Strengthening Cybersecurity Defenses

Luxshare Precision continues to refine its information security and privacy protection management system. Through institutionalized and standardized management, the Company reduces data security and privacy risks, safeguarding the legitimate rights and interests of the Company, its customers, and other relevant stakeholders.

Information Security Management

We aim to build a compliant, secure, and stable business environment. Relying on the ISO/IEC 27001 information security management system standard, we implement measures including business continuity management, information security audits, data protection management, and security awareness promotion. We conduct a series of training and management activities for employees and suppliers to continuously strengthen the overall robustness of the Company's information security and its ability to resist risks, thereby solidifying the Company's information security defense line.

Highlights of Information Security Management Measures

Business Continuity Management

Conduct multi-dimensional emergency drills for all nodes of critical business operations, including backup recovery, network interruption, critical node server failures, and misconfigurations

Information Security Audit

Conduct penetration testing, vulnerability scanning, and information security audits across all facilities, and remediate identified risks

Data Protection Management

Continuously implement full coverage of equipment within confidential areas

Safety Awareness Promotion

Conduct information security training by integrating current hot topics and utilizing posters and comics to promote information security awareness. Special emphasis is placed on communicating information security management requirements to newly acquired companies

Information Security Training

Employees

- Information security training for new hires
- Semi-annual refresher training
- Regular distribution of information security publicity materials
- Targeted phishing email security drill
- Specialized training materials customized for key positions

Supplier

- Ad-hoc information security investigations
- Regular information security training
- Online information security audits and offline inspections of key suppliers

During the Reporting Period, Luxshare Precision:

Major information leakage incidents	Total hours of employee information security training	Number of online information security audits and offline inspections of key suppliers
0	614,387 hours	325 times

Privacy Protection

Luxshare Precision places high importance on the protection of personal information and customer privacy. Strictly adhering to applicable privacy protection laws and regulations in all operating locations, we are committed to safeguarding customer rights and ensuring the security and compliance of cross-border personal information transfer processes.

Personal Information Protection

The Company has issued the *Personal Information Protection Policy* and fully implemented the requirements of the *Personal Information Protection Law of the People's Republic of China (PIPL)*, the *General Data Protection Regulation (GDPR)* of the European Union, and other applicable laws and regulations in the jurisdictions where its business operates. The Company has formulated the *Employee Personal Information Protection Statement*, clearly defined retention periods for personal information, and systematically strengthened the management of personal information throughout its entire lifecycle. We established fundamental principles for personal information processing, including "legality, propriety and integrity, minimization of necessity, openness and transparency, data quality, and information security". We constructed a cross-border compliance management system covering processes, contracts, and technical measures. Through multi-channel monitoring and reporting mechanisms, we encourage the proactive submission of security incidents. The Compliance Committee coordinates risk assessment and implements a comprehensive response system. **In 2025, the Company obtained ISO/IEC 27701 privacy information management system certification**.

Case | Luxshare Precision Conducted Awareness Training on Cross-Border Data Transfer Regulations

In October, Luxshare Precision conducted a specialized training session on "Regulatory Frameworks and Response Measures for Cross-Border Data Transfers between China and Europe." The session provided an in-depth interpretation of the core provisions under the PIPL and GDPR regarding requirements and application scenarios for cross-border personal data transfers. Additionally, through case studies and operational guidelines, the training offered specific analysis of actual data flow processes. This training further clarified the Company's legal liability boundaries regarding cross-border data transfers, enhanced awareness of personal information protection, and effectively improved the Company's compliance governance level in international operations.

During the Reporting Period, Luxshare Precision:

Major regulatory penalty or litigation case resulting from violations of personal information protection

0

Customer Privacy Protection

We strictly comply with applicable laws and regulations, customer requirements, and industry standards by formulating and implementing a series of privacy management policies and data desensitization standards, including the *Commercial Secret Management Procedure* and the *Information Security Management Procedure for Relevant Parties*. Concurrently, we have clarified privacy protection requirements through internal regulations such as COC and the *Employee Handbook*. We primarily rely on regular training and assessments to effectively guide and constrain employee behavior, ensuring strict compliance with these regulations and preventing any leakage of partners' privacy and commercial information.

During the Reporting Period, Luxshare Precision:

Verified complaint involving the infringement of customer privacy, and loss or leakage of customer data

0

Customer Privacy Protection Initiatives

Classified Management

- **Privacy Protection Content**

  Define 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 usernames, passwords or passphrases, and should not be disclosed to any irrelevant or unauthorized 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

- **Email Security Management**

  Implement two-factor authentication for email and additionally incorporate SMS/password generator dynamic codes into email access permissions

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 secure storage facilities when not in use, and the keys are managed by designated personnel