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。

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，以降低內部資安風險。

三、外部稽核：每年第四季均由外部單位對公司資訊安全做全面檢查，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損害與不便。

資訊安全具備管理方案：

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.電腦機房備有獨立空調，確保機房內電腦設備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不斷電設備，可避免電力瞬間斷電造成系統停機，也確保臨時停電時不會中斷電腦應用系統的運作。

二、網路安全與病毒防護管理：

1.與外界網路連線的入口，配置企業級防火牆與設定存取規則，經常更新版本以因應各種網路攻擊。

2.伺服器與同仁終端電腦設備內均安裝有端點防護軟體，並自動更新病毒碼方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。

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。

4.租用兩條電信公司數據線路，一條屬公司內部使用，一條經分享器提供 WiFi 給公司內部人員或訪客使用。

三、系統存取控制

1.同仁對各應用系統的使用，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做授權方得存取。

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，必須會簽資訊處，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，其餘備份資料存放於異地。

2.災害復原演練：重大系統每年實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機確認回復資料的完整性，以確保備份媒體的正確性與有效性。

五、資安宣導與教育訓練：每月對員工發送宣導資安事項郵件以強化員工資安意識。