# Sovrin Steward Technical Policies

This is a Controlled Document of the Sovrin Governance Framework V2 approved by the Sovrin Board of Trustees. 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. If you are interested in joining the Sovrin Governance Framework Working Group, please visit our Meeting Page.

| | |
|---|---|
| **Document Name** | Sovrin Steward Technical Policies |
| **Version** | V1 |
| **Approval Date** | 2018-12-18 |
| **Status** | Final |
| **Governs** | General Requirements, Node Technical Requirements, Security Requirements, Operating Requirements, Node Selection Algorithm, Reporting Requirements |
| **Governed By** | Technical Governance Board |

## 1. General Requirements

A Steward Node:

1. MUST be available to run as a Validator Node or Observer Node on any of the formal ledgers that make up the Sovrin Network.
2. MUST run a release of the Sovrin Open Source Code as approved and designated by the Technical Governance Board (TGB).
3. MUST facilitate an upgrade to a new version of the Sovrin Open Source Code within three (3) business days of a new release that has been: a) recommended by the Sovrin TGB, and b) accepted by a vote of any other relevant Sovrin Governing Body (such as the Steward Council).
4. MUST register all Node configuration data required by the Pool Ledger in a timely

manner, keeping information up to date within three (3) business days of changes.

5. MUST have at least two (2) IT-qualified persons assigned to administer the node, and at least one other person that has adequate access and training to administer the Node in an emergency, such as the network being unable to reach consensus or being under attack. See the Sovrin Crisis Management Plan for details.
6. MUST supply contact info for all administrators to the Sovrin Foundation, whose accuracy is tested at least quarterly (e.g., by sending an email and/or text that doesn't bounce).
7. MUST maintain a system backup or snapshot or image such that recovering the system from failure could be expected to take one hour or less.

# 2. Node Technical Requirements

The following requirements apply to Steward Nodes on the Mainnet. Nodes on any other net should be similar, but requirements may be downgraded from MUST to SHOULD.

1. MUST run on robust server-class hardware.
2. If a Node is run on a VM, the Steward:
    a. MUST run on a mainstream hypervisor that receives timely patches from its vendor or community.
    b. SHOULD apply hypervisor patches on a regular basis.
3. The Node MUST run in an OS that is dedicated to the validator, i.e., a single-purpose (physical or virtual) machine that MUST run Sovrin Open Source Code, MAY run other software approved by the TGB, and MUST NOT run any other software. Software required to support the node, such as monitoring, backup, and configuration management software, are approved as a general category. However, stewards should discuss with the TGB any software packages that transmit data from the steward node to the outside.
4. MUST run a server with compatible versions of the operating systems supported by the Hyperledger Indy Node requirements as documented in release notes.
5. MUST have adequate compute power (in late 2018, 8 or more cores is considered adequate).
6. MUST have adequate RAM (in late 2018, 32 GB of RAM is considered adequate).
7. MUST have at least 1 TB, with ability to grow to 2 TB, of reliable (e.g., RAIDed) disk space, with an adequately sized boot partition.
8. MUST have a high-speed connection to the internet with highly available, redundant pipes (as of late 2018, 100 Mbps was considered adequate).
9. MUST have at least one dedicated NIC for Sovrin Validator Node consensus traffic, and a different NIC to process external requests. Each NIC must have a stable, static, world-routable IP address.
10. MUST be implemented in a way that does not endanger Sovrin's high availability architecture, which is pool-based rather than node-based. Nodes should not take more

responsibility for high availability than what is contemplated by the Node Selection Algorithm. For example, they should listen at exactly one pair of network addresses (see 2.9 above), using exactly one set of credentials that are responding to Sovrin/Indy protocol traffic at any one time whereby the system process adheres to a minimal failover recovery delay period specified by the Sovrin Foundation (or 30 seconds if not specified).

11. MUST have a system clock that is demonstrably in sync with well-known NTP servers.
12. SHOULD have a power supply consistent with high availability systems.

# 3. Security Requirements

A Steward:

1. MUST maintain Steward keys on a separate machine from the machine that runs their node. This machine, called the “CLI (Command Line Interface) system”, uses Steward keys to authorize the Node to participate in the pool, and is thus the basis for trust for the node and the Steward’s identity on the network. The CLI system is not required to have high-end hardware, but in terms of IT best practices, it must meet or exceed the standards for the Node (see following items).
2. MUST provide certification that their Node runs in a locked datacenter with appropriate levels of security, including the specifications that they target (e.g., SSAE 16 type II compliance; other standards may also be acceptable).
3. MUST assert that their Node is isolated from internal systems of a Steward (because the Validator Node is publicly visible and thus an inappropriate candidate for access to privileged internal networks).
4. MUST assert that their Node, and its underlying systems, uses state-of-the-art authentication for remote access (at least SSH with key plus password plus source IP firewall rule, and two-factor authentication wherever possible).
5. MUST NOT allow access (remote or local) to the Node or CLI systems by anyone other than assigned admins.
6. MUST apply the latest security patches within one (1) week or less (24 hours or less is recommended).
7. MUST attest that the Node runs on a server protected by a firewall that, at minimum:
    - Disallows public ingress except on ports used by the Node software (different machines may choose to expose ledger features on different ports, so no standard port setup is required).
    - Optionally enables SSH, Remote Desktop, and similar remote access tools but constrains ingress for these tools in some way that excludes the public but allows access for admins.
    - Locks down egress ports to limit the ability to jump from Node to some other location.
8. MUST run the Steward security check tool as requested, and MUST receive TGB

approval of the results before the Node is authorized to participate in consensus.
9. MUST run the Steward security check tool from time to time as requested by the TGB and provide the test results report to the TGB within three (3) business days.

# 4. Operating Requirements

A Steward:

1. MUST equip at least two (2) technical points of contact responsible for administering the Steward Node with an SMS-capable device for alerting.
2. SHOULD aim to achieve at least 99.9% (three nines) uptime for their Node (this amounts to about 1.4 minutes of downtime per day or 9 hours per year).
3. SHOULD coordinate downtime with other Stewards in advance via a mechanism as determined from time to time by agreement between the Sovrin TGB and any other relevant Sovrin Governing Body.

# 5. Node Selection Algorithm

1. The selection of active Validator Nodes at any point in time MUST be governed by the Node Selection Algorithm as specified by the Sovrin TGB.
2. Non-technical inputs or policy decisions implemented by the Node Selection Algorithm MUST be approved by the Sovrin Board of Trustees.
3. At any point in time, the Node Selection Algorithm MUST represent the TGB's best efforts at designing an algorithm that applies the Core Principles of the Sovrin Governance Framework. Recognizing the inherent tension and tradeoffs between some of the Core Principles, the design of this algorithm should give priority to balancing:
    a. The Decentralization by Design principles, in particular the principles of Diffuse Trust and High Availability.
    b. The Security by Design principles, in particular the principles of System Diversity and Secure Failure.
4. A human-readable, understandable, and explainable description of the current design of the algorithm as approved by the TGB MUST be published by the TGB in the official Sovrin Code Repository and made publicly visible via a web page on the Sovrin Foundation website.

# 6. Reporting Requirements

1. A Steward MUST report to the responsible Sovrin Governing Body any substantive change to the configuration or location of a Node within five (5) business days of the change.