



Document No	I-MS-02-003-F02	Document Name	資訊安全政策
Confidential Level	公開	Current Version	A

資訊安全政策

本公司秉持維護交易作業環境之資訊安全理念，對於本公司資訊系統及所產生、蒐集、處理、儲存、傳遞或揭露之自身和客戶的各類型資料及資訊實施周全的保護與防範，以保護資訊的機密性、完整性和可用性，並杜絕內部或外部的毀損、失竊、洩漏、竄改、濫用與侵權等事故威脅，特訂定本資訊安全政策，以為遵循。

管理職責：目標

- 一、 必要時，確保適當存取正確的資訊，避免未經授權存取；(存取控制的目標)
- 二、 制定並實施標準所要求之資訊安全控制措施，以保護資訊免遭洩露，濫用和欺詐；(資安事件的目標)
- 三、 定義資訊安全的角色和職責，成立資訊安全專責組織；並通過提供適當的資訊安全培訓和實作課程來支援人員和員工，以提高安全意識和風險最小化；(教育訓練的目標)
- 四、 每年應至少進行一次營運持續計畫及資訊安全事件通報之演練、測試、檢討。(BCP和通報演練的目標)

政策要求

- 一、 瞭解『資通安全管理法』、『個人資料保護法』、『著作權法』等資訊安全相關法令，以及與客戶或委外廠商的合約或協議。
- 二、 進行資訊處理時，若含有個人資料，應依據『個人資料保護法』及相關規定審慎處理，不私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。
- 三、 應使用具合法版權軟體，避免上網下載來路不明之軟體。
- 四、 為能有效確保本公司之資訊安全，應針對各資訊安全領域訂定相關的規範。
- 五、 建立資訊資產風險評鑑機制，每年至少進行一次風險評鑑，並由管理代表決定可接受風險值。
- 六、 遵循本公司資訊安全事件通報機制，對於資訊安全事件須有完整的通報及應變措施，通報所發現之資訊安全事件或資訊安全弱點，以確保資訊系統及重要業務的持續運作。
- 七、 本公司主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾。依角色及職能為基礎，針對不同層級人員辦理資訊安全教育訓練及宣導，促使全體人員瞭解資訊安全的重要性，各種可能的安全風險，以提高資訊安全意識並熟悉工作中之資訊安全職責，促其遵守資訊安全規定。



Document No	I-MS-02-003-F02	Document Name	資訊安全政策
Confidential Level	公開	Current Version	A

- 八、 委外廠商應遵循本政策以及相關程序之規定，不得未經授權使用或濫用本公司之各類資訊資產，若涉及限定使用等級以上業務，應要求委外廠商所派遣之服務人員個別簽署「I-MS-02-008-F01 保密切結書」。
- 九、 每年至少召開一次管理審查會議，審核本公司資訊安全業務執行狀況，建立管理指標量測方式與評估管理指標量測結果。
- 十、 違反本政策或資訊安全相關規範，依本公司相關辦法規定及決策辦理。

對本政策之要求事項如有例外或排除或不適用者，須以正式申請過程，經管理代表向總經理確認可接受後，得以該申請事由豁免遵循本政策全部或部分要求事項。申請方式無限制，但必須留存記錄。

本政策由總經理指派管理代表進行編撰並經總經理核可後實施。本政策至少每年或當有重大事件時，須由管理代表提出，並邀請相關同仁進行檢討或修訂，以落實持續改善之精神。

本政策之頒布，明確宣示維護資訊安全的重要性，本公司全體人員、與本公司有業務往來之廠商及其員工或臨時派遣人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。

本政策經總經理核可後施行，修正時亦同。