

啟迪國際資訊股份有限公司

資訊安全暨個資保護管理系統

(ISMS)

資通安全暨個資保護政策

機密等級：普通 內部使用 敏感 機密

文件編號：ISMS-01-01

版 本：V2.1

2025 年 08 月 22 日

目 錄

壹、目的.....	4
貳、依據.....	4
參、適用範圍	4
肆、權責.....	4
伍、名詞定義	4
陸、內容.....	5
柒、資通安全政策之核定程序.....	6
捌、資通安全政策之宣導.....	7
玖、資通安全政策之檢討程序.....	7
壹拾、輸出文件/紀錄	7

壹、目的

啟迪國際資訊股份有限公司(以下簡稱本公司)為確保資訊、資通系統、設備及網路通訊與個人資料等之安全，有效降低因人為疏失、蓄意或天然災害等導致之資通資產遭竊、不當使用、洩漏、竄改或毀損等風險，並建立資訊安全暨個資保護管理系統(ISMS)，特訂定「資通安全暨個資保護政策(ISMS-01-01)」(以下簡稱本政策)以資遵循。

貳、依據

本政策依據下列相關法令法規及標準訂定：

- 一、 ISO 27001 : (Information security, cybersecurity and privacy protection — Information security management systems — Requirements)。
- 二、 ISO 27701 : Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

參、適用範圍

本政策適用於本公司同仁(正式及約聘雇人員)、接觸本公司業務資訊或提供服務之廠商及第三方人員，及其相關資通安全暨個資保護相關活動。

肆、權責

本公司同仁(正式及約聘雇人員)、接觸本公司業務資訊或提供服務之廠商及第三方人員皆應遵循資通安全暨個資保護政策之相關規範。

伍、名詞定義

本政策所記載之專用名詞說明如下：

- 一、 資訊安全管理系統(ISMS)：是一套有系統地分析和管理資訊安全風險的方法，透過控制措施的執行，把資訊風險降低至可接受的程度內。
- 二、 機密性：保護資訊避免未經授權的存取或揭露。
- 三、 完整性：確保資訊在任何階段沒有被不適當的修改或偽造。
- 四、 可用性：經授權的使用者能適時的存取所需資訊。
- 五、 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性

生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

- 六、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
- 七、蒐集：指以任何方式取得個人資料。
- 八、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
- 九、利用：指將蒐集之個人資料為處理以外之使用。
- 十、當事人：指個人資料之本人。

二、內容

為使本公司業務順利運作，防止資訊或資通系統及所保管之個人資料等受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，特制訂本政策如下，以供全體同仁共同遵循：

- 一、本公司各項資通安全管理規定必須遵循政府相關法令法規(如：資通安全管理法、刑法、國家機密保護法、個人資料保護法、著作權法…等)之規定。
- 二、本公司依據可能影響資通安全之內外部議題，與關注方對於資通安全之要求事項，擬定完整的資訊安全管理系統(ISMS)。
- 三、由本公司「資通安全暨個資保護推動委員會」負責資通安全及個資保護管理制度之建立及推動事宜。
- 四、應建立資通安全及個資風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全及個資風險管理之有效性。
- 五、應保護機敏資訊或資通系統等之機密性與完整性，避免未經授權的存取與竄改。
- 六、為因應資通安全威脅情勢變化，確保同仁完成資通安全教育訓練，宣導資通安全暨個資保護政策及相關實施規定，以提高本公司同仁之資通安全意識，本公司同仁亦應確實參與訓練。
- 七、建立資通硬體設施及軟體之管理機制，以統籌分配、有效運用資源。

- 八、新資通系統應於建置前將資通安全因素納入，防範危害系統安全之情況發生。
- 九、建立實體及環境安全防護措施，並定期施以相關維護或保養。
- 十、明確規範資通系統及網路服務之使用權限，防止未經授權之存取行為。
- 十一、訂定資通安全及個資保護之內部稽核計畫，定期檢視資訊安全暨個資保護管理系統(ISMS)之落實情形，並依內部稽核報告，針對不符合事項擬定及執行矯正措施。
- 十二、應強固核心資通系統之韌性，訂定資通安全之營運持續計畫並實際演練，確保本公司業務持續營運。
- 十三、本公司基於合法的組織目的，蒐集最少的必要個人資料，並採行適當安全措施，確保個人資料被公平合法的處理及利用。
- 十四、本公司所有人員皆負有維持資通安全之責任，且應遵守資訊安全暨個資保護管理系統(ISMS)相關規定，並應針對辦理資通安全業務有功人員進行獎勵。

柒、資通安全政策之核定程序

本公司之資通安全暨個資保護政策應簽呈資通安全長核定後實施。

捌、資通安全政策之宣導

本公司之資通安全暨個資保護政策應每年透過教育訓練、內部會議或張貼公告等方式，向公司內所有人員及利害關係人進行宣導。

玖、資通安全政策之檢討程序

本公司之資通安全暨個資保護政策應定期進行檢討，以反映政府資通安全管理政策、法令、技術、關注方之需要及期望、內外部議題與本公司業務之最新狀況，並確保本公司資通安全及個資保護實務作業之可行性及有效性。

壹拾、輸出文件/紀錄

無。