公司資訊安全政策

1、目的：

明訂公司資訊安全政策規範，以規範公司有關資訊安全事宜，並定期以書面、電子或其他方式告知全體同仁遵照，以防公司因資訊安全事故而遭受嚴重損失，用以確保公司資訊安全並永續經營。

2、適用範圍：

全公司。

3、名詞定義：

無

4、相關文件：

資訊安全緊急應變實施辦法
公司資訊安全組織與權責
公司資訊系統安全管理
公司資訊網路安全管理
公司系統存取控制規範
ERP 系統資料備份作業辦法
ERP 系統異常處理作業辦法

5、內容說明：

5.1 資訊安全政策制定及評估

5.1.1 資訊安全政策制定

當公司營運電腦化的程度越深，資訊安全問題的重要性也就日益增加。為避免公司因資安疏失而蒙受損失，特訂定本作業規範，以建立「資訊安全，人人有責」觀念，並全方位做好資訊安全措施。

5.1.1.1 資訊安全之定義

5.1.1.1.1 資訊安全之本質可歸為以下三類：

5.1.1.1.1.1 機密性（Confidentiality）：確保各項業務相關資料之機密安全，並予以適當的規範及保護。

5.1.1.1.1.2 完整性（Integrity）：確保各項資訊資產的完整，以期組織能正確運用該項資產。

5.1.1.1.1.3 可用性（Availability）：確保各項資訊資產能提供即時且正確的服務，以滿足使用者之需求。

5.1.1.1.2 資訊安全政策應由專人或專責單位進行維護，並

由資訊安全組織定期作必要之審查及調整，以維護資訊安全政策之適切性及有效性。

5.1.1.2 資訊安全之目標

5.1.1.2.1 確保資訊之可用性與完整性，使資訊系統正常且持續運作。

5.1.1.2.2 確保資訊之機密性，保障資料之隱私權。

5.1.1.2.3 確保資訊之正確性，保障使用資訊系統之品質。

5.1.1.2.4 根據以上安全政策，另訂定各項目標以為資訊安全維護之明確指標。

5.1.1.2.4.1 資訊存取具有明確且適當的控制程序。

5.1.1.2.4.2 軟體開發與維護納入安全考量。

5.1.1.2.4.3 組織業務之持續運作。

5.1.1.2.4.4 配合公司稽核單位進行資通安全內部稽核工作，以確保公司之資通安全。

5.1.1.2.4.5 確保公司之相關委外作業須符合資通安全，並制定相關控管機制，進行委外管理。

5.1.1.2.4.6 資訊作業符合政策、相關法令與規定。

5.1.1.3 資訊安全之範圍

資訊安全之範圍共分十大項：

5.1.1.3.1 資訊安全政策制定及評估

5.1.1.3.2 資訊安全組織及權責

5.1.1.3.3 人員安全管理及教育訓練

5.1.1.3.4 電腦系統安全管理

5.1.1.3.5 網路安全管理

5.1.1.3.6 系統存取控制

5.1.1.3.7 系統發展及維護之安全管理

5.1.1.3.8 資訊資產之安全管理

5.1.1.3.9 實體及環境安全管理

5.1.1.3.10 業務永續運作計畫之規劃及管理

5.1.2.1 本作業規範應視需要進行獨立及客觀的評估，以反映政府資訊安全管理政策、法令、技術及公司業務之最新狀況，確保資訊安全之實務作業，確實遵守資訊安全政策，以及確保資訊安全實務作業之可行性及有效性。

5.1.2.2 資訊部門應定期檢討及評估各項軟、硬設備的安全性，以確保其符合安全標準；評估對象應包括作業系統之評估，以確保系統軟體及硬體的安全措施，正確及有效地執行。

5.1.2.3 資訊系統使用單位應配合定期的資訊安全評估，檢討人員是否遵守資訊安全政策、規範及有關安全規定。

5.2 資訊安全組織及權責

參考公司資訊安全組織與權責

5.3 公司資訊系統安全管理

參考公司資訊系統安全管理

5.4 公司資訊網路安全管理

參考公司資訊網路安全管理

5.5 公司系統存取控制規範

參考公司系統存取控制規範

5.6 業務永續運作計畫之規劃及管理

5.6.1 資訊安全事件緊急處理機制

參考資訊安全緊急應變實施辦法

5.6.2 ERP 系統之永續運作

參考 ERP 系統資料備份作業辦法

參考 ERP 系統異常處理作業辦法

6、附件：

無