



# 資訊安全政策

## Information Security Policy

### 一. 目的

#### Purpose of the Policy

禾伸堂企業股份有限公司（以下簡稱本公司）為確保本公司相關資訊資產，包括實體環境、軟體、硬體、網路、資料之完整防護，以降低資安事件帶來之衝擊與威脅，並確保資訊系統維運之機密性、完整性及可用性，特訂定本資訊安全政策，以為遵循。

This Information Security Policy is specifically formulated for compliance to ensure the complete protection of Holy Stone Enterprise Co., Ltd (hereinafter “the Company”)’s relevant information assets, including the physical environment, software, hardware, network and data, to reduce the impact and threat of information security incidents and to ensure the confidentiality, integrity and availability of maintenance and operation of the information system.

### 二. 資訊安全政策內容

#### Content of the Policy

1. 本公司各項資訊安全管理必須遵守政府相關法規（如：資通安全管理法、專用法、商標法、著作權法、個人資料保護法等）及ISO27001資訊安全國際標準之相關規定。  
The company’s various information security management regulation must comply with relevant government regulations (Cyber Security Management Act, Patent Act, Trademark Act, Copyright Act, Personal Data Protection Act.) and ISO27001 Information Security International Standard.
2. 為確保本公司資訊安全之落實實施，應針對各資訊安全領域訂定資安規範及資通安全管理辦法，本公司全體員工須嚴格遵循。  
To ensure the implementation of the Company’s information security regulation, information security regulations and information security management measures should be formulated for each information security field, and all employees of the Company must strictly follow.
3. 本公司資通安全管理辦法內容包含：裝置使用、傳統文件、媒體儲存裝置、存取控制、軟體使用、無線網路、實體環境與安全、帳號密碼與金鑰、系統開發和維運、電子郵件與通訊軟體、供應商與人員任用、資訊安全事件管理及資安懲處等相關規範。  
The Company’s information security management measures include: device usage, traditional files, media storage, access control, software usage, wireless network, physical environment and security, IT credentials, system development and maintenance, email and communication software, supplier and personnel appointment, information security incident



management and information security punishment etc.

4. 委外廠商應遵循本政策及相關程序之規定，未經授權不得使用本公司之各類資訊資產，若涉及使用限制等級之資訊資產，應簽署保密切結書。

The subcontractors shall abide by the provisions of this policy and related procedures and shall not use the Company's various information assets without authorization. If the use of restricted information assets is involved, Non-Disclosure Agreement (NDA) shall be signed.

5. 本公司員工須定期實施資通安全教育訓練及社交工程演練，提升員工資訊安全認知。

The Company's employees must regularly take information security education and training courses and social engineering drill program to reinforce employees' information security awareness.

6. 本公司應定期評估各種人為及天然災害對本公司資訊資產之影響，並制定緊急應變管理辦法及災難復原演練計畫暨建立資安事件通報程序，定期進行演練、測試及檢討。

The Company shall regularly assess the impact of various man-made and natural disasters on the Company's information assets, and formulate contingency plan, disaster recovery plan and information incident response plan and conduct regular drills, tests and reviews.

7. 違反本政策與本公司之資訊安全相關規範，將依資安懲處規範辦理。

Violation of this policy and the Company's information security regulations shall be handled in accordance with the information security punishment regulations.

本政策之頒布，明確宣示維護資訊安全的重要性，本公司全體員工、與本公司有業務往來之廠商及其員工或臨時雇員等應確實瞭解本資訊安全政策，以維護本公司所有業務之資訊安全與永續經營。

The promulgation of this policy clearly declares the importance of maintaining information security. All employees of the Company, manufacturers and their employees or temporary employees who have business dealings with the Company shall understand this policy in order to maintain the information security and sustainable operation of all business of the Company.

總經理 唐錦榮