GLEIF

Enabling global identity
Protecting digital trust

Information Security Policy

Public
Version 1.0
2026-01-27

Contents

Version	1.0
Date of version	2026-01-27
Created by	GLEIF
Approved by	GLEIF CEO
Confidentiality level	Public

About this Policy

This document describes GLEIF's External Information Security Policy. The intended audience includes GLEIF's partners and other interested parties.

Change History

This section records the history of all changes to this document.

Date	Version	Description of Change	Author
2026-01-27	1.0	First version	GLEIF

1 Overview

1.1 Purpose

This External Information Security Policy defines the information security principles applied by the Global Legal Entity Identifier Foundation (GLEIF) to support the effective management and delivery of services in accordance with ISO/IEC 20000-1:2018. The policy is intended to provide transparency to external parties, including LEI and vLEI Issuers, regarding how information security supports agreed service levels.

1.2 Scope

This policy applies to information, systems, and services within the scope of GLEIF's Service Management System (SMS) that support the Global Legal Entity Identifier System (GLEIS). It covers information processed or managed by GLEIF in the delivery of services to external partners. This document intentionally excludes internal operational procedures and confidential security controls.

1.3 Alignment with ISO/IEC 20000-1:2018

GLEIF has implemented and maintains a Service Management System (SMS) that is aligned with the requirements of ISO/IEC 20000-1:2018. The SMS provides the governance framework through which services are planned, delivered, monitored, and improved. The SMS includes, but is not limited to, the following service management processes:

- Service portfolio management
- Configuration management
- Business relationship management
- Service level management
- Supplier management
- Demand and capacity management
- Change management
- Release and deployment management
- Incident and service request management
- Problem management
- Service availability management
- Service continuity management
- Information security management
- Service reporting
- Continual improvement

Information security is managed as an integral part of GLEIF's SMS. Controls and practices are designed to support:

- The fulfilment of agreed service requirements (ISO/IEC 20000-1:2018, clause 4 and 8)

- The management of risks that could impact service availability, continuity, integrity, or confidentiality
- Continual improvement of services and service management processes

2 Policy

2.1 Information Security Objectives

GLEIF establishes information security objectives that are consistent with service requirements and business needs. These objectives ensure:

- Confidentiality of service-related information
- Integrity of data and processing supporting GLEIF services
- Availability of systems and services in line with agreed service levels

2.2 Governance and Responsibility

GLEIF maintains a defined governance structure to manage information security within the Service Management System. Roles, responsibilities, and authorities are assigned to ensure that information security supports service management objectives. Management provides oversight to ensure that information security remains effective and aligned with service requirements.

2.3 Risk-Based Control Framework

Information security risks that could impact the delivery or quality of services are identified and assessed on a regular basis. Controls are selected and implemented using a risk-based approach to reduce the likelihood and impact of service disruptions, data compromise, or non-fulfilment of service commitments.

2.4 Access and Information Handling

Access to information and service-related systems is controlled based on defined roles and service needs. GLEIF applies logical access controls and information handling practices appropriate to the sensitivity of the information and its role in service delivery.

2.5 Incident and Service Disruption Management

Information security incidents are managed in coordination with GLEIF's incident and service request management processes. Events that may impact service levels, service continuity, or external partners are addressed in accordance with service management procedures and contractual obligations.

2.6 Supplier and Partner Relationship Management

GLEIF defines information security expectations for suppliers and partners, including LEI and vLEI Issuers, where they contribute to service delivery. These expectations are addressed through

agreements and service arrangements consistent with ISO/IEC 20000-1:2018 supplier and business relationship management principles.

2.7 Monitoring, Review, and Improvement

The effectiveness of information security controls supporting services is monitored and reviewed as part of the Service Management System. Findings from audits, assessments, incidents, and service reviews are used to drive continual improvement.

3 Policy Review

This policy is reviewed annually to ensure continued alignment with ISO/IEC 20000-1:2018, service requirements, and changes to GLEIF services or risks.

4 Effective Date

This Policy, and any amendments thereof, shall enter into force upon approval by the GLEIF CEO.