

# 資訊安全政策

## Information Security Policy

為建構安全的智慧化高速鐵路運輸系統及保護本公司所有資通系統之相關資訊資產，包括實體環境、軟硬體設施、網路、雲端、資料、資訊、人員等安全，免於因內部或外在之威脅，遭受破壞、遺失、洩密或不當控制等資通安全風險，特制訂本政策。

THSRC formulates the Information Security Policy to establish a secured Intelligent High Speed Rail Transportation System and to protect all THSRC's information and communication systems and related information assets that include physical environment, software and hardware facilities, network, cloud, data, information, and personnel, from cybersecurity risks such as damage, loss, information leakage or improper control resulted from internal or external threats.

本公司應採取以下措施：

THSRC should adopt the following actions：

1. 恪遵法令訂定相關資訊安全管理規章，對本公司資訊資產提供適當的保護措施，以確保其機密性、完整性、可用性及法律遵循性。

Comply with the laws to ensure the confidentiality, integrity, availability, compliance of the information assets, it is necessary to establish the correlative information security regulation to provide the appropriate protection.

2. 定期評估各種人為及天然災害對本公司資訊資產之影響，並訂定重要資訊資產及關鍵性業務之防災對策及災變復原計畫，以確保本公司業務持續運作。

Evaluate the influence of the negligence or natural disaster on the information assets regularly, and establish the precaution solution and disaster recovery plan to ensure the continuity of business operation.

3. 督導本公司同仁落實資訊安全防護工作，建立「資訊安全、人人有責」觀念，提升各業務部門及人員對資訊安全之認知。

Guide all employees to carry out information security protection, and set up "Information Security Is Everyone's Responsibility" to raise all units' and employees' understanding of information security.

4. 要求本公司全體同仁以及連結本公司資通系統或提供服務之往來廠商，應確實遵守本公司資訊安全相關規定，如有違反者，視其情形分別依本公司規定懲處或依契約罰責辦理外，情節嚴重者另將受相關法律之訴追。

Demand employees and contractors who connect to the THSRC's information and communication systems or provide service should comply with the related information security regulation. The violator will be punished according to the THSRC's regulation or contract. And if it is serious, the violator will be sued by law.

董事長：  
Chairman

江耀宗

日期：  
Date

2021.05.27