堡達實業股份有限公司

資訊安全風險管理架構

一、 本公司資訊安全組織

本公司依據已建置之資訊安全政策建構公司之資訊安全風險管理架構，並配置資訊安全主管及資安人員，負責資訊安全事務之各項規劃與執行。包含定期檢討修正資訊安全政策，資訊安全主管每年至少一次於高階主管會議中報告本公司重大資安議題或執行規劃說明。

二、 資訊安全目標

建立本公司安全作業環境，確保本公司資料、系統、設備、網路安全，避免公司營運資訊機密外洩。以提昇公司員工工作效率。

三、 資訊安全政策範圍

1. 資訊安全權責分工
2. 人員管理及資訊安全教育訓練
3. 電腦系統安全管理
4. 網路安全管理
5. 系統存取控制管理
6. 系統發展及維護之安全管理
7. 資訊資產安全管理
8. 實體及環境安全管理
9. 業務永續運作計畫管理
10. 個人資料保護管理

堡達實業股份有限公司

四、 資訊安全具體管理

項目	具體管理措施
資訊資產安全管理	機房主機配置不斷電系統。 配置適用滅火器。 配置可視電壓機櫃專用延長線。確保隨時用電不會超過負荷。
網路安全管理	與外網配置企業級防火牆。 使用遠端登入內網 ERP 系統 VPN 得以保留。 防火牆設置過濾存取權限，可阻擋非必要或已有風險之網站。 定期查看可疑主旨郵件。
病毒防護管理	員工電腦設備均安裝有防護軟體。病毒碼自動定時更新。 終端設備設定有過濾高風險網站軟體。
系統存取控制管理	員工於系統內僅能存取自己工作相關權限。 設置員工存取權限，需經權責主管核准後，始得開放。 員工離職手續依人資離職通知後，即進行系統帳號刪除。
永續運作計畫管理	建置系統備份，重要資料並建立異地備份資料，以確保資料安全。
資安宣導	員工定期更換密碼。 定期進行資安宣導知會員工，並依近期重點資安事件分享說明。

五、 資通安全的資源投入

針對系統主機與員工終端主機進行重要更新及軟體升級作業，定期檢查計劃與執行進度。並透過定期的檢視資安狀況，判斷資訊設備是否存在漏洞，提出修補辦法後編列資安預算後執行。

六、 緊急通報程序

當發生資訊安全事件或疑為資安事件，通報資安人員，判斷事件類型並找出問題，呈報資安主管並且保留記錄。