v

Enabling global identity
Protecting digital trust

verifiable LEI (vLEI) Ecosystem Governance Framework v1.0

vLEI Ecosystem Information Trust Policies

Public
Document Version 1.0
2022-12-16

Version	1.0
Date of version	2022-12-16
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework vLEI Ecosystem Information Trust Policies
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2022-12-16_verifiable-LEI-(vLEI)-Ecosystem-Information-Trust-Policies_v1.0_final.docx
Governing Authority	Global Legal Entity Identifier Foundation (GLEIF)
Copyright	The verifiable LEI (vLEI) Ecosystem Governance Framework is published on the GLEIF website. All documents published on the GLEIF website are published under the Creative Commons Attribution license.

1 Introduction

This is a Controlled Document of the GLEIF vLEI Ecosystem Governance Framework (vLEI Ecosystem Governance Framework). The document defines the information security, privacy, availability and confidentiality policies that apply to all vLEI Ecosystem stakeholders regardless of their particular role or the particular type of vLEI being exchanged. Policies that apply to the issuance, holding, or verification of a specific type of vLEI are defined in the vLEI Credential Governance Framework for that credential type.

2 Terminology

All terms in First Letter Capitals are defined in the vLEI Glossary.

3 Regulatory Compliance

vLEI Ecosystem stakeholders MUST comply with any governmental regulations for information security to which their activities within the vLEI Ecosystem will be subject. This includes International or trans-national governance authorities (e.g., ISO/IEC 27001 – Information Security Management, EU General Data Protection Regulation (GDPR).

4 vLEI Ecosystem Stakeholder Privacy Policies

1. Legal Entities that receive vLEI Legal Entity Credentials SHOULD ensure that their privacy policies adequately protect the persons to whom the Legal Entity requests Legal Entity Official Organizational Role vLEI Credentials and Legal Entity Engagement Context Role vLEI Credentials.

2. The vLEI Ecosystem Credential Governance Frameworks MUST specify the information to be protected by the applicable privacy policy in the jurisdiction of the Legal Entity.

5 vLEI Ecosystem Stakeholder Data Protection Policies

1. vLEI Ecosystem stakeholders MUST confirm that they respect and comply with data protection legislation as applicable and in force.
2. Where no such legislation is in force, and as a material minimum standard, vLEI Ecosystem stakeholders MUST comply with the provisions of the Swiss Federal Data Protection Act specified in the Appendix to this policy document.
3. vLEI Ecosystem stakeholders MAY use Personal Data for the purpose of performing their obligations and rights under this Agreement. vLEI Ecosystem stakeholders MUST comply with:
    a. the material applicability of the provisions of the Swiss Federal Data Protection Act or
    b. about local data protection legislation applicable to the vLEI Ecosystem stakeholder if such legislation is equivalent or more rigorous.
4. Qualified vLEI Issuers MUST annually review and document that the provisions are implemented and enforced. Other vLEI Ecosystem stakeholders SHOULD undertake to regularly review and ensure that the provisions of this Section 5 are implemented and enforced.
5. When a privacy breach is suspected, the involved vLEI Ecosystem stakeholders MUST inform each other about actual or potential disclosure(s) of Personal Data and promptly take appropriate measures to address the situation and to limit the risk of such disclosure(s) from reoccurrence.
6. Qualified vLEI Issuers MUST document privacy breaches in an Incident Report.

6 vLEI Ecosystem Stakeholder Security Policies

1. vLEI Ecosystem stakeholders MUST publish, review annually, maintain, and comply with IT security policies and practices sufficient to protect all services that a vLEI Ecosystem stakeholder provides in conformance with this Ecosystem Governance Framework and meets the minimum elements of the following recommendations: https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/#gref

2. These policies MUST be mandatory for all employees of the vLEI Ecosystem stakeholder involved with vLEI Data. The vLEI Ecosystem stakeholder MUST designate its Information Security Manager or another officer to provide executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.
3. vLEI Ecosystem stakeholder employment verification policies and procedures MUST include, but may not be limited to, criminal background check and proof of identity validation.
4. Qualified vLEI Issuers MUST recertify annually that they maintain a law abiding and ethical status in the business community as evidenced in the Annual vLEI Issuer Qualification.
5. If a Qualified vLEI Issuer performs handling of vLEI Data in its own data center, the Qualified vLEI Issuer's security policies MUST also adequately address physical security and entry control according to industry best practices.
6. If a Qualified vLEI Issuer uses providers of Third-Party Services in functions that involve the handling of vLEI Data, the Qualified vLEI Issuer MUST ensure that the security, privacy, and data protection policies of the third-party providers meet the requirements in this document.
7. Qualified vLEI Issuers MUST make available evidence of stated compliance with these policies and any relevant accreditations held by the Qualified vLEI Issuer during Annual vLEI Issuer Qualification, including certificates, attestations, or reports resulting from accredited third-party audits, such as ISO 27001, Statement on Standards for Attestation Engagements Service Organization Controls 2 (SSAE SOC 2), or other industry standards.

7 Security Incidents Policies

1. Qualified vLEI Issuers MUST maintain and follow documented incident response procedures and guidelines for computer security incident handling and will comply with data breach notification terms of the vLEI Issuer Qualification Agreement. ITIL (Information Technology Infrastructure Library) Incident Management is followed by GLEIF and is certified as part of GLEIF's ISO 20000 certification.
2. Qualified vLEI Issuers MUST define and execute an appropriate response plan to investigate suspected unauthorized access to vLEI data. GLEIF and the Qualified vLEI Issuers will handle through the Incident Management process.

8 Availability Policies

1. GLEIF and Qualified vLEI Issuers MUST maintain defined availability targets as part of the vLEI Ecosystem Governance Framework.
2. GLEIF and Qualified vLEI Issuers MUST maintain records to evidence the availability of their services.

9 Developer Security Policies

1. GLEIF MUST provide technical changes/upgrades to the vLEI software to Qualified vLEI Issuers.
2. Qualified vLEI Issuers MUST successfully install, test and implement the vLEI software within stated timeframes.
3. Developers of Qualified vLEI Issuers SHOULD follow the security recommendations in section 8 of the W3C Verifiable Credentials Data Model 1.0 specification and the Trust over IP Authentic Chained Data Containers (ACDC) specification when designing software or services for use with vLEI Credentials and the vLEI Ecosystem.