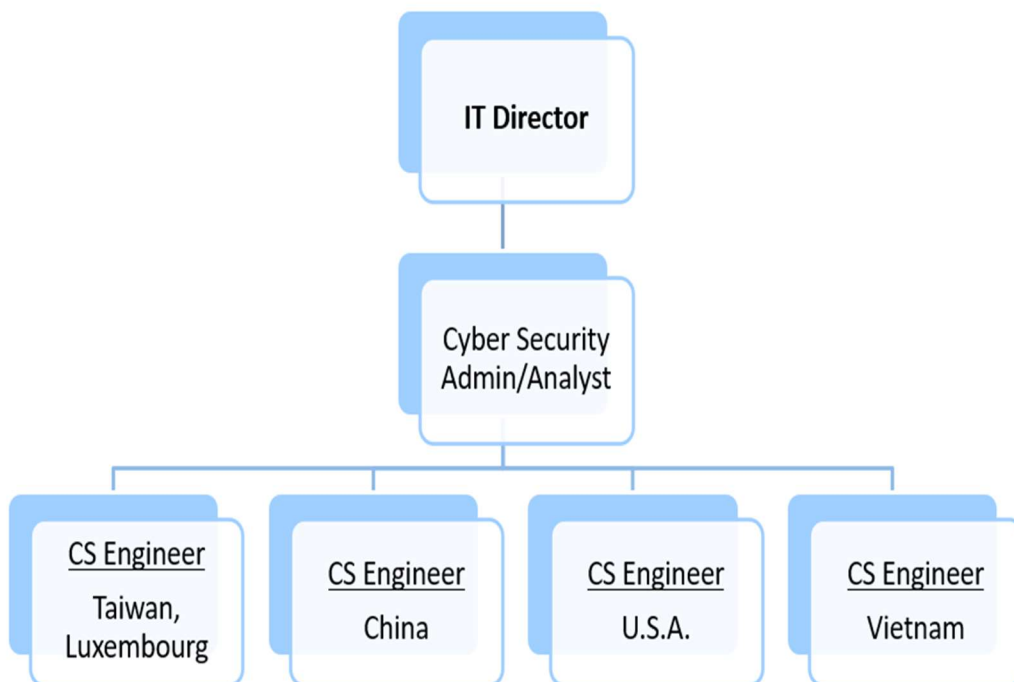


## Cyber Security Policy and Management

### 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 lead by IT director, one cyber security administrator 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

TSRC cyber security policy applies to reporting and handling of illegal, dishonest, or ethical behaviors within the company and its subsidiaries (hereinafter referred to as external personnel or collectively the "company")

#### 2.1 Objective

The purpose of defined the Cyber Security Policy is to prevent the cyber security threat by planned or incident attack from internal or external network, to protect the critical infrastructure asset and data of the company.

## **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/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

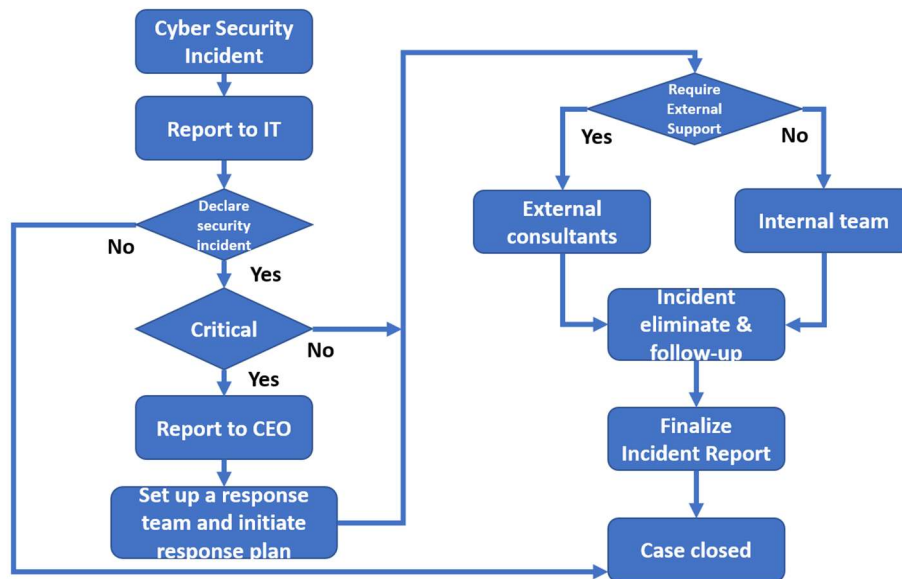
IT Department shall take the following necessary measures to reduce the possibility of cyber security risks and mitigate the damages of cyber security.

- (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 Incident Response Plan

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



## 2.6 Computer system recovery and operation methods

To ensure that the company's computer system can be quickly restored to maintain the integrity of the data after it is damaged

2.6.1 Servers and hosts will be divided into three levels, implementing different levels of backup mechanisms

- (1) The first level server is: it has a significant impact on the company's business, if it is damaged, it will affect the company's business
- (2) The second level server is: it has no direct impact on the company's business, but has a significant impact on the company's internal processes
- (3) The third level server is: it has no impact on the company's business, only affects a small part of the company's internal processes and has no obvious impact on the daily operations of the company's colleagues

2.6.2 Carry out system recovery verification test based on host level every year

## 2.7 Employee Training

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

2.7.2 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.