資訊安全風險管理架構、政策及具體管理方案

資訊安全風險管理架構：

一、 資安單位：本公司設置有資訊部，負責本公司資訊安全管理。為有效管理及妥善維護電腦資訊環境，確保資訊使用及作業的機密性、完整性與可用性，並使相關人員執行作業有所依循，以降低任何資訊安全事件所可能帶來之衝擊，資訊部訂有資訊安全政策，其中即包含如：資訊授權、資料備份、系統開發、委外廠商管理、智慧財產權等具體管理方案。 為強化公司資安防護及管理，經金管會公告上市櫃公司之分級標準，本公司屬第二級公司，已於 112 年 11 月 10 日董事會通過設置資訊安全專責主管及一名資訊安全專責人員。

二、 內部稽核：本公司稽核室擬定資訊安全監理之查核單位，並就相關內部控制程序管理及定期進行內部稽核(第一方稽核)，以降低內部資安風險。

三、 外部稽核：每年第四季均由外部資安風險諮詢服務單位對公司資訊安全做全面檢查(第三方稽核)，以確保資安的完整性。

資訊安全政策：

目的：為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之資訊業務持續運作之資訊環境,並符合相關法規之要求,使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範，作為本公司全體員工資訊安全之依循。
定義與目標：為確保各項資訊系統免受任何因素之干擾、破壞、入侵或任何不當之行為，經由適當的系統規劃、程序規範及行政管理，以防範來自內、外部的威脅，達到維護資訊系統安全的目的。並在資訊系統遭受來自內、外部人員不當使用或蓄意破壞等緊急事故時，公司能迅速應變處置，在最短時間內回復正常運作，降低該事故可能帶來的損害與不便。

資訊安全具體管理方案：

一、 電腦設備安全管理：

1. 本公司各系統的主機伺服器等設備，均設置於專用機房內，機房門平時均上鎖，非資訊人員如需進入機房需經過資訊人員的同意，且須登記於機房出入紀錄本上。
2. 電腦機房備有獨立冷氣空調系統，確保機房內電腦設備處於適當的溫度下運轉；並設置二氧化碳式滅火器與定期檢查滅火器的有效性，防止意外災害發生。
3. 機房主機配置穩壓與 UPS 不斷電設備，可避免電力瞬間斷電造成系統不正常關機的損壞，也確保臨時短暫停電時不會中斷電腦應用系統的運作，如遇電力公司發佈停電公告時，則資訊人員將會提前關閉各系統的主機伺服器等設備，待電力公司復電後再予以重新啟動開放各系統的主機伺服器等設備。

二、 網路安全與病毒駭客防護管理：

1. 與外界網路連線的入口(untrust)，配置企業級防火牆並設定各項管制條例嚴格控管，並經常更新防火牆韌體版本以因應各種網路病毒及駭客的攻擊。
2. 伺服器與同仁終端電腦設備內均安裝有端點防護軟體，並具備自動更新病毒碼的功能，以確保病毒碼維持在最新狀態，避免電腦遭受到零時差攻擊並阻擋最新型的病毒，同時可即時自動防護及偵測、防止具有潛在威脅性的惡意及木馬程式植入系統執行檔內執行及安裝之行為。

3. 電子郵件伺服器前端有配置郵件防毒、與垃圾郵件過濾閘道器，防堵病毒或垃圾郵件進入使用者端的電腦，另外建置黑白名單管制表，以避免系統誤判而阻檔正常的郵件收發。
4. 公司租用兩條電信公司數據線路，一條屬公司內部網路連至外網使用，另一條除供公司監控系統及對外 VPN 使用之外，另架設路由分享器，提供 WiFi 連線以提供公司內部人員或訪客使用。

三、 系統存取控制：

1. 公司同仁對各應用系統的使用，須透過公司內部規定的系統權限申請程序，經權責主管核准後，由資訊部建立系統帳號，並經各系統管理員依所申請的功能權限經授權後方得進行存取。
2. 帳號的密碼設置，規定適當的強度，要求必須英文數字、特殊符號混雜， 且至少 8 位以上以符合密碼原則。
3. 同仁辦理離(休)職手續時，必須會簽資訊部，進行各系統帳號的刪除或停用作業。

四、 資料備份與復原演練：

1. 建置備份管理系統，採取數份備份原則，本地端機房使用不同的備份媒介儲存，其餘備份資料存於備份媒體內，並存放於離公司 10 公里以上之異地。
2. 災害復原演練：重大系統每年實施一次災害復原演練，選定還原日期基準點後， 由備份媒體回存於系統主機後再確認回復資料的完整性及可用性，以確保備份媒體的完整性與有效性。

五、 資安宣導與教育訓練：

1. 每月對員工發送宣導資安事項郵件以強化員工資安意識。
2. 資安相關人員須取得相關證照，或進行相關資訊安全相關教育訓練並留下紀錄。 113 年 7 月 16 日及 7 月 17 日參加工研院產業學院之「資訊安全工程師中級培訓班」專業研習課程計 12 小時，並取得「資訊安全工程師-中級能力鑑定」證照。

資訊部每年均定期執行各項資訊安全相關之檢測及評估作業，113 年度各項資安檢測評估作業頻率及執行結果如下：

項目	作業頻率	113 年度作業期間	結果
ERP 系統災難復原測試	每年一次	113/6	無應列重大風險情形
電腦合法性軟體檢查	每年一次	113/6	無應列重大風險情形
ERP 系統權限設定檢查	每年一次	113/8	無應列重大風險情形
ERP 系統個人密碼定期通知	每年二次	113/6、113/12	無應列重大風險情形
資訊安全宣導	不定期，每年至少一次	113/5、113/6	無應列重大風險情形
機房巡檢	每日	國定假日除外	無應列重大風險情形
資料庫備份作業	每日(採系統自動+人工手動異地備份)	星期日除外	無應列重大風險情形