

Luxshare Precision aligns with the ISO 27001 Information Securi

 **Zero** information
leakage incident

Privacy Protection Management

The Company adheres to national laws and regulations, including the , as well as customer requirements and industry standards. The Company has established a comprehensive suite of privacy management procedures and data desensitization standards, such as the *Commercial Secret Management Procedure* and the *Information Security Management Procedure for Relevant Parties*. Through the COC and the , Luxshare Precision outlines specific privacy protection requirements. Regular trainings and assessments are conducted to guide employees' behaviors and strictly prohibit the unauthorized disclosure of partners' personal and commercial information.

Privacy Protection Measures

Classified Management

- Privacy protection content
 - Defined according to customers' requirements or the Company's classification standards
- Privacy protection mark
 - According to the determined level of confidentiality and confidentiality period, attach a confidential mark or affix a similar seal for the commercial secret data
- Desensitization resources protection
 - Develop desensitization standards according to different businesses, departments, and relevant parties

Access Permission

- Authorization management
 - Require to use standardized and complexity-compliant user-names, passwords or pass-phrases, and should not disclose to any irrelevant or authorized personnel
- Equipment inspection and maintenance
 - The installation, debugging, and overhaul of computer equipment involving company secrets shall be undertaken by internal professional technical personnel, and other personnel shall not disassemble and overhaul the computer equipment

Personnel Management

- Confidential Meeting
 - The organizing department shall strictly determine the attending personnel for any confidential meeting. For online meetings, the organizing department shall set up passwords and encrypted links and review attendees beforehand
- Access permission terms
 - All parties providing various products or services to the Company that require physical or logical access to the Company's information assets must sign a confidentiality agreement or confidentiality clauses document
- Privacy protection training
 - Require employees to complete privacy protection-related trainings and assessments

Asset Management

- Confidential information management
 - Persons involved should properly safeguard confidential materials obtained for official purposes. Individuals must not take them home or to any public place, nor disclose them to outsiders
- Storage of confidential information
 - Confidential documents, records, disks, optical discs, or other storage media should be placed in locked file cabinets, safes, or other forms of safe furniture when not in use, and the keys are managed by designated personnel

Case | Luxshare Precision Established a Cybersecurity Posture Awareness System

The Company has operationalized a cybersecurity posture awareness platform spanning hardware infrastructure and systems. This solution enables continuous monitoring of emerging attack vectors, asset exposure risks, and systemic vulnerabilities through organization-wide real-time data aggregation and multidimensional behavioral analytics. Combining with our closed-loop automated response protocols, we have established a cross-factory coordination cyber defense architecture.

In 2024, we refined alert rules and threat cases detection analysis, achieving a reduction in false-positive alerts and a decrease in the total number of alerts and security incidents by more than 60%. Concurrently, we remediated more than 50 vulnerabilities through systematic patch management, substantially elevating enterprise-wide cybersecurity safeguards.

