Strengthening C bersecurit Defenses

Luxshare Precision continues to refne 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.

aŠĶũƆşúfŃũš Ãġėł Ɔ Ńfƶ yúšúķġşġšf

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.

^ŃķĿŻŃķĿfD ũĶ aŠĶũƆşúfŃũš Ãġėł Ɔ Ńfƶ yúšúķġşġšf yġúDł ƆġD

;łDŃšġDD <ũšfŃšłŃfƶ yúšúķġşġšf

Conduct multi-dimensional emergency drills for all nodes of critical business operations, including backup recove r , network interruption, critical node se r er failures, and miscon fgurations

aŠĶũƆşúfŃũš Ãġėł Ɔ Ńfƶ łĝŃf

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

Búfú ¼ƆũfġėfŃũš yúšúķġşġšf

Continuously implement full coverage of equipment within con fdential areas

ÃúĶġfƶ urúƆġšġDD ¼ƆũşũfŃũš

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

aŠĶũƆşúfŃũš Ãġėł Ɔ Ńfƶ ÊƆúŃšŃšķ

F şƀřũżġġD

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

ÃłƃƀŃġƆ

- Ad-hoc information security investigations
- Regular information security training
- Online information security audits and o f ine inspections of key

During the Repo r ing Period, Luxshare Precision:

[illegible] information security training

614,387 hours

Total hours of employee information security training

Number of online information security audits and o f ine inspections of key suppliers

325 times

¼ƆŃŮúėƶ ¼ƆũfġėfŃũš

Luxshare Precision places high impo r ance 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.

¼ġƆDũšúř aŠĶũƆşúfŃũš ¼ƆũfġėfŃũš

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 de fned 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 repo r ing mechanisms, we encourage the proactive submission of security incidents. The Compliance Committee coordinates risk assessment and implements a comprehensive response system. aš ƇdƇ¢ fŁġ <ũşƀúšƶ ũÉfúŃšġĝ aÃ¢ aF< ƇfƔdƆ ƁƆŃŮúėƶ ŃšĶũƆşúfŃũš şúšúķġşġšf ƊƶƊfġşėġŤŃNjéúfŃũš.

<úĎġ słƵƊŁúƆġ ¼ƆġèŃĎŃũš <ũšĝłėfġĝ urúƆġšġDD ÊƆúŃšŃšķ ũš <ƆũĎĎ ; ũƆĝĝƆ Búfú ÊƆúšĎĶġƆ ¿ġķłřúfŃũšĎ

In October, Luxshare Precision conducted a specialized training session on "Regulato r 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 o fered speci fc analysis of actual data fow processes. This training fu r her clari fed the Company's legal liability boundaries regarding cross-border data transfers, enhanced awareness of personal information protection, and e fectively improved the Company's compliance governance level in international operations.

<łDƒũşġƆ ¼ƆŃŰúėż ¼ƆũƒġėƒŃũš

We strictly comply with applicable laws and regulations, customer requirements, and indust r standards by formulating and implementing ú DġƆŃġD ũĶ ƁƆŃŰúėż şúšúķġşġšƒ ƁũřŃèŃġD úšĝ ĝúƒú ĝġDġšDŃƒŃŠúƒŃũš DƒúšĝúƆĝĐ. ŃšěřłĝŃšķ ƒŁġ *Commercial Secret Management Procedure* and the *Information Security Management Procedure for Relevant Pa r ies*. Concurrently, we have clari fed privacy protection requirements through internal regulations such as COC and the *Employee Handbook*. We primarily rely on regular training and assessments to e fectively guide and constrain employee behavior, ensuring strict compliance with these regulations and preventing any leakage of pa r ners' privacy and commercial information.

<łDƒũşġƆ ¼ƆŃŰúėż ¼ƆũƒġėƒŃũš aš‴ƒŃúƒŃŰġD

¼ƆŃŰúėż ¼ƆũƒġėƒŃũš <ũšƒġšƒ

Def ne according to customers' requirements or the Company's classi fcation standards

¼ƆŃŰúėż ¼ƆũƒġėƒŃũš y úƆf

According to the determined level of con fdentiality and con fdentiality period, attach a con fdential mark or a f x a similar seal for the commercial secret data

BġDġšDŃƒŃŠúƒŃũš ¿ġDũłƆèġD ¼ƆũƒġėƒŃũš

Develop desensitization standards according to di f erent businesses, depa r ments, and relevant pa r ies

łƒŁũƆŃŠúƒŃũš y úšúķġşġšƒ

Require to use standardized and complexity-compliant usernames, passwords or passphrases, and should not be disclosed to any irrelevant or unauthorized personnel

Fbł‴Ɓşġšƒ ašDƁĝġėƒŃũš úšĝ y úŃšƒġšúšėġ

The installation, debugging, and overhaul of computer equipment involving company secrets shall be unde r aken by internal professional technical personnel, and other personnel shall not disassemble and overhaul the computer equipment

Fşúŕř Ãġėł‴ƒz y úšúķġşġšƒ

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

<ũšŃĵĝġšƒŃúř y ġġƒŃšķ

The organizing depa r ment shall strictly determine the attending personnel for any con fdential meeting. For online meetings, the organizing depa r ment shall set up passwords and enc r pted links and review attendees beforehand

ėėġDD ¼ġƆşŃDDŃũš ÊġƆşd

All pa r ies providing various products or se r ices to the Company that require physical or logical access to the Company's information assets must sign a con fdentiality agreement or con fdentiality clauses document

¼ƆŃŰúėż ¼ƆũƒġėƒŃũš ÊƆúŃšŃšķ

Require employees to complete privacy protection-related trainings and assessments

<ũšŃĵĝġšƒŃúř ašĶũƆşúƒŃũš y úšúķġşġšƒ

Persons involved should properly safeguard con fdential materials obtained for o f cial purposes. Individuals must not take them home or to any public place, nor disclose them to outsiders

ÃƒũƆúķġ ũĶ <ũšŃĵĝġšƒŃúř ašĶũƆşúƒŃũš

Con fdential documents, records, disks, optical discs, or other storage media should be placed in locked f le cabinets, safes, or other forms of secure storage facilities when not in use, and