建德工業股份有限公司
報告事項
資訊安全政策

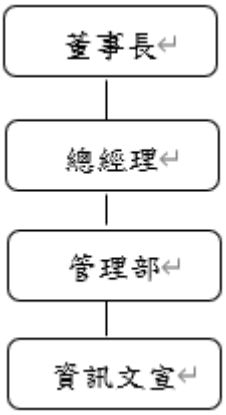
◆檢查時間:111年

◆資訊安全政策

為管控或降低資訊安全意外事件所可能造成的損失，本公司制定「內部控制制度—電子計算機循環」及「資通安全檢查辦法」，進行資訊安全查核，評估公司資訊作業內部控制之有效性，以確保資訊系統與資料之安全性、可用性及完整性，並辨識出可能發生的意外事件或風險，採取適當回應，控管可能產生的損失在一個可接受的範圍內。

資訊安全治理架構

◆資訊安全治理架構



◆資訊安全管理機制

項目	管理內容
資訊安全管控	1. 公司之系統設備及軟體，在非經權責主管授權之情況下不得使用或接近該資產。 2. 公司應指定專責人員進行資訊安全之維護及檢討。 3. 公司應對員工私人電腦作必要之安全控管，以防止公司資訊遭不法之利用。 4. 系統開發測試與正式作業須使用不同之登入環境。 5. 設備報廢前應先將機密性、敏感性資料及版權軟體移除。 6. 機房設置門禁管制，人員進出應填寫登記備查，禁止未被授權的人員進出。 7. 資訊管理部門須建置資訊軟體、硬體之資產清冊且隨時更新。
存取控制	1. 凡對外簽訂之資料存取契約須事先經權限主管核准，契約中應包含資料保護及智慧財產權等條款。

	2. 因業務需要開放給外單外(含顧問、維護廠商、委外承包商、臨時人員)使用相關資訊時，其存取權限須嚴加控管。 3. 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工應妥適分工及分散權責。 4. 對於輪調、調派或晉升之員工，應適當予以取消各項識別碼或權限。
網際網路安全管理	1. 設置防火牆，以防止駭客非法竊取或侵害，並定期檢查網路運作環境是否有安全上之漏洞。 2. 資訊人員每日檢查網路設備是否有異常情形並記錄備查。 3. 公司之伺服器及個人電腦須加裝防毒軟體並即時更新病毒碼，並公告相關病毒資訊予終端使用者。 4. 禁止使用或下載未經授權或與業務無關之軟體。以避免佔用公司之網路資源及增加病毒感染機會。
電腦軟體與程式著作權保護	1. 資訊軟體之取得及使用須為合法授權之軟體，並應遵守授權者之相關約定條款。 2. 對於有使用人數限制之授權軟體，公司應確實遵守及履行使用人數限制，資訊人員須不定期檢查公司是否有非經授權使用之軟體。 3. 資訊管理部門須保留合法軟體之授權證明、原版程式及使用說明書。
資料備份及復原機制	1. 建立系統備份機制，落實異地備份。 2. 定期執行災害系統復原計畫演練。 3. 定期檢視緊急應變計畫。
資訊安全政策宣導及檢核	1. 隨時宣導資訊安全資訊，提升員工資安意識。 2. 每年定期執行資通安全檢查，並呈報董事長，並予以揭露。

◆資訊安全具體作為

項次	項目	具體作為或預防措施
1	資訊安全政策	每年檢視資訊安全政策，並呈報董事長後，向董事會報告。
2	資訊安全管控	(1) 指定資訊專責人員。 (2) 資訊機房進出管控，製表紀錄進出人員、時間及業務。
3	存取控制	(1) 資訊存取需有憑證及紀錄。

		(2) 人員異動須會簽資訊專責人員，俾利設定存取權限。
4	網際網路安全管理	(1) 定期蒐集及分析防火牆數據，滾動式調整公司資安防禦， 於110年10月9日簽訂網路防火牆設置及授權。 (2) 定期健檢防毒軟體:依據前述契約，隨時更新。
5	電腦軟體與程式著作權保護	定期檢視各項軟體授權: (1)Windows(2)office(3)solidworks(4)Adobe軟體(5)Autodesk軟體
6	資料備份及復原機制	備份-資料庫及File Server遵從備份3-2-1原則，進行每日備份。
7	資訊安全政策宣導及檢核	(1) 每年6月、11月定期宣導資安:6/15宣導 (2) 定期呈報董事長，並報告董事會:8/11報告董事會。