CYBER SECURITY POLICY

Last updated: 30 January 2026

1. Purpose

This Cyber Security Policy defines the principles and measures applied by LUMIFRAME, UNIPESSOAL LDA ("Lumiframe") to protect its digital infrastructure, website, systems, and data against cyber threats, unauthorized access, and security incidents.

This Policy supports compliance with:

1) GDPR (EU Regulation 2016/679);
2) applicable Portuguese data protection and cybersecurity requirements.

2. Scope

This Policy applies to:

1) the website https://lumiframe.eu;
2) internal IT systems and digital tools used by Lumiframe;
3) personal data and digital content processed in the course of business;
4) employees, contractors, and authorized persons with system access.

3. Security Principles

Lumiframe follows the following core cybersecurity principles:

1) confidentiality of data;
2) integrity of systems and information;
3) availability of services and digital content;
4) proportionality of security measures to business risks.

4. Technical and Organizational Measures

Lumiframe implements appropriate security measures, including but not limited to:

1) secure hosting and infrastructure providers;
2) access control and authentication mechanisms;
3) regular software and system updates;
4) use of secure communication protocols (HTTPS, encryption where applicable);
5) restriction of access to systems on a need-to-know basis;
6) data backup and recovery procedures.

5. Payment Security

Payments on the Website are processed exclusively by independent third-party payment service providers.

Lumiframe:

1) does not store full payment card details;
2) does not process payment credentials directly;
3) relies on payment providers compliant with applicable security standards.

6. Data Breaches and Incident Response

In the event of a data breach or cybersecurity incident, Lumiframe will:

1) promptly assess the scope and impact of the incident;
2) take immediate steps to mitigate risks;
3) notify affected users and supervisory authorities where required by law;
4) document the incident and corrective actions taken.

7. User Responsibilities

Users are responsible for:

1) maintaining the confidentiality of their access credentials;
2) using secure devices and networks;
3) refraining from any actions that may compromise website security.

Unauthorized access attempts or misuse of the Website are prohibited.

8. Third-Party Services

Lumiframe may rely on third-party service providers (hosting, payment, analytics).
Such providers are selected based on security, reliability, and compliance considerations and process data under contractual safeguards.

9. Monitoring and Review

Cybersecurity measures are periodically reviewed and updated to address emerging risks and technological developments.

10. Contact

Security-related concerns or suspected vulnerabilities should be reported to:
Email: compliance@lumiframe.eu