INFORMATION SECURITY POLICY FOR CUSTOMERS

LIBNOVA

Version: 1.0

Date: January 2025

Purpose

This document outlines the Information Security Policy designed to protect the integrity, confidentiality, and availability of information managed by Libnova for the benefit of its clients. It is made publicly available to ensure transparency and trust in our commitment to information security.

Scope

This policy applies to all information systems, processes, and digital preservation services provided by Libnova, including but not limited to Libsafe, Libsafe Classic, and OpenAccess. It ensures that all client-related data and digital assets are securely handled and protected throughout their lifecycle.

Commitment to Information Security

Libnova recognizes the critical nature of the information it manages on behalf of its clients. As such, the company is committed to:

- **Maintaining Confidentiality:** Ensuring that client data is accessible only to authorized individuals and systems.
- **Ensuring Integrity:** Protecting client information from unauthorized modification or corruption.
- **Guaranteeing Availability:** Providing reliable and uninterrupted access to client information and systems.

Compliance with Standards

Libnova's Information Security Management System (ISMS) is aligned with the ISO 27001:2022 standard to meet the highest international benchmarks for information security. Regular audits and improvements are conducted to maintain compliance and adapt to emerging security challenges.

General Principles

1. **Data Protection:** All client information is treated as confidential and is safeguarded using state-of-the-art security measures.

2. **Access Control:** Access to client data is restricted based on roles and responsibilities and follows strict authentication protocols.
3. **Incident Management:** Any security incidents affecting client data are managed promptly, with appropriate corrective actions taken to minimize risks.
4. **Encryption:** Sensitive data is encrypted during storage and transmission to prevent unauthorized access.
5. **Third-Party Assurance:** All external providers involved in handling client data comply with equivalent security standards, including ISO 27001 or similar.
6. **Continuous Improvement:** Policies and processes are regularly reviewed and updated to ensure alignment with the latest security practices.

Responsibilities

- **Libnova Management:** Ensures the implementation and continuous improvement of the ISMS. It is responsible for approving policies and allocating resources to maintain security measures.
- **ISMS Team:** Oversees the operational aspects of information security, including risk assessments, monitoring, and incident resolution.
- **Employees:** Adhere to established security protocols to protect client information and report any potential security concerns.

Client Responsibilities

Clients are encouraged to:

1. Use secure methods for sharing sensitive information with Libnova.
2. Notify Libnova promptly in case of any detected anomalies or breaches affecting shared data.
3. Comply with mutually agreed security requirements during collaborations or integrations.

Transparency and Communication

Libnova prioritizes open communication with its clients regarding security measures and any incidents that may affect their data. Regular updates and reports can be requested through our designated communication channels. For more information or inquiries about this policy, please contact us at: security@libnova.com.

Policy Availability and Updates

This policy is publicly accessible on the Libnova website and is reviewed annually or whenever significant changes are required. Updated versions will be published promptly to reflect any modifications.

Contact Information Libnova Headquarters
Calle Orense 6
28046 Madrid, Spain
Email: info@libnova.com
Website: www.libnova.com