政伸企業股份有限公司

資訊安全管理及執行情形

一、資訊安全與管理制度：

本公司由管理部資訊室負責資安風險管控，以建全資訊安全。若發生資安風險事件時，資訊室彙整通報管理部主管，並由技術性相關資訊人員提出解決方案與後續預防改善措施，由管理部主管決策或召集各相關部門主管與會商討解決方式。

二、資訊安全風險管理：

1. 各項機密資料檔案,各廠部應設專人管理或統一放置由公司規定之儲存檔案資料夾中，以防止資料洩漏或損毀。
2. 使用儲存設備(如 USB 隨身碟、行動硬碟、無線傳輸設備、光碟等)須提出資訊系統使用申請表並載明用途，呈各廠部主管簽核後轉資訊權責單位作業，資訊權責單位得依資訊作業安全評估是否核准。
3. 本公司所有同仁於使用網路時應以公務使用為限，使用者不得將個人之登入帳號與密碼交付他人使用。(如：政伸 MIS 系統、網域登入帳號密碼等。)
4. 資料或軟體之下載、複製、取用、傳遞與提供，需遵守專利、智慧財產權及個人資料保護相關法令之規定，並禁止下載使用或傳送非法軟體或來路不明的檔案，且網路使用者不得在本公司網路使用任何點對點傳輸（Peer to Peer）軟體。
5. 禁止將工作現場或涉及公司機密之相關資訊上傳至網站或網路儲存空間等相關網路資源(例：FaceBook、Google Drive、Dropbox、百度雲等)，以及禁止將公司機密檔案以即時通訊軟體傳輸(包含 Skype、騰訊 QQ、Line、WeChat 等)。

三、具體管理方案：

1. 全體同仁欲利用本公司電腦使用即時通訊者，需填妥資訊系統使用申請表，經單位主管核准後轉資訊權責單位登錄控管，始可使用。
2. 本公司現有資訊設備均有監控紀錄之功能，全體同仁於本公司內的網際網路行為均經申請並同意留下記錄。
3. 建置防火牆阻絕外界攻擊和 Websense 員工上網過濾機制,防禦過濾惡意網址及進階持續性威脅攻擊防禦等系統。
4. 安裝防毒軟體、更新原廠安全性修補程式，並定期進行弱點掃描等稽核機制，以強化防護。
5. 關注資安議題及擬定因應計劃，並定期對員工進行資訊安全教育訓練，強化員工的資安風險意識。
6. 今年已委託顧問公司進行 ISO27001 資訊安全標準導入，目前專案進行中。
7. 本公司資通安全風險管理及執行情形已於 111/11/04 提報董事會報告。