達方電子股份有限公司資訊安全政策及說明

西元 2022 年 10 月 08 日

1.資訊安全政策

達方電子股份有限公司（以下簡稱本公司）為強化資訊安全管理、確保資訊的機密性、完整性與可用性、資訊設備（包括電腦硬體、軟體、週邊）與網路系統之可靠性以及同仁對資訊安全之認知，並確保上述事項所需之資源免受任何因素之干擾、破壞、入侵、或任何不利之行為與企圖，在符合機密管理原則下，做到將正確的資訊適時的送達正確的人，特訂定本政策。

2.權責

依下列分項原則，配賦適當之人員其權責：

- 資訊安全政策、計畫及技術規範之研議、建置及評估等事項。
- 資料及資訊系統之安全需求研議、管理及保護等事項。
- 資訊機密維護及安全稽核等事項。

3.範圍

本政策之範圍如下，有關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效：

- 人員管理及資訊安全教育訓練。
- 電腦系統安全管理。
- 網路安全管理。
- 系統存取控制。
- 系統發展及維護安全管理。
- 資訊資產安全管理。
- 實體及環境安全管理。
- 遵守客戶端資訊安全管理要求。
- 業務永續運作計畫之規劃與管理。

4.人員管理及資訊安全教育訓練

- 對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。各業務主管人員，應負責督導所屬員工之資訊作業安全，防範不法及不當行為。
- 針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升資訊安全水準。

- 熟悉客戶端資訊安全管理要求，避免違反客戶規定而造成公司損失。

資安目標：定期教育訓練

5.電腦系統安全管理

- 辦理業務委外作業，應於事前研擬資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守。
- 依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。
- 採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。
- 對各種系統變更作業，應建立控管制度，並建立紀錄，以備查考。
- 採購資訊軟硬體設施，應依公司標準或權責主管訂定之政府資訊安全規範，研提資訊安全需求，並列入採購規格。

資安目標：核心系統訂定累計系統可用度

6.網路安全管理

- 開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。
- 與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。
- 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未同意之個人隱私資料及文件，不得上網公布。
- 訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。
- 為避免網路使用者不慎違反本公司相關網路安全規定，網路管理人員可考慮以相關網路技術以不干擾正常網路使用為原則下，主動管制違反本公司相關網路規定之使用者。

資安目標：核心網路訂定 MTPD

7.系統存取控制

- 訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者相關權限責任。
- 離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。
- 建立系統使用者註冊管理制度，加強使用者通行密碼管理。
- 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。
- 建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

8.資訊資產安全管理

- 建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等。
- 依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施。
- 已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

9.實體及環境安全管理

就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。

資安目標：核心網路訂定 RTO 及 RPO

10.系統使用客戶資訊安全管理要求

- 提供優質的網路系統服務。
- 網路系統修訂滿足使用者期望。
- 協助/輔導系統使用者避免遭受外部網路攻擊與保護電腦資訊安全。

資安目標：服務滿意度

11.業務永續運作計畫之規劃與管理

- 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。
- 建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。
- 依相關法規及承諾的相關方要求/期望，訂定及區分資料安全等級，並依不同安全等級，採取適當及充足之資訊安全措施。

資安目標：核心系統分別訂定 RTO 及 RPO

12.持續改善

本公司透過以下方法進行持續改善：

- 每年至少一次透過本政策於管理審查時進行持續檢討改進檢討與措施擬定、執行、追蹤。
- 資訊安全目標的定期統計、審核並在管理月報會議中討論改善機會。
- 內外部稽核。
- 即時 BPM 管理的可用度登錄(管理)系統。

總經理 蔡耀坤

西元 2022 年 10 月 08 日