

## 1 目的

宏遠電訊股份有限公司（以下簡稱本公司）為提升同仁的安全意識已參考相關國際標準並陸續進行導入，為使同仁更能了解相關管理系統之內容，特訂定「安全管理政策」（以下簡稱本政策）以期能內化為組織文化的一部份。

## 2 依據

- 2.1 ISO/IEC 27001:2013 (Information technology — Security techniques — Information security management systems — Requirements)
- 2.2 ISO/IEC 27011 增項稽核要求
- 2.3 ISO/IEC 27002:2013 (Information technology — Security techniques — Code of practice for information security management)
- 2.4 ISO/IEC 29100:2011 (Information technology — Security techniques — Privacy framework)
- 2.5 BS 10012 : 2009 (Data protection - Specification for a personal information management system)
- 2.6 國家通訊傳播委員會(NCC)電信事業資通安全管理手冊

## 3 資通訊安全政策

本公司為確保主機、網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資通訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資通訊安全管理規範，以期能確保本公司業務資通訊之機密性、完整性與可用性。

- 機密性：確保被授權之人員才可使用資訊。
- 完整性：確保使用之資訊正確無誤、未遭竄改。
- 可用性：確保被授權之人員能取得所需資訊。

以下為本公司資通訊安全政策之內容：

- 3.1 本公司各項資通訊安全管理規定必須遵守政府相關法規（如：刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法、**資通安全管理法**等）之規定。
- 3.2 成立資通訊安全管理組織負責資通訊安全制度之建立及推動事宜。
- 3.3 定期實施資通訊安全教育訓練，宣導資通訊安全政策及相關實施規定。

- 3.4 建立主機及網路使用之管理機制，以統籌分配、運用資源。
- 3.5 新設備建置前，須將風險、安全因素納入考量，防範危害系統安全之情況發生。
- 3.6 建立資通訊機房實體及環境安全防護措施，並定期施以相關保養。
- 3.7 明確規範網路系統之使用權限，防止未經授權之存取動作。
- 3.8 訂定資通訊安全管理系統內部稽核計畫，定期檢視本公司推行資通訊安全管理系統範圍內所有人員及設備使用情形，依稽核報告擬定及執行矯正預防措施。
- 3.9 訂定營運持續管理辦法並實際演練，確保本公司業務持續運作。
- 3.10 本公司所有人員負有維持資通訊安全之責任，且應遵守相關之資通訊安全管理規範。
- 3.11 資通訊安全管理系統文件應有明確之管理規範。

## 4 個資安全政策

本公司為落實我國個人資料保護法（以下簡稱個資法）之規定，確保公司所有活動均能合理的蒐集、處理及利用個人資訊，以下為本公司個資安全政策之內容：

- 4.1 各項安全管理規範必須遵守政府相關法規之規定。
- 4.2 應成立個資安全管理組織負責個人資料保護制度之建立及推動事宜以確認本公司個資安全政策能被實施並配置相當資源。定期召開會議以確保個人資料安全維護之整體持續改善。
- 4.3 應鑑別出內部與外部的利害關係人以及這些利害關係人參與組織個資安全保護的程度，並辨識工作人員的職責及權責。
- 4.4 應維持一份組織處理個人資訊的清單(如：個人資料檔案彙整清冊)，並建立個人資料之風險評估及管理機制。
- 4.5 應建立設備、資料安全及人員管理規範及個資事故之預防、通報與應變機制。
- 4.6 應建立資料安全稽核及必要之使用紀錄、軌跡資料及證據之保存機制，以為後續舉證或證明已盡善良管理人之用。
- 4.7 定期對同仁實施個資安全認知宣導，並針對個資維護(專責)人員施以適當之教育訓練，以宣導本公司個資安全政策及相關實施規定。

- 4.8 定期訂定個資內部稽核計畫，檢視本公司個資保護之情形，依稽核報告擬定及執行矯正預防措施。
- 4.9 僅會基於合法之目的及執行法定義務的必要的範圍內公平並合法的處理個人資訊。
- 4.10 僅會基於合法之目的蒐集最少且必要的個人資訊，處理相關且適當的個人資訊亦不會超出蒐集之目的，對於保存個資的時間須為法律或規定的需求理由或為合法的組織目的。
- 4.11 維持正確的個人資訊並確保其安全，且於必要時維持其資訊為最新的狀態。
- 4.12 於處理或利用前清楚告知當事人，本公司將會以何種方式使用他們的個人資訊，並且尊重當事人與其個人資訊的相關的權利，包括對於個人資訊的存取權。
- 4.13 本公司保有之個人資訊僅限於台灣地區使用，若有轉移到國(境)外之必要將於使用前取得當事人同意後並在有適當且充分保護下為之。
- 4.14 本公司若有特定目的外之利用，應符合個人資料保護法第 20 條之例外情形。

## **5 政策之評估及檢討**

- 5.1 本政策每年應至少評估一次，以反映政府各項安全政策、法令、技術及本公司業務之最新狀況，確保安全實務作業之可行性及有效性。
- 5.2 本政策經安全管理委員會審查或依行政流程陳請總經理簽核後頒布實施，修正時亦同。