

# 耀勝電子股份有限公司

## 資通安全事件緊急應變計畫暨作業處理程序

### 壹、目的

- 一、為利本公司於遭遇資通安全事件時，能迅速通報及緊急應變處置，並在最短時間內回復，以確保本公司各項業務之正常運作，特訂定本計畫暨程序。
- 二、適用時機：於發生重大資通安全事件或其他災害涉及資通安全事件時，應立即依本計畫暨程序辦理。

### 貳、資通安全處理小組

- 一、本公司成立「資通安全處理小組」，負責督導執行資通安全預防及危機通報、緊急應變處理等相關工作。

### 參、安全防護機制

- 一、本公司規劃建置資通系統及網路安全整體防護環境，含系統存取控管機制、連線紀錄資料庫、建構防火牆軟硬體、虛擬私人網路（VPN）、病毒掃描機制、入侵偵測系統（IDS）、外部弱點掃描、頻寬管理、系統內部安全漏洞檢測（更新、補強）、儲備必要之備份資料、程式或異地備援、重要文件資料檔案採取加密方式儲存等防護工具或措施。並制訂資通安全管理政策及制度等相關措施，定期實施安全稽核、網路監控、人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。
- 二、訂定之資訊安全政策，應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

### 肆、建立資訊安全組織

- 一、依下列分工原則，配賦有關單位及人員之權責：
  - （一）資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。
  - （二）資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。
  - （三）資訊機密維護及稽核使用管理事項，由稽核單位會同相關單位負責辦理。
- 二、稽核單位應進行定期或不定期之資訊安全稽核。
- 三、資訊單位負責資訊安全管理事項之協調及推動。
- 四、各部門應視資訊安全管理需要，指定適當人員負責辦理資訊安全相關事宜。

### 伍、人員安全與管理

- 一、各部門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。
- 二、各部門應針對管理、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，提升部門資訊安全水準。
- 三、各部門應加強資訊安全管理人力之培訓，提升資訊安全管理能力。
- 四、各部門負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。
- 五、各部門主管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。

### 陸、電腦系統安全管理

- 一、各部門辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。
- 二、各部門對系統變更作業，應建立控管制度，並建立紀錄，以備查考。
- 三、各部門應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。
- 四、各部門應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。

#### **柒、網路安全管理**

- 一、各部門利用公眾網路傳送資訊或進行交易處理，應評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求，並針對資料傳輸、撥接線路、網路線路與設備、接外連接介面及路由器等事項。
- 二、各部門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。
- 三、各部門與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與部門內部網路之資料傳輸與資源存取。
- 四、各部門開放外界連線作業之資訊系統，必要時應以代理伺服器等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。
- 五、各部門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、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。  
部門存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭不當或不法之竊取使用。
- 六、各部門機密性資料及文件，不得以電子郵件或其他電子方式傳送。  
機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各部門應視需要以適當的加密或電子簽章等安全技術處理。  
部門業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管部門認可之加密或電子簽章等安全技術處理。
- 七、各部門採購資訊軟硬體設施，應依本公司採購程序請購及採購，並知會資訊部門評估之。

#### **捌、系統存取控制**

- 一、以書面、電子或其他方式告知員工及使用者之相關權限及責任。
- 二、各部門應賦予各級人員必要的系統存取權限；部門員工之系統存取權限，應以執行法定任務所必要者為限。對被賦予系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估。
- 三、各部門離（休）職人員，應立即取消使用部門內各項資訊資源之所有權限，並列入部門人員離（休）職之必要手續。  
部門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。
- 四、應建立系統使用者註冊管理制度，加強使用者通行密碼管理，並要求使用者定期更新；使用者通行密碼之更新周期，由部門視作業系統及安全管理需求決定，最長以不超過六月個為原則。  
對部門內外擁有系統存取特別權限之人員，應建立使用人員名冊，加強安全控管，並縮短密碼更新周期。

- 五、各部門開放外界連線作業，應事前簽訂契約或協定，明定其應遵守之資訊安全規定、標準、程序及應負之責任。
- 六、各部門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。
- 七、各部門之重要資料委外建檔，不論在部門內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。
- 八、應確立系統稽核項目，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。

#### **玖、系統發展及維護安全管理**

- 一、自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。
- 二、對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。  
基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。但使用完畢後應立即取消其使用權限。
- 三、委託廠商建置及維護重要之軟硬體設施，應在相關人員監督及陪同下始得為之。

#### **拾、業務永續運作之規劃**

- 一、訂定業務永續運作計畫，評估各種人為及天然災害對部門正常業務運作之影響，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。
- 二、應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，立即向權責主管單位或人員通報，採取反應措施。
- 三、應依相關法規，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。

#### **拾壹、其他**

- 一、應就設備安置、周邊環境及人員進出管制等，訂定妥善之實體及環境安全管理措施。