Ablerex Electronics Co., Ltd.

Implementation of Information Security Risk Management

Date : Nov 6, 2023

Foreword:

The Company has always attached great importance to the rights and interests of investors, shareholders, customers, suppliers, employees, financial institutions, governmental organizations, neighbors and other stakeholders in its sustainable operation and development. In addition to good corporate governance and the fulfillment of the Company's social responsibility, the daily operations are also complemented by appropriate internal control systems and operational management mechanisms to achieve goals such as the effectiveness and efficiency of corporate operations, the accuracy of financial reports, and compliance with laws.

With the progress of time, the development of information and the spread of the Internet, the risks to information security are increasing day by day and may even affect the operation of enterprises or cause financial and business losses. The Company has established information security risk operation and management mechanisms to respond to these risks, such as ”internal control information cycle”, “internal important information processing procedures”, ”insider trading prevention management procedures”, ”personal information protection management“ procedures” and “computer operation management measures”. In 2023, the information security management system ISO 27001 will be implemented and certified to enable all employees to implement and comply with the regulations in order to protect the rights and interests of all stakeholders and the results of the company's operations.

Information security management mechanism

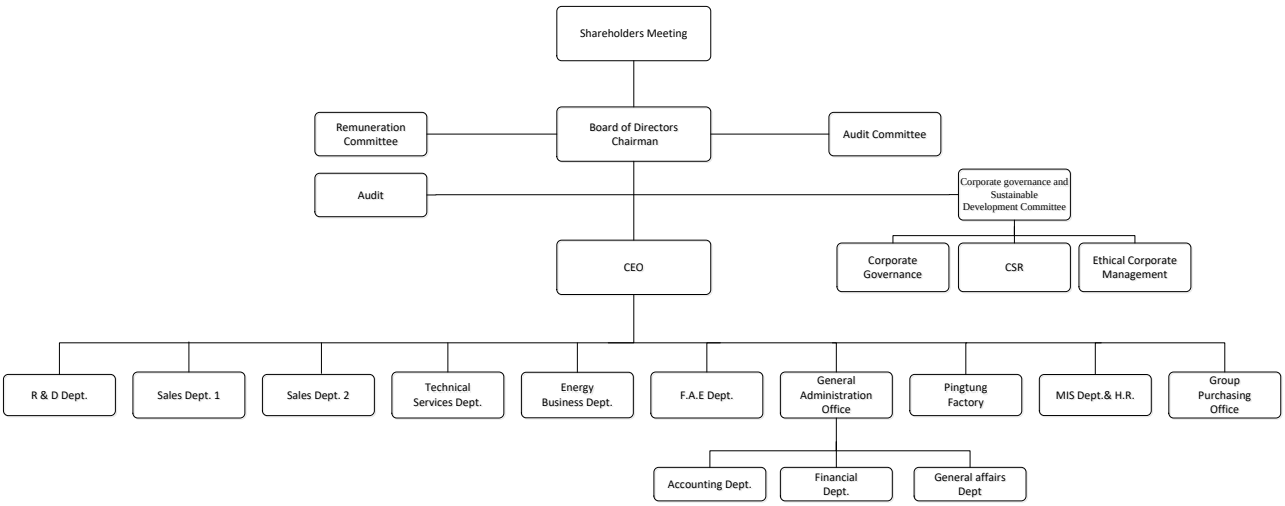
In the spirit of sustainable operation and development, the Company implements the objectives of the Information Security Risk Management Policy through three main aspects: Information Security Governance, Regulatory Compliance, and Technology Adoption. It strengthens the company's information security management and establishes” "security-based information development" The concept of ensuring the confidentiality, integrity and availability of customers' and colleagues' data processing ensures that the company's data processing is secure throughout the process, provides safe, stable and efficient information services, and advocates the implementation of measures and continuous improvement of the information security management system.

Information Security Policy	
Information security governance	Physical and environmental security: ensures that the organisation's physical facilities and environment are subject to appropriate security controls. Asset Management: The management of an organisation's assets, including their identification, classification, tracking, and protection. Information Security Incident Management: Establishing policies and procedures for responding to information security incidents and incidents. Information assurance: ensuring adequate plans are in place to secure and recover information. Classifying, categorising, and processing information: Ensure that information is classified, categorised, and processed according to its sensitivity.
Compliance	Cybersecurity: Follow relevant regulations and standards to protect the organization's network and data transmission. Security Development Policy: Develop and implement appropriate security policies to ensure regulatory compliance. Technical Vulnerability Management: Monitor and manage system and application security vulnerabilities.
Technology application	Data transfer: Ensure data is appropriately protected during transmission. Security configuration of endpoint devices: Manage and maintain the security configuration of terminal devices.

	Cryptography: Using appropriate encryption techniques to protect sensitive information and communications. Technology Vulnerability Management: Integrated use of technology tools to identify, assess, and address vulnerabilities.

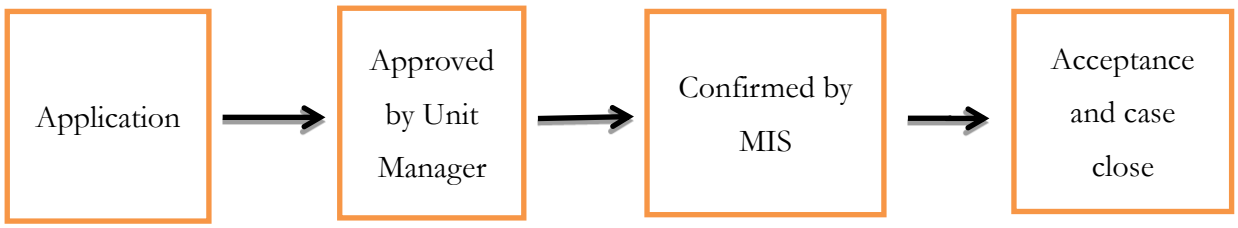
Information security management unit

The information security management unit of the company is the Information and Human Resources Department, which is responsible for reviewing the information security governance policies, planning, supervision, and information security management operations of each branch of the company, and monitoring the information security situation of each branch at any time. In case of major information security risk events, report to the general manager in a timely manner, regularly assess information security risks and report to the board of directors.



Information service process management

Applications and changes to resource permissions for information application software and hardware, systems, emails, networks, etc. required by personnel in each unit of the company shall be handled through an electronic application process, which shall be reviewed and approved by the relevant responsible person in charge, and shall be handled after confirmation of authorization.



Information Security Management Solution

The company reviews information security risks through risk identification and risk assessment, confirms the degree of adverse impact of the information security risks on corporate operations, takes corresponding management measures, and reviews information architecture, network activities, network equipment, servers and terminals Focusing on equipment detection and security settings review, we can check and evaluate whether there are vulnerabilities or old equipment problems at any time, and also respond to the challenges faced by information security, such as APT advanced persistent attacks, DDoS attacks, ransomware, and social engineering attacks. , information theft and other information issues, the planned information security management plan is as follows:

1. Risk Assessment: Conduct comprehensive risk assessments on a regular basis to identify potential threats, vulnerabilities, and risks.
2. Security policies and procedures: Implement access controls, password policies, data classification, and other requirements.
3. Access control: implement authentication and authorization mechanisms to ensure that only authorized personnel can access sensitive information.
4. Cybersecurity: protecting network infrastructure, including firewalls, intrusion detection systems, vulnerability scans and security updates to reduce cyber threats.
5. Security Training and Education: Conduct security training and education for employees to increase their awareness of information security.
6. Monitoring and alerting: Implement monitoring systems to observe network activity and detect abnormal behavior in a timely manner to respond quickly to security incidents.
7. Incident response plan: Develop a security incident response plan and data recovery strategy to mitigate losses and quickly resume operations.
8. Regular reviews and updates: Review and update security measures regularly to ensure they are responsive to new threats and vulnerabilities.

Resources in information security management

project	2021	2022	2023
Antivirus software	58,500	58,500	58,500
Maintenance costs	1,170,800	2,210,687	2,363,149
Computer room door control fee	0	0	0
Equipment and software upgrade costs	2,256,518	2,675,750	3,259,830
total	3,485,818	4,944,437	5,681,479

Information security incidents and insurance

of the company's information security governance and management mechanism is implemented by all employees in accordance with regulations. No serious information security incidents have occurred. The overall information security risk management is appropriate and the expected goals can be achieved. The company has insurance on its physical assets, and adopts off-site backup of major file data, as well as an information system disaster recovery plan. If future legal regulations and information security management needs require the purchase of information security insurance, the company will evaluate and understand the relevant regulations and supporting facilities. Measures will be decided later.

Information security risk management review and improvement

implements information security internal control implementation and risk supervision and management based on the business scope of its responsibilities and operates the management mechanism process. It also conducts self-inspections on the risk internal control system on an annual basis, conducts self-inspections on information cycle internal controls, and self-assesses information security. Management implementation. The audit unit also tracks the implementation status, and the annual audit plan is included in the inspection items to ensure implementation and effectiveness review or improvement reference basis.

.

Implementation in 2023 is as follows:

✧ Adopt ISO 27001

In order to better protect the company's information, improve risk management and enhance customer confidence, we introduced ISO 27001 Information Security Management System (ISMS) this year. By implementing ISO 27001, we have reviewed the company's overall information security implementation. We have reduced risks, improved compliance with relevant information security regulations and legal requirements, implemented clearer internal processes, and will continue to

improve employees' information security awareness in the future to ensure that all our assets are properly protected.

- ✧ Regular system updates
  Regularly monitor the update status of the system , patch known vulnerabilities , and ensure that all systems are in the latest security state.
- ✧ Regularly review user permissions before the end of each year to prevent unauthorized access to data.
- ✧ Use a centralized antivirus system - Kaspersky monitors and eliminates virus incidents at any time.
- ✧ Promote information security concepts from time to time.
  Software vulnerabilities are a major challenge in the modern threat landscape and one of the most common ways for malicious attackers to penetrate systems. However, timely software updates can significantly reduce potential risks and ensure the security of systems and data. This is key to maintaining digital security. one of the most important steps. Much software does not have automatic updating capabilities, such as Winrar software, which became obsolete this year The software vulnerabilities also have attracted the attention of the information security industry. Through this incident, we once again advocate not to install software that has not been confirmed by the company to avoid becoming the target of attackers.

Reporter: Manager of Information and Human Resources Department/ T.M. Lin

(Submit the ”Information Security Risk Management Report ” to the Audit committee and Board of Directors for review on 2023.11.6)