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.資訊安全組織架構：

本公司資訊部門為電腦中心，設置資訊主管一名及專業資訊人員數名，負責訂定資訊安全政策規範、規劃及執行資訊安全技術支援，並定期宣導資訊安全觀念，降低資訊安全風險。

針對風險管理，本公司使用三個面向對應及減少風險的影響程度。

項目	風險管理計畫	風險事件處理	風險對策改善
機制	導入適當控制措施	及時與正確處理	風險持續改善
具體行動	1.防毒、防駭機制。 2.防資料外洩。 3.弱點掃描、偵測與回應備份機制。	1.減少影響範圍，防止擴大。 2.及時還原，恢復運作。	1.依缺失進行檢討。 2.提出改善計畫。 3.納入風險管理。

2.資訊安全政策：

本公司制定之資訊安全政策規範，依下列項目做實際控管：

(1)帳號與密碼原則：制定嚴謹之密碼原則，定期更換密碼，嚴禁密碼交付他人使用。

(2)資訊硬體使用：嚴禁攜帶與使用非公司資產之資訊設備。

(3)資訊軟體使用：嚴禁員工自行安裝任何未經電腦中心安裝或同意之非授權軟體。

(4)檔案管理：個人公務檔案、實體機密文件、與檔案文件資訊之儲存設備，需妥善保管，不得讓人輕易存取。

(5)郵件管理：來歷不明，有質疑性郵件勿開啟並立即刪除。

(6)網路使用：不得冒用、竄改配發 IP，不得私自接續公司網路環境，不得私自架設無線發收設備等擴張使用。

(7)定期發布資安政策、案例與宣導：定期於公司內部網站，或以郵件方式發佈相關資安政策、發生案例、及相關宣導等，員工應隨時注意並配合遵守。

3.具體管理方案及投入資通安全管理之資源：

(1)更新與提升 IT 基礎架構：

①購置新伺服器硬體與軟體，並更新伺服器與用戶端作業系統到最新版本。

②導入弱點掃描系統，減少因漏洞而產生的資安問題。

③網路設備更新，增加備援線路與設備，避免因單一設備或線路損壞而影響公司營運。

(2)強化備份機制：

①購置新款備份方案。

②制定新備份、還原與災難演練 SOP。

③設置主機備援機制，減少災難後停機的時間。

(3)加強員工資安概念：

現在的資安事件不只是外部入侵，越來越多是由內部員工設備感染，進而引發大規模資安事件。

①定期發布資安政策、案例與宣導。

②員工資訊安全教育訓練，不只是在公司，在任何地方都應提高資安意識。