109 年度資訊安全風險評估

項次	評估類別	風險評比(%)			重要管控措施
		低	中	高	
1	資訊安全政策	50	50	0	1.定期審查、修訂資訊安全政策。 2.內部稽核單位每年定期稽查管控措施。
2	建立資訊安全組織	64	36	0	1.設資安管理小組及個人資料保護小組。 2.訂立資安事件之緊急應變處理及回報程序。
3	人員安全與管理	40	60	0	1.內部控制制度定義資訊人員、使用者之作業權限畫分，及人員異動、離職之作業準則。 2.每年執行作業權限複核。 3.每年定期普查個人電腦，防止公器私用。
4	資產分類與控管	17	83	0	1.資訊類軟、硬體資產列冊管理。 2.每年定期普查電腦，確認軟、硬體資產。
5	實體及環境安全管理	55	45	0	1.專用電腦機房具溫度、電力自動控管。 2.伺服器及重要職務之電腦，安裝防毒軟體，每日定時備份，其備份份數至少二代。 3.營運資料庫資料每日壓縮後以磁帶儲存備份，每年定期模擬事故演練於廠商備援機房還原測試。
6	通訊與操作管理	42	52	0	1.電子郵件主機具自我防護及保存稽核之功能。 2.每日分析防火牆紀錄，並使用上網行為記錄器，即時防堵內、外部異常行為。 3.即時宣導資安事件、通告或案例，提升防護意識。 4.使用 Hinet 資安艦隊之防護方案，擴展防護廣度。
7	存取控制	25	58	0	1.電子檔資料依部門、個人設定存取權限。 2.對外連線作業申請需經部門主管及總經理同意。 3.電子郵件區分內、外部，不須對外連絡之人員僅能內部寄信。 4.人力資源系統於讀取個資時，自動記錄存取軌跡。
8	系統開發與維護	53	47	0	應用系統自行開發、維護，在規劃分析時主動將安全需求納入設計考量，防範外部的侵入篡改。
9	永續運作之計畫管理	67	33	0	1.營運資料庫每年定期演練、測試。 2.重要設備訂立緊急應變計劃，供發生重大資安事件時遵循及應變。
10	內部稽查及其它	45	56	0	1.每年電腦普查時告知公司軟體所授權之範圍，實際查核若有規範以外軟體則要求移除或提供授權證明；軟、硬體普查資料，隨時依資產狀況更新。 2.資訊單位每年定期自評資訊作業環境安全。 3.內部稽核人員每年定期稽查資訊控制作業。
總評 (%)		53	47	0	1.舊版 Windows 個人電腦應汰換。 2.應加強機敏性資料的防護措施。