資通安全管理

(一)、資通安全風險管理策略與架構：

本公司為強化各項資訊資產之安全管理，提昇資料、系統、設備及網路安全，確保本公司資訊處理之正確性，避免人員所使用之電腦軟體、硬體、週邊及網路系統免受干擾、破壞、入侵之行為或企圖，訂定資通安全管理架構、策略及具體管理方案。

1. 資通安全風險管理架構

(1) 企業資訊安全治理組織

本公司資訊安全之權責單位為資訊部，隸屬在管理處下，將集合公司各部門主要主管，包括管理處副總經理、業務部副總經理、生產研發部經理及生物資訊部經理，一同納入公司資訊安全管理組織內。

資訊部負責提出各部門同仁使用電腦應遵守的資訊安全規範，交由資訊安全管理組織內的各部門主管，由各部門主管負責監督同仁是否確實遵守，如發現可能的威脅情事立即通報資訊部，由資訊部立即做應對處置。

各部門主管負責監督項目:

1. 檢查同仁電腦是否有安裝非公務使用或非法軟體
2. 檢查同仁電腦作業系統是否有定期更新
3. 檢查同仁電腦是否有登入不安全的網站
4. 檢查同仁是否有定期參加資安宣導會議並留下出席紀錄
5. 檢查同仁電腦是否有設定開機密碼
6. 檢查同仁電腦重要檔案是否定期備份

(2) 資訊安全組織架構

2. 資通安全政策及具體管理方案

（1）企業資訊安全管理策略與架構

為落實資訊安全管理，資訊部定期檢視資訊安全政策之適用性，並進行資安風險評估，對資安措拖持續進行改善，另為保護資訊資產安全，建立資訊資產清冊並加以分類分級管理，重要電腦機房進出建立管控機制，以維護機房設備的安全性。定期舉行資訊安全通識及隱私保護相關課程，以實體或是線上會議的形式進行資訊安全相關之教育宣導，每年至少 1 次，促使同仁瞭解資訊安全之重要性及資訊安全風險，以提高同仁資訊安全意識，促其確實遵守資通安全規定。

（2）具體管理方案

a. 網路安全:導入防火牆設備，制定防火牆政策以管控內外網路連線，另額外導入資安防護設備，針對網路流量頻寬監控、惡意網址及中繼站、木馬程式、勒索病毒等進行偵測及即時阻斷，以及針對電腦應用程式進行管控。

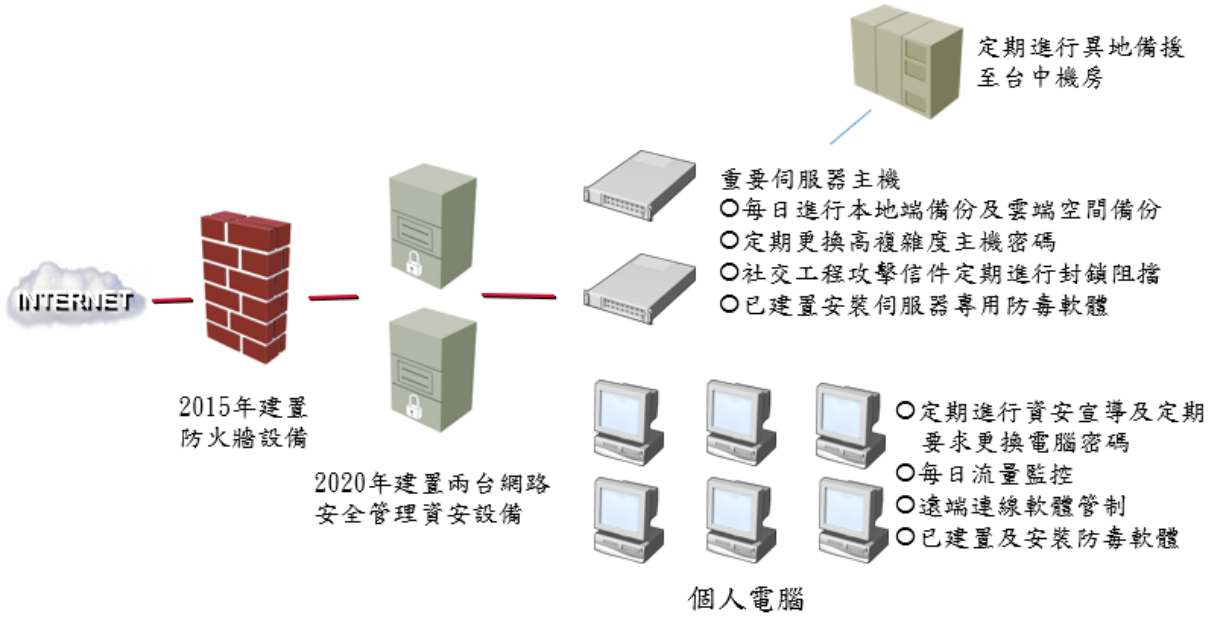
b. 裝置安全:公司伺服器及個人電腦使用者端設備皆安裝防毒軟體，針對惡意軟體行為進行偵測，防止勒索病毒等惡意程式進入公司設備。

c. 實體與環境安全:為確保電腦機房維運及資訊資產使用區域之安全，訂定人員進出機房登記文件、建立資訊設備資產清冊、每日機房檢查文件。

d. 資料安全保護:定期進行伺服器內重要資料及資料庫本地備份、異地備援及雲端空間備份，確保資料的安全性及完整性。並訂定資訊安全緊急應變計畫，針對天然災害應變、人為破壞應變、停電時緊急應變和一般當機及服務中斷之應變處理。

e. 教育訓練與宣導:定期舉行資訊安全通識及隱私保護相關課程，以實體或是線上會議的形式進行資訊安全相關宣導，每年至少 1 次，提升員工資安意識，加強員工對資安風險的觀念，另因應近年詐騙郵件及勒索郵件攻擊的頻率增高，定期加強宣導讓員工對社交工程攻擊郵件提高警覺性。

（3）投入資通安全管理之資源



(二)、 資通安全風險與因應措施：

近年來社交工程攻擊電子郵件信件增多，可能造成伺服器或個人電腦中毒、駭客攻擊入侵風險增加，另外公司網站如遭受網路攻擊，也可能造成公司營運之影響以及重要機密資料之遺失或遭竊取，勒索軟體也會讓公司檔案遭加密，而造成資料之損失，如因駭客攻擊事件造成案件延誤或中斷，也會對公司營運造成嚴重的損失，為了預防及避免此類攻擊事件造成的損失，公司制定資訊安全政策，執行資安相關工作計畫，建置防火牆及制定防火牆政策以阻擋網路攻擊事件，另額外採購買建置網路資安設備，加強網路流量及應用程式之控管，安裝商業版防毒軟體定時進行掃毒及防毒，定期進行伺服器及電腦內重要資料及資料庫備份，定期加強員工資安宣導，提昇同仁對於資安風險意識。

項目	內容	週期	執行狀況
資安管理人員設置	設有資訊安全管理組織，集合本公司各部門主要主管，負責制定資安策略與實施計劃	每年	一共 5 名
資安相關會議次數	定期召開資安工作會議，跨部門協調資安措施	每年	執行日期 113 年 12 月 27 日
防毒軟體	安裝並定期更新防毒軟體，保護內部系統不受病毒威脅	每年	1 年 1580 元
弱點掃描	進行定期的弱點掃描，識別並修補系統漏洞	每年	113 年度執行弱點與掃描:36000 元
資安訓練與教育	進行員工資安教育與訓練，提高資安意識與應急反應能力	每年	執行日期 113 年 3 月 5 日(發資安宣導) 113 年 3 月 19 日(線上資安宣導課程)
資安應急演練	進行資安事件應急演練，提升員工應對資安事件的能力	每年	執行日期 113 年 9 月 30 日

1. 資訊技術安全之風險及安全管理措施

資安風險說明	安全管理措施
機房硬體設備損壞	每日執行機房檢查作業，如發現異常狀態立即處理。
通訊網路服務中斷	每日執行機房檢查作業，如發現異常狀態立即處理。
個人電腦中毒	宣導個人電腦定期掃毒、定期更新作業系統與軟體、定期宣導資安事件，加強人員資安觀念。

駭客攻擊入侵	使用防火牆設備並制定適當防火牆政策、伺服器安裝商業等級防毒軟體、伺服器定期更新系統與掃毒。
備份作業失效	定期檢視自動備份排程，如發現異常狀態立即修正與調整。
因垃圾郵件造成電腦中毒等異常情形	郵件主機設定防堵垃圾信黑名單機制，定期宣導資安事件加強人員資安觀念。
因電力保養而中斷電力，造成設備異常	定期執行設備保養，測試電力中斷後系統回復狀態。
因系統或設備故障，造成設備功能無法使用	每日檢視系統及設備狀態，如發現異常情形立即調整修正，並備妥備援設備視情形立即更換。
因天然災害造成設備損壞或異常	制定系統災害復原計畫，定期執行演練預防，平時執行系統備份與異地備援。

(三)、 最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：無此情形。

(四)、其他重要風險及因應措施：

資安風險評估分析及因應措施：

為落實資訊安全管理，公司制定「資訊安全政策」，並據以執行資訊工作計畫，同時建置防火牆 、制定防火牆政策、安裝防毒軟體、訂定資訊備份計畫、資訊安全緊急應變計畫、進出機房登記表、機房檢查表等，管理資料之利用與安全維護，同時管制人員進出及使用權限等，以減少公司資訊安全風險。

資安風險相關評估分析及因應措施如下:

資安風險說明	發生次數	實施安全控制措施
機房硬體設備損壞	0	每日執行機房檢查作業，如發現異常狀態立即處理。定期汰換老舊設備及備妥備援設備視情形立即更換。
通訊網路服務中斷	0	每日執行機房檢查作業，如發現異常狀態立即處理。定期汰換老舊網路設備及線路。
個人電腦中毒	0	宣導個人電腦定期掃毒、定期更新作業系統與軟體、定期宣導資安事件，加強人員資安觀念。

駭客攻擊入侵	0	使用防火牆設備並制定適當防火牆政策、伺服器安裝商業等級防毒軟體、伺服器定期更新系統與掃毒。
備份作業失效	0	定期檢視自動備份排程，如發現異常狀態立即修正與調整。
因垃圾郵件造成電腦中毒等異常情形	0	郵件主機設定防堵垃圾信黑名單機制，定期宣導資安事件加強人員資安觀念。
因電力保養而中斷電力，造成設備異常	0	定期執行設備保養，測試電力中斷後系統回復狀態。
因系統或設備故障，造成設備功能無法使用	0	每日檢視系統及設備狀態，如發現異常情形立即調整修正，並備妥備援設備視情形立即更換。
非相關人員進入機房	0	增加機房門禁系統管制，並有人員進出機房登記表管控。
因天然災害造成設備損壞或異常	0	制定系統災害復原計畫，定期執行演練預防，平時執行系統備份與異地備援。