資通安全管理：

（一）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：

1.資通安全風險管理架構

本公司資訊組人員共計7名，其中資安主管1名及2名資安人員，公司相當注重資訊安全防護作業，從業人員充分瞭解執行業務保密範圍與罰則，對於新進人員亦進行宣導訓練，避免個資及機密文件外洩，影響公司營運及客戶權益，相關資安訊息，資安人員會不定期發送郵件進行宣導。

本公司各單位主管（依公告之組織表為準）及稽核室主管為「資訊安全管理委員會」之當然委員，督導其所屬人員影響資訊安全事件，若有，則以『資訊安全管理查核表』送交資訊組進行必要處置。若有事件發生時資訊組於每個月一日匯總交予稽核室，若情節重大由稽核主管向董事會報告。

2.資通安全政策

(1)公司訂有內部控制制度—資訊循環及機房管理辦法、資訊安全定期檢查控制項目。

(2)確保公司內部資訊無外露之可能性。

(3)確保客戶資訊不虞外露且機密保護。

(4)確保公司資訊系統可正常持續運轉。

(5)宣導最新資訊安全相關防護提供同仁資安防護之重要性。

3.具體管理方案

(1)裝設防火牆，嚴格限制非法入侵、竊取或破壞資料行為。

(2)電腦系統皆安裝防毒軟體，定期以防毒軟體掃毒，以提供員工更安全的作業環境。

(3)定時進行資料備份作業，並將備份資料存放異地，以維護資料的安全。

(4)定期進行系統漏洞修補更新，以維持系統最安全狀態。

(5)建立災難復原作業程序，定期演練系統災害復原。

(6)加強資訊安全觀念，每季進行資安宣導。促使員工瞭解資訊安全的重要性，以提高員工資訊安全意識。

(7)資訊組依『電腦主機現況表』每月排定部門接受資訊安全檢查，以維護資訊安全。

（二）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。