



Transaction Endorser Technical and Organizational Policies V1

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	Transaction Endorser Technical and Organizational Policies
Version	V1
Approval Date	2019-12-04
Status	Final
Governs	General Security Policies, Security Incident Policies
Governed By	Steward Qualification Committee

1. General Security Policies

1. Transaction Endorser MUST maintain and follow IT security policies and practices that are integral to maintain protection of all services provided in association with the Transaction Endorser Agreement (“Endorser Services”). These policies MUST be mandatory for all employees of the Steward involved with providing the Endorser Services. The Transaction Endorser shall designate its CIO or another officer to provide executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.
2. Transaction Endorser MUST review its IT security policies at least annually and amend such policies as the Steward deems reasonable to maintain protection of its Endorser Services.
3. Transaction Endorser MUST maintain and follow its standard mandatory employment

verification requirements for all new hires involved with providing its Endorser Services and will extend such requirements to wholly-owned subsidiaries involved with providing its Endorser Services. In accordance with the Transaction Endorser's internal process and procedures, these requirements MUST be periodically reviewed and MUST include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by the Transaction Endorser. Each Transaction Endorser company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

4. Employees of a Transaction Endorser involved with its Endorser Services MUST complete security and privacy education annually and certify each year that they will comply with the Transaction Endorser's ethical business conduct, confidentiality, security, privacy, and data protection policies. Additional policy and process training MUST be provided to persons granted administrative access to components that are specific to their role within the Transaction Endorser's operation and support of its Endorser Services.
5. If a Transaction Endorser performs its Endorser Services in its own data center, the Transaction Endorser's security policies MUST also adequately address physical security and entry control according to industry best practices.
6. If a Transaction Endorser performs its Endorser Services using a third-party Hosting Provider, the Transaction Endorser MUST ensure that the security, privacy, and data protection policies of the Hosting Provider meet the requirements in this document.
7. Transaction Endorser MUST make available to the Sovrin Foundation upon request evidence of stated compliance with these policies and any relevant accreditations held by the Transaction Endorser, including certificates, attestations, or reports resulting from accredited third-party audits, such as ISO 27001, SSAE SOC 2, or other industry standards.

2. Security Incident Policies

1. Transaction Endorser MUST maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notification terms of the Transaction Endorser Agreement.
2. Transaction Endorser MUST investigate unauthorized access of which the Transaction Endorser becomes aware (security incident), and the Transaction Endorser will define and execute an appropriate response plan. The Foundation may notify the Transaction Endorser of a suspected vulnerability or incident by submitting a technical support request.
3. Transaction Endorser MUST notify the Foundation without undue delay upon confirmation of a security incident that is known or reasonably suspected by the Transaction Endorser to affect the Foundation. The Transaction Endorser will provide the Foundation with the reasonably requested information about such security incident

and the status of any of the Transaction Endorser remediation and restoration activities.

3. General Technical Policies

In performing its Endorser Services, Transaction Endorser MUST:

1. Comply with all relevant [Sovrin Ledger Access Policies](#).
2. Follow any additional guidelines published by the Sovrin Technical Governance Board on the Sovrin Foundation website or github site.

© 2019 by Sovrin Foundation. This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License (<http://creativecommons.org/licenses/by-sa/4.0/>).