrastructure, within which the NDID system operates as a secure and resilient identity platform, supported by coordinated cybersecurity measures including incident response and threat management.
- **Samoa National eCommerce Policy (2025-2030)** - identifies digital identity as a key enabler for secure online trade, payments, and consumer protection. The NDID provides the trusted credentials needed to unlock growth in Samoa's digital economy.
- **National Communications and Information Technology Policy 2025/26 – 2030/31** - provides the national framework for digital transformation, including digital government, interoperability, and digital economy development. NDID acts as a foundational enabler within this framework, providing secure and verifiable identity services required for trusted digital interactions across government and private sector systems.

Laws and Regulations

NDID depends on a strong legal foundation that integrates identity with Samoa's broader governance and regulatory systems.

Primary Legislations

- **Births, Deaths and Marriages Registration Act 2002** – provides the civil registration basis for continuous and universal identity coverage.
- **Statistics Act 2015** – empowers the Samoa Bureau of Statistics to manage data ethically and securely, enabling integration of NDID into the national statistical system.
- **Electronic Transactions Act 2008** – grants legal recognition to electronic records and signatures, validating digital credentials and online authentication.
- **Immigration Act 2004** – defines categories of residents and non-citizens, ensuring that NDID issuance for foreign nationals is aligned with immigration status.
- **Citizenship Act 2004** – governs acquisition and recognition of citizenship, ensuring NDID registration is grounded in nationality law.
- **Crimes Act 2013** – provides offences and penalties for identity fraud, unauthorised access to electronic systems, data interference, and misuse or unlawful disclosure of personal information, supporting enforcement and integrity of the NDID system.

Supporting Acts

- **Money Laundering Prevention Act 2007** – requires strong identity verification for compliance with financial integrity standards; NDID provides the secure KYC mechanism.
- **Labour and Employment Relations Act 2013** – regulates foreign workers and permits; NDID supports lawful employment verification.
- **Tax Administration Act 2012** – defines residency for taxation purposes; NDID streamlines compliance by providing a single verified identity.
- **Electoral Act 2019** – sets residency requirements for voter registration; clarifies that while all registered persons may hold an SDIN, voter eligibility is determined separately under electoral law and does not apply to all SDIN holders.

Regional Agreements

Samoa's NDID is not an isolated initiative but part of a wider Pacific vision for digital cooperation and resilience. Regional frameworks provide the political momentum, technical direction, and interoperability requirements needed for successful implementation:

- **Pacific Digital Economy Strategy (2021–2030)** – This strategy sets a regional roadmap for integrating Pacific economies into the global digital marketplace. NDID provides Samoa with the trusted digital identity backbone needed to enable secure e-commerce, digital payments, and cross-border services.
- **Pacific Islands Forum “Blue Continent” Vision** – The Blue Continent frames the Pacific as a region united by shared ocean resources and digital connectivity. NDID supports Samoa's role in this vision by ensuring all citizens can participate in the digital economy and access regional services such as mobility, education, and financial inclusion.
- **Regional CRVS and legal identity initiatives** – Samoa's NDID builds on regional efforts to improve civil registration and strengthen identity systems. These provide technical guidance, donor alignment, and peer learning, which are essential for overcoming implementation challenges.

International Agreements

International frameworks provide Samoa with the benchmarks, legitimacy, and safeguards required for NDID to be trusted globally:

- **United Nations Sustainable Development Goals (SDG 16.9)** – Legal identity is recognised as a development right. By implementing NDID, Samoa contributes directly to this global target, reinforcing its international reputation and access to donor support.
- **Principles on Identification for Sustainable Development (World Bank, 2018)** – These principles guide NDID implementation by ensuring inclusivity, security, and interoperability. Aligning with them helps Samoa avoid common pitfalls and ensures donor-funded investments meet global best practice.

- **International Civil Aviation Organization (ICAO) Standards** – Secure ID credentials that meet ICAO standards enable Samoan citizens to use their national ID in travel, immigration, and cross-border recognition. This gives NDID international credibility and utility.
- **ITU, OECD, and ISO Standards** – Technical standards for interoperability, cybersecurity, and biometrics ensure NDID systems can exchange data securely and remain future-proof. Compliance with these standards is critical for building trust with international partners and service providers.

To ensure that Samoa's NDID system is trusted, future-proof, and globally interoperable, its design and operation will be guided by recognised international standards. These cover areas such as biometric data formats, digital identity assurance, information security, data protection, accessibility, and interoperability. Aligning with these benchmarks not only strengthens the technical robustness of the NDID, but also positions Samoa to meet international obligations under the SDGs, human rights conventions, and regional digital economy frameworks. (Refer Annex B)

- **Human rights conventions (ICCPR, CRPD, CEDAW, CRC)** – NDID protects the right to recognition before the law and ensures equal access to services. Embedding human rights in NDID implementation safeguards against exclusion, discrimination, and misuse of personal data.

By grounding NDID in these international commitments, Samoa ensures that its system is not only a national tool for service delivery, but also a globally trusted identity platform that protects rights, supports economic growth, and opens opportunities for international cooperation.

5. SCOPE OF APPLICATION

The scope of this Policy extends to both the use and protection of the SDIN and all associated digital or physical credentials. It ensures that every stakeholder—government, state-owned enterprises, private sector, civil society, development partners, and individuals—upholds the obligations of the National Digital Identification Act 2024 and NDID Regulation 2025, while contributing to a trusted, inclusive, and rights-based national identity ecosystem.

This Policy applies to all entities and actors operating within the National Digital Identification (NDID) framework.

Government Alignment and Interoperability

Government Ministries, Authorities and State-Owned Enterprises are encouraged to align their digital systems and service processes with the NDID framework to enable secure authentication, verification, and information exchange. This alignment shall follow the guidance of the Registrar General and support each entity's broader digital transformation and e-governance strategies.

The Registrar General, supported by the NDID Advisory Board, will work collaboratively with government entities to strengthen interoperability frameworks, provide technical guidance, and ensure consistency with existing information-management systems and sectoral initiatives.

Data processors operate under the authority of the Registrar General and shall not access, use, disclose, or retain NDID data except as expressly authorised. All data processing activities shall be subject to contractual, technical, and audit controls in accordance with the Act and Regulations.

The Advisory Board will periodically review and report on progress toward government alignment and interoperability to promote coordinated implementation, transparency, and continuous improvement across the public sector.

1. Government Ministries

Role	
• Lead national registration and verification efforts in collaboration with the Registrar General. • Incorporate NDID-enabled authentication and verification within key sectors such as health, education, taxation, electoral, and social protection. • Act as authorised relying parties and/or data processors under the NDID Act 2024, ensuring compliance with data-protection, consent, and security standards. • Provide oversight, coordination, and policy stewardship for the overall NDID system.	
Impact	Benefits
– Strengthens accuracy and reliability of identity data across government. – Reduces duplication of records and fraudulent claims. – Enables data-driven planning and resource allocation.	– Faster and more reliable public services. – Lower operational costs and improved efficiency. – Increased public trust in government systems.

2. State-Owned Enterprises (SOEs)

Role
• Utilise NDID-based authentication for customer identification in essential services (electricity, water, telecommunications, etc.). • Operate as authorised relying parties under the standards established by the NDID Regulations. • Uphold privacy and data-protection obligations in identity-related processes.

Impact	Benefits
– Reduces identity misuse and fraud in billing and service delivery. – Enables accurate verification for subsidies and targeted benefits. – Enhances operational efficiency and financial accountability.	– Improved customer satisfaction and confidence in public utilities. – Improved financial sustainability by reducing revenue leakage. – Increased customer trust in state services.

Private-Sector Participation

Private-sector organisations in regulated industries such as banking, telecommunications, insurance, and utilities are encouraged to participate as authorised relying parties within the NDID ecosystem. Participation shall be subject to approval by the Registrar General and adherence to applicable privacy, data-protection, and consent standards under the National Digital Identification Act 2024 and the NDID Regulation 2025.

The NDID Advisory Board will engage with industry bodies to support interoperability, promote innovation, and ensure alignment with national digital-governance objectives.

3. Private Sector Organisations (Banks, Telecoms, Utilities, etc.)

Role	
	• Act as regulated relying parties (Regulations 6–8). • Use NDID for e-KYC (electronic Know Your Customer) in financial services, SIM registration, and secure transactions. • Ensure compliance with data protection and consent requirements (Act, Part 7).
Impact	Benefits
– Reduces compliance costs for customer due diligence. – Expands financial inclusion, especially for rural and underserved communities. – Strengthens consumer protection by minimising identity fraud.	– Lower costs and risks of onboarding customers. – Faster access to banking, credit, and mobile money. – Growth of digital services and innovation in fintech.

4. Civil Society Organisations

Role	
• Support community awareness, outreach, and public education on the purpose, safeguards, and benefits of the NDID system. • Advocate for inclusive registration and equitable access, particularly for women, youth, persons with disabilities, and rural communities. • Monitor human rights protections, privacy safeguards, and grievance redress mechanisms in line with sections 23–24 of the Act. • Collaborate with District Councils (Fono Fa’avae) to facilitate culturally and community appropriate engagement and feedback.	
Impact	Benefits
– Strengthens community trust and transparency in the NDID system. – Promotes rights-based implementation and social accountability.	– Increased citizen awareness and informed participation. – Greater equity in registration and service access.

– Ensures vulnerable and underserved populations are not excluded.	– Stronger community ownership of digital identity initiatives.
--	---

5. Development Partners

Role	
• Provide technical assistance, capacity building, and institutional strengthening support. • Support system design, cybersecurity standards, and interoperability frameworks aligned with international best practice. • Assist in financing, monitoring, and evaluation of NDID implementation. • Facilitate knowledge exchange and regional collaboration on Digital Public Infrastructure.	
Impact	Benefits
– Enhances institutional capability and implementation readiness. – Strengthens alignment with global standards on data protection and digital identity. – Supports sustainable and resilient system development.	– Accelerated implementation and risk mitigation. – Improved governance and compliance frameworks. – Long-term sustainability and regional leadership positioning.

6. Relying Parties and Data Processors

Role	
• Relying parties (government or private sector entities) use the NDID for identity verification and authentication (Act, Part 6; Regulations 6–8). • Data processors shall process NDID data strictly under the authority and instruction of the Registrar General and shall not access, use, disclose, retain, or repurpose such data beyond what is expressly authorised. under the Act (sections 45–50).	
Impact	Benefits
– Ensures consistent and secure use of NDID across all sectors. – Protects individuals by mandating compliance with data security and consent standards. – Creates accountability for handling personal data.	– Clear legal framework and guidelines for operation. – Reduced liability through compliance with regulated safeguards. – Opportunities to innovate with NDID-enabled services.

7. Individuals

Role	
• Register with the NDID to obtain a unique Samoa Digital Identification Number (SDIN) and associated credentials. • Provide accurate biographic information and, from age 18, biometric data to ensure uniqueness and trust. • Use NDID credentials (physical card, digital token) to access public and private sector services securely. • Exercise their rights to consent, data protection, and grievance redress in line with policy safeguards.	

Impact	Benefits
– Empowers individuals with a legally recognised identity that is secure, portable, and verifiable. – Enhances inclusion by ensuring all citizens and eligible residents can participate in the digital economy and access essential services. – Builds trust through strong privacy protections, consent mechanisms, and avenues for redress in cases of misuse.	– Universal access to government and private sector services (healthcare, education, banking, social protection). – Greater control over personal data, with transparency and accountability in how identity is used. – Improved convenience and security in daily transactions, from e-services to financial access.

This Policy defines the strategic and operational framework for NDID implementation. Detailed technical design, system architecture, and implementation sequencing shall be further specified through regulations, technical standards, and implementation guidelines issued by the Registrar General in coordination with relevant authorities.

6. FOUNDATIONAL FEATURES OF THE NDID SYSTEM

The NDID has been structured to ensure every registered person in Samoa receives a secure, lawful, and reliable identity credential, in accordance with the legal and operational standards established under the NDID Act 2024 and the NDID Regulations 2025.

System-Generated, Non-Intelligent Identifier (SDIN)

The SDIN is assigned through an automated generation process and contains no encoded personal information. This supports privacy protection, minimises the risk of profiling, and aligns with the Act's requirements for the safe and lawful handling of identity data.

The SDIN is unique, non-recycled, and permanently associated with the registered individual. Where an SDIN is temporarily suspended or deactivated in accordance with the Act and Regulations, reactivation will restore the same SDIN, preserving continuity of identity and preventing reassignment to another person.

Single, Persistent Identity Record

Each eligible person is recorded once in the NDID system and retains the same SDIN throughout their lifetime. Deactivation of an identity status does not result in the issuance of a new SDIN.

Biometric de-duplication for adults (where applicable) ensures that individuals cannot be registered multiple times, promoting the accuracy, integrity, and uniqueness of identity as required under the Act.

Digital-First Credential

The NDID credential is primarily issued and maintained in digital form, consistent with the verification and authentication functions enabled under the Act. Printed or physical representations may be made available for accessibility, but they are not the basis of identity validity.

Validity Based on Secure Verification

Authentication of an individual relies on approved verification methods set out in the Regulations—such as biographic checks, biometric matching (for adults), one-time passwords, and digital tokens—rather than the physical presentation of a number or document. This supports trusted access across government and regulated services.

Functionality in Connected and Unconnected Environments

The NDID system supports both online and offline authentication modes, enabling service continuity in areas with limited connectivity and ensuring equitable access across Samoa, as required under the inclusion and service access provisions of the Regulations.

Disaster Resilience and Emergency Use

The NDID system shall function as critical national digital infrastructure during disasters, public health emergencies, and system disruptions.

The system shall:

- enable rapid identification and verification of affected individuals for emergency response and humanitarian assistance;
- support offline and low-connectivity authentication mechanisms in disaster-affected or remote areas;
- ensure continuity of identity services, including authentication and verification, during system or infrastructure disruptions;
- provide mechanisms for recovery and reissuance of credentials where individuals have lost documentation due to disasters; and
- support coordination with authorised disaster response systems, in accordance with the Act and applicable safeguards.

All emergency use shall remain subject to lawful authority, necessity, proportionality, and data protection requirements.

Not an Indicator of Citizenship or Immigration Status

The NDID establishes identity for authentication and service access purposes but does not grant or confirm nationality, residency class, or immigration status. These remain governed by their respective statutory frameworks.

Inclusive Enrolment Pathways

Alternative verification and enrolment procedures are provided for individuals who may not be able to supply biometric data or use digital tools. This ensures nondiscrimination and supports the Act's obligations relating to equitable access and protection of vulnerable groups.

Strong Security, Encryption, and Data Separation

Biographic and biometric data are collected, stored, and managed under strict security controls, including encryption, access restriction, audit logging, and the separation of biometric records from biographic information, in line with Part 7 of the NDID Act and the technical safeguards mandated by the Regulations.

Designed for Cross-Sector Interoperability

The SDIN serves as a foundational identifier that can be used across authorised government entities and accredited relying parties. The Regulations outline how systems must interconnect through standardised APIs, secure data exchange protocols, and approved verification services to enable consistent and lawful identity authentication.

The NDID system shall implement a centralised integration framework, including an API gateway, as the exclusive interface for all identity verification and authentication requests between the NDID platform and authorised entities.

This framework shall enforce standardised protocols, access controls, and audit requirements, ensuring that all system interactions are secure, traceable, and compliant with the National Digital Identification Act 2024 and supporting Regulations.

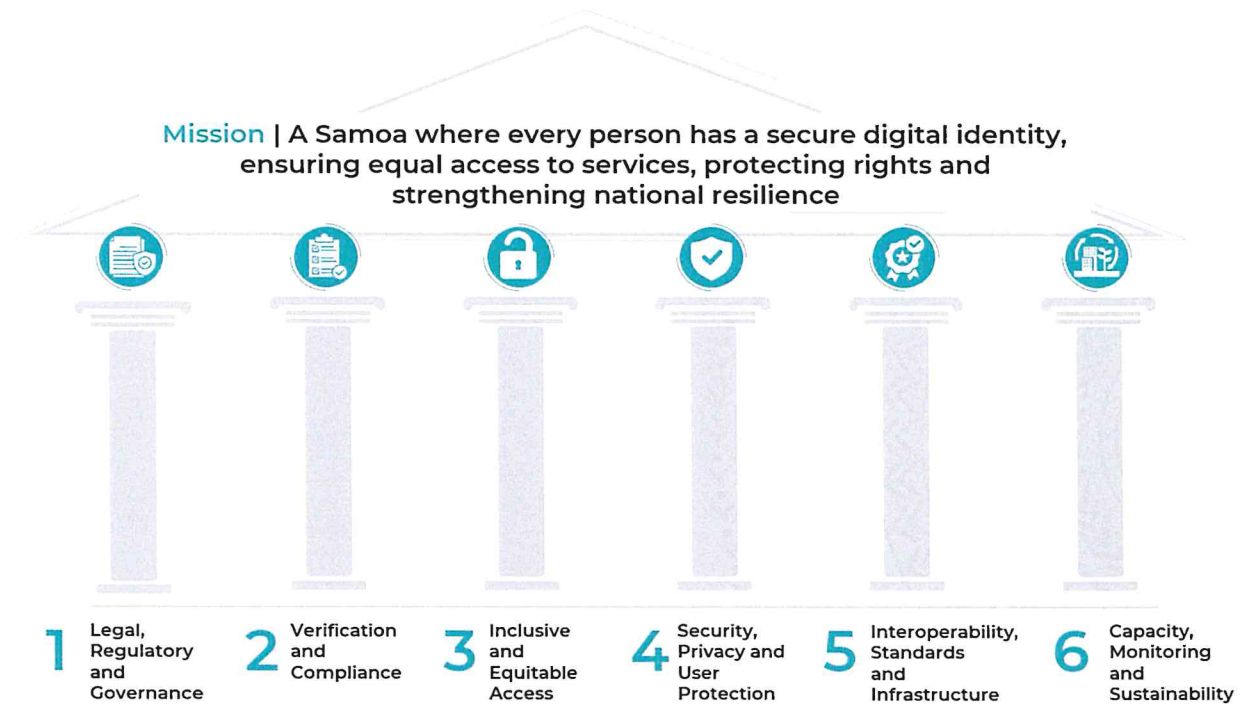
The Registrar General shall establish and maintain an interoperability governance framework, in coordination with the Ministry responsible for Communications and Information Technology and relevant ICT authorities.

This framework shall:

- define technical standards and API protocols
- establish onboarding and certification requirements for relying parties
- enforce compliance through monitoring, audit, and reporting mechanisms
- ensure alignment with national ICT architecture and cybersecurity standards

7. POLICY STATEMENTS

The NDID Policy is structured around six interdependent pillars that translate Samoa's digital identity vision into coordinated action.



Collectively, they establish the legal, operational, technical, and institutional foundations required to achieve a trusted, inclusive, and sustainable digital identification system.



Objective:

Maintain legal alignment, clear roles, and strong governance oversight for NDID.

Strategic Goal

To operationalise the NDID Act 2024 and Regulation 2025 through an enforceable governance framework that guarantees legal compliance, institutional accountability, and effective oversight.

Corresponding Strategies

- Implement Legal and Regulatory Framework
- Define and Operationalise Roles and Responsibilities
- Establish Oversight and Accountability Mechanisms
- Regulate Data Sharing and Credential Issuance
- Strengthen Cross-Sector Governance

**Objective:**

Enforce robust verification standards, ensure compliance with NDID protocols, and build trust through consistent application of assurance levels and audits.

Strategic Goal

To establish a secure, trusted, and transparent identity verification and compliance framework that ensures the authenticity of information, prevents misuse, and upholds integrity across all NDID operations.

Corresponding Strategies

- Establish and Maintain the National Levels of Assurance (LoA) Framework
- Enforce standards for credential issuance and lifecycle management
- Implement continuous compliance auditing and quality assurance
- Enforce legal obligations, accountability, and penalties

**Objective:**

Ensure all Samoans — including persons with disabilities, older persons, women, youth, rural communities and other underserved populations — have continuous and equitable access to NDID services

Strategic Goal

To ensure that all eligible individuals — including those in rural areas, people with disabilities, women, and youth — have equitable access to registration and NDID-related services through inclusive design, outreach, and awareness initiatives.

Corresponding Strategies

- Expand nationwide outreach and mobile registration coverage
- Enable inclusive and assisted registration options
- Remove language, communication, and accessibility barriers
- Monitor and promote equity in access and participation



Objective:

Protect NDID data and user rights through continuous safeguards, oversight, and redress.

Strategic Goal

To safeguard personal information and uphold individual rights through robust data protection measures, privacy-by-design principles, and user protection mechanisms that foster public trust in the NDID system.

This includes ensuring the system can operate securely during disasters and emergencies, and that emerging technologies such as Artificial Intelligence are used responsibly under clear governance and human oversight.

Corresponding Strategies

- Strengthen data protection and information security
- Enforce user consent, rights, and transparency
- Establish accessible and accountable grievance and redress mechanisms
- Institutionalise continuous risk management and system resilience and disaster response readiness.
- Govern the responsible use of emerging technologies, including Artificial Intelligence.



Objective:

Ensure interoperability of NDID with national systems, develop and strengthen interoperability standards, and build resilient infrastructure to support secure and sustainable service delivery.

Strategic Goals

To develop and maintain a reliable, scalable, and secure technical infrastructure for the NDID system, underpinned by national standards that enable consistent authentication, data integrity, and operational efficiency.

This includes ensuring infrastructure supports offline verification, disaster recovery and continuity of identity during emergencies.

Corresponding Strategies

- Establish and enforce national interoperability standards
- Strengthen cross-sector alignment and compliance readiness
- Build and sustain a resilient and secure NDID infrastructure
- Test, Validate, and Scale Interoperability Use Cases
- Strengthen regional and global interoperability
- Establish coordinated integration standards, under the Registrar General and relevant ICT agencies, to ensure secure and consistent interoperability.



Objective:

Build the institutional, technical, financial, and human capacity required to operate NDID effectively and sustainably, strengthen public understanding and digital literacy, and embed a robust monitoring, evaluation, and learning framework that ensures accountability, transparency, resilience, and continuous improvement.

Strategic Goal

To strengthen institutional capacity, workforce skills, public awareness, and resource management to ensure the long-term financial and operational sustainability, system resilience, effective monitoring, and trusted adoption.

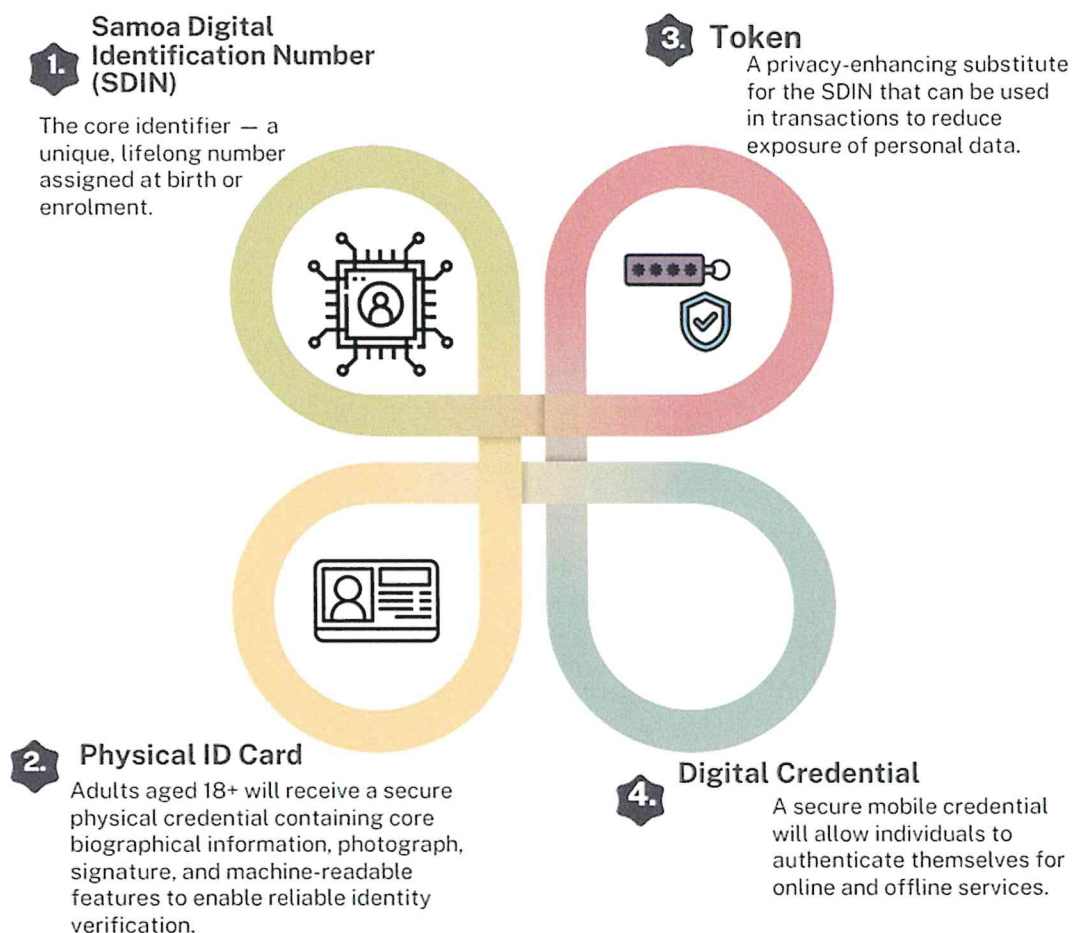
Corresponding Strategies

- Strengthen institutional capacity and workforce readiness
- Develop and Implement National Training, Digital Literacy, and Public Awareness Programs
- Implement Monitoring, Evaluation, and Learning (MEL) framework, including periodic evaluation of system performance, inclusion outcomes and user trust.
- Strengthen coordination, oversight, and implementation management
- Ensure long-term financial and operational sustainability of the NDID system

8. MEANS OF IDENTITY (CREDENTIALS)

When an eligible individual registers under the NDID system and they are assigned a SDIN, based on eligibility (e.g. age, service use), one or more credentials will be issued.

4 means of Identity Credentials



Validity and Renewal

- Credentials are valid for a fixed period (up to 10 years) or until personal details or biometric data (such as photo or fingerprints) need updating.
- The NDID Office will issue reminders ahead of expiry to prompt renewal.
- During renewal, identity and biometric details are re-verified to ensure accuracy.
- Updated credentials automatically replace older versions, maintaining system integrity.



Loss, Theft or Damage

- If a credential (card, token, or digital credential) is lost, stolen, or damaged, the holder must report it promptly to the Registrar General.
- The reported credential will be immediately deactivated to prevent unauthorised use.
- A replacement process will be undertaken, including appropriate verification to confirm the identity of the rightful holder. Where applicable, the associated SDIN will be reactivated, and no new SDIN will be issued.

- Replacement credentials will be issued securely in accordance with the same standards and safeguards applied to initial issuance.



Updates and Changes

- Where a person's name or other personal information has been legally changed, the individual must notify the NDID Office and provide appropriate documentary evidence in accordance with the Act and Regulations.
- Upon verification, the NDID system will update the individual's biographical record accordingly. Biometric records will only be updated where required and in accordance with prescribed procedures.
- Updated credentials will be reissued to reflect the verified changes, following a secure verification process to confirm the rightful holder's identity.
- The SDIN remains unchanged and continues to be permanently associated with the individual, notwithstanding any updates to personal information.



Responsibilities of Credential Holders

- Individuals must keep their credentials secure and must not share, lend, or allow unauthorised use by any other person.
- Credentials may only be used for lawful personal identification and authentication purposes.
- Any loss, theft, suspicious use, or attempted fraud must be reported promptly to the Registrar General. Knowingly making a false report of loss, including intentional destruction or concealment of a credential, may constitute an offence under the Act.
- Users must participate in periodic verification or update processes when requested by the NDID Office to maintain the accuracy and integrity of their records.
- Misuse, lending, alteration, or tampering with credentials constitutes an offence under the National Digital Identification Act 2024 and its Regulations.
- Where a credential or associated SDIN is deactivated due to suspected illegal activity, fraud, or misuse, reactivation may only occur following appropriate investigation and confirmation by the relevant legal or competent authority, in accordance with the Act and Regulations.

9. CONSENT AND CONTROL

The National Digital Identification (NDID) system is founded on individual trust and autonomy. Every person must retain control over how their personal information and identity credentials are accessed, verified, or shared.

Consent and control are therefore central to ensuring that the NDID system remains rights-based, transparent, and secure.

9.1. Principle of Consent

No personal data, SDIN, token, or NDID credential shall be accessed, used, or shared through the NDID system without the explicit, informed, and recorded consent of the individual, except where access is:

- expressly permitted by law; or
- required for the performance of lawful public functions under due process.

Consent must always be

- Freely given – without coercion or undue pressure.
- Informed – based on clear and understandable information.
- Specific – limited to a defined purpose, data type, and timeframe and
- Revocable – able to be withdrawn at any time by the individual.

Data Processors shall not obtain, manage, or override individual consent and may process NDID data only where valid consent has been lawfully obtained by the Registrar General or an authorised Relying Party.

9.2. Informed and Granular Consent

Individuals shall be provided with clear and understandable information before granting consent, including:

- what specific data is being accessed or shared.
- the purpose for which the data is being used.
- which entities or systems will receive, access, or verify the data; and
- how long the access or authorisation will remain valid.

Consent shall be granular, allowing individuals to authorise or restrict different types of data sharing for specific services, including but not limited to:

- health services.
- education and training.
- financial services; and
- social protection or other public services.

As part of the consent process, individuals shall also be informed of the mechanisms available to seek clarification, lodge a complaint, or pursue redress in relation to the use, misuse, or unauthorised access to their personal data or NDID credentials, including the role of the Registrar General and the grievance processes established under the Act.

9.3. Consent Management and Record

All consent transactions shall be managed and recorded electronically within the NDID system to ensure accountability and traceability.

The NDID system shall ensure that:

- every data access or authentication request by a relying party is automatically logged.

- individuals are able to view, manage, and review their current and past consent authorisations; and
- consent records are securely stored as part of the system's official audit trail.

The Registrar General shall oversee this process, with periodic compliance reviews by the NDID Advisory Board.

9.4. Right to Withdraw and Limit Access to an Individuals Identity Records

Individuals may withdraw or limit their consent at any time, through NDID service channels, including:

- online platforms or mobile applications; or
- in person at designated NDID service or registration centers.

Once consent is withdrawn or limited:

- the relying party's access to the individual's data shall be immediately terminated for future requests.
- subsequent verification or authentication attempts for that purpose shall be denied; and
- records of prior access shall remain preserved within the audit log for accountability and oversight purposes.

Withdrawal of consent shall not invalidate the individual's registration or SDIN.

9.5. Exceptional Circumstances

Access to personal data without individual consent may occur only under specific and lawful circumstances, including:

- where required under national law for national security, criminal investigations, or public health emergencies; or
- where ordered by a court or other lawful authority in accordance with due process.

Any access under such exceptional circumstances must be:

- explicitly authorised by the Registrar General.
- fully recorded and justified within the NDID audit log and
- reported to the National Identification Advisory Board as part of periodic oversight and accountability reviews.

9.6. Accountability and Oversight

The Registrar General shall ensure that all NDID operations adhere to consent and privacy safeguards, including the maintenance of comprehensive audit trails of data access, authorisation, and revocation.

The NDID Advisory Board shall review these reports regularly to verify compliance, ensure transparency, and uphold public trust in the NDID system.

10. REGISTRATION PROCESS

The NDID registration process establishes the SDIN as a unique and lifelong identifier for all eligible individuals.

Registration is implemented through three legally distinct mechanisms:

- i. Mass Registration
- ii. Registration at Birth
- iii. Continuous Registration

Each mechanism is governed by specific provisions under the Act.

10.1. Eligible Persons

In accordance with section 18 of the NDID Act, an eligible person for registration is:

- a citizen of Samoa; or
- a person lawfully permitted to reside in Samoa under applicable law

The Samoa Bureau of Statistics is responsible for ensuring that all eligible persons are registered, in accordance with the applicable Act¹ and subject to the Registrar General's lawful discretion.

10.2. Biographical Data Collected (Core Identity Fields)

For each registered individual, the NDID system shall collect and store only the minimum biographic data required by law.

The following nine (9) core biographic fields shall be recorded in the Identity Database, where applicable and available:

1. SDIN and any associated token.
2. name.
3. date of birth.
4. place of birth.
5. sex.
6. home address.
7. names of parents including adoption.
8. date of death; and
9. data relating to issued, revoked or cancelled ID credentials.

No additional fields may be collected unless authorised under law or regulation.

10.3. Mass Registration



A one-time nationwide Mass Registration campaign shall be undertaken at the commencement of NDID implementation to establish the foundational Identity Database.

Mass Registration shall be implemented in accordance with procedures, timelines, and modalities designated by the Registrar General and publicly notified.

During the Mass Registration period:

- All eligible persons aged 18 years and above shall be registered, with the collection of biographic and biometric data (photograph, fingerprints, and signature).
- Biometric data shall be collected only from individuals aged 18 years and above.
- Children under 18 years shall be registered and assigned an SDIN through an approved registration process, ensuring continuity of identity records from birth to adulthood.
- New births occurring during the Mass Registration period shall also be registered and assigned an SDIN through designated procedures determined by the Registrar General, pending full operational integration with the Civil Registration System (CRS).

Registration during this phase shall be conducted independently of the CRS, with subsequent alignment and integration following system upgrades.

The Registrar General shall request and accept official documentary evidence of identity, including:

- a birth certificate issued under the Births, Deaths and Marriages Registration Act 2002 or an equivalent overseas authority
- a passport, certificate of identity, or other recognised identity document issued under the Passports Act 2008 or an equivalent overseas authority
- or alternative official documentation where primary documents are unavailable, as determined by the Registrar General.

Upon verification of identity and data integrity, the Registrar General shall:

- record biographical data in the Identity Database
- record biometric data, where applicable, in the Biometric Database; and
- assign an SDIN and associated credential or token to the registered person.

Measures shall be implemented to ensure inclusive access, including mobile registration services for rural and remote communities.

10.4. Registration at Birth (Post-Mass Registration)



Following the completion of Mass Registration, registration at birth shall be conducted through the Civil Registration System (CRS), in accordance with section 21 of the Act.

- All children born in Samoa shall be registered in the National Digital Identification System (NDIDS) as part of the birth registration process under the Births, Deaths and Marriages Registration Act 2002.
- Lawful notifications of birth submitted through authorised channels, including health facilities and recognised community authorities, shall be recorded in the CRS system and used to initiate registration in the NDIDS.
- Registration at birth shall result in the creation of a corresponding identity record within the NDIDS, without the collection of biometric

data and without the issuance of an ID credential, consistent with the Act.

This approach ensures early inclusion in the national identity system while maintaining alignment with existing civil registration processes.

10.5. Continuous Registration



Following the completion of Mass Registration and associated system upgrades, Continuous Registration shall apply to:

- Eligible persons who were not registered during the Mass Registration period, subject to the discretion and direction of the Registrar General;
- Persons who become eligible for registration after the Mass Registration period; and
- Eligible citizens or lawful residents born overseas.

For Continuous Registration:

- Eligible citizens or residents born overseas shall register directly with the NDID Office in accordance with prescribed procedures.
- For local births, the Civil Registration System shall serve as the primary and ongoing entry point into the NDIDS.
- Updates arising from legally recognised life events, including births, deaths, marriages, adoptions, and name changes, shall be captured through CRVS processes and reflected in the NDIDS.

This approach ensures continuity, accuracy, and legal integrity of identity records across the individual's lifecycle.

10.6. Registration of Children and Persons Requiring Assistance

In accordance with the Act:

- children, persons with disabilities, senior citizens, and other specified persons may be registered by a parent, legal guardian, lawful administrator, or authorised community representative.
- Special measures shall be implemented to ensure accessibility, dignity, and non-discrimination throughout the registration process.

10.7. Implementation Responsibility

The NDID registration process will combine central coordination by the SBS and community-based registration approaches that ensure equitable access across Samoa.

National Coordination

The Registrar General, through the National Identification Division within the Samoa Bureau of Statistics (SBS), will maintain overall responsibility for policy direction, registration standards, and system integrity.

SBS will provide the technical systems, guidelines, and training required for consistent registration practices across all levels.

Community-Level Registration Pathways

To reach every eligible person, NDID registration will be carried out through multiple, community-based access points coordinated under the national framework.

1. Village Registration Hubs

- Designate village councils and community halls as temporary or semi-permanent NDID registration hubs.
- Village representatives (Sui o Nu'u ma Sui Tamaita'i o Nu'u) can assist coordinate enrolment schedules, verify local residents, and assist with community mobilisation.

2. Health Facilities and Schools

- Integrate NDID registration into health clinics, hospitals, and immunisation programs, especially for newborns and children.
- Partner with schools to register youth transitioning to secondary or tertiary levels, ensuring continuity from childhood to adulthood.

3. Mobile Registration Units

- Operate mobile registration teams equipped with portable biometric devices to serve rural villages, coastal communities, and outer islands.
- Mobile units will also conduct home visits for persons with disabilities, the elderly, or those with mobility challenges.

4. Civil Society and Faith-Based Partnerships

- Collaborate with churches, NGOs, disability organisations, and women's committees to support outreach, awareness, and registration drives.
- These groups can help identify unregistered individuals and build trust in the NDID process.

5. District Council Offices (Fono Fa'avae)

- Ofisa o Fono Fa'avae shall serve as community-based facilitation and outreach points to support registration awareness, document pre-verification, and scheduled enrolment activities. Direct access to the NDID central database shall remain restricted to authorised NDID personnel operating under secure technical and governance protocols.
- Local administrators can facilitate document verification and support grievance redress.

10.8. Data Integrity and Reporting

- Community registration activities will feed directly into the national NDID database through secure digital transmission or scheduled data uploads, depending on connectivity.
- Each community registration centre will maintain a local registry log (digital or manual) for reconciliation and audit.
- Data collected at community level will undergo verification, deduplication, and approval by SBS before SDIN assignment.

10.9. Coordination and Support

Coordination of NDID implementation shall be led by the Registrar General through structured engagement mechanisms with implementing agencies, authorised relying parties, and relevant public institutions. This approach ensures streamlined decision-making, avoids duplication of governance structures, and maintains clear accountability across the NDID ecosystem.

Effective rollout shall be supported by collaboration with:

- Community-facing ministries and agencies responsible for social services, outreach, and local government engagement, to facilitate inclusive registration and public awareness; and
- Technical and digital governance ministries responsible for national ICT infrastructure, cybersecurity standards, interoperability frameworks, and digital transformation initiatives, to ensure secure and scalable system integration.

Relying parties—including government agencies, state-owned enterprises, and approved private sector organisations—shall comply with all obligations set out under the NDID Act and accompanying regulations. These include requirements relating to authorised use, consent management, data minimisation, security safeguards, audit trails, and reporting.

Legal interpretation and compliance assurance shall be supported by the competent legal authority of Government. Alignment with broader digital government strategies and emerging data protection frameworks shall be coordinated through established inter-agency mechanisms.

Monitoring, compliance enforcement, and grievance handling shall be undertaken in accordance with the NDID Act, ensuring transparency, accountability, and the protection of individual rights throughout implementation.

11. BIOMETRIC ENROLMENT & VERIFICATION

Biometric enrolment and verification form a core integrity safeguard within the NDID system, supporting the uniqueness, authenticity, and reliability of registered identities. Biometric modalities are used to prevent duplication, impersonation, and identity fraud, while strengthening trust in identity verification for public services and regulated private sector transactions.

All biometric processes under the NDID system shall be implemented in accordance with the National Digital Identification Act 2024, and shall adhere to the principles of lawfulness, necessity, proportionality, consent, data minimisation, and individual control, as set out in Section 9 (Consent and Control) of this Policy.

Biometric data shall be used solely for identity verification and authentication purposes and shall not be used for surveillance, profiling, or any unrelated purpose

11.1. Age-Based Enrolment Rules

1. Children under 18 years of age

- No biometric data shall be collected from individuals under the age of 18, in order to safeguard their privacy, rights, and personal safety, in accordance with the Act.
- Registration for this group shall rely on biographic information submitted through legally authorised registration processes, which require the physical presence and consent of a parent or legally recognised guardian.
- Children shall be recognised within the NDID system through the creation of a biographic identity record and the assignment of an SDIN, which shall be securely linked to the SDIN or identity record of their parent or legal guardian for verification and relationship validation purposes.
- Upon reaching adulthood (18 years), individuals may voluntarily and with informed consent, update their NDID records to include biometric data for enhanced verification and authentication.
- Any future policy change relating to the biometric inclusion of minors shall be subject to:
 - explicit legislative or regulatory approval.
 - appropriate safeguards consistent with child protection and human rights principles.

2. Adults aged 18 years and above

- During the Mass Registration phase, all adults (18+) will be required to provide both biographic and biometric data to establish a unique and verifiable identity record, subject to informed consent
- The set of biometric modalities to be collected
 - Facial image
 - Fingerprints
 - Electronic or digital signature
- These modalities will conform to international best practice and standards, such as ISO/IEC 19794 (biometric data interchange) and ICAO 9303 (machine-readable identity documents).
- After the completion of the Mass Registration, all new records and updates — including births, deaths, and changes to personal information — will be captured through the CRS, ensuring ongoing accuracy and synchronisation with the NDID register.

11.2. Deduplication and Biometric Verification

All biometric enrolments within the NDID system shall be processed through an Automated Biometric Identification System (ABIS) or an equivalent biometric verification mechanism approved by the Registrar General.

Biometric matching and deduplication processes shall comply with internationally recognised biometric performance, interoperability, and security standards, including, but not limited to:

- ISO/IEC 19794 series – Biometric data interchange formats for fingerprint and facial image data.
- ISO/IEC 39794 series – Next-generation biometric data formats supporting interoperability and future system evolution.
- ISO/IEC 30107 series – Biometric presentation attack detection to prevent spoofing, impersonation, and fraudulent enrolment.
- ISO/IEC 30136 – Performance testing of biometric systems to ensure acceptable accuracy, reliability, and error rates; and
- ISO/IEC 2382-37 – Standardised biometric terminology to ensure consistency across systems, vendors, and oversight processes.

Deduplication processes shall ensure that:

- each individual is registered only once within the NDID system; and
- each SDIN is uniquely and permanently associated with a single individual, in accordance with the principle of “one person, one identity.”

Where potential matches, false positives, or duplicate records are identified through biometric matching:

- the Registrar General shall initiate a controlled verification and resolution process, including manual review where required; and
- no SDIN shall be confirmed or issued until the identity has been conclusively verified.

All biometric verification, matching, and deduplication activities shall be:

- automatically logged within the NDID system
- supported by secure, tamper-resistant audit trails; and
- retained in accordance with data protection, cybersecurity, and record-keeping requirements under the National Digital Identification Act 2024.

11.3. Quality Assurance and System Standards

All biometric capture devices, software, and verification processes used within the NDID system shall comply with internationally recognised standards for accuracy, reliability, interoperability, and system security.

These shall include, where applicable:

- ISO/IEC 19794 and ISO/IEC 39794 series – Biometric data formats to ensure consistency and interoperability
- ISO/IEC 19795 and ISO/IEC 30136 – Biometric system performance testing and reporting; and
- ISO/IEC 30107 series – Presentation attack detection and resistance to spoofing.

The NDID technical team shall establish and maintain a Biometric Quality and Assurance Framework, aligned with international best practice, which shall include:

- minimum quality and performance thresholds for biometric enrolment and matching

- calibration, testing, validation, and certification procedures for all biometric equipment and software
- lifecycle management, version control, and controlled updates of biometric technologies.

Automated quality assurance mechanisms shall be implemented to:

- detect and reject incomplete, inconsistent, or poor-quality biometric captures;
- prevent enrolment where minimum quality thresholds are not met; and
- trigger controlled re-enrolment or corrective actions in accordance with approved operational procedures.

Independent technical assessments or audits may be commissioned periodically to evaluate compliance with:

- biometric quality and performance standards; and
- information security and cybersecurity controls, including those aligned with ISO/IEC 27001 and related standards.

11.4. Data Protection and Privacy Safeguards

Biometric data collected under the NDID system shall be protected in accordance with the National Digital Identification Act 2024 and relevant international data protection and cybersecurity standards.

Specifically:

- Biometric data shall be encrypted using internationally accepted cryptographic standards.
- Biometric data shall be securely stored within a dedicated Biometric Database, logically and technically segregated from biographic data; and
- Secure key management, access controls, and system hardening measures shall be applied to protect biometric repositories.

Access to biometric information shall be strictly controlled on a role-based and least-privilege basis, and shall ensure that:

- every access, use, modification, or deletion event is automatically logged.
- audit trails are tamper-resistant and retained for oversight and investigation; and
- unauthorised access attempts are detected, recorded, and responded to.

Processing of biometric data shall follow the principles of privacy by design and privacy by default, consistent with international good practice, including:

- ISO/IEC 29100 (Privacy framework);
- ISO/IEC 27701 (Privacy Information Management Systems); and
- data minimisation, purpose limitation, consent, and accountability requirements under the Act.

The Registrar General, with oversight from the National Identification Advisory Board, shall ensure that all biometric operations comply with:

- national data protection and confidentiality obligations.
- information security management standards, including ISO/IEC 27001 and ISO/IEC 27002.
- incident management and resilience standards, including ISO/IEC 27035 (incident response) and ISO/IEC 22301 (business continuity); and
- applicable national cybersecurity policies and international best practices.

11.5. Special Measures for Inclusion and Accessibility

No person shall be excluded from National Digital Identification (NDID) registration or access to services on the basis of an inability to provide biometric data.

The NDID system shall incorporate alternative and inclusive identity verification mechanisms to ensure equitable access for all individuals, consistent with international accessibility, usability, and human rights standards.

Where biometric enrolment or verification is not feasible or appropriate, alternative mechanisms may include:

- witness validation by authorised local officials, community leaders, or other persons approved by the Registrar General;
- token-based, PIN-based, or knowledge-based authentication mechanisms; and
- photographic verification or other official documentary evidence approved by the Registrar General.

Priority Groups for Assisted and Alternative Registration

Assisted or alternative registration and verification measures shall be prioritised for individuals who may face barriers to biometric capture or use, including:

- persons with disabilities;
- elderly individuals with age-related or physical biometric limitations; and
- persons living in rural, remote, or outer island communities where biometric capture is not technically feasible.

These measures shall be implemented in a manner that preserves dignity, autonomy, and informed consent, and avoids discrimination or exclusion.

Accessibility and Inclusion Standards

The design and implementation of NDID registration processes, service channels, and user interfaces shall align with international accessibility and inclusive design standards, including:

- W3C Web Content Accessibility Guidelines (WCAG) 2.1 or higher – for accessible digital platforms and mobile applications;
- ISO/IEC 40500:2012 – WCAG adopted as an international standard;
- ISO 9241-171 – Ergonomics of human-system interaction, including software accessibility; and
- ITU-T F.790 – Accessibility guidelines for telecommunications and ICT services.

Accessible formats, assisted service options, and culturally appropriate support mechanisms shall be made available to ensure that all individuals can effectively participate in NDID registration and use.

Oversight and Safeguards

The Registrar General shall ensure that inclusion and accessibility measures are consistently applied across all NDID registration and service delivery channels.

The National Identification Advisory Board shall provide oversight to confirm that alternative verification practices:

- are applied fairly and proportionately;
- do not undermine system integrity; and
- uphold Samoa's commitments to inclusion, equity, and universal access.

12. DIGITAL AUTHENTICATION

Digital authentication is the process of confirming an individual's identity to enable secure, lawful, and trusted access to services.

The NDID system will provide a unified, multi-channel authentication framework to support both public and private sector service delivery.

This function operationalises the NDID Act 2024 and complements the Electronic Transactions Act 2008, ensuring the legal validity of digital interactions, signatures, and identity confirmations.

All authentication services shall be designed and managed in accordance with the principles of privacy, consent, proportionality, security, and accountability, consistent with Part VII of the NDID Act (Protection and Management of Data) and Section 9 (Consent and Control) of this Policy.

12.1. Core Functions

Authentication under NDID shall serve as the national verification mechanism to:

- Confirm identity across digital and physical channels
- Enable secure access to e-government and financial services
- Reduce identity fraud and impersonation risks and
- Enhance public trust in online and in-person transactions.

Authentication services shall be available through both online and offline mechanisms, including tokens, smart cards, or mobile credentials, to ensure continuity of service delivery in low-connectivity or remote environments.

12.2. Methods of Authentication

The NDID adopts a multi-factor authentication model based on risk levels, service needs, and legal requirements.

These mechanisms will comply with ISO/IEC 29115 (Entity Authentication Assurance Framework) and relevant AML/CFT standards under the Money Laundering Prevention Act 2007.

Authentication Methods and Use Cases

Authentication Type	Description	Applicable Use Cases / Risk Level
Biographic Authentication	Verification by matching the SDIN and basic personal details (e.g., name, date of birth, address).	Suitable for low-risk or informational transactions such as checking eligibility, registration validation, or service enrolment.
Biometric Authentication	Verification through fingerprint or facial recognition to confirm identity for sensitive or high-value transactions.	Used for high-risk services such as banking, immigration control, border management, or law enforcement.
One-Time Password (OTP)	Dynamic security codes sent via SMS, email, or mobile application to verify identity for digital transactions.	Applied in medium-risk e-services (e.g., online applications, payments, or document access).
Digital Token Authentication	Authentication using a mobile app, QR code, or smart card-based digital token enabling both online and offline verification.	Critical for connectivity-limited areas or where continuous internet access is unavailable; supports rural inclusion.

All authentication methods shall be implemented in a manner that:

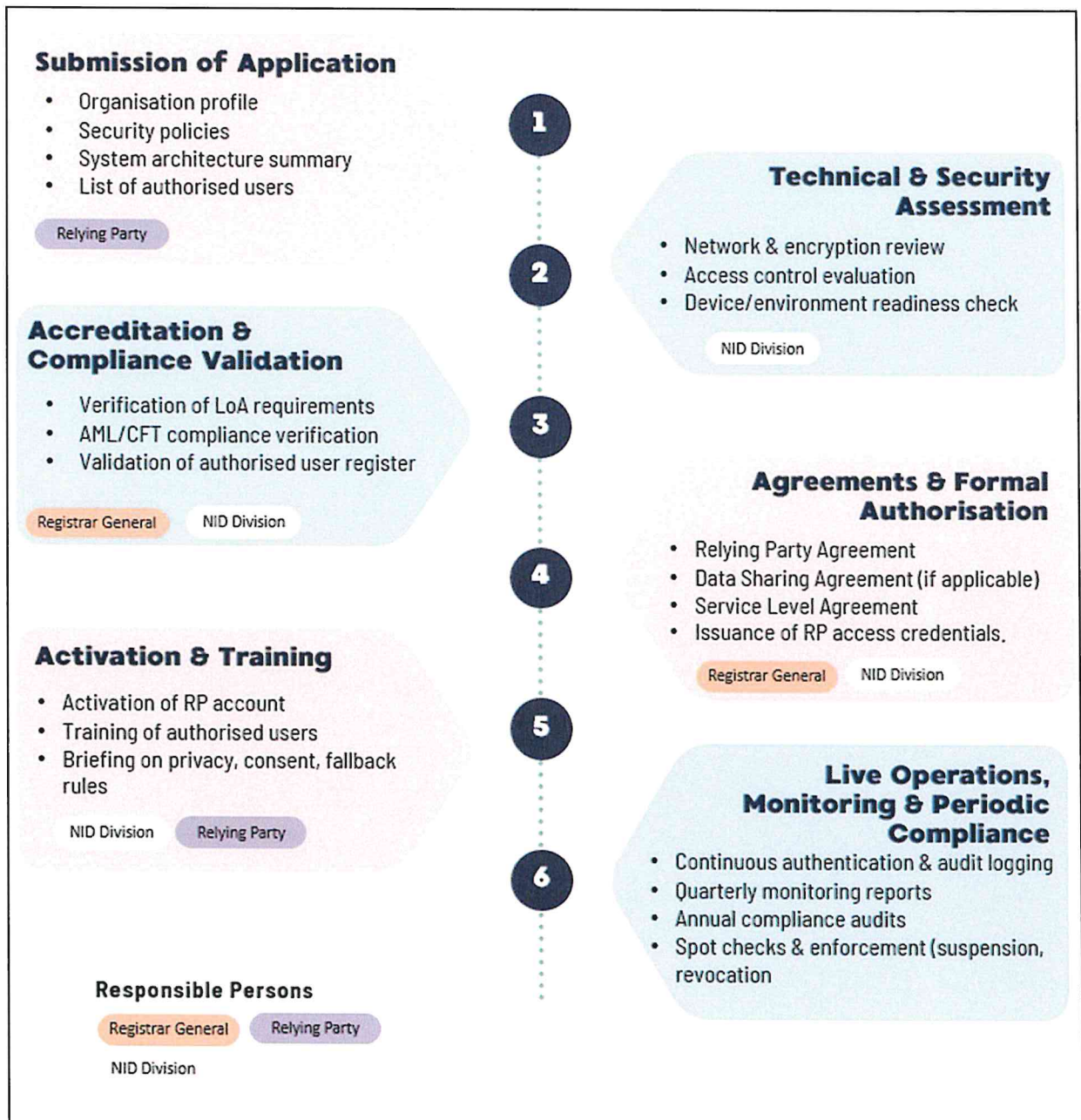
- limits data shared to what is strictly necessary;
- respects individual consent and choice; and
- supports inclusive access, consistent with Section 11.5 of this Policy.

12.3. Use of NDID Authentication by Relying Parties

NDID authentication services will be provided only to authorised relying parties (RPs) — including government ministries, state-owned enterprises, financial institutions, utilities, health providers, and other regulated private entities.

Access is conditional on meeting defined onboarding, security, and compliance requirements to protect individuals' data and maintain trust in NDID verification.

Relying Party Onboarding Workflow



Relying Party Obligations

NDID authentication services shall be accessed only by authorised relying parties that meet the requirements established by the Registrar General.

All relying parties must:

- obtain formal authorisation from the Registrar General prior to accessing any NDID authentication or verification service.
- meet minimum technical and security standards, including secure network environments, encrypted communications, and audit logging capabilities.
- comply with applicable data protection, AML/CFT, and ICT security requirements relevant to their sector;
- enter into mandatory legal instruments, including the NDID Relying Party Agreement and any applicable Data Sharing Agreements or Service-Level Agreements (SLAs);
- maintain an up-to-date register of authorised users, supported by documented procedures for:
 - staff training and awareness,
 - role-based access control, and
 - immediate revocation of access when staff leave or change roles; and
- report any security incidents, suspected misuse, or data breaches in accordance with established incident reporting and notification requirements.

Relying parties shall access NDID services only for approved purposes and shall not retain or reuse authentication data beyond what is lawfully permitted.

12.4. Verification and Compliance Framework

A dedicated Verification and Compliance Framework shall be developed to o change govern all NDID authentication and verification activities undertaken by relying parties.

This framework shall:

- define technical, operational, and procedural standards for NDID authentication and identity verification
- specify accreditation and onboarding requirements, including system readiness, security controls, and user management practices
- establish ongoing compliance obligations, including maintenance of audit trails, verification logs, and access oversight
- describe monitoring, audit, and enforcement mechanisms, including periodic compliance audits, spot checks, and corrective or sanctioning measures where non-compliance is identified
- set clear rules governing data access, consent practices, fallback verification procedures, and redress mechanisms; and
- provide a single, authoritative reference to ensure consistent, lawful, and user-centred verification practices across all relying parties.

The Verification and Compliance Framework shall be maintained by the Registrar General and reviewed periodically to reflect legal, technical, and risk developments.

12.5. Consent and Transparency in Authentication

All NDID authentication processes shall operate in accordance with the consent and control principles set out in Section 9 of this Policy.

In particular:

- authentication shall be initiated only with the explicit and informed consent of the individual, unless otherwise permitted by law
- individuals shall be clearly informed of:
 - the purpose of the authentication request,

- the specific data being verified, and
- the entity requesting verification and
- individuals shall receive a confirmation or notification (via mobile application, SMS, email, or other approved channel) each time their identity is authenticated.

Clear and accessible mechanisms shall be provided for individuals to withdraw or limit consent, and relying parties must immediately cease authentication activities where consent is not provided or has been withdrawn.

12.6. Security, Oversight and Audit

All NDID authentication activities shall be governed by a security-by-design and privacy-by-design approach, ensuring the confidentiality, integrity, and availability of identity data.

Accordingly:

- every authentication request and response shall be securely timestamped and logged within the NDID audit trail
- authentication logs shall be subject to periodic review and compliance audits, under the oversight of the Registrar General and the National Identification Advisory Board; and
- all authorised relying parties shall implement, at a minimum:
 - end-to-end encryption for data transmission and storage
 - role-based access controls aligned with staff responsibilities; and
 - incident response and breach notification procedures consistent with national ICT security requirements.

Independent technical or security audits may be commissioned to verify compliance, assess emerging risks, and strengthen system resilience.

Security controls shall be continuously reviewed and updated to respond to evolving cyber threats.

12.7. Fallback Procedures and Accessibility

The NDID system shall ensure that no individual is denied access to essential public or regulated private services due to technical failures, connectivity challenges, accessibility barriers, or temporary system limitations.

Fallback and continuity mechanisms shall be established to maintain safe, lawful, and inclusive identity verification in situations where standard digital authentication cannot be used.

Circumstances Triggering Fallback Procedures

Fallback mechanisms may be activated in situations including, but not limited to:

- network or power outages affecting digital authentication;
- temporary system downtime, maintenance, or device malfunction;
- individuals lacking access to digital devices, mobile connectivity, or stable internet;
- individuals with limited digital literacy; or
- individuals unable to use biometric or digital authentication due to disability, age, or other legitimate constraints.

Fallback procedures shall be risk-based, time-limited, and proportionate to the service being accessed.

Approved Fallback Authentication Options

Where fallback procedures are required, one or more of the following mechanisms may be applied, subject to approval by the Registrar General:

1. **Assisted In-Person Verification**

Identity verification conducted in person at:

- NDID registration centres;
- Civil Registration and Vital Statistics (CRVS) offices; or
- other authorised government service points, using biographic information, SDIN lookup, or approved records.

2. **Witness or Community Validation**

Identity confirmation provided by:

- authorised public officials.
- village representatives or recognised community leaders; or
- other approved persons acting under defined procedures, particularly in remote or outer island communities.

3. **Temporary Record-Based Verification**

Time-bound verification using:

- civil registration records.
- NDID system records; or
- other official databases approved by the Registrar General, where full authentication is temporarily unavailable.

4. **Offline Credentials or Tokens**

Use of approved offline credentials such as:

- QR codes.
- smart cards; or
- other secure tokens that allow limited verification in low- or no-connectivity environments.

Safeguards for Fallback Use

All fallback authentications shall be subject to safeguards to ensure system integrity and individual protection, including:

- clear documentation of the reason for fallback use;
- recording of fallback events in NDID audit logs where feasible;
- application of fallback methods **only for essential services**;
- automatic expiry or review of temporary verifications; and
- prohibition on using fallback mechanisms for surveillance, profiling, or non-essential purposes.

Oversight and Review

The Registrar General shall:

- approve fallback procedures and authorised users;
- monitor the frequency and appropriateness of fallback use; and
- review fallback arrangements periodically to prevent misuse or over-reliance.

The National ID Division shall regularly review fallback usage patterns and provide formal advice to the Registrar General for approval, to ensure that fallback mechanisms are applied only where necessary, remain proportionate, and respect individual rights.

13. DIGITAL IDENTITY ASSURANCE LEVELS

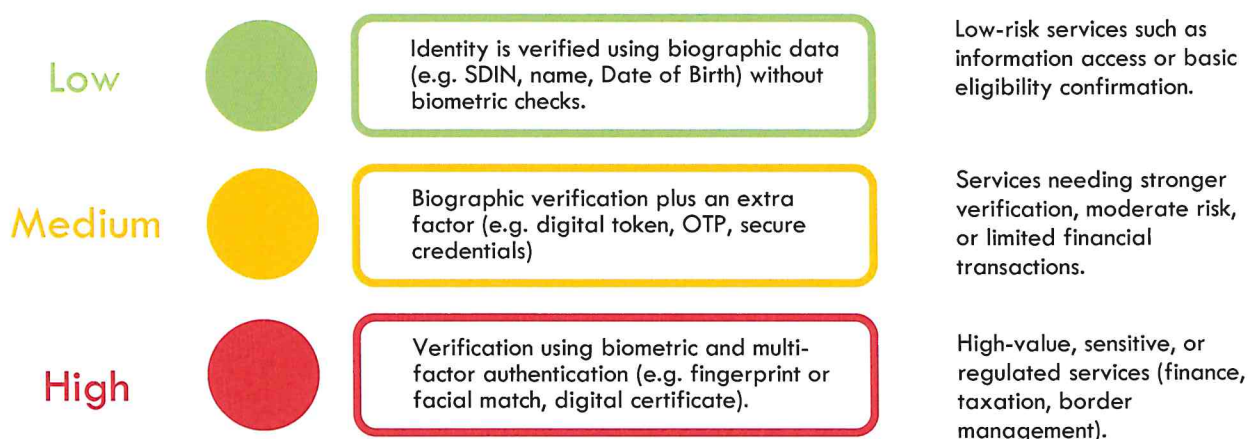
Levels of Assurance (LoA) define the degree of confidence that a person claiming an identity is the legitimate holder of that identity. LoA is determined by the strength of enrolment, credential issuance, and authentication processes, and helps relying parties apply the appropriate verification method according to the risk of the service.

A structured LoA framework ensures consistency, user protection, and trust, supporting secure service delivery across government, financial services, social protection, and other regulated sectors.

The NDID adopts a three-tier LoA model aligned with recognised global standards such as ISO/IEC 29115 (Entity Authentication Assurance Framework).

13.1. Level of Assurance Categories

Levels of Assurance determine how identity is verified, not whether a person may access a service.



13.2. Application of Levels of Assurance by Sector

Sector / Service	Typical LoA Required	Rationale
Education (school enrolment, student identification)	Low	Biographic verification is generally sufficient; limited fraud risk.
Health (hospital admissions, e-prescriptions)	Medium	Higher confidence needed to protect patient safety and prevent misuse of services.
Finance (bank accounts, loans, mobile money)	High	Required for AML/CFT compliance and fraud prevention.
Taxation (filing, compliance, payments)	High	Involves sensitive financial data and legal obligations.
Social Protection (pensions, benefits, subsidies)	Medium	Strong assurance needed to prevent duplication or fraud; biometric use applied selectively and lawfully.
E-Government Services (general)	Low–Medium	Routine services may require Low LoA; transactions involving payments or sensitive data may require Medium.
Elections (voter registration and verification)	Medium – High	Essential to protect electoral integrity and prevent impersonation.

Annex A is an example Tier Framework to better highlight the different scenarios at the different levels.

13.3. Governance and Use of Levels of Assurance

- Relying parties shall apply only the minimum LoA necessary to deliver a service lawfully and securely.
- No relying party may require a higher LoA than is justified by:
 - service risk,
 - legal or regulatory obligations, or
 - approved sectoral requirements.
- Levels of Assurance must be:
 - clearly documented during relying party onboarding;
 - reviewed as part of the Verification and Compliance Framework; and
 - subject to oversight by the Registrar General.

Misapplication of LoA (including unnecessary use of biometric or high-assurance methods) shall be treated as a compliance issue.

13.4. Relationship to Authentication Methods

Levels of Assurance are operationalised through the authentication methods defined in Section 12, including:

- biographic authentication (typically Low LoA);
- OTP or token-based authentication (typically Medium LoA); and
- biometric or multi-factor authentication (typically High LoA).

The specific authentication method used must always:

- respect individual consent;
- align with Section 9 (Consent and Control); and
- comply with inclusion and fallback provisions under Sections 11 and 12.

13.5. Review and Adaptation

The Levels of Assurance framework shall be:

- reviewed periodically to reflect emerging risks, technologies, and legal developments; and
- updated through policy or regulatory instruments as required.

Any changes shall be communicated clearly to relying parties and reflected in the Verification and Compliance Framework.

14. GRIEVANCE REDRESS AND ACCOUNTABILITY

A strong, accessible, and culturally appropriate grievance redress and accountability system is essential to maintaining public trust in Samoa's National Digital Identification (NDID) system. Because digital identity underpins access to essential public and private services, every individual must have a fair, timely, and barrier-free mechanism to challenge decisions, correct errors, raise concerns, and seek remedy.

The NDID system shall operate a formal Grievance Redress Mechanism (GRM), informed by the NDIDS Strategic Communications Strategy (2022), providing clear and transparent pathways for individuals (referred to as Affected Persons (APs)) to lodge grievances relating to:

- registration and enrolment;
- data accuracy or correction;
- credential issuance or management;
- authentication or access failures;
- privacy, confidentiality, or data misuse; and
- staff conduct or service delivery concerns.

The GRM functions as both an operational complaints-handling mechanism and a governance safeguard, ensuring the NDID system remains rights-based, inclusive, user-centred, and accountable. All grievances shall be formally recorded, reviewed, investigated, and resolved with clear documentation at each stage.

Where appropriate, grievances may be escalated to independent oversight bodies to ensure impartiality, fairness, and resolution of complex or unresolved matters. The GRM also serves as a feedback loop to identify systemic issues, strengthen service delivery, and support continuous improvement across the NDID ecosystem.

Grievances under this mechanism may also relate to misuse of consent, unauthorised authentication, or access to personal data without lawful authorisation, consistent with the rights and protections set out in Section 9 (Consent and Control) of this Policy.

14.1. Access Channels

To uphold accessibility and equity, the GRM will provide multiple entry points that accommodate different user needs, literacy levels, and geographical realities. Grievances may arise at any stage of the NDID process—planning, mass registration, or steady-state operations—and the following channels are available to support affected persons:

Direct Submission Channels

- Project Administrator (ACEO NDID): Complaints may be submitted in person, by email, or in writing.
- Registrar General (SBS): Complaints specifically concerning NDID staff conduct must be directed here.
- Official NDID Grievance Form: The prescribed form (Annex 2 of the Communications Strategy) may be completed and submitted electronically or physically at NDID service points.

Digital Channels

- Online grievance submission through an NDID portal, with the ability to upload supporting documents.

- Mobile application with simplified forms, accessibility-friendly design, and step-by-step guidance.
- Automated acknowledgment messages providing a unique reference number for tracking the complaint.

Phone Channels

- Toll-free hotline, staffed by trained operators (/OR NID staff) fluent in Samoan and English.
- Extended operating hours to assist rural, remote, and outer-island communities.
- Hotline operators can lodge grievances directly on behalf of callers who may have difficulty completing forms.

In-person Channels

- Walk-in counters at NDID registration centers and selected government service locations
- Trained staff available to assist with form completion, especially for elders and persons with disabilities or individuals with limited literacy.
- Priority or accessible service queues may be provided to ensure user comfort and dignity.

Community-Based Channels

- Village councils, district representatives, NGOs, youth groups, women's committees, and disability organisations will serve as trusted focal points
- Community focal points help document complaints, verify concerns, and support follow-up
- Useful for rural, outer-island, and low-connectivity communities

14.2. Mandatory Public Communication

In accordance with the Communications Strategy (2022), all NDID public information channels—website, banners, infographics, consultation materials—must include the official GRM notice:

“Anyone affected by an NID service(s) should fill in the grievance form and email or hand directly to the Project Administrator to be actioned accordingly. Where the grievance is about the NID staff, the grievance form should be emailed or handed directly to the SBS Registrar General...”

All information will be made available in Samoan and English, with alternative formats including braille, large print, audio recordings, and sign language-supported channels to ensure full accessibility.

14.3. Grievance Handling Process and Timelines

The National ID Division shall support the administration and coordination of the Grievance Redress Mechanism, including intake, tracking, and reporting, but shall not adjudicate grievances that are escalated to independent oversight bodies, in order to preserve impartiality and procedural fairness.

The GRM follows a structured five-step workflow to ensure timely and fair resolution of all grievances:

1. Register – Individual lodges grievance via digital, in-person, or community channel.

2. Review – Registrar General's office screens and acknowledges within 3 working days.
3. Investigate – Relevant unit investigates within 30 working days, engaging technical or legal experts as required.
4. Resolve – A formal response is provided, detailing findings and corrective measures (e.g., data correction, re-registration, clarification, or service remediation).
5. Escalate – If the grievance remains unresolved or the citizen is dissatisfied, the case may be escalated to:
 - Public Service Commission (PSC) – for staff conduct, performance, or administrative matters
 - Ombudsman – for systemic, rights-based, good-governance, or unresolved issues
 - Identification Advisory Board – for broader NDID governance or system-wide issues

Grievances that result in immediate denial or interruption of access to essential services, including health care, social protection benefits, or legal identification, shall be prioritised and expedited in accordance with procedures approved by the Registrar General.

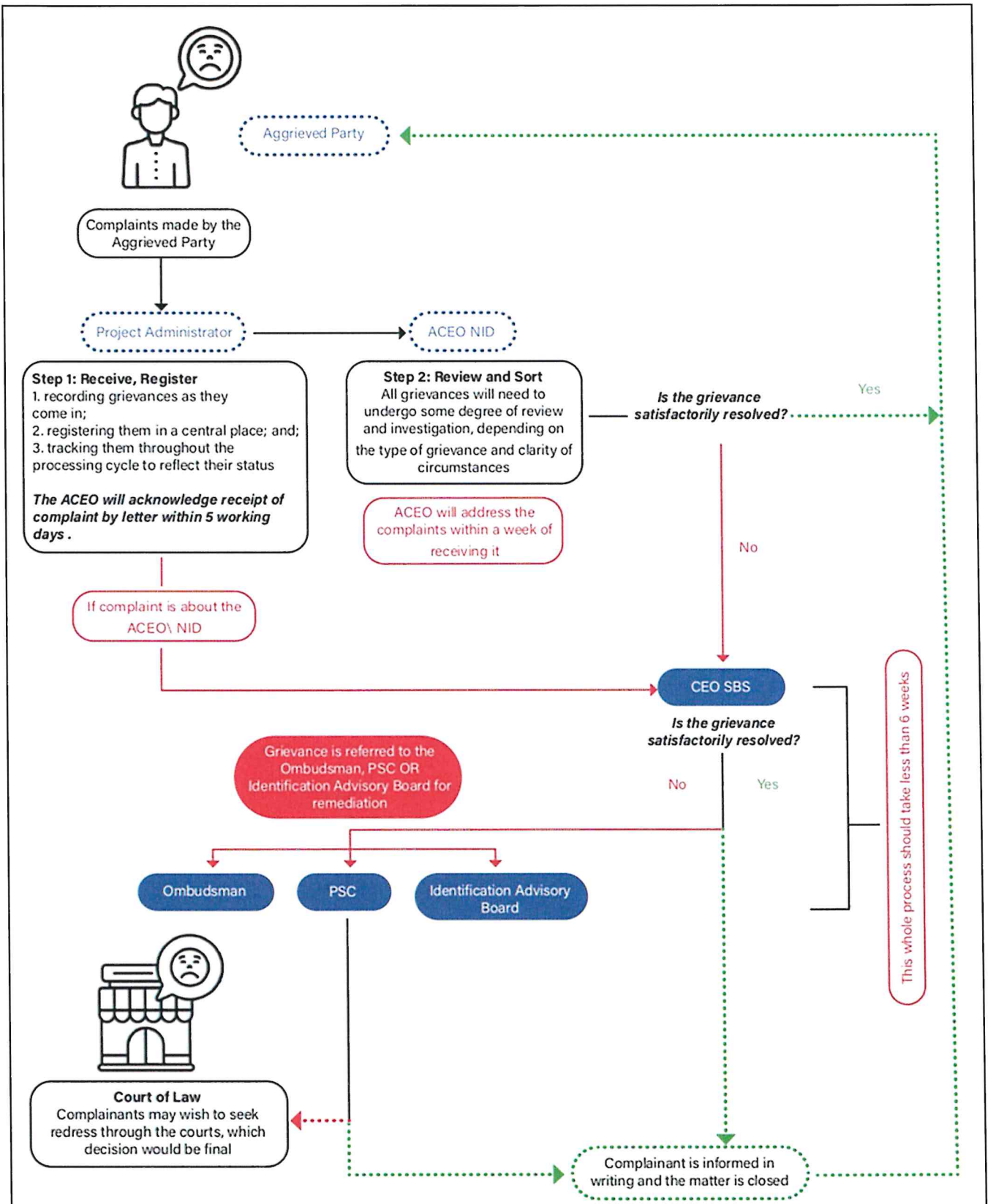


Figure Grievance and Redress Mechanism (NDIDS Communication Strategy (2022))

14.4. Scope of Complaints

The GRM will address issues arising throughout the NDID lifecycle, including:

- Incorrect, incomplete, or duplicate registration records
- Errors in biographical or biometric data
- Denial or delay in registration or credential issuance without valid grounds
- Misuse, breach, or unauthorised disclosure of personal information
- Authentication failures that prevent access to services
- Misconduct, negligence, or unprofessional behaviour by NDID staff, registrars, or associated personnel

The mechanism is designed to support individuals throughout the NDID lifecycle, acknowledging that grievances may arise during design, planning, mass rollout, or operational phases.

14.5. Transparency, Awareness, and Feedback

Lodging a grievance shall not affect an individual's eligibility for registration, credentials, or access to services, nor result in any form of retaliation or disadvantage.

- Quarterly dashboards on grievances will be published by the SBS, disaggregated by sex, age, disability, and region.
- Annual reports will summarise complaints, resolutions, systemic reforms, and staff training improvements.
- Public awareness campaigns will inform citizens of their rights and the available grievance channels, with interoperability into school and tertiary curricula under civic and digital literacy education.
- GRM data will feed into the NDID Monitoring and Evaluation (M&E) framework, ensuring continuous improvement in service delivery, accountability, and trust-building.

15. FEES AND CHARGES

The National Digital Identification system shall operate on the principle of equitable access. No eligible person shall be denied registration due to inability to pay prescribed fees.

15.1. Initial Registration

Initial registration and assignment of an SDIN during Mass Registration and through Registration at Birth shall be provided free of charge.

The Government may determine, through Regulation or approved fee schedules, whether a standard fee applies for initial registration outside the Mass Registration period.

15.2. Replacement and Reissuance

Fees may be prescribed for:

- Replacement of lost, stolen, or damaged physical credentials;
- Reissuance due to repeated negligence or misuse;
- Expedited processing requests;
- Optional premium or enhanced credentials, where applicable.

15.3. Updates and Corrections

No fee shall be charged for correction of errors attributable to the NDID Office. Reasonable administrative fees may apply for updates initiated by the holder, subject to Regulation. Other fees may be prescribed under the Regulations relating to the fee structure.

16. APPROVAL AND REVIEW

This Policy shall take effect upon official endorsement and shall remain in force until amended or replaced.

In recognition of the evolving nature of digital identity, technology, cybersecurity risks, and digital public infrastructure frameworks, the Policy shall be formally reviewed every three (3) years to ensure continued alignment with:

- Emerging data protection and cybersecurity standards
- National digital transformation priorities and
- Implementation experience and public feedback.

An earlier review may be initiated where required due to legislative amendments, significant operational changes, technological advancements, or material security or governance considerations.



NATIONAL DIGITAL IDENTIFICATION POLICY

IMPLEMENTATION PLAN



Government of Samoa
Samoa Bureau of Statistics

17. IMPLEMENTATION PLAN

PURPOSE

This Implementation Plan forms an integral part of the National Digital Identification (NDID) Policy. It sets out how the policy will be implemented in practice, translating the National Digital Identification Act 2024 and the National Digital Identification Regulations 2025 into coordinated actions, responsibilities, and delivery mechanisms.

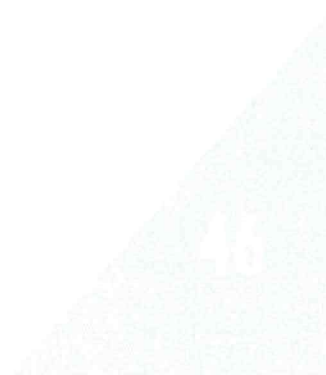
The Plan guides government agencies, regulated private sector entities, and civil society partners in sequencing actions, mobilising resources, and coordinating efforts to deliver a secure, inclusive, and trusted NDID system in Samoa.

GUIDING PRINCIPLES:

Implementation will be guided by the following principles:

- Inclusion-first – ensuring that women, youth, people with disabilities, and remote communities are registered and able to access services.
- Privacy-by-design – embedding data protection into every process and technology choice.
- Security-by-default – implementing strong authentication, encryption, and system safeguards.
- Interoperability – enabling NDID to integrate seamlessly across government and private platforms.
- Resilience – ensuring NDID systems and services remain operational during disasters, emergencies, cyber incidents, and connectivity disruptions through business continuity, disaster recovery and offline verification mechanisms.
- Transparency and accountability – ensuring open communication, public trust, and independent oversight.
- Whole-of-government coordination – aligning NDID with national digital transformation strategies and sectoral service delivery priorities

In addition to routine monitoring, the NDID implementation framework shall incorporate periodic evaluation to assess system effectiveness, inclusion outcomes, user trust, and overall impact. Evaluation findings shall inform continuous improvement of policies, regulations, and operational processes.



IMPLEMENTATION ROADMAP

Target 1 - Legal Alignment

- Operationalise the National Identity Advisory Board as mandated by the Act.
- Establish a cross-agency NDID Taskforce for coordination, security, and risk management.
- Publish the NDID Regulations 2025 covering registration, credential issuance, authentication, biometrics, relying-party access, consent safeguards, data correction, and offences.
- Harmonise NDID with Civil Registration, Immigration, Vital Statistics, Health, Tax, Education, Electoral, and Data Protection frameworks.
- Approve relevant SOPs, job descriptions, key operational procedures, and authentication standards.
- Prepare GRM implementation materials (public notices, forms, registration channels) as required by the Act and Communications Strategy.
- Operationalise consent management, grievance redress, and accountability mechanisms in line with Sections 9 and 14 of the NDID Policy.
- Activate community outreach partners (village councils, women's groups, CSOs, disability networks, youth groups) to support inclusive registration
- Assess, plan, and prioritise digitisation of legacy CRVS records, including standards, resourcing, and data quality safeguards.

Target 3 - Registration through CRVS

Focus: Maintain a living, accurate and authoritative register.

- Full integration of CRVS and NDID so registrations and lifecycle updates are captured through authorised civil registration processes.
- Update SDIN status automatically upon birth, death, marriage, change of name, or adoption, in accordance with law and regulations.
- Establish exception and correction workflows (late registration, disputed identity).
- Strengthen data quality, reconciliation workflows, and regular updates from line ministries.
- Use CRVS–NDID interoperability for sector policies, population estimates, and service eligibility checks.
- Digitise, index, and quality-check priority legacy CRVS records to support accurate NDID lifecycle management.
- Implement data validation, reconciliation, and de-duplication processes for digitised CRVS records prior to integration with NDID.

Target 2 - Mass Registration Campaign

Focus: Issue SDINs to the population with maximum inclusion, minimum friction.

- Launch national awareness and mobilisation campaign.
- Roll out fixed and mobile registration teams nationally.
- Register all eligible persons aged 18 and above, collect biographic data and biometrics (where applicable), and issue SDINs.
- Conduct mop-up registration for remote villages and outer islands.
- Operate grievance, correction, and consent-related support desks throughout the campaign.
- Begin issuing temporary digital tokens for early adopting sectors.

Target 4 - Credential Issuance

Focus: Give people credentials that work anywhere—online/offline, urban/rural.

- Issue credentials digitally and/or physically:
 - Mobile wallet
 - Issue QR-based digital ID
 - Digital credential (ID app)
 - Physical ID card (durable, secure, printable)
- Ensure offline capability for outer islands and low-connectivity areas.
- Provide replacement, renewal, and update pathways (standard, urgent, remote).
- Establish policy and fee frameworks for the credential lifecycle.
- Align credential use with Levels of Assurance (Low, Medium, High) based on service risk

Target 5 - Priority Service Rollout

Focus: Demonstrate value through priority services while managing risk before scaling

- Priority pilots:
 - Social protection: eligibility assessments, cash transfers, food distribution.
 - Health: patient identity management (e.g. linking to EMR workflows).
 - Financial inclusion: digital KYC for AML/CFT-aligned risk checks.
 - Education: student verification, exam registration, scholarships.
 - Immigration and labour mobility: border identity verification.
 - Birth correction workflows: NDID-CRVS combined identity recovery.
- Service operations:
 - Authentication integration (APIs, SDKs).
 - Helpdesk, grievance support, user assistance.
 - Monitoring for fraud, duplication, and identity recovery.
 - Apply fallback and offline verification procedures to ensure uninterrupted access to essential services

Target 6 - Cross-Sector Integration

Focus: Move from pilots to "whole-of-economy" adoption.

- Enable NDID use across priority public-facing services (e.g. Immigration, Customs, Health, Education, Social Protection, Finance, Electoral Office, Telecom, SBS).
- Support government agencies to adopt NDID for identity verification, service eligibility, and authentication.
- Enable regulated private-sector uptake (banks, fintech, remittance providers) through clear accreditation and onboarding frameworks.
- Enforce the Verification and Compliance Framework across all relying parties.
- Strengthen cybersecurity safeguards and ensure compliance with relevant ISO/IEC standards for identity issuance and data protection.
- Establish continuous monitoring of system performance, including usage volumes, authentication attempts, error rates, and potential fraud patterns.

Target 7 - Consolidation and Scaling

Focus: Make it resilient, trusted, and region-ready.

- Strengthen cybersecurity, continuity planning, and disaster recovery.
- Expand NDID use across priority national areas (mobility, trade, tourism, remittances, diaspora services).
- Introduce a user-friendly consent and data-access dashboard.
- Maintain strong governance through ongoing monitoring, audits, and risk reviews.
- Review grievance, fallback, and consent usage patterns to ensure rights-respecting operation at scale.
- Keep the system aligned with evolving international and regional standards (ISO/IEC 18013-5, ICAO, W3C Verifiable Credentials).

POLICY MEASURES, TIMEFRAME AND IMPLEMENTING PARTNERS

Implementation is delivered through six strategic pillars. Each pillar has specific actions, timelines, and responsible agencies, ensuring accountability and coordinated delivery.

PILLAR 01 - Legal, Regulatory, and Governance			
Objective: Maintain legal alignment, clear roles, and strong governance oversight for NDID.			
Action	Policy Measure	Implementing Agency / Partners	Timeline¹
1.1 Implement Legal and Regulatory Framework	1.1.1. Enforce the NDID Act 2024 and NDID Regulations 2025 as a standing obligation across all NDID operations.	SBS (lead), OAG	Ongoing
	1.1.2. Maintain alignment of related legislation (Births, Deaths and Marriages, Statistics, Data Protection, Citizenship, Immigration).	OAG, MJCA, SBS, MCIT	Medium Term (initial alignment) + Ongoing review
	1.1.3. Issue and periodically update regulatory guidance for ministries, SOEs, and regulated private sector partners.	SBS, MCIT	Short Term (before Mass) + Ongoing updates
	1.2.1. Formalise and sustain the mandates of the Registrar General, Advisory Board (as a strategic oversight body) and implementing agencies.	SBS, Relevant Ministries	Short Term
1.2 Define and Operationalise Roles and Responsibilities	1.2.2. Keep Terms of Reference and reporting structures updated.	SBS, PSC	Ongoing
	1.2.3. Conduct induction and refresher sessions for implementing agencies as part of ongoing governance support.	SBS, MCIT	Medium Term + Ongoing
	1.3.1. Operate a compliance reporting system for NDID across all sectors.	SBS, Audit Office, MCIT	Medium Term
1.3. Establish Oversight and Accountability Mechanisms	1.3.2. Conduct regular governance and performance audits, with public release of summaries.	SBS, MOF, Ombudsman, MCIT	Ongoing
	1.3.3. Standardise and maintain data sharing agreements across ministries and private sector.	SBS, MCIT	Short Term
1.4. Regulate Data Sharing and Credential Issuance	1.4.1. Define and continuously refine credential issuance and renewal processes.	SBS, MJCA	Short Term

¹ “Short Term” refers to preparatory and Mass Registration activities; “Medium Term” to post-Mass expansion; “Long Term” to strategic enhancements; and “Ongoing” to continuous governance and operational functions. “Short Term + Ongoing” indicates actions initiated early and sustained thereafter.

	1.4.2. Apply penalties for misuse, non-compliance, or fraud as a standing enforcement function.	SBS, OAG ²	Ongoing
1.5. Strengthen Cross-Sector Governance	1.5.1. Operationalise governance structures established by the NDID Act 2024, formalising the Advisory Board as a strategic oversight mechanism.	SBS, MCIT	Short Term
	1.5.2. Empower the NDID Office to convene quarterly review meetings and provide cross-sector coordination.	SBS, Relevant Ministries	Ongoing
	1.5.3. Integrate NDID governance into national digital transformation agendas on a sustained basis.	SBS, MoF, MCIT	Medium Term + Ongoing
PILLAR 02 - Verification and Compliance			
Objective: Enforce robust verification standards, ensure compliance with NDID protocols, and build trust through consistent application of assurance levels and audits.			
Action	Policy Measure	Implementing Agency / Partners	
2.1. Establish and Maintain the National Levels of Assurance (LoA) Framework	2.1.1. Apply nationally defined Levels of Assurance proportionate to service risk.	SBS (Lead), MCIT, Relevant Ministries, Accredited Relying Parties (Public and Private)	Medium Term
	2.1.2. Pilot and progressively expand LoA application across priority services.		Short Term
	2.1.3. Provide guidance and training to relying parties on LoA application.		Short Term + Ongoing
2.2. Enforce Standards for Credential Issuance and Lifecycle Management	2.2.1. Define biometric/biographic thresholds for enrolment and keep them under review. (e.g., photo, fingerprints).	SBS	Short Term
	2.2.2. Standardise ID formats (NDID card design, SDIN attributes, digital tokens) and update as needed.	SBS, MCIT	Short Term
	2.2.3. Maintain protocols for renewal and replacement of credentials.	SBS	Ongoing
2.3. Conduct Continuous Compliance Auditing and Quality Assurance	2.3.1. Establish and maintain an NDID Compliance and Assurance Framework applicable to registration centres and accredited relying parties.	SBS, Audit Office	Ongoing
	2.3.2. Conduct periodic operational and technical compliance reviews using standardized tools and reporting templates.	SBS, Audit Office	Short Term
	2.3.3. Maintain an internal quality oversight function reporting to the Registrar General and Advisory Board.	SBS, Advisory Board	Ongoing
	2.4.1. Ensure all NDID participants comply with their legal obligations under the NDID Act and Regulations.	CBS, SBS, Financial Institutions, Telecom,	Medium Term + Ongoing

2.4. Enforce Legal Obligations, Accountability, and Penalties	2.4.2.	Establish clear administrative enforcement procedures to address non-compliance, including compliance notices, corrective orders, and suspension or termination of access where necessary.	SIFA, MOF, Relying Parties	
	2.4.3.	Operate grievance redress and whistleblowing mechanisms in accordance with the NDID Act and Regulations.	OAG, SBS	Ongoing
	2.4.4.	Ensure serious breaches involving fraud, unauthorised access, misuse of identity data, or security violations are investigated and dealt with under the offence and penalty provisions of the NDID Act and Regulations.	Ombudsman, PSC, SBS	Ongoing
PILLAR 03 – Inclusive and Equitable Access				
Objective: Ensure all Samoans — including persons with disabilities, older persons, women, youth, rural communities and other underserved populations — have continuous and equitable access to NDID services				
3.1. Expand Nationwide Outreach and Mobile Registration Coverage	Action	Policy Measure	Implementing Agency / Partners	Timeline
	3.1.1.	Sustain and strengthen the deployment of mobile registration units to rural, remote, and outer island communities to ensure equitable geographic access.	SBS, MCIT, MWCSD, District Councils	Short Term (Mass) + Ongoing
	3.1.2.	Maintain structured partnerships with village councils and community leaders to support enrolment campaigns.	SBS, Village Councils, MWCSD, Relevant CSOs and Faith-Based Organisations	Short Term + Ongoing
	3.1.3.	Ensure consistent and accessible public communication on registration through digital platforms, radio, print media and local networks.	SBS, MCIT, MWCSD, Relevant CSOs and Faith-Based Organisations	Short Term + Ongoing
3.2. Enable Inclusive and Assisted Registration Options	3.1.4.	Regularly monitor outreach and adapt strategies based on evidence and participation data to improve effectiveness and inclusion.	SBS, MWCSD	Medium Term + Ongoing
	3.2.1.	Provide legally compliant non-biometric registration alternatives, where appropriate, particularly for children, elderly, PWDs. ³	SBS, MWCSD, OPDs	Short Term
	3.2.2.	Establish clear procedures for assisted registration for individuals who require support during the registration process	SBS, MWCSD, OPD, ⁴ Relevant CSO's	Short Term + Ongoing
	3.2.3.	Provide assisted registration through mobile outreach, home visits, and other accessible locations where needed.	SBS, MWCSD	Medium Term

³ PWD – Persons with Disabilities

⁴ OPD – Organisations of Persons with Disabilities (eg. Senese, Loto Taumafai, Spinal Association etc)

	3.2.4. Recognise alternative forms of identity verification, including structured community-based attestation, in exceptional circumstances where documentary evidence is unavailable, subject to verification and audit requirements under the NDID Act and Regulations.	SBS, MWCSD, Village Councils	Short Term
3.3. Remove Language, Communication, and Accessibility Barriers	3.3.1. Provide registration forms and public information materials in Samoan and ensure plain-language versions are available to enhance comprehension across age groups and literacy levels.	SBS, MWCSD, MCIT	Short Term + Ongoing
	3.3.2. Ensure registration information is available in accessible formats — including Braille, large print, audio materials, sign language interpretation, and easy-to-understand formats — to accommodate diverse disabilities, in accordance with recognised accessibility standards (e.g., W3C, WCAG).	SBS, MWCSD, NOLA, OPDs	Short Term + Ongoing
	3.3.3. Ensure the availability of sign-language interpretation and other communication support services during registration and public awareness activities to guarantee equal communication access.	SBS, MWCSD, NOLA, OPDs	Short Term + Ongoing
	3.3.4. Develop and implement plain-language communication standards to improve clarity and accessibility of NDID information.	SBS, MWCSD	Short Term + Ongoing
	3.4.1. Collect and analyse disaggregated registration data (including by gender, age, disability status, and geographic location) to monitor equitable participation.	SBS, MWCSD	Medium Term + Ongoing
3.4. Monitor and Promote Equity in Access and Participation	3.4.2. Provide periodic reporting on inclusion indicators to the NDID Advisory Board and, where required, to Parliament.	SBS, Advisory Board	Ongoing
	3.4.3. Review and refine outreach and registration strategies in response to monitoring findings to address identified participation gaps.	SBS, MWCSD	Ongoing
PILLAR 04 – Security, Privacy and User Protection Objective: Protect NDID data and user rights through continuous safeguards, oversight, and redress.			
Action	Policy Measure	Implementing Agency / Partners	Timeline
4.1 Strengthen Data Protection and Information Security	4.1.1. Separate biometric from biographic data storage.	SBS, MCIT	Short Term (setup) + Ongoing
	4.1.2. Apply encryption, secure authentication, and access controls on a continuing basis.	SBS, MCIT	Short Term (setup) + Ongoing
	4.1.3. Enforce the principle of data minimisation across all NDID operations.	SBS, MCIT	Short Term (setup) + Ongoing
	4.1.4. Regularly review compliance with data protection standards.	SBS, MCIT	Ongoing
4.2 Enforce User Consent, Rights, and Transparency	4.2.1. Apply informed consent protocols during registration and authentication as standard practice.	SBS, OAG	Short Term

	4.2.2. Provide opt-in/opt-out mechanisms for third-party data sharing.	SBS, MCIT	Medium Term
	4.2.3. Maintain user dashboards so individuals can view their authentication history.	SBS, MCIT	Medium Term
	4.2.4. Run awareness campaigns on NDID rights and responsibilities continuously.	SBS, MWCSD	Ongoing
4.3 Establish Accessible and Accountable Grievance and Redress Mechanisms	4.3.1. Provide multiple grievance channels (online, hotline, in-person, community-based).	SBS, Ombudsman	Short Term + Ongoing
	4.3.2. Operate a clear appeals process for disputed enrolments and data errors.	SBS, OAG	Short Term + Ongoing
	4.3.3. Publish reports on complaints received and resolved annually.	SBS, Ombudsman	Short Term + Ongoing
	4.3.4. Protect whistleblowers reporting misuse.	SBS, Ombudsman, OAG	Short Term + Ongoing
4.4 Institutionalise Continuous Risk Management and System Resilience	4.4.1. Enforce regular cybersecurity and privacy risk assessments.	SBS, MCIT	Ongoing
	4.4.2. Require third-party vulnerability audits.	SBS, MCIT, Independent Auditors	Ongoing
	4.4.3. Maintain incident response and breach notification protocols.	SBS, MCIT	Ongoing
	4.4.4. Embed NDID resilience into national disaster, cyber, and financial risk management frameworks.	SBS, MCIT, MNRE	Ongoing
PILLAR 05 – Interoperability, Standards and Infrastructure Objective: Ensure interoperability of NDID with national systems, strengthen interoperability standards, and build resilient infrastructure to support secure and sustainable service delivery.			
5.1 Establish and Enforce National Interoperability Standards	Action	Implementing Agency / Partners	
	5.1.1. Enforce open standards and secure data formats continuously.	SBS, MCIT	Short Term
	5.1.2. Publish, maintain and update NDID API guidelines for relying parties.	SBS, MCIT	Short Term
	5.1.3. Operate a certification system to approve systems that can interoperate securely with NDID.	SBS, MCIT	Short Term
5.2 Strengthen Cross-Sector Alignment and Compliance Readiness	5.1.4. Review and update standards regularly to remain future proof.	SBS, Advisory Board	Short Term
	5.2.1. Enable NDID interoperability with priority systems such as CRVS, Health Information Systems, Education, Tax, Finance, and Social Protection.	SBS, Line Ministries	Medium Term

	5.2.2. Certify external systems for compliance with NDID standards before allowing connections.	SBS, MCIT	Medium Term
	5.2.3. Conduct regular readiness assessments with ministries, SOEs, and private sector relying parties.	SBS, MCIT	Medium Term
	5.2.4. Formalise MoUs with explicit data protection and privacy clauses.	SBS, MoF	Medium Term
	5.3.1. Invest in hybrid infrastructure — maintaining the NDID registry on national servers while leveraging cloud services for accessibility, resilience, and scalability.	SBS, MoF, MCIT	Short Term (initial build) + Ongoing
5.3 Build and Sustain a Resilient and Secure NDID Infrastructure	5.3.2. Maintain backups, redundancy, and disaster recovery systems.	SBS, MCIT	Short Term (initial build) + Ongoing
	5.3.3. Strengthening connectivity for rural and outer islands with redundant networks.	SBS, MCIT, Telcos	Short Term (initial build) + Ongoing
	5.3.4. Operate business continuity planning as an ongoing practice.	SBS, MCIT	Short Term (initial build) + Ongoing
	5.4.1. Pilot and scale connectedness with high-priority services to test functionality.	SBS, MOH, CBS	Medium Term
5.4 Test, Validate, and Scale Interoperability Use Cases	5.4.2. Roll out phased interoperability roadmaps based on lessons learned.	SBS, MCIT	Medium Term
	5.4.3. Gather user and relying party feedback to refine processes.	SBS, Line Ministries	Medium Term
	5.4.4. Commission external evaluations following pilots to ensure accountability and trust.	SBS, Development Partners	Medium Term
	5.5.1. Align Samoa's NDID standards with the Pacific Digital Economy Strategy (2021–2030) and Blue Continent Vision.	SBS, MOH, CBS	Long Term + Ongoing
5.5. Strengthen Regional and Global Interoperability	5.5.2. Explore future cross-border interoperability for mobility, remittances, education, and trade.	SBS, MCIT	Long Term + Ongoing
	5.5.3. Engage with SPC, PIF, other regional and development partners to harmonise standards and build trust.	SBS, Line Ministries	Long Term + Ongoing
PILLAR 06 – Capacity, Monitoring and Sustainability Objective: Build the institutional, technical, financial, and human capacity required to operate NDID effectively and sustainably, strengthen public understanding and digital literacy, and embed a robust monitoring, evaluation, and learning framework that ensures accountability, transparency, resilience, and continuous improvement. Capacity building shall prioritise technical competencies in: – biometric system management – API integration and system interoperability – cybersecurity operations and incident response			

Action	Policy Measure	Implementing Agency / Partners	Timeline
6.1. Strengthen Institutional Capacity and Workforce Readiness	6.1.1. Conduct regular readiness and capacity assessments of SBS and partner ministries	SBS, PSC	Short Term + Ongoing
	6.1.2. Recruit, train, and retain NDID officers with specialised skills in ICT, law, and community engagement.	SBS, PSC	Short Term + Ongoing
	6.1.3. Provide structured training for registrars, IT officers, frontline staff, and community leaders.	MoF, SBS	Short Term + Ongoing
	6.1.4. Develop succession planning to ensure continuity of NDID leadership and expertise.	SBS, PSC	Short Term + Ongoing
6.2. Develop and Implement National Training, Digital Literacy, and Public Awareness Programs	6.2.1. Train registrars, IT officers, and community leaders to manage NDID processes.	SBS, MWCSD	Short Term (Mass phase) + Ongoing
	6.2.2. Run sustained nationwide awareness and education campaigns on NDID rights, obligations, benefits, and safeguards.	SBS, MCIT, MWCSD	Short Term (Mass phase) + Ongoing
	6.2.3. Integrate NDID awareness, digital identity literacy, and rights protections under the NDID Act/Regulation into school and tertiary curricula.	SBS, MEC, SQA	Short Term (Mass phase) + Ongoing
	6.2.4. Develop accessible e-learning and community-based learning modules for youth, women, persons with disabilities, and rural communities on the use, benefits, and protections under NDID.	SBS, MEC, MWCSD	Short Term (Mass phase) + Ongoing
	6.2.5. Collaborate with CSOs and community leadership structures to support outreach and inclusive participation among marginalised groups.	SBS, NGOs, MWCSD	Short Term (Mass phase) + Ongoing
6.3. Monitoring, Evaluation and Learning (MEL)	6.3.1. Track implementation progress and service uptake.	SBS, Advisory Board	Medium Term
	6.3.2. Report periodically to oversight bodies and Cabinet.	SBS	Medium Term
	6.3.3. Commission independent mid-term and final evaluations.	SBS, Development Partners	Medium Term
	6.3.4. Use real-time dashboards to track implementation.	SBS, MCIT	Medium Term
	6.3.5. Conduct periodic public perception and trust surveys to inform policy adjustments and outreach strategies.	SBS and all relevant stakeholders	Medium Term + Ongoing
	6.3.6. Incorporate lessons learned into annual NDID system and policy updates.	SBS and all relevant stakeholders	Medium Term + Ongoing
6.4. Strengthen Coordination, Oversight, and Implementation Management	6.4.1. Formalise the NDID Office as the permanent technical authority for identity management, authentication governance, and cross-sector integration.	SBS, PSC, MOF	Ongoing
	6.4.2. Hold quarterly stakeholder review meetings to assess progress and address implementation challenges.	SBS, Advisory Board	Ongoing

6.5 Strengthen Financial and Operational Sustainability	6.4.3.	Maintain and update the national rollout plan as a living document	SBS, MOF	Ongoing
	6.4.4.	Report NDID progress annually to Cabinet for oversight and accountability	SBS	Ongoing
	6.5.1.	Develop multi-year operational budgeting for NDID system maintenance and cybersecurity	SBS, MOF	Medium Term
	6.5.2.	Establish a cost-recovery and fee framework for relying parties where appropriate	SBS, MOF	Medium Term
	6.5.3.	Plan lifecycle replacement of biometric hardware and authentication infrastructure	SBS, MCIT	Medium Term
	6.5.4.	Secure sustainable funding streams for continuous digital literacy and outreach programs	SBS, MOF	Ongoing

CROSS-CUTTING TRACKS (APPLIED ACROSS ALL PHASES)

While the Implementation Plan is structured into distinct phases and pillars, there are several dimensions that must be applied continuously and consistently across every stage of NDID implementation. These are not one-off activities; they are foundational safeguards and enablers that ensure the system is inclusive, trusted, resilient, and sustainable.

- **Inclusion & Accessibility**

Ensures that NDID reaches all citizens and residents, especially those most at risk of exclusion. By adopting disability-inclusive design standards (WCAG 2.2), providing outreach to rural and remote areas, and enabling attestation and proxy¹ registration with safeguards, the NDID system guarantees that women, youth, people with disabilities, and those without formal documents are not left behind.

- **Security & Privacy**

Principles must be embedded from the start and carried forward in every update. Privacy impact assessments, strong encryption, role-based access controls, and a zero-trust architecture are reinforced with third-party audits to safeguard personal data and build public trust in the system.

This includes safeguards governing the use of automated systems and Artificial Intelligence to ensure transparency, accountability, and protection against bias or misuse.

- **AML/CFT & eKYC**

Alignment ensures that the NDID system supports Samoa's obligations under the Money Laundering Prevention Act and international financial integrity frameworks. By enabling risk-based onboarding, sanctions and politically exposed persons (PEP) checks, immutable audit trails, and lawful disclosure mechanisms, NDID provides a secure and compliant foundation for financial services and economic growth.

- **Capacity & Change Management**

Recognises that technology alone is not enough. Ongoing training for registrars, ICT officers, auditors, frontline staff, and developers is essential to sustain system performance, adapt to evolving needs, and ensure smooth uptake across sectors.

- **Communications & Trust**

Is about maintaining continuous public engagement. The NDID Communications Plan must be executed throughout implementation with accessible, plain-language guides, community outreach, radio and TV campaigns, and myth-busting FAQs. Building trust requires transparency, two-way communication, and active involvement of civil society and community leaders.

- **Disaster Response and Continuity**

NDID shall support national disaster preparedness and response by enabling rapid identity verification, offline authentication, and continuity of services during emergencies. Business continuity planning and disaster recovery mechanisms shall be maintained as core operational requirements.

¹ **Proxy Registration** means the enrolment of an eligible person into the NDID system by a legally recognised guardian, parent, or authorised representative acting on the person's behalf, in accordance with procedures, eligibility criteria, and verification safeguards prescribed by the Registrar General.

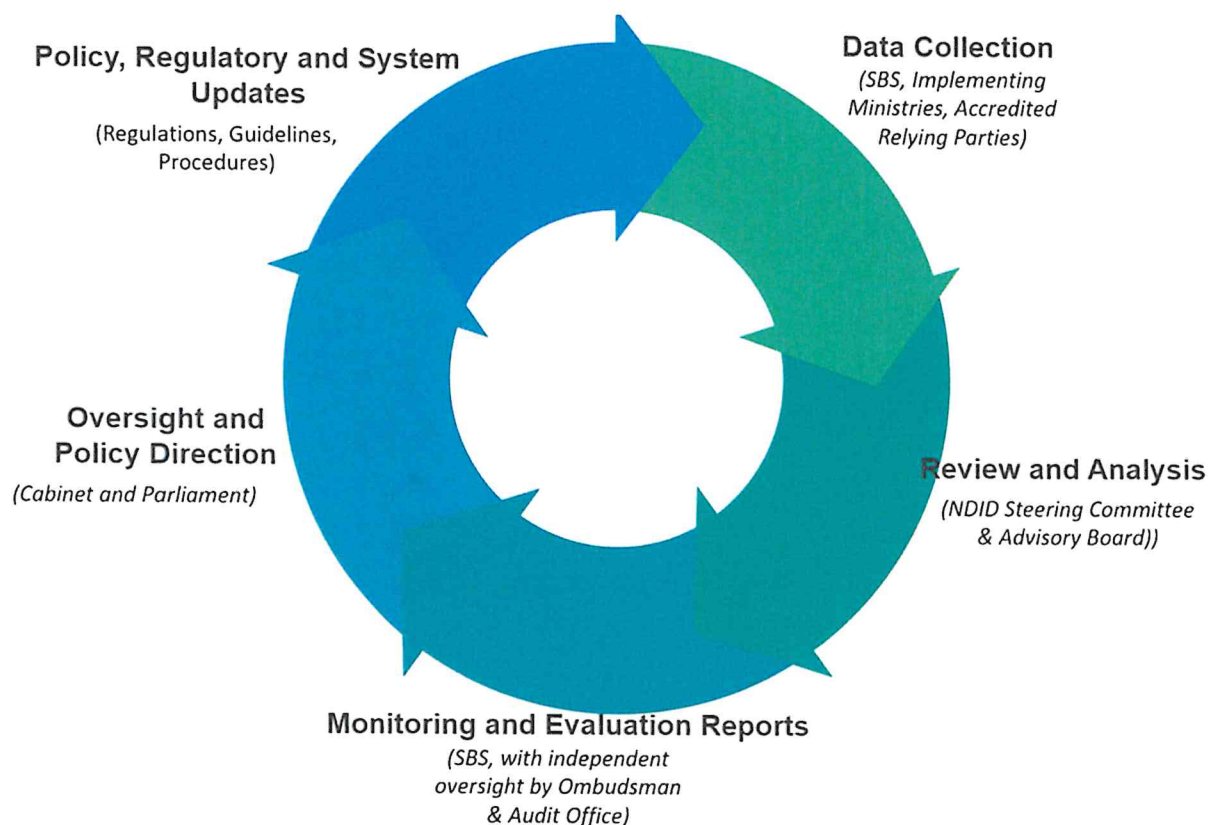
Together, these cross-cutting tracks form the backbone of the Implementation Plan. They ensure that every action under the six pillars is anchored in inclusion, security, accountability, and trust. Without them, the technical and legal achievements of the NDID system would risk being undermined by weak adoption, exclusion, or mistrust. With them, Samoa can confidently deliver a digital identity system that is people-centred, rights-based, and future-ready.

TOP RISKS AND MITIGATIONS

Risk	Mitigation
Low turnout in rural/outer islands	Mobile units, village liaisons, travel stipends, pop-up weekends
Data mismatches/duplicates	ABIS dedupe, adjudication committees, quality dashboards
Privacy/cyber incident	Zero-trust, pen tests, 24/7 monitoring, rapid breach comms plan
Vendor lock-in	Open standards, modular architecture, escrowed source/docs
Relying Party misuse of data	Certification, audits, fines/suspension, user-facing access logs
Exclusion of PWD/elderly	Accessible UX, assisted enrolment, home visits
Connectivity outages	Offline capture & verification, store-and-forward queues
Public mistrust	Transparent reporting, civil society oversight, redress visibility
Budget overrun	Phased procurement, milestone gates, benefits tracking
Legal gaps linger	Time-boxed law reform plan; interim directives where lawful
Loss of identity credentials during disasters	Rapid reissuance protocols, offline verification, linkage to CRVS
Misuse or bias in AI/automated processes	AI governance guidelines, human oversight, audit mechanisms

MONITORING AND EVALUATION

National Digital Identification Monitoring and Evaluation Feedback Loop



Step 1: Data Collection

Data is collected on an ongoing basis from the Samoa Bureau of Statistics, implementing ministries, and accredited relying parties. This includes information on registration coverage, service usage, system performance, inclusion outcomes, security events, and grievance handling. Data collection ensures that implementation progress and emerging risks are visible across the NDID ecosystem.

Step 2: Review and Analysis

Collected data is reviewed through structured quarterly and annual review processes led by the NDID Office and Advisory Board. These reviews assess system performance, compliance with policy and legal requirements, inclusion outcomes, and risk management effectiveness. This step enables evidence-based assessment and early identification of issues requiring attention.

Step 3: Reporting and Transparency

Monitoring and evaluation findings are consolidated into formal reports prepared and published by the Samoa Bureau of Statistics. Independent oversight bodies, including the Ombudsman and the Audit Office, contribute to review and assurance. Public and institutional reporting strengthens transparency, accountability, and trust in the NDID system.

Step 4: Oversight and Policy Direction

Monitoring and evaluation reports inform oversight and policy direction by Cabinet and Parliament. This step ensures that senior decision-makers are equipped with timely and credible evidence to

guide strategic direction, resource allocation, legislative adjustments, and accountability measures related to NDID implementation.

Step 5: Policy, Regulatory, and System Updates

Insights from oversight and review processes feed into updates to policies, regulations, guidelines, and system operations. These updates are implemented by the responsible institutions and reflected in operational practices, closing the feedback loop and ensuring that the NDID system remains adaptive, inclusive, secure, and responsive to evolving needs.

Key Performance Indicators

The following Key Performance Indicators (KPIs) operationalise the Monitoring and Evaluation framework by providing measurable benchmarks for tracking NDID performance, inclusion, security, and user protection.

Category	Indicator	Description	Data Source	Target / Benchmark
Coverage	% of eligible population registered	Proportion of citizens/residents issued with SDIN.	SBS registration data	95%+ within 2 years of rollout
	% registered by sex, age, disability, region	Disaggregated to measure equity in access.	Registration reports; CRVS	No disparities greater than 2% across groups
Quality	Duplicate rate	% of records flagged as potential duplicates.	ABIS, Registry audits	<0.5%
	Correction SLA	Avg. days to correct/amend user records.	Registrar logs	≤15 days
	Data freshness	Time lag between CRVS event and population register update.	CRVS–NDID sync logs	≤7 days
Usage	Authentications/day	Number of identity checks performed.	Auth Gateway logs	Baseline by Year 1; ≥20% annual growth thereafter
	# of integrated services	Ministries, SOEs, private entities connected to NDID.	SBS system registry	≥5 priority services by Year 2 (incl. health, education, finance, social protection, ID/legal)
	Pilot→production conversion rate	% of pilot interoperability scaled to national rollout.	SBS/sector reports	≥80%
User Protection	Grievance volumes	Number/type of complaints logged.	Ombudsman/SBS complaint system	Trend of decreasing unresolved

				complaints year-on-year
	Resolution times	Avg. time to resolve complaints.	Ombudsman/SBS	≤30 days
	% consent revocations honoured	Proportion of revocation requests successfully actioned.	Consent dashboard logs	100%
Reliability & Security	System uptime	Availability of NDID systems.	IT Ops monitoring	≥99%
	Mean time to detect/respond (MTTD/MTTR)	Average time to detect and respond to incidents.	Security Ops logs	≤24 hrs detection; ≤72 hrs response
	Audit findings resolved	% of compliance/security recommendations addressed.	Audit Office reports	≥75% within 6 months; 100% within 12 months

Annex A — Tier Framework

To operationalise Levels of Assurance (LoA) in Samoa's context, the NDID system applies a tiered authentication framework. This framework translates abstract LoA categories (Low, Medium, High) into practical tiers with defined authentication methods, required fields, and sector-specific use cases.

The NDIDS Authentication Tier Framework ensures that:

- **Service providers** can match the risk of their services with the appropriate level of identity verification.
- **Relying parties** have clear technical and legal guidance for applying NDID authentication consistently.
- **Individuals** experience proportionate, secure, and convenient authentication — avoiding unnecessary complexity for low-risk services while ensuring strong safeguards for high-risk or sensitive transactions.

This approach also positions Samoa's NDID for regional and international interoperability, by aligning with global LoA standards while tailoring implementation to local needs. The table below outlines the NDIDS Tiers, their corresponding LoA categories, and example use cases.

Tier	Assurance Level	Authentication Methods	Minimum Fields Used	Use Case Examples	Remarks
Tier 0 (Low)	Low / Unverified Identity	- Password only - Security Qs	Name only (manual entry)	Access to generic online forms, pre-registration, public portals	No identity verification; low risk services
Tier 1 (Basic)	Basic / Remote Verified	- Password or PIN + OTP via SMS/email	Name SDIN or Token DOB	Utility billing login, school e-services, citizen surveys	Uses fields that can be matched remotely; no biometrics
Tier 2 (Moderate)	Moderate / Token-Verified	- SDIN + OTP or - SDIN + Face Image Match	SDIN Face Image QR/Token	eHealth access, NPF, tax filing, driver registration	Useful for digital service access; uses non-biometric matching
Tier 3 (High)	High / Biometric Authentication	- SDIN + Fingerprint or - SDIN + Face Match + OTP	SDIN Face Image Signature QR Code	Border control, police ID checks, financial services, eKYC	In-person or remote biometric authentication required
Tier 4 (Trusted Delegated) (optional future)	Trusted Delegated / Federated	- Login via accredited provider (bank, telco, SPT)	Token + federated assertion	Regional interoperability, diaspora login	Future-ready, depends on SPT or federated ID system maturity

Annex B — Relevant International Standards for NDID Implementation

The Samoa National Digital Identification (NDID) system aligns with recognised international standards to ensure security, privacy, interoperability, accessibility, and user trust. These standards serve as benchmarks for technical design, governance, and ongoing system operations.

1. Biometric Standards

- **ISO/IEC 19794 series** – Biometric data interchange formats:
 - 19794-2 Finger minutiae data
 - 19794-4 Finger image data
 - 19794-5 Face image data
- **ISO/IEC 39794 series** – Next-generation biometric data formats (finger, face, iris).
- **ISO/IEC 30107 series** – Biometric presentation attack detection (anti-spoofing).
- **ISO/IEC 30136** – Performance testing of biometric systems.
- **ICAO Doc 9303** – Machine-readable travel documents; standards for ID cards with machine-readable zones (MRZ), chips, or QR codes.

2. Digital Identity and Authentication Standards

- **ISO/IEC 24760 series** – Framework for identity management and terminology.
- **ISO/IEC 29115** – Entity authentication assurance framework (Levels of Assurance).
- **ISO/IEC 29146** – A framework for access management.
- **ISO/IEC 18013-5** – Mobile driving licence (mDL) standard, relevant for digital credentials.
- **ITU-T X.1254** – Assurance framework for identity management.
- **W3C Verifiable Credentials Standard** – For digital identity portability and interoperability.
- **OpenID Connect / OAuth 2.0** – Secure authentication and authorisation protocols for online services.

3. Information Security, Privacy, and Data Protection

- **ISO/IEC 27001** – Information security management systems (ISMS).
- **ISO/IEC 27002** – Code of practice for information security controls.
- **ISO/IEC 27018** – Protection of personally identifiable information (PII) in cloud services.
- **ISO/IEC 27701** – Privacy information management systems (PIMS).
- **ISO/IEC 29100** – Privacy framework.
- **ISO/IEC 27035** – Information security incident management.
- **ISO/IEC 22301** – Business continuity management.
- **ISO/IEC 27037** – Digital evidence handling.
- **ISO/IEC 27040** – Storage security.
- **ISO/IEC 27050** – Electronic discovery.
- **ITU-T X.805** – Security architecture for end-to-end communications.

4. Data Interoperability and Exchange

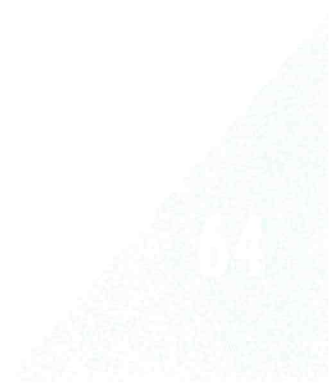
- **ISO/IEC 11179 series** – Metadata registries for consistent data exchange.
- **ISO/IEC 20933** – Governance of metadata.
- **HL7 FHIR (Fast Healthcare Interoperability Resources)** – For interoperability with health systems.
- **W3C XML / JSON standards** – Data interchange formats.

5. Accessibility and Inclusion

- **W3C Web Content Accessibility Guidelines (WCAG 2.1/2.2)** – Digital accessibility standards for web and mobile platforms.
- **ISO/IEC 40500:2012** – WCAG 2.0 adopted as an ISO/IEC standard.
- **ISO 9241-171** – Ergonomics of human-system interaction: accessibility of software.
- **ITU-T F.790** – Accessibility guidelines for telecommunications services.
- **EN 301 549** – European accessibility requirements for ICT products and services.

7. Cloud and Infrastructure Standards

- **ISO/IEC 27017** – Information security controls for cloud services.
- **ISO/IEC 27018** – Protection of PII in cloud computing.
- **NIST Cloud Computing Standards (SP 800 series)** – Guidance for secure use of cloud services.



Annex C – Grievance Registration Form

National Digital ID System (NDIDS)

ANNEX 2

Grievance Registration Form

Grievance Registration ID:	SDIN:
Name:	Email:
Gender:	Phone No.:
Village:	P.O Box:
Date of Complaint:	
Do you wish to keep your personal details confidential? ☐ No ☐ Yes	
Complainant (check boxes) ☐ Affected Person/s (AP) ☐ Government Ministry/ Organisation ☐ AP Representative ☐ Other (please specify) ☐ Relying Party	
Mode of Complaint: ☐ Letter ☐ In-person Complaint (walk-in) ☐ Phone Call ☐ Other (please specify) ☐ Email	
Type of Complaint (check boxes): ☐ Identity theft ☐ Wrongful release of information ☐ Stolen NID Card ☐ Misuse of information ☐ Fake NID Card ☐ Inaccurate recorded information ☐ Fees ☐ Wrongful cancellation of credentials ☐ Hackers ☐ Other (please specify) ☐ Breach of confidentiality	

National Digital ID System (NDIDS)

Documents comprising the complaint (*letter from financing institution, photo of fake ID, etc.*)

- 1.
- 2.
- 3.
- 4.

Short description and SPECIFIC location of the problem.

Person/Agency responsible for causing the problem:

- | | |
|--|--|
| ☐ Village/Individual | ☐ Financing institution |
| ☐ Hospital/Clinic | ☐ Bank |
| ☐ Educational institution | ☐ Other (<i>please specify</i>) |
| ☐ Government agency | |

Have you discussed or lodged this complaint with anyone else? If yes – what was their response?

Once your grievance has been resolved/responded to, how would you like to receive feedback/decision?
(tick boxes)

- | | | | |
|--------------------------------|---------------------------------|-------------------------------------|------------------------------------|
| ☐ Email | ☐ Letter | ☐ Phone Call | ☐ In-person |
|--------------------------------|---------------------------------|-------------------------------------|------------------------------------|

Signature of Complainant:

Date:

FOR OFFICE USE ONLY

Date received: _____

Name of Receiving Officer: _____ Signature: _____

Name & Signature of Person Lodging GRM: _____

