僑威科技股份有限公司

資訊安全管理計畫

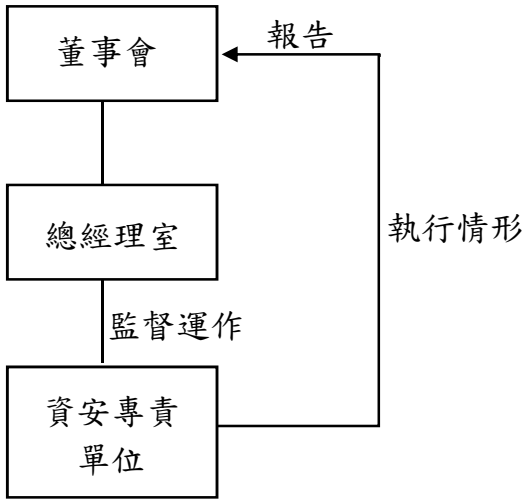
一. 資通安全管理策略與架構

(一) 資通安全風險管理架構

1. 資訊安全治理組織:

   本公司資安專責單位由資訊部負責，目前設置資安主管(資訊部主管兼任)，資安人員各一員，負責資訊安全政策之制定，執行及風險管理，定期檢討及調整資訊安全政策，並向董事會報告資通安全執行情形，確保運作之適切性及有效性。

2. 資訊安全組織架構



(二) 資通安全政策

本公司已制訂「電腦設備管理、公開資訊申報辦法、網路與資訊管理程序」等作業辦法。

1. 保護公司核心資通系統，確保公司的核心業務可以順暢運作，不受外來干擾中斷營運。
2. 員工之工作職掌應作適當區隔，並僅授予完成工作所需之必要權限與必要資訊。
3. 定期辦理資安宣導教育，以提高同仁之資訊安全意識及個人防護能力。
4. 不論客戶是在哪一個地區或國家，不論該地區有否立法，妥善保護客戶資訊及隱私。

5. 不外洩員工個資，落實個人資料保護法。
6. 本公司資訊安全措施應符合法律之規範及本公司資訊安全相關辦法之要求。
7. 所有資訊安全規範或程序之建置及修改，須符合並遵循資訊安全管理制度之機制。

（三） 具體管理方案

1. 人員資安意識教育訓練: 定期實施資訊安全教育訓練及宣導，以提高公司同仁對資訊安全之認知及風險意識。
2. 資訊系統安全管理:
   2.1公司主機伺服器、個人電腦及筆記型電腦統一安裝防毒軟體，並自動更新病毒碼，並定期檢視更新狀況。
   2.2郵件系統建置垃圾郵件過濾功能，惡意郵件偵測功能等，提升整體郵件資訊安全。
   2.3應用系統及資料庫，每日進行資料備份，每年定期實施系統資料還原演練作業，並監控每日備份結果，以確保資料儲存安全性。
   2.4管控各系統管理者權限，規範各系統只能使用公司授權之合法軟體，並遵守相關法令規定，非經合法授權及與業務無關之軟體，無法安裝使用，以確保公司軟體授權合規性，並降低使用非法軟體感染病毒，後門程式之風險。
   2.5資訊系統業務委外時，於事前審慎評估可能潛在安全風險，確保委外廠商執行委外作業時，具備完善之資通安全管理措施。
3. 網路安全管理:
   3.1公司對外服務應用系統以防火牆與外部網際網路隔離。
   3.2公司內部辦公區域針對無線網路設備進行管控，避免外部人員經由無線網路入侵公司系統。
4. 系統存取控制:
   4.1有新進員工時，人資單位需協助上系統提出申請，通知資訊部執行使用者之新增其使用權限，確保系統存取安全。
   4.2當員工調整職務及離職時，人員異動單據需會簽資訊部門調整或刪除其使用權限，確保系統存取安全。
   4.3內部應用系統依照人員工作需求，由員工使用電子簽核系統填寫權限申請單會簽稽核部門審查，核准後才交資訊單位處理執行。

4.4資訊系統必需設定帳號密碼，使用者通行密碼應符合安全原則，並要求使用者定期更改系統密碼。

5. 資通安全健診:

公司每年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

5.1網路架構檢視。

5.2網路惡意活動檢視。

5.3使用者端電腦惡意活動檢視。

5.4伺服器主機惡意活動檢視。

5.5安全設定檢視。

6. 資安永續管理與運作:

6.1成立資安專責單位，負責資安政策，管理辦法之建立及推行，審議資安問題與因應對策，並要求全體員工確實遵守，維護公司資訊安全。

6.2若發生資訊安全事件，依資通安全事件等級，迅速通報總經理室、資安主管及資安人員，並進行適當處置及快速執行復原作業。

（四） **投入資通安全管理之資源**

1. 本公司定期檢視整體資通安全計畫，以應對現在快速發展的資訊環境，並加強宣導同仁資訊安全概念。

2. 本公司將電腦化資訊系統相關控制作業列入年度稽核計畫之稽核項目定期查核，以落實資安計畫執行。

二. 資通安全風險與因應措施:

本公司已建立資安防護措施，雖無法保證能完全避免資安事件，但是可以最短時間回復資訊系統運作使公司核心業務不受影響中斷並與時俱進持續改善資安規範，減少公司核心業務受到干擾。

三. 提報董事會日期: 112 年 12 月 28 日