DignifID™ Animals Foundation Governance Framework V1

Master Document v01

2019-06-01

This is an official document of the DignifID Governance Framework V1,
as approved by the DignifID Animals Foundation Directors.

If you have comments or suggestions, we invite you to contribute them to the living community version of this document—access is open to anyone.

NOTE: *This document is based on the content of the Sovrin Governance Framework Master Document.*

This page intentionally left blank

1 PREAMBLE

This document was produced on behalf of the DignifID Board of Directors by the DignifID Governance Framework Working Group. The latest version (v0.2) was approved by the DignifID Animals Foundation Board of Directors on **XX YY 2019**.

Acknowledgements—DignifID Governance Framework Working Group: Drummond Reed (Chair), Darrell O'Donnell, Nicky Hickman, Scott Perry, Chris Raczkowski, Andrew Rowan, Celia Yeung, Liwen Zhang, etc., etc., etc. [NOTE: final list is TBD]

Note: All terms in First Letter Capitals *except those in italics* are defined in: (a) the DignifID Glossary if the term begins with "Animal" or "DignifID," or (b) the Sovrin Glossary otherwise. Terms in italic *First Letter Capitals* are either heading names in this document or names of Controlled Documents listed in Appendix A.

2 INTRODUCTION

The DignifID Governance Framework (DGF) serves as the constitution for the DignifID Community. The DGF is a Domain-Specific Governance Framework (DSGF), which is founded on and leverages the Sovrin Governance Framework, as illustrated in Figure 1.

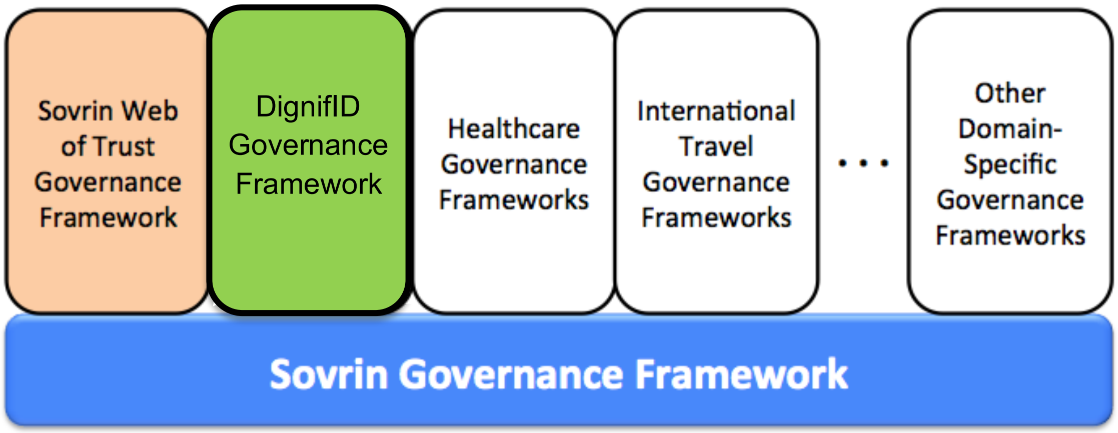
Sovrin Web of Trust Governance Framework
DignifID Governance Framework
Healthcare Governance Frameworks
International Travel Governance Frameworks
• • •
Other Domain-Specific Governance Frameworks
Sovrin Governance Framework

Figure 1: *The Sovrin Governance Framework (SGF) provides a foundation for Domain-Specific Governance Frameworks, such as the DignifID Governance Framework.*

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 white papers, FAQs, readiness checklists, design guidelines, sample schemas, etc., as needed.

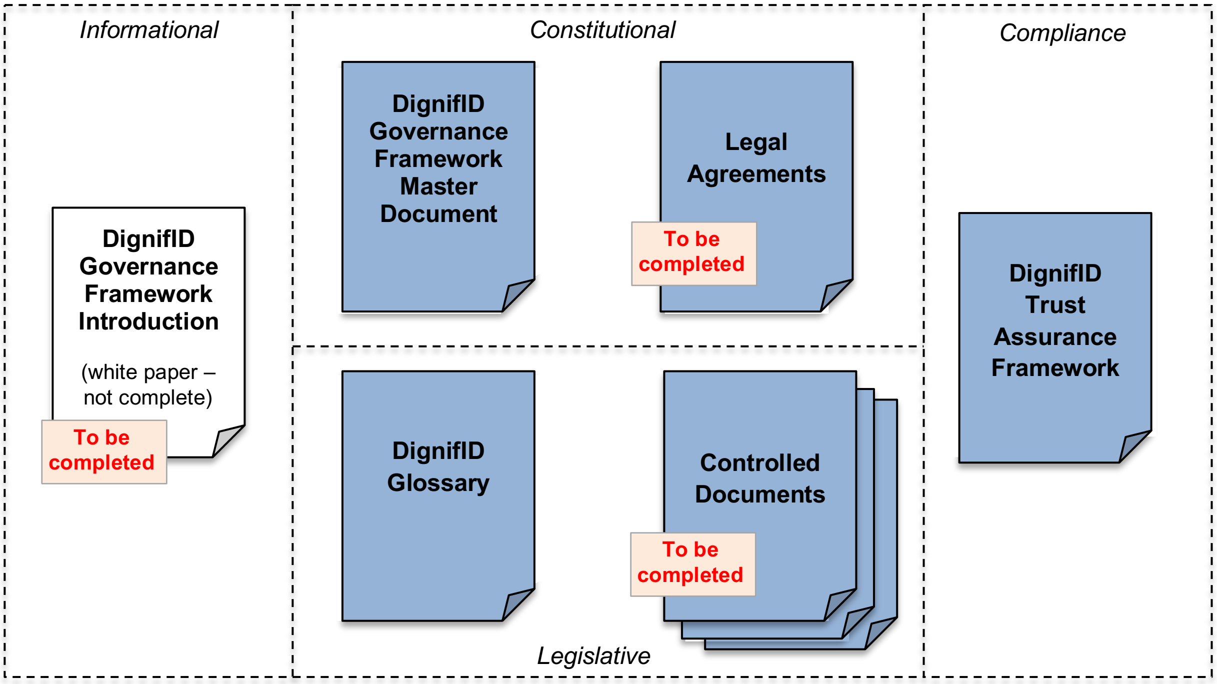
Informational
Constitutional
Compliance
DignifID Governance Framework Master Document
Legal Agreements
To be completed
DignifID Governance Framework Introduction
(white paper – not complete)
To be completed
DignifID Trust Assurance Framework
DignifID Glossary
Controlled Documents
To be completed
Legislative

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

The normative documents in the DGF are:

- **DignifID Governance Framework -** the present document.
- XX legal agreements: (TBD)
  a. **Transaction Author Agreement -** ??
  b. **Transaction Endorser Agreement** - ??
- **DignifID Glossary -** the terminology and definitions that apply to all SGF documents and across Sovrin infrastructure as a whole.
- **Controlled Documents -** technical specifications, standards, and policies that are independently maintained and versioned either by the DignifID Animals Foundation or external standards bodies (e.g., Sovrin, W3C, etc.).

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

The final document is an informational white paper, **An Introduction to the DignifID Governance Framework,** intended to serve as an overall guide to the DGF.

The DGF adopts and leverages all aspects of the Sovrin Governance Framework, and DGF documentation follows the same structure, purpose and policies as the Sovrin Governance Framework, except as may be explicitly stated otherwise within the DignifID Governance

Framework. Furthermore, the DGF depends on the Sovrin Network for identity related communications.

3 PURPOSE

The DignifID Governance Framework (***DGF***) establishes the structures and policies that govern the DignifID Digital Identity System (***DDIS***). The core purpose of the DDIS is to provide universal trusted identity for Animals, as well as for humans and organizations that participate in the DignifID Community.

The purpose of the DignifID Animals Foundation (***DignifID***), with regard to the DGF, is to govern and administer the DDIS on behalf of all DignifID Identity Owners, DignifID Credential Issuers, and the entire DignifID Community, such that any animal can have access to robust digital identity managed by the animal’s guardian (i.e. a person or organization).

4 CORE PRINCIPLES

The following principles guide the development of policies in the DignifID Governance Framework.

4.1 Provide Trusted Identity

The leading Principle of the DignifID Governance Framework is that all Animals and Animal Guardians should have access to a free, secure, private, decentralized and robust digital identity system. Furthermore, the DignifID Digital Identity System should be at least equal in capability with any other digital identity service enjoyed any humans and Organizations.

4.2 Decentralized Digital Identity

(NOTE: this section is the same as SGF Master Document section 2.1)

Identity Owners should have the ability to permanently control, directly or with the support of a Guardian, one or more Decentralized Digital 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.
6. If a Guardian is fully responsible for a Dependent Identity Owner, said Guardian is responsible to manage all rights outlined above for said Dependent.

4.3 Guardianship

An Individual who does not have capability to control said Individual's Identity Data (i.e. a Dependent) shall have the right to have another Individual or Organization which does have such capability to serve as a 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, and such Dependent's 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 DignifID Governance Framework endeavors to accommodate any legal and cultural constructs, including legal guardianship, power of attorney, conservatorship, living trusts, and generally accepted standards established by a society which may or may not be codified in laws or regulations, and so on.

4.4 Openness and Interoperability

(NOTE: this section is the same as SGF Master Document section 2.3)

DignifID and 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.

4.5 Accountability

(NOTE: this section is the same as SGF Master Document section 2.4)

Identity Owners shall be accountable to each other for conformance to the purpose, principles, and policies of the Sovrin and DignifID Governance Frameworks. All DignifID Entities shall be responsible for, and within the scope of their individual abilities, be able to demonstrate compliance with, any other requirements of applicable law. Nothing in the DignifID Governance Framework shall require a DignifID Entity to breach applicable law in order for it to perform its obligations under the DignifID Governance Framework.

4.6 Sustainability

DignifID and Sovrin Infrastructure shall be designed and operated to be technically, economically, socially, and environmentally sustainable, and contribute to the improvement of the well-being of Animals and their guardians for the long term.

4.7 Transparency

The DignifID Animals Foundation shall practice Open Governance. It shall operate with full openness and transparency to the greatest extent feasible consistent with the principles herein, including the proceedings of the DignifID Board of Directors and all DignifID Governing Bodies, and any revisions to the DignifID Governance Framework.

4.8 Collective Best Interest

The DignifID Animals Foundation shall act in the collective best interests of the DignifID

Community and shall not favor the interests of any single Identity Owner, or group of Identity Owners, over the interests of the DignifID Community as a whole.

4.9 Decentralization by Design

(NOTE: this section is materially the same as SGF Master Document section 2.8)

4.9.1 General

DignifID and 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 DignifID Animals Foundation shall continuously examine all points of control, decision, and governance to seek ongoing conformance with this principle.

4.9.2 Diffuse Trust

DignifID and 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.

4.9.3 Web of Trust

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

4.9.4 Censorship Resistance

DignifID and Sovrin Infrastructure shall be designed to resist censorship of any Entity while remaining compliant with all applicable laws.

4.9.5 High Availability

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

4.9.6 No Single Point of Failure

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

4.9.7 Regenerative

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

4.9.8 Distributive

DignifID and Sovrin Infrastructure shall be designed and implemented such that authority is vested, functions are performed, and resources are used broadly across the DignifID and Sovrin

Communities, such that any relevant and affected parties may participate. DGF 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]

4.9.9 Innovation at the Edge

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

4.10 Inclusive by Design

(NOTE: this section is materially the same as SGF Master Document section 2.9)

4.10.1 General

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

4.10.2 Identity for All

Consistent with the United Nations Sustainable Development Goal 16.9, the DignifID Animals 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, species or other limitations of Identity Owners, to the greatest extent feasible.

4.10.3 Animal + Human Centric Design

DignifID Developers shall put all Animals and their Guardians (humans or organizations) at the heart of the design process and enable Animal Guardians, to control their own user experience. Animal + HumanCentered Design takes into consideration the care and sustainability of natural and built environments necessary for the wellbeing of all Animals and humans.

4.10.4 Design for Difference

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

4.10.5 Test Across Contexts

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

4.10.6 Offer Choice

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

DignifID Developers shall design for flexibility, by offering a choice of ways to achieve the same outcome where necessary.

4.10.7 Maintain Consistent Experience

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

4.11 Privacy by Design

(NOTE: this section is materially the same as SGF Master Document section 2.10)

4.11.1 General

The design, governance, and operation of DignifID and Sovrin Infrastructure, shall follow the Seven Foundational Principles of Privacy by Design to the greatest extent possible, and 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

4.11.2 Pairwise Pseudonyms by Default

Agents using Sovrin and DignifID Protocols 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.

4.11.3 Selective Disclosure by Default

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

4.11.4 Governance Framework Disclosure by Default

DignifID 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.

4.11.5 Owner Controlled Storage by Default

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

4.11.6 Anti-Correlation by Design and Default

DignifID and Sovrin Infrastructure shall be designed and implemented to avoid correlation of an Identity Owner, or of a Thing associated with an Identity Owner, without the direct knowledge and informed consent of the Identity Owner.

4.11.7 Guardian and Delegate Confidentiality

Utilization of a Guardian or Delegate by a DignifID Identity Owner may be confidential information and shall only be disclosed with the authorization of the Identity Owner (where possible) and of the Guardian and/or Delegate.

4.12 Security by Design

(NOTE: this section is materially the same as SGF Master Document section 2.11)

4.12.1 General

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

4.12.2 System Diversity

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

4.12.3 Secure Defaults

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

4.12.4 Least Privilege

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

4.12.5 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.

4.12.6 Auditability

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

4.12.7 Secure Failure

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

4.12.8 Pervasive Mediation

Applications using DignifID and 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, in a timely manner.

4.13 Data Protection by Design and Default[2]

(NOTE: this section is materially the same as SGF Master Document section 2.12)

4.13.1 General

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

4.13.2 Lawfulness, Fairness, and Transparency

DignifID Entity Data must be processed lawfully, fairly, and in a transparent manner in relation to the relevant DignifID Entity, or the DignifID Entity's Guardian or Controller.

4.13.3 Purpose Limitation

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.

4.13.4 Data Minimization

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

4.13.5 Accuracy

DignifID Entity 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.

4.13.6 Storage Limitation

DignifID Entity data must be kept in a form which permits identification of Entities for no longer than the duration necessary for the purposes for which such data is being processed.

[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"—https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en). 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.

4.13.7 Integrity and Confidentiality

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

5 CORE POLICIES

5.1 Guardianship

DignifID governance policies for Animal Guardianship are equal to the SGF policies for Guardianship. However, the DGF is unique in that a DignifID Animal is an Identity Owner and has a Guardian (i.e. and Animal Guardian). In keeping with generally accepted Guardianship principles, a Guardian SHOULD:

1. Act in the Dependent's best interest.
2. Exercise good judgment and carefully manage Guardianship responsibilities.
3. Avoid commingling—keep Dependent's property separate (e.g., separate DIDs, Public Keys, Wallets, Vaults, etc.).
4. When necessary, 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.

5.2 Inclusion

(NOTE: this section is materially the same as SGF Master Document section 3.3)

In keeping with the Inclusive by Design principles:

1. Access to the Sovrin Network and DignifID Infrastructure 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 limitations (e.g., access to connected devices)
    b. Physical or cognitive limitations (e.g., disability or incapacity)
    c. Political & social status (e.g., stateless individuals; being a child, a woman, an Animal, Natural Thing, etc.)
    d. Financial status (e.g., having no income)
    e. Literacy & language (e.g., low literacy or not speaking a language)

5.3 Trust Assurance

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

1. The DignifID Animals Foundation MUST specify policies, practices, and procedures for assessing conformance to the Sovrin Governance Framework and DignifID Governance Framework by publishing and maintaining the *DignifID Trust Assurance Framework* as a Controlled Document managed, as specified, by *DignifID Governing Bodies*.
2. The DignifID Animals Foundation MUST publish the *DignifID Trust Mark Policies* as a Controlled Document managed as specified by *DignifID Governing Bodies*.
3. A DignifID Entity who meets the requirements in the DignifID Trust Assurance Framework MAY use the appropriate DignifID Trust Mark as specified in *DignifID Trust Mark Policies*.

5.4 Economics

In keeping with the Sustainability principle:

1. The DignifID Animals Foundation MUST publish the *DignifID Economic Policies* as a Controlled Document managed as specified by *DignifID Governing Bodies* in conjunction with DignifID Animals Foundation legal counsel.
2. The DignifID Animals Foundation MUST publish Ledger Fees and any DignifID fees to ensure economic viability and sustainability for the DignifID Animals Foundation, in keeping with its charter as a non-profit public trust organization.
3. The DignifID Animals Foundation MUST retain a qualified Auditor to publish an annual public audit of DignifID Animals Foundation finances and DignifID Credentials management performance.

6 GOVERNANCE

(NOTE: this section is materially the same as SGF Master Document section 4)

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

6.1 General

1. The DignifID Animals Foundation MUST publish *DignifID Governance Bodies* as a Controlled Document managed by the DignifID Board of Directors.
2. *DignifID Governance Bodies* MUST specify the DignifID Governing Body for each Controlled Document.
3. All DignifID Governance Framework documents, including Controlled Documents, MUST use keywords in policies as defined in IETF RFC 2119.
4. All DignifID Governance Framework documents MAY be revised to add non-normative content, such as references to appendices, white papers, or other explanatory materials, without triggering a formal revision review process as defined in this Section 6.

6.2 Revisions to the DignifID Governance Framework Master Document

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

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

6.3 Revisions to Controlled Documents

These policies apply to any normative revision 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 DignifID 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 DignifID Document Repository at the permanent location for the document published in Appendix A.
3. Proposed revisions MUST be subject to a minimum 30 day DignifID Community review period announced by the DignifID Animals Foundation.
4. Revisions to a Controlled Document MUST be approved by the DignifID Board of Directors after the conclusion of the review period and before the revision takes effect.

APPENDIX A: CONTROLLED DOCUMENTS

The following Controlled Documents are normative components of the DignifID Governance Framework V1 as defined in section 6.3. All documents in the DignifID Governance Framework are published by the DignifID Foundation in two forms:

1. A static PDF document representing the current approved version. This document is hosted on the Sovrin Foundation web server. A link is always available via the DignifID Governance Framework page and the table below.
2. A living community version of the document on which anyone can comment. This is hosted as a Google document so anyone can make suggestions about future improvements to be considered by the DignifID Governance Framework Working Group.

All SGF documents may be found at the following link: SGF Public Documents

All DGF documents may be found at the following link: XXX

Definitions

Document Name	Description	Governed By	Normative Location
DignifID Glossary	Definitions of all terms used in the DGF	DignifID Governance Framework Working Group	Approved PDF Version Approved Linkable Version (see note above) Living Community Version
DignifID Governing Bodies	Definitions of governing bodies within the DignifID Animals Foundation	DignifID Board of Directors	Approved PDF Version Living Community Version

Specifications

Document Name	Description	Governed By	Normative Location
DignifID Credential Specifications	Credential specifications, and Credential Issuer Policies	DignifID Governance Framework Working Group	
Verifiable Credentials Data Model 1.0	Specification for verifiable credentials	W3C Verifiable Claims Working Group	https://w3c.github.io/vc-data-model/

Policies

Document Name	Governs	Governed By	Normative Location
DignifID Governing Body Policies	Chartering and functioning of DignifID Governing Bodies	DignifID Board of Directors	Approved PDF Version Living Community Version
DignifID Economic Policies	Fees for DignifID services	Economic Advisory Council	Approved PDF Version Living Community Version
DignifID Credential, and Credential Issuer Policies			
DignifID Trust Mark Policies	Acceptable uses of the DignifID Trust Mark	DignifID Governance Framework Working Group	Approved PDF Version Living Community Version

Frameworks

Document Name	Governs	Governed By	Normative Location
DignifID Trust Assurance Framework	Trust assurance for DGF actors	DignifID Governance Framework Working Group	Approved PDF Version Google Doc Version