資訊安全風險管理架構

1. 資訊安全風險管理架構：由行政處所轄之資訊部負責統籌資訊安全及相關事宜，並由稽核室擬定相關內部控制程序管理及定期進行內部稽核。
2. 資訊安全政策：請參閱附件。
3. 具體管理方案：

- 為確保公司資訊安全，資訊部於 Hinet 網路端向中華電信申租入侵防護服務，阻絕網路型病毒及入侵攻擊，再透過防火牆的建置，進一步阻擋病毒及入侵攻擊於公司內部網路之前，於用戶端部分，透過 Windows Update Services Server，自動將 Windows Update 更新派送至用戶端，修補用戶端 Windows 漏洞，防止病毒與駭客透過 Windows 漏洞，進行攻擊。另外安裝趨勢科技企業級防毒軟體，加強伺服器及用戶端防護。資訊部也在評估是否投保資安險，降低若是發生重大資安事件所產生的營運損失。
- 其餘具體措施請參閱附件。

附件: 資訊安全管理政策

一、目的

由於資訊系統及網際網路應用日趨發達，為確保本公司軟體、設備及網際網路之安全，特訂定此資訊安全管理政策，作為本公司全體員工遵循資訊安全之依據。

二、定義

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。

三、目標

避免資訊系統遭受來自內、外部人員不當使用或蓄意破壞，或當已遭受不當使用、蓄意破壞等緊急事故時，公司能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之經濟損害及營運中斷。

四、範圍

適用於本公司所有資訊系統及其使用者。資訊使用者係包含正式員工、聘僱人員、建置維護廠商及其他經授權使用之人員。

五、組織

由行政處所轄之資訊部負責統籌資訊安全及相關事宜，並由稽核室擬定相關內部控制程序管理及定期進行內部稽核。

六、程序

(一)人員資安意識及訓練

為降低內部人為因素對資訊安全之影響，資訊室需經常實施資訊安全教育訓練及宣導，以提高人員對資訊安全之認知及意識。

(二)資訊系統安全管理

1.電腦主機、各伺服器等設備應設置於專用機房，由資訊部負責管理，未經授權不可隨意進入，機房無人在場時，應處於上鎖狀態。
2.個人電腦及各項周邊設備等應依業務性質及場地空間等因素做妥適的配置，並應連接不斷電系統以確保供電穩定，以防設備受損影響公司營運。
3.主要設備維護及運作狀況應做成紀錄，設備故障應儘速自行排除或聯繫維護廠商緊急處理。
4.機房溫度須維持在 20~25℃之間，濕度維持在 40~60％RH 之間，若溫、濕度異於標準值時，透過警報系統和溫、濕度監控 APP 通知資訊部人員和值班主管，若狀況無法自行排除，須要求相關部門協助處理，以防設備受損影響公司營運。
5.新資訊系統建置，若與 ERP 系統相關，要經過安裝測試、功能測試、介面測試、性能測試、文檔測試等驗證，通過之後，才能上線，確保系統可以準確和穩定的運作。
6.各部門需使用經授權之合法軟體，並遵守相關法令及契約規定，非經合法授權及與業務無關之軟體，不得安裝使用，違者除應擔負有關法律責任外，倘若導致各單位設備毀損，尚應負相關損害賠償責任。
7.定期執行資料備援回復作業，以能在發生災害時，可迅速回復正常作業。備援媒體應異地存放於安全之環境，以確保資料完整可用。
8.資訊業務委外時，應於事前審慎評估可能潛在安全風險，並與廠商簽訂適當的資訊安全協定，課予相關的安全管理責任，納入契約條款。

(三) 網路安全管理

1.與外部網路連接之網點，應以防火牆及其他安全設施，控管外部與內部網路之資料傳輸與存取。
2.安裝企業版之防毒軟體，建置入侵偵測等防駭軟體以保護公司資訊系統免受病毒感染及惡意軟體或駭客入侵，此外資訊設備應隨時下載及更新最新病毒碼、作業系統漏洞修補程式。
3.網路如發現有被入侵或有疑似被侵入情形，需通知資訊部進行相關處理，必要時採取法律行動。

(四) 系統存取控制

1.使用者新進、調整職務及離（停）職時，應以書面通知資訊部執行使用者之新增、調整或刪除其使用權限，確保系統安全。
2.資訊系統皆必須設定通行密碼，使用者通行密碼應符合安全原則，並要求定期更改通行密碼。
3.人員暫時離開時應將電腦鎖定，不使用電腦設備時，必須完全登出資訊系統。
4.對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，隨時派人監控其處理情形。
5.依照專業機構提供之資訊環境控制與應用系統查核事項，資訊部定期進行自主性查核，確保資訊處理相關作業之安全。

(五) 資訊系統發展及維護之安全管理

1.系統之開發建置、維護、更新、上線執行及版本異動作業，應予安全管制，委託合法及合格廠商處理，避免不當軟體、後門及電腦病毒等危害系統安全。
2.對廠商之系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。基於實際作業需要核發短期或臨時性之系統辨識及通行密碼供廠商使用，事先須書面申請並於使用完畢後立即取消其使用權限。
3.委託廠商建置及維護重要之資訊系統，應在本公司資訊室人員監督及陪同下始得為之。
4.程式和系統權限修改需填寫申請單，由資訊室人員或顧問執行，使用者填寫測試報告確認無誤後由資訊主管放行後上線。

(六) 業務永續運作計畫之規劃與管理

1.如發生資訊安全事件，致資訊系統無法運作或影響執行效率時，應迅速通報單位主管及資訊部人員，做相關的處置。
2.通報後應立即停止使用受影響之資訊系統或設備，並保留現況，資訊部人員獲報後應記錄相關的訊息，進行相關處置程序。
3.資訊部定期評估資安風險造成損失之可能性，必要時投保適當之保險以降低損失金額。