Sovrin Governance Framework V2
Master Document

PUBLIC REVIEW DRAFT 01

2018-10-31

https:/sovrin.org

STATUS NOTE

This is a living document maintained by the Sovrin Governance Framework (SGF) Working Group. This is NOT the latest version approved by the Sovrin Foundation Board of Trustees. Rather it is a "live" draft of the Sovrin Governance Framework V2 (SGF V2) open for comments and input from the Sovrin community.

To see the latest version approved by the Trustees in PDF format, see the links below. Note that the previous version was called the "Sovrin Trust Framework".

- Sovrin Provisional Trust Framework 2017-06-28 ⇐ LATEST APPROVED VERSION
- Sovrin Provisional Trust Framework 2017-03-22

The organization of SGF V2 represents a new overall document structure as explained in the Introduction section below. Under this new structure, this document serves as Annex 1 of the revised Sovrin Steward Agreement. Annex 2 is the standalone Sovrin Glossary.

PUBLIC REVIEW PERIOD

This document and all others in the Sovrin Governance Framework V2 are listed on the Sovrin Governance Framework page of the Sovrin Foundation website together with instructions about how to comment during the public review period.

Comments Received Via Separate Documents

1. 2018-11-18—From Stephan Wolf, CEO, GLEIF (Global Legal Entity Identifier Foundation)
2. 2018-11-18—from Eric Welton—on Sovrin Economic Policies

PREAMBLE

This document was produced by the Sovrin Governance Framework Working Group. The latest version was approved on_____ by the Sovrin Foundation Board of Trustees to become the operational trust framework for the Sovrin Network and the foundation for other Domain-Specific Governance Frameworks.

Sovrin Governance Framework Working Group: Drummond Reed (Chair), Scott Blackmer, John Best, Luca Boldrin, Mike Brown, Tim Brown, Shaun Conway, Mawaki Chango, Rick Cranston, Scott David, Oskar van Deventer, Steve Fulling, Nathan George, Dan Gisolfi, Nicky Hickman, Riley Hughes, Adam Lake, Jason Law, Darrell O'Donnell (SGF Coordinator), Adewale Omoniyi, Nick Thomas, Scott Perry, Antti Jogi Poikola, Elizabeth Renieris, Markus Sabadello, Joyce Searls, Peter Simpson, Andy Tobin, Eric Welton, George Simons, and Phil Windley.

Note: All terms in First Letter Capitals *except those in italics* are defined in the Sovrin Glossary. Terms in italic *First Letter Capitals* are names of Controlled Documents listed in Appendix A.

INTRODUCTION

The Sovrin Governance Framework (SGF) serves as the constitution for the Sovrin Network as well as a foundation for more specialized Domain-Specific Governance Frameworks (DSGFs) as shown in Figure 1.

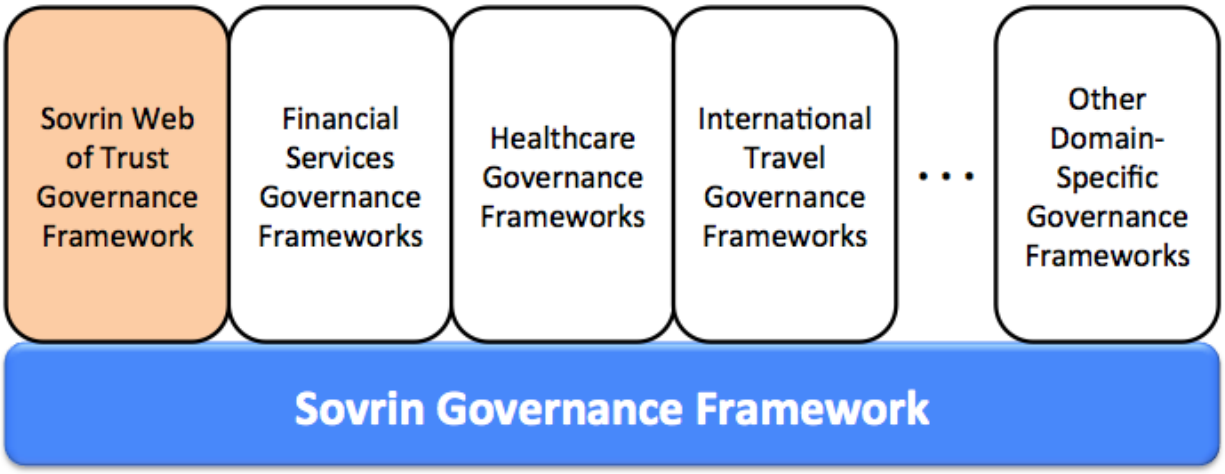

Figure 1: *The Sovrin Governance Framework provides a foundation for Domain-Specific Governance Frameworks.*

DSGFs leverage the principles, policies, terminology, and standards defined in the SGF to enable different Trust Communities to create their own specific governance frameworks, including their own digital credential definitions and issuance policies, to address their specific needs, e.g.:

- Governmental/Jurisdictional Bodies (e.g., countries, provinces, states, cities, sectors, consortia, distributed organisations)
- Accreditation Bodies (e.g., Colleges of Medicine; Legal Societies; Professional Associations)
- Formal Organizations and Affiliations (e.g., Non-Government Organizations; Trade Organizations; Credit Unions)
- Educational Institutions (e.g., Universities and Colleges)

Note that one specific DSGF, the Sovrin Web of Trust Governance Framework, is being developed by the Sovrin Foundation to define a standard set of digital credentials and Agent services for discovering, navigating, and verifying other DSGFs anywhere in the world.

The SGF formally consists of a set of interrelated documents as shown in Figure 2. The Sovrin Foundation will also publish additional operational documents, including FAQs, readiness checklists, design guidelines, sample schemas, etc., as needed.

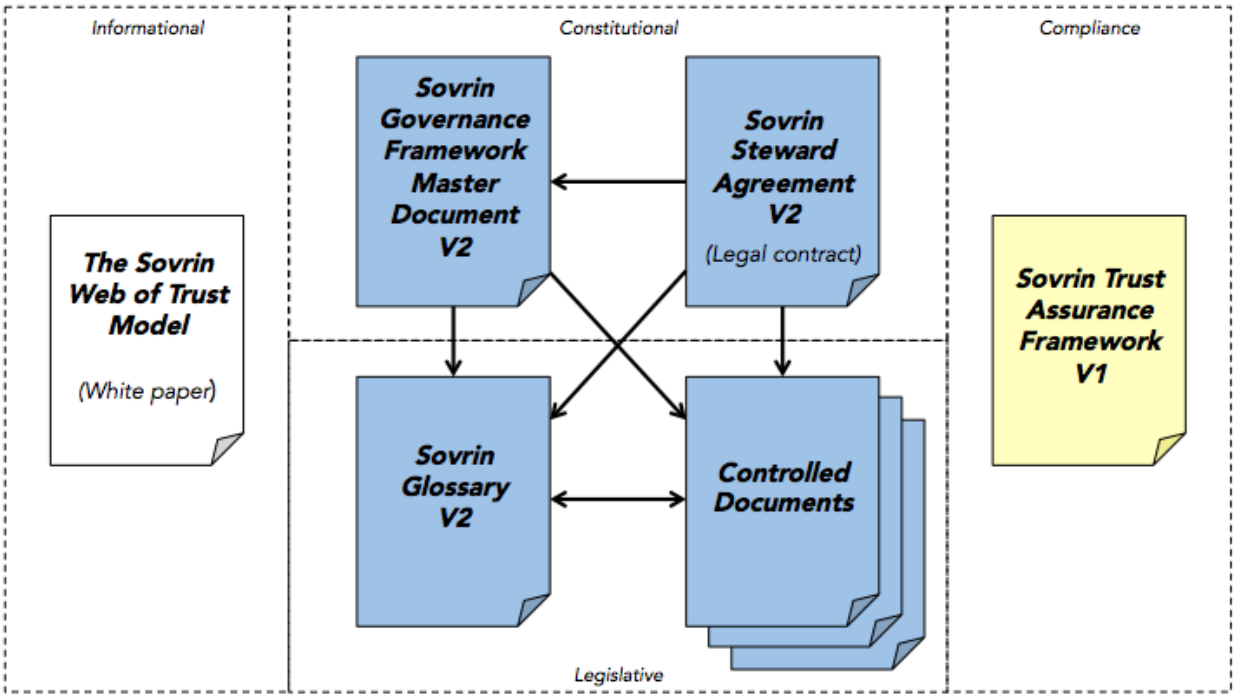

***Figure 2**: Documents in the Sovrin Governance Framework V2*
(Blue = Normative, Yellow = Assessment, White = Informative)

The normative documents in the SGF V2 are:

- **Sovrin Governance Framework V2**—the present document.
- **Sovrin Steward Agreement V2**—the legal contract between a Sovrin Steward and the Sovrin Foundation.
- **Sovrin Glossary V2**—the terminology and definitions that apply to all SGF documents and across Sovrin infrastructure as a whole.
- **Controlled Documents**—technical specifications, standards, policies, etc., that are independently maintained and versioned either by the Sovrin Foundation (e.g., the Sovrin Crisis Management Plan) or by external standards bodies (e.g., W3C, OASIS).

Another document, the **Sovrin Trust Assurance Framework**, does not directly govern Sovrin Infrastructure; rather it defines criteria and processes for assessing conformance of different Sovrin actors, including the Sovrin Foundation, to the policies of the Sovrin Governance Framework.

The final document is an informational white paper, **The Sovrin Web of Trust Model**, intended to serve as an overall guide to the SGF V2. It explains the key concepts of the decentralized web of trust architecture that is the mission of the Sovrin Foundation, the role of each of the documents in the SGF V2 family, how the governance model for the Sovrin Foundation and the SGF V2 works, and how it lays the foundation for DSGFs.

1 PURPOSE

The purpose of the Sovrin Ledger is to provide a decentralized global public utility for self-sovereign identity that serves as the foundation for the Sovrin Network.

The purpose of the Sovrin Network is to enable the Sovrin Web of Trust—a decentralized global web of trust interconnecting all Identity Owners and the Things they control.

The purpose of the Sovrin Governance Framework (SGF) is to define the business, legal, and technical policies for the Sovrin Web of Trust, thereby providing a foundational layer upon which Domain-Specific Governance Frameworks (DSGFs) can be built.

The purpose of the Sovrin Foundation is to administer decentralized governance for Sovrin Infrastructure on behalf of all Identity Owners.

2 CORE PRINCIPLES

The following principles guide the development of policies in the SGF and all DSGFs that inherit them.

2.1 Self-Sovereignty

Individuals are endowed with and possess an inalienable right to be Identity Owners with the ability to permanently control one or more Self-Sovereign Identities without reliance on any external administrative authority.

1. An Identity Owner alone shall determine which Identity Data describe its Identities.
2. With regard to managing its own Identity Data, an Identity Owner alone shall determine how and for what purpose(s) it is processed.
3. An Identity Owner alone shall determine who has access to its Identity Data.
4. An Identity Owner's Identity Data shall be portable as determined by the Identity Owner and enabled via Open Standards.
5. An Identity Owner alone shall have the right to Delegate control of these functions.

2.2 Guardianship

An Individual who does not have the capability to directly control that Individual's Identity Data (a Dependent) shall have the right to appoint another Identity Owner who has that capability (an Independent or an Organization) to serve as the owner's Guardian. If a Dependent does not have the capability to directly appoint a Guardian, the Dependent shall still have the right to have a Guardian appointed to act on the Dependent's behalf. A Dependent has the right to become an Independent by claiming full control of the Dependent's Identity Data. A Guardian has the obligation to promptly assist in this process provided the Dependent can demonstrate that the Dependent has the necessary capabilities. Guardianship shall not be confused with Delegation or Impersonation. Guardianship under the Sovrin Governance Framework should be mapped in the proper contexts to various legal constructs, including legal guardianship, power of attorney, conservatorship, living trusts, and so on.

2.3 Openness and Interoperability

Sovrin Infrastructure shall use Open Standards and avoid mechanisms that would prevent Identity Owners from having interoperability or portability of their Identity Data both within the Sovrin Network and with other networks and systems.

2.4 Accountability

Identity Owners shall be accountable to each other for conformance to the purpose, principles, and policies of the Sovrin Governance Framework. All Sovrin Entities shall be responsible for, and be able to demonstrate compliance with any other requirements of applicable law.

2.5 Sustainability

Sovrin Infrastructure shall be designed and operated to be technically, economically, socially, and environmentally sustainable for the long term.

2.6 Transparency

The Sovrin Foundation shall practice Open Governance, and the Sovrin Foundation and the Stewards in their Sovrin Ledger Roles shall operate with full openness and transparency to the greatest extent feasible consistent with the principles herein, including the proceedings of the Sovrin Board of Trustees and all Sovrin Governing Bodies, the development and distribution of Sovrin Open Source Code, the qualification and operation of Stewards, and any revisions to the Sovrin Governance Framework.

2.7 Collective Best Interest

The Sovrin Foundation shall act in the collective best interests of all Identity Owners and shall not favor the interests of any single Identity Owner or group of Identity Owners over the interests of the Sovrin Community as a whole.

2.8 Decentralization by Design

2.8.1 General

Sovrin Infrastructure shall be decentralized to the greatest extent possible consistent with the other principles herein. As the business, legal, and technical limitations of decentralization may change over time, the Sovrin Foundation shall continuously examine all points of control, decision, and governance to seek ongoing conformance with this principle.

2.8.2 Diffuse Trust

Sovrin Infrastructure shall not concentrate power in any single Individual, Organization, Jurisdiction, Industry Sector, or other special interest to the detriment of the Network as a whole. Diffuse Trust shall take into account all forms of diversity among Identity Owners.

2.8.3 Web of Trust

Sovrin Infrastructure shall be designed to not favor any single root of trust, but empower any Sovrin Entity to serve as a root of trust and enable all Sovrin Entities to participate in any number of interwoven Trust Communities.

2.8.4 High Availability

Sovrin Infrastructure shall be designed and implemented to maximize availability of the Sovrin Network.

2.8.5 No Single Point of Failure

Sovrin Infrastructure shall be designed and implemented to not have any single point of failure.

2.8.6 Regenerative

Sovrin Infrastructure shall be designed so that failed components can be quickly and easily replaced by other components.

2.8.7 Distributive

Sovrin Infrastructure shall be designed and implemented such that authority is vested, functions performed, and resources used by the smallest or most local part of the Sovrin Community that includes all relevant and affected parties. Deliberations should be conducted and decisions made by bodies and methods that reasonably represent all relevant and affected parties and are dominated by none[1].

2.8.8 Innovation at the Edge

The continued development of the Sovrin Infrastructure shall encourage innovation to take place at the edges of the network among the members of the Sovrin Community most directly involved or impacted.

2.9 Inclusive by Design

2.9.1 General

The design, governance, and operation of Sovrin Infrastructure shall follow the principles of Inclusive Design to serve the widest possible community of Identity Owners.

2.9.2 Identity for All

Consistent with the United Nations Sustainable Development Goal 16.9, the Sovrin Foundation and the Sovrin Network shall promote peaceful and inclusive societies for sustainable development; enable access to justice for all; and facilitate effective, accountable, and inclusive institutions at all levels by being accessible to, and inclusive of all Identity Owners without discrimination and with accommodation for physical, economic, or other limitations of Identity Owners to the greatest extent feasible.

2.9.3 People-Centered Design

Sovrin Developers shall put people at the heart of the design process and enable them to control their own user experience.

2.9.4 Design for Difference

Sovrin Developers shall strive to understand differences in capabilities and preferences across all potential members of the Sovrin Community and provide adaptable solutions to meet the needs of all potential members.

2.9.5 Test Across Contexts

Sovrin Developers shall test Sovrin solutions for use in different Identity Owner environments and contexts.

[1] Attribution to the Core Principles of Chaordic Commons: http://www.chaordic.org/

2.9.6 Offer Choice

Sovrin Developers shall design flexibility by offering a choice of ways to achieve the same outcome.

2.9.7 Maintain Consistent Experience

Sovrin Developers shall design comparable experiences for all of their user communities that use consistent design elements and language.

2.10 Privacy by Design

2.10.1 General

The design, governance, and operation of Sovrin Infrastructure shall follow the Seven Foundational Principles of Privacy by Design to the greatest extent possible consistent with the other principles herein. These principles can be summarized as:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality—Positive-Sum, not Zero-Sum
5. End-to-End Security—Full Lifecycle Protection
6. Visibility and Transparency—Keep it Open
7. Respect for User Privacy—Keep it User-Centric

2.10.2 Pairwise Pseudonyms by Default

Agents using the Sovrin Protocol shall default to assigning Pairwise Pseudonyms, Pairwise Public Keys, and, when necessary, Pairwise Service Endpoints whenever forming a Connection unless specifically directed otherwise by an Identity Owner.

2.10.3 Selective Disclosure by Default

Issuers, Holders, and Verifiers using the Sovrin Protocol shall default to issuing, holding, and accepting Credentials that support Zero-Knowledge Proofs and privacy-respecting Revocation Registries by default.

2.10.4 Governance Framework Disclosure by Default

Sovrin Entities shall by default disclose the Governance Framework under which a Connection is created, an Interaction is performed, or a Credential is exchanged. Agents shall by default notify their Identity Owner of any conflict between the Identity Owner's privacy preferences and the Governance Framework's privacy policies.

2.10.5 Owner Controlled Storage by Default

Agents shall store Private Data in decentralized data storage controlled by the Identity Owner by default.

2.10.6 Anti-Correlation by Design and Default

The design and implementation of all components of Sovrin Infrastructure shall avoid any unnecessary correlation.

2.10.7 Guardian and Delegate Confidentiality

The use of a Guardian or Delegate may be confidential information and shall only be disclosed with the authorization of the Identity Owner.

2.11 Security by Design

2.11.1 General

The design, governance, and operation of Sovrin Infrastructure shall follow the principles of Security by Design to the greatest extent feasible consistent with the other principles herein.

2.11.2 System Diversity

The process and policies for selecting Stewards shall optimize availability and security by maximizing diversity of hosting locations, environments, networks, and systems.

2.11.3 Secure Defaults

The default configuration settings and user experience of the applications using Sovrin Infrastructure shall enforce strong protection by default, including encryption by default.

2.11.4 Least Privilege

Access and authorization of the applications, Agents, and network services that use and comprise Sovrin Infrastructure shall subscribe to the concept of least privilege.

2.11.5 Anti-Impersonation

Applications shall be designed to not knowingly allow any party other than the Identity Owner to act as (impersonate) the Identity Owner. Impersonation does not include Guardianship or Delegation.

2.11.6 Auditability

Transactions in Sovrin Infrastructure and actions of application using Sovrin Infrastructure that require auditing shall be immutably logged, in a tamper-evident way, and be available to verify processing.

2.11.7 Secure Failure

Applications using Sovrin Infrastructure shall be designed to take an exception or error path that will not create a security weakness exploitable by bad actors.

2.11.8 Pervasive Mediation

Applications using Sovrin Infrastructure shall not assume authorization is transitive across time and/or space—rather security mechanisms shall check every access to every object, and authorize each action on its own merits, just in time.

2.12 Data Protection by Design and Default[2]

2.12.1 General

Sovrin Entities, in the processing of personal data, shall adhere to the following data protection principles to the greatest extent feasible consistent with the other principles herein.

2.12.2 Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the Individual.

2.12.3 Purpose Limitation

Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes, shall not be considered incompatible with the original processing purposes.

2.12.4 Data Minimization

Personal data must be relevant and limited to that which is necessary in relation to the purposes for which it is being processed.

2.12.5 Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that where personal data is inaccurate it is erased or rectified without delay.

2.12.6 Storage Limitation

Personal data must be kept in a form which permits identification of Individuals for no longer than the duration necessary for the purposes for which the personal data is being processed.

2.12.7 Integrity and Confidentiality

Personal data must be processed in a manner that provides appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures (i.e., information security).

---

[2] Privacy and data protection are separate but related concepts. The right to privacy is enshrined in Article 12 of the Universal Declaration of Human Rights (http://www.un.org/en/universal-declaration-human-rights/) and Article 7 of the EU Charter of Fundamental Rights (the "EU Charter"—http://www.un.org/en/universal-declaration-human-rights/). Data protection is a fundamental right under Article 8 of the EU Charter. While privacy—and data privacy by extension—have to do with the freedom from interference in the private and family life of an individual, data protection has to do with a specific set of enumerated principles for the protection of an individual's personal data. Data protection is also important when the data belongs to Organizations or Things.

3 CORE POLICIES

3.1 Stewardship

In keeping with all Core Principles and especially the Decentralization by Design and Security by Design principles:

1. Policies, practices, procedures, and algorithms governing participation of Stewards and operation of Nodes MUST follow all Core Principles.
2. The Sovrin Foundation MUST publish the *Steward Business Policies* as a Controlled Document managed as specified by *Sovrin Governing Bodies*.
3. The Sovrin Foundation MUST publish the *Steward Technical Policies* as a Controlled Document managed as specified by *Sovrin Governing Bodies*.

3.2 Guardianship

In keeping with the Guardianship principle, a Guardian SHOULD:

1. Act in the Dependent person's best interest.
2. Exercise good judgment and carefully manage responsibilities.
3. Avoid commingling—keep Dependent's property separate (e.g., separate DIDs, Public Keys, Wallets, Vaults, etc.).
4. Keep detailed records of all actions taken on behalf of the Dependent.
5. Not violate the Anti-Impersonation principle (section 2.11.5).
6. Be subject to applicable legal structures regarding the granting and revocation of Guardianships.

3.3 Inclusion

In keeping with the Inclusive by Design principles:

1. Access to the Sovrin Network MUST be open to all Individuals and Organizations on a comparable basis without intentional exclusion of specific persons or communities.
2. Developers SHOULD design for different capabilities in different contexts considering:
    a. Digital Exclusion (e.g., access to connected devices)
    b. Physical or Cognitive Exclusion (e.g., disability or incapacity)
    c. Political & Social Status (e.g., stateless individuals; being a child or a woman)
    d. Financial Status (e.g., having no income)
    e. Literacy & Language (e.g., low literacy or not speaking local language)

3.4 Trust Assurance

In keeping with all Core Principles and especially the Decentralization by Design principles:

1. The Sovrin Foundation MUST specify policies, practices, and procedures for assessing conformance to the Sovrin Governance Framework the *Sovrin Trust Assurance Framework* as a Controlled Document managed as specified by *Sovrin Governing Bodies*.

2. The Sovrin Governance Framework MUST be designed to provide a foundation for Domain-Specific Governance Frameworks (DSGFs) based on the Sovrin Web of Trust Model.
3. As soon as feasible, the Sovrin Foundation MUST publish a DSGF, the Sovrin Web of Trust Governance Framework, whose purpose is to enable standard decentralized discovery, navigation, and verification services for DSGFs.
4. The Sovrin Foundation MUST publish the *Sovrin Trust Mark Policies* as a Controlled Document managed as specified by *Sovrin Governing Bodies*.
5. An Entity serving in one of the Sovrin Infrastructure Roles who meets the requirements in the Sovrin Trust Assurance Framework MAY use the appropriate Sovrin Trust Mark as specified in *Sovrin Trust Mark Policies*.

3.5 Economics

In keeping with the Sustainability principle:

1. The Sovrin Foundation MUST publish the *Sovrin Economic Policies* as a Controlled Document managed as specified by *Sovrin Governing Bodies* in conjunction with Sovrin Foundation legal counsel.
2. The Sovrin Foundation MUST manage Ledger Fees and any mechanism used for paying them to ensure economic viability and sustainability for Sovrin Infrastructure in keeping with its charter as a non-profit public trust organization.
3. Transactors MUST have write access to any of the publicly available Transaction Types for the Main Ledger and the Payment Ledger provided the Entity includes the associated Ledger Fee for the Transaction Type as specified in the Ledger Fee Table.
4. The Sovrin Foundation MUST retain a qualified Auditor to publish an annual public audit of Sovrin Foundation finances.

4 GOVERNANCE

The Sovrin Governance Framework Master Document and the Controlled Documents listed in Appendix A shall be revised from time to time as Sovrin Infrastructure grows and evolves. The policies in this section govern this process.

4.1 General

1. The Sovrin Foundation MUST publish *Sovrin Governance Bodies* as a Controlled Document managed by the Sovrin Board of Trustees.
2. *Sovrin Governance Bodies* MUST specify the Sovrin Governing Body for each Controlled Document.
3. All Sovrin Governance Framework documents, including Controlled Documents, MUST use keywords in policies as defined in IETF RFC 2119.

4.2 Revisions to the Sovrin Governance Framework Master Document

These policies apply to the present document, exclusive of Appendix A.

1. Revisions to the SGF Master Document MUST respect the Purpose and Core Principles.
2. The commencement of any revision process MUST be publicly announced by the Sovrin Foundation no later than the time of commencement.
3. Participation in the revision process MUST be available to all members of the Sovrin Community.
4. Proposed revisions MUST be publicly announced by the Sovrin Foundation and subject to a minimum 30 day public review period following the announcement.
5. Revisions MUST be approved by a supermajority vote of at least two-thirds of the Sovrin Board of Trustees after the conclusion of the public review period and before the revision takes effect.
6. Prior to the next major revision of the SGF Master Document, the Sovrin Foundation MUST put in place new governance policies implementing the Sovrin Decentralization by Design principles.

4.3 Revisions to Controlled Documents

These policies apply to the Controlled Documents listed in Appendix A.

1. The list of Controlled Documents in Appendix A, as well as each Controlled Document on that list, MAY be revised independently from the Sovrin Governance Framework Master Document (the present document).
2. A Controlled Document MUST be stored in and use the change control mechanisms established by the official Sovrin Code Repository at the permanent location for the document published in Appendix A.
3. Proposed revisions MUST be subject to a minimum 30 day public review period publicly announced by the Sovrin Foundation.
4. Revisions to a Controlled Document MUST be approved by the Sovrin Board of Trustees after the conclusion of the public review period and before the revision takes effect.

5 APPENDIX A: CONTROLLED DOCUMENTS

The following Controlled Documents are normative components of the Sovrin Governance Framework V2. See section 4.3.

5.1 Definitions

Document Name	Description	Governed By	Normative Location
Sovrin Glossary	Definitions of all terms used in the SGF	Sovrin Governance Framework Working Group	Google Doc Version Final location will be: https://sovrin.org/library/glossary/
Sovrin Governing Bodies	Definitions of governing bodies within the Sovrin Foundation	Sovrin Board of Trustees	Google Doc Version
Sovrin Ledger Transaction Data	Defines the data and metadata process by a Steward Node	Sovrin Technical Governance Board	Google Doc Version

5.2 Specifications

Document Name	Description	Governed By	Normative Location
Decentralized Identifiers 1.0	Specification for DIDs and DID documents	W3C Credentials Community Group	https://w3c-ccg.github.io/did-spec/
Sovrin DID Method 1.0 Specification	Specification for DIDs on the Sovrin Ledger or Sovrin Microledgers	Sovrin Technical Governance Board	[Permanent link] https://github.com/sovrin-foundation/sovrin/blob/master/spec/did-method-spec-template.html
Verifiable Credentials Data Model 1.0	Specification for verifiable credentials	W3C Verifiable Claims Working Group	https://w3c.github.io/vc-data-model/

5.3 Policies

Document Name	Governs	Governed By	Normative Location
Sovrin Governing Body Policies	Chartering and functioning of Sovrin Governing Bodies	Sovrin Board of Trustees	Google Doc Version
Sovrin Ledger Access Policies	Read and write access to the Sovrin Ledger	Sovrin Governance Framework Working Group	Google Doc Version
Sovrin Steward Business Policies	Steward qualification, enrollment, and operational status	Steward Qualification Committee	Google Doc Version
Sovrin Steward Technical Policies	Technical requirements for operating and protecting a Node	Sovrin Technical Governance Board	Google Doc Version
Sovrin Economic Policies	Market incentives in the Sovrin Network	Economic Advisory Council	Google Doc Version
Sovrin Trust Mark Policies	Acceptable uses of the Sovrin Trust Mark	Sovrin Governance Framework Working Group	Google Doc Version

5.4 Frameworks

Document Name	Governs	Governed By	Normative Location
Sovrin Trust Assurance Framework	Trust assurance for SGF actors	Sovrin Governance Framework Working Group	Google Doc Version