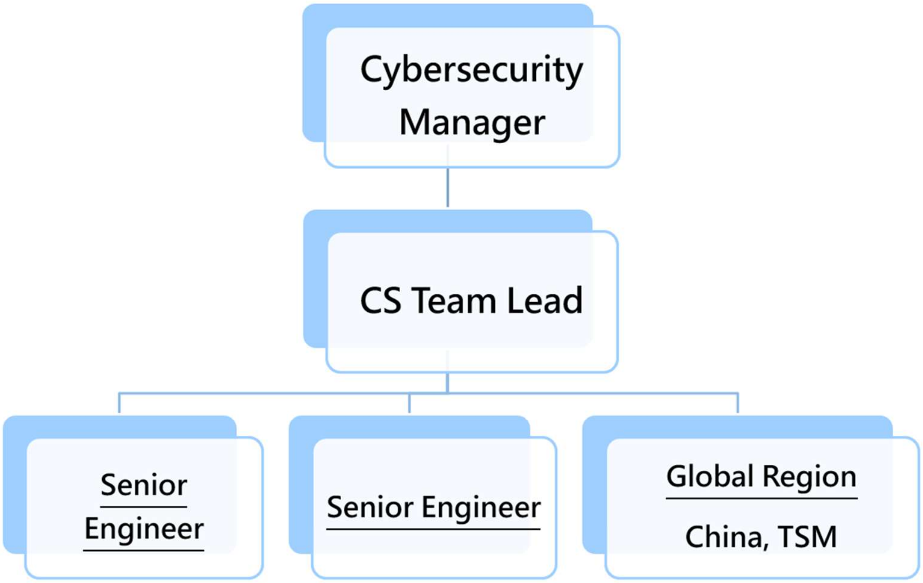
台橡股份有限公司
TSRC CORPORATION

Cyber Security Policy and Management

1 Cyber Security Organization Structure

TSRC cyber security is dedicated and managed by Cyber Security team, which is subordinated to IT department. The organization is led by Cybersecurity Manager, one cyber security team lead and several professional IT staffs. They are planning and implementing cyber security operations and the promotion and implementation of cyber security policies, and regularly reporting the company's cyber security governance overview to the board of directors every year.



2 Cyber Security Policy

The organization establishes and maintains an Information Security Management System (ISMS) in accordance with the ISO 27001:2022 standard to ensure that information and assets are properly protected.

Through systematic regulations, we safeguard the confidentiality, integrity, and availability of information assets, demonstrate the Company’s commitment to information security, reduction of the impact of security incidents, continuous improvement, and protection of the interests of the company, customers, and stakeholders.

2.1 Objective

The purpose of establishing the Cyber Security Policy is to defend against all planned or accidental threats, whether internal or external, in order to protect the security of the company’s critical information assets. It also serves to communicate the company’s support and determination in promoting information security.

2.2 Scope

It is the obligation of all users of the company systems to protect the technology and information assets of the company. This information must be protected from unauthorized access, theft, and destruction. The technology and information assets of the company are made up of the following components:

2.2.1 Computer hardware, software

2.2.2 Communications Network hardware and software

2.2.3 System Software

2.2.4 Application Software

2.2.5 Data: used by the various departments within the company. This includes employee data, supplier data, customer data, material master data, inventory data, sales data, financial data, manufacturing data, also those data generated by system or programs etc.

2.3 User Responsibilities

This section establishes usage policy for the computer systems, networks, and information systems of the office.

2.3.1 Acceptable Use

(1) User accounts on company computer systems are to be used only for business of the company and not to be used for personal activities.

(2) Users are personally responsible for protecting all confidential information under their accounts.

(3) Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system or gain access to company systems for which they do not have authorization.

(4) Users shall not install unauthorized hardware/software on their PCs or workstations, unless they have received specific authorization from the employees’ manager and/or the company IT.

(5) Users are required to report any incidents of cyber security to their immediate supervisor.

2.3.2 Use of the Internet

(1) The company’s computer and network equipment are tools provided by the company for employees to perform the business-related purpose. For the purpose of promoting the rational use of resources, protecting the company’s business secrets, and safeguarding the company’s rights and interests, the company may conduct necessary supervision or management of the employees’ computers and network equipment.

(2) Employees should legally use computers and network equipment within reasonable limits. Employees should not use computers and network equipment to handle personal affairs, hinder work efficiency, interfere with Internet circulation, occupy too much network bandwidth, or browse websites with improper content, or download or upload, send or reproduce any software, data or files that are harmful, illegal, or that are sufficient to damage the company's reputation, rights, or cause the company to be legally liable for third parties.

(3) Do not circulate improper or harmful information that contains obscenity, defamation, computer viruses, discrimination, harassment, etc., otherwise you shall bear legal responsibility.

(4) Employees shall not snoop on, read, or tamper with the internal data of others' computers without the express consent of others.

(5) R&D related employees and contractors/vendors/consultants must obtain suitable permission from supervisor and file a request with the Cyber Security Administrator for the Internet usage.

2.3.3 System Access Control

Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The meaning of access control is that permissions are assigned to individuals or systems. Access control is implemented by logon ID and password. For the critical information system, further access control methods can be implemented like two factors authentication.

2.3.4 Remote Access to Corporate network

The only acceptable method of remotely connecting into the internal network is using a VPN connection. The VPN access require username / password and two factors authentication.

2.4 Prevention measures of Cyber Security

2.4.1 Employees

Employees must take the following necessary measures to reduce the chance of cyber security threats:

(1) If employee is located at non-corporate network, he/she can only access corporate network through VPN connection.

(2) Do not use shared accounts to access systems. Never share your login information with co-workers.

2.4.2 IT Department

IT Department shall take the following necessary measures to reduce the possibility of cyber security risks and mitigate the damages of cyber security.

(1) End User Security Management

(2) When employees are resigned or disciplined, IT must remove or limit the account to access the systems based on the IT procedure definition.

(3) Regularly perform vulnerability scans on important systems.
(4) Monitor the logs of the information systems to analysis and handle the suspicious threat events.
(5) Regularly evaluate the latest solutions of cyber security to improve the company's security protection capabilities.

2.5 External Vendor Information Security Management Guidelines

Guidelines for Security Considerations When Outsourcing Information Processing or Assistance to Third Parties

2.5.1 Management Responsibilities

(1) External Parties: Comply with and sign the Information Security Operational Standards and Confidentiality Agreement, communicate access methods, and provide acceptance documentation.
(2) Information Coordinator: Inform external parties of relevant security standards, assist in signing the Information Security Operational Standards and Confidentiality Agreement, help with access permission applications, supervise contract compliance, conduct risk assessments and review reports, and remove permissions after the requirement ends.

2.5.2 Information Provision and Access Management

(1) When providing confidential information to external parties, a “Confidentiality Agreement” must be signed.
(2) Access permissions must be approved, and the “Information Security Operational Standards for Outsourced Vendors” explained, along with completing the “Third-Party Outsourcing Risk Assessment Form.”

2.5.3 External Party Responsibilities

(1) Access control must follow the Confidentiality Agreement, and information is limited to the original application scope.
(2) Comply with the company’s contract template and undergo legal review.

2.5.4 Security Management of Information Requirements

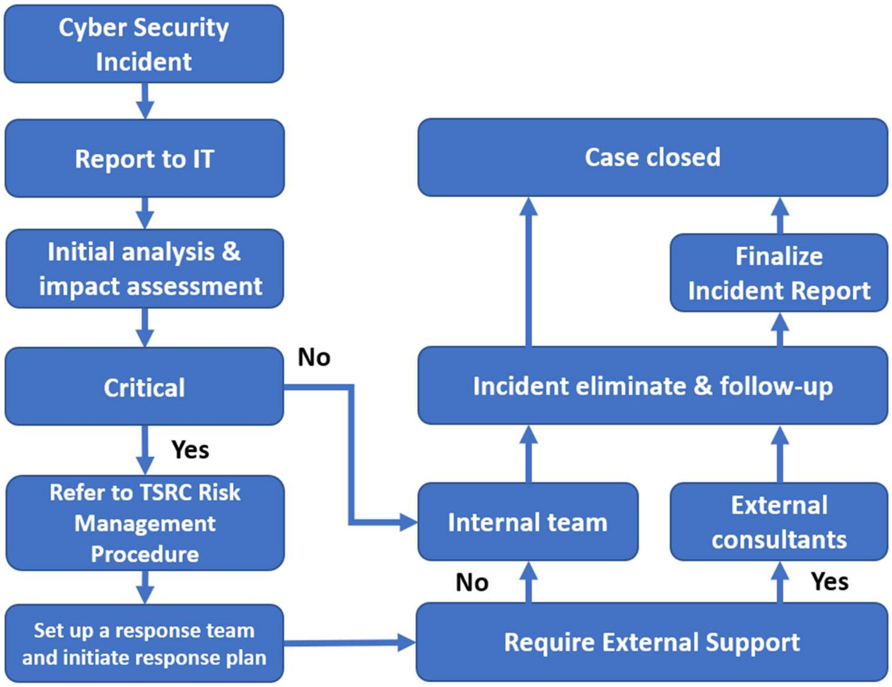
(1) During the process: Review external party services and equipment connections.
(2) After termination or completion: Ensure the return or destruction of information assets and remove access permissions.

2.5.5 Other Controls

System security acceptance, service change management, and third-party service audits.

2.6 Incident Response Plan

TSRC’s cyber security incidents are reported and handled by the following security incident response procedures.


Cyber Security Incident
Report to IT
Initial analysis & impact assessment
Critical
No
Yes
Refer to TSRC Risk Management Procedure
Set up a response team and initiate response plan
Require External Support
No
Yes
Internal team
External consultants
Incident eliminate & follow-up
Finalize Incident Report
Case closed

2.7 Business Continuity Management Procedures

To reduce the impact of unexpected incidents on information systems, contingency strategies and response plans are established according to business and ICT continuity requirements to ensure uninterrupted critical operations.

2.7.1 Business Impact Analysis

(1) Complete the “Business Impact Analysis Form” to identify critical operations and set RTO, RPO, and MTPD.

(2) Assess information security levels, recovery resources, and budget requirements.

(3) Develop backup mechanisms and continuity plans based on cost-benefit analysis.

2.7.2 Business Continuity Plan

(1) The plan should include impact analysis, recovery plan, and testing drills.

(2) Clearly define notification mechanisms, role assignments and contact lists, recovery sites, and procedures.

2.7.3 Plan Updates and Maintenance

(1) Update promptly upon changes; verify contact lists and recovery procedures at least annually.

(2) Test at least one core system each year and complete testing of all systems within three years.

(3) Review, revise, and submit for approval by the Information Security Management Committee.

2.8 Employee Training

2.8.1 New employee orientation - ensure the understanding of cyber security policy and align with related cyber security regulations.

2.8.2 Cyber Security Awareness Training - In order to elevate the sense of cyber security, IT department will provide cyber security awareness training annually and publish the information of cyber security and the recent security incidents via email quarterly to enhance the awareness of information security.