資訊安全風險管理及揭露

- 資訊安全風險管理架構：由資訊部負責統籌資訊安全及相關事宜建立資訊安全管理制度，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。並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。

- 資訊部制定相關資訊安全規範，確認資訊安全管理運作之有效性。
- 為確保公司資訊安全，公司資訊透過網路防火牆,Mail 過濾及防毒軟體等資訊安全相關系統的建置，阻擋病毒及入侵攻擊公司內部網路.另評估各系統的漏洞並針對主機進行漏洞修補，防止病毒與駭客透過系統漏洞，進行攻擊。
- 相關人員錄用應簽署相關保密條約作業規定之文件，以確保新進同仁均了解機密文件之保護之必要性並以提昇資訊安全防護之認知觀念。
- 本公司在和第三方廠商簽訂之服務合約中均要求其遵守本公司的資訊安全規定及保密協定，但並不能保證所有第三方廠商都將履行或嚴守相關規定與協定。
- 本公司並進行資訊安全宣導,讓所有員工了解應依照公司所頒布的相關資訊保護辦法做好自我管理，並具備資安意識。除了資訊系統所提供服務之資訊安全控管措施，更著重保護重要個人及交易資料等資訊之機密性、完整性及可用性。同時強化資訊安全管理，確保資料、系統、設備及網路等軟硬體資訊安全。
- 同仁遇有資訊安全事件，應立即通報資訊部門，避免事件擴大，並配合權責部門共同解決。
- 嚴禁同仁私自架設網路設備串接外部網路與公司內部網路，內外部網路均設置防火牆、非武裝區（DMZ）、及必要之安全設施保護之，重要設備應建置適當之備援或監控機制，維持其可用性。
- 同仁之個人電腦及主機應安裝防毒軟體且定期確認病毒碼之更新，並禁止使用未經授權軟體。
- 同仁個人持有之帳號、密碼與權限應善盡保管與使用責任、管理人員應定期清查覆核，重要系統運作資料應定期備份並執行回復測試。

- 同仁日常作業應落實確認覆核機制，維持資料準確性，主管人員應督導資訊安全遵行制度落實情況，強化同仁資訊安全認知及法令觀念。

- 當同仁新進、調整職務及離（停）職時，應以帳號申請單進行申請簽核再由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。

- 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。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。

- 軟體系統之開發建置、維護、更新、上線執行及版本異動作業，由資訊人員執行或者在安全管制下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。程式和系統權限修改需填寫資訊需求申請單，經主管同意後由資訊人員執行，並填寫測試報告確認無誤後由資訊主管放行後上線。

- 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，基於實際作業需要核發短期或臨時性之系統密碼供廠商使用或者在資訊人員授權及監控下進行並於使用完畢後立即取消其使用權限。