Ensuring Information Security

Luxshare Precision is dedicated to fostering a compliant, secure, and stable operational environment. By effectively implementing its information security and privacy protection management system, the Company safeguards itself, its customers, and all relevant stakeholders against potential risks associated with data breaches and privacy violations.

Information Security Management

Luxshare Precision aligns with the ISO 27001 Information Security Systems and strengthens the robustness of its information security through management measures such as BCM, information security audits, data protection management, and security awareness advocacy.

Key Measures of Information Security Management

Business Continuity Management

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

Information Security Audit

- Conduct penetration testing, vulnerability scanning, and information security audits across all facilities, completing 280 improvement projects

Data Protection Management

- Continuously implement full coverage of equipment within the confidential area
- Conduct study on the risks of transferring personal information and data abroad to protect privacy data

Security Awareness Advocacy

- Utilize posters and comics combined with trending topics to raise information security awareness

In 2024, after conducting a comprehensive assessment of potential information security risks tied to third-party translation platforms, the Company self-developed a fully enclosed localized translation processing system. This internally managed intelligent processing system effectively reduces the likelihood of commercial secrets being leaked. Additionally, we deployed a terminal sentinel system for sensitive areas linked to new product introductions. The system monitors endpoint security statuses in real time, regular reports on key indicators, and features anomalies self-resolution and timely alerts. Even when faced with complex scenarios, such as isolated irregularities, the system can achieve early warnings upon first detection, thereby improving monitoring and visual tracking of security metrics. These enhancements allow security team to react quickly and decisively, significantly strengthening overall data security.

During the Reporting Period, Luxshare Precision:

Zero information leakage incident

Information Security Training

We have organized a series of information security trainings for employees and suppliers, to enhance employees' information security awareness and competencies, as well as the level of information security along the supply chain.

Employees

The Company has implemented information security training programs across multiple manufacturing factories, focusing on critical areas such as information security awareness, confidentiality protocols, information security management systems, and phishing emails preventions. Cumulatively, employees have completed 506,805 hours of trainings.

Suppliers

To ensure compliance with information security management practices, we have established a stringent assessment system, mandating that supplier personnel pass a professional certification exam prior to site access. In 2024, Luxshare Precision undertook comprehensive training and audits for suppliers engaged in confidential projects, with over 300 on-site audits and guidance accomplished. These efforts emphasized the significance of information security and provided practical insights, ensuring the information security of suppliers' work equipment and environment.

Privacy Protection Management

The Company adheres to national laws and regulations, including the *Personal Information Protection Law of the People's Republic of China*, 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 *Employee Handbook*, 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.

Cybersecurity Posture Awareness System

During the Reporting Period, Luxshare Precision:

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