資通安全管理

(一)敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。

1.資訊安全風險管理架構

本公司雖未成立跨部門資訊安全委員會，目前由資訊安全主管與資訊室主管一同擔任資訊安全相關事務。

2.資通安全政策

(1)訂定定期盤點資訊資產及個人資料清冊，對資訊安全及個人資料風險評鑑進行風險管理，落實各項控措施。

(2)不定期辦理資訊安全及個人資料保護教育訓練及宣導作業。

(3)委外廠商須簽訂保密協議，以確保使用本公司提供的資訊服務或執行相關資訊業務者，有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。

(4)重要資訊系統或設備已建置適當的備份、備援或監控機制並定期演練，以維持正常運作。

(5)個人電腦均安裝防毒軟體且定期更新病毒碼，並禁止使用未經授權的軟體。

(6)要求同仁帳號、密碼與權限應善盡保管與使用責任，並定期更新密碼。

(7)建立業務持續運作管理機制，並定期測試演練，維持其適用性。

(8)每年定期實施內部稽核，以確保資訊安全、個資保戶管制制度之有效性。

3.具體管理方案及投入資通安全管理之資源

(1)將資訊安全及個資保護檢查控制作業，列為年度稽核項目，稽核單位每年度至少進行一次稽核；且公司每年度依據內部控制制度自行檢查作業，將總結內部控制實施成效提報董事會覆核確認，並依據評估的結果出具內部控制制度聲明書。

(2)完成年度六次[緊急應變復原計畫]測試演練。

(3)完成網路防火牆汰換更新採購與建置案。

(4)資通安全之經費、資源投入配置情形，每年定期檢討並持續改善相關管理計畫。

(二)列明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。