



Information Security Policy of Electrozemper, S.A.

ZEMPER



1. Commitment and Purpose

Electrozemper, S.A., dedicated to the design, manufacture, and distribution of emergency lighting, recognizes that information is a vital asset for the success of its business and its reputation. The Management is committed to protecting information against all threats, whether internal or external, deliberate or accidental, guaranteeing the **Confidentiality, Integrity, and Availability (CIA)** of the information we manage and safeguard. This Policy establishes the framework for the implementation, maintenance, and continuous improvement of an **Information Security Management System (ISMS)**, in line with the requirements of the **ISO/IEC 27001:2022** standard.

2. Fundamental Principles

2.1. Confidentiality

Ensure that information is only accessible by those authorized individuals, entities, or processes and when necessary. This includes protecting design data, patents, financial information, personal data of customers and employees, and trade secrets.

2.2. Integrity

Safeguard the accuracy and completeness of information and its processing methods, ensuring that data has not been altered or destroyed in an unauthorized manner.

2.3. Availability

Guarantee that authorized users have access to information and associated assets when required. This applies to systems, processes, and data critical for manufacturing and distribution.

3. Information Security Framework

3.1. Compliance with Requirements

We are committed to **compliance with all legal, regulatory, and contractual requirements** applicable to information security. This includes legislation on data protection (such as GDPR/RGPD, if applicable), intellectual property, and any other relevant sectoral requirement.

3.2. Risk Management

We will establish and maintain a **risk management process** that will identify, analyze, and evaluate information security risks. Security controls (Annex A of ISO 27001:2022) will be implemented based on the organization's risk appetite.

3.3. Security Objectives

Management will establish measurable **information security objectives** consistent with this Policy and the organization's context. These objectives will be reviewed annually; see Annex 1 of this policy.

3.4. Continuous Improvement

We are committed to the **continuous improvement** of the suitability, adequacy, and effectiveness of the ISMS. The Policy will be reviewed annually or in the event of significant changes in the context of Electrozemper, S.A.

4. Roles and Responsibilities

- **General Management:** Lead, provide resources, and ensure compliance with the Policy.
- **ISMS Manager (or Quality and Information Security Manager):** Maintain the ISMS, coordinate risk management, and report performance to Management.
- **All Employees and Third Parties:** They have the obligation to know, understand, and comply with this Policy and the ISMS security procedures. Participation in information security training and awareness programs will be required.

5. Sanctions

Failure to comply with this Policy may result in **disciplinary measures**, including termination of the employment contract or legal action, in accordance with applicable labor and legal regulations.

*Fdo.: Jesús María Espinosa
General Management
Ciudad Real, 3 de marzo de 2025*



ANNEX 1

Information Security Objectives (ISMS)

Domain (ISO 27001 Requirement)	Qualitative Objective	Quantitative Goals (KPIs)	Measurement Frequency
Confidentiality (Access Management)	Reduce the risk of unauthorized access to critical design and financial information.	Maintain 0% of security incidents related to unauthorized access to design plans (CAD), customer lists, or financial information.	Monthly
Integrity (Change Management)	Ensure accuracy and no unauthorized alteration of technical documentation and production data.	Achieve a 100% rate of formal review and approval of all changes in quality control (QC) software and product design specifications (BOMs).	Quarterly
Availability (Business Continuity)	Guarantee the continuous operability of key production and distribution systems (ERP and SCADA).	Reduce the average downtime of critical production systems to less than 4 hours per serious incident.	Semi-annually
Awareness and Training (Human Resources)	Strengthen the information security culture throughout the organization.	Achieve a 100% annual participation rate in mandatory security awareness training.	Annually
Legal and Contractual Compliance (Legal Requirements)	Ensure compliance with current regulations regarding privacy and data protection.	Maintain a 0% rate of sanctions or fines imposed by regulatory bodies due to non-compliance with applicable data protection law .	Annually

Domain (ISO 27001 Requirement)	Qualitative Objective	Quantitative Goals (KPIs)	Measurement Frequency
Incident Management (Incident Response)	Improve the response and recovery capacity against any security incident.	Reduce the Mean Time to Detection (MTTD) and the Mean Time to Response (MTTR) to critical incidents by 15% compared to the previous year.	Quarterly

Additional Considerations

1. **Business Alignment:** These objectives focus on protecting the most critical assets of Electrozemper, S.A.: the intellectual property of its designs (**Confidentiality**), the accuracy of manufacturing processes (**Integrity**), and the ability to continue producing and distributing luminaires (**Availability**).
2. **Review and Adjustment:** Management, together with the ISMS Manager, must **review these objectives annually** during the Management Review to ensure they remain relevant and that necessary resources are allocated for their fulfillment.
3. **Documentation: Quantitative Goals (KPIs)** must be documented and monitored through a measurement plan within the ISMS.



Entirely designed and
manufactured in **Spain**



The Zemper Way to a Better World

We use recycled paper in the production of our catalogues, thus contributing to the conservation of forests and biodiversity.

This paper requires up to 50% less energy and 90% less water, which significantly reduces environmental impact, reduces carbon dioxide emissions and promotes the circular economy. The ink we use is free of mineral oils, cobalt salts and VOCs (volatile organic compounds) so we contribute to limiting the environmental impact. We make more sustainable decisions and help protect our planet.

ZEMPER

THE EMERGENCY LIGHTING SPECIALIST

Zemper España

Avda. de la Ciencia, 3 · Pol. Industrial Avanzado
13005 Ciudad Real (Spain)

Tel. +34 **677 476 876** · export@zemper.com

Zemper BeLux

Baronstraat 122
8870 IZEGEM · Bélgica
Tel. +32 51 800 210
belux@zemper.com

Zemper France

ZA des Berthilliers
189 Chemin des Frozières
71850 Charnay-lès-Mâcon · Francia
Tel. +33 3 85 34 66 20
commercial@zemperfrance.com

Zemper UK

Thornhill House, Thornhill Road,
Solihull, B91 2HB
Tel. +44 (0)121 703 2867
hello@zemper.co.uk

Commercial Offices

Marruecos
maroc@zemper.com
Colombia
colombia@zemper.com
Dubai
dubai@zemper.com

www.zemper.com

The information given in this catalogue is typical and must not be interpreted as a guarantee of individual product performance and/or characteristics.
We reserve the right to alter specifications and designs without prior notice.