資通安全管理規定	版　　本	V1.0
	文件編號	

一、 目的

為確保公司網路和資訊使用環境安全、穩定，通過制定本規定並推行落實，達到建立公司資通安全管理環境目標，避免員工因疏忽或無知導致影響企業的正常運作。

二、 內容範圍

本規定資通安全內容包括以下幾個方面：網路安全、電腦安全、應用系統管理、人員安全、委外等類別。公司資安保護目標的實際作業遵循基本要求再進階強化，並據以評估實效，按需進行修正改善。

三、 網路安全

1、 本部分包括網路資源管理、防火牆與特殊連線安全控制以及無線上網等。公司通過強化內部網路基礎建設及網路服務的相應保護措施，提升網路資料傳輸安全，降低風險，減少遭受網路攻擊的傷害。

2、 網路資源管理

2.1 關閉網路設備不使用的服務與功能，降低安全的風險。

2.2 評估建立網路監控系統的必要性，及時瞭解網路運作情況，及早發現網路失效的情形或潛在風險。

3、網路安全管理

3.1 依實際情況，設置適當的防火牆（Firewall ）於公司的內部網路與外部網際網路接界處，防止外部未經授權進入公司內部網路。

3.2 依業務需求，進行防火牆規則的適當設定；防火牆規則的設定須經過部門主管核准。

3.3 定期就防火牆規則進行檢視。

3.4 在資訊系統委外廠商必須以遠端登入方式進行系統維修的情況下，只在需要時才可啟動遠端登入連線，並採取管制或監控措施。

3.5 不定期委由外界專家或自行評估網路系統安全並進行安全修補，提高安全防禦能力。

3.6 針對開發外界連線的資訊系統，依照資料及系統的重要性，採取資訊加密、身份識別、電子簽章（若可行）等不同安全等級的技術或措施，降低資訊及系統受到入侵、破壞、篡改、刪除及未經授權存取的安全風險。

4、無線網路安全

4.1 無線網路架設與使用須經過審慎的安全評估。

4.2 無線網路卡與無線基地台（Access Point ）間使用加密通訊協定。

四、 電腦安全

1、本部分包含各式電腦(含伺服器及個人電腦、筆記型電腦等)系統與設備的保護、防毒軟體、存取安全、帳號密碼管理等，主要針對電腦系統進行安全保護措施，提高系統運作穩定性與持續可用能力，降低被攻擊的風險。

2、電腦系統與實體設備保護

2.1 公司所使用的各式電腦（含伺服器、個人電腦、筆記型電腦等）的系統應及時進行安全修補。

2.2 公司所使用的各式電腦軟體及版權，集中由資訊單位管理。

2.3 任何電腦均應設定螢幕保護裝置程式並設定密碼保護，防止他人未經過授權使用電腦。

2.4 使用任何電腦設備時，必須注意其電源使用不可超過電源負載量。

2.5 廠商維護電腦主機設備時應有公司資訊單位人員陪同。

2.6 公司的任何電腦設備發生故障，資訊單位應酌情考量記錄，以供未來分析查考。

3、防毒軟體

3.1 所有電腦系統（伺服器、個人電腦、筆記型電腦等）均應安裝防毒軟體，實施並自動更新病毒庫。

3.2 所有電腦系統實施自動定期病毒掃描。

4、存取安全

4.1 每位元電腦系統使用者（包含系統管理者），應賦予獨立的通行帳號；帳號應業務需求，賦予使用者最低能滿足作業的許可權。

4.2 當發生職員離職或調動的情況，需立即取消或調整其帳號許可權。

4.3 定期審查帳號及使用權限情況，確保符合現狀。

5、密碼安全管理

5.1 所有通行帳號的登錄 LOG IN 應設立獨立密碼，密碼設定避免使用容易猜測的字串（例如生日、地名或密碼與帳號相同）。

5.2 輸入密碼時，電腦螢幕不得明白顯示所輸入的密碼。

5.3 保存密碼的檔案應予以加密。

5.4 設定強制使用者定期更新密碼的要求，更新密碼週期視公司情況而定，原則上不宜超過 6 個月。

5.5 設定使用者密碼輸入錯誤達 3 次後，系統自動將帳號暫時鎖定。

5.6 在帳號第一次啟用後，強制使用者更新密碼，預設密碼設定的有效期限（視系統而定）。

5.7 制定並強制使用密碼內容至少包含：

- 密碼長度至少 6 個字元；
- 密碼同時包含英文字母與數字；

五、 應用系統管理

1、本部分包含電子郵件、及時通訊軟體、資料備份、異常事件處理常式等，主要針對公司日常運作的應用系統使用安全，降低不當操作所造成的傷害，提升在事件發生時的應變與處理能力。

2、電子郵件使用安全

2.1 明確規定員工禁止利用公司電子郵件從事工作業務以外的活動，並宣導員工不開啟來路不明的電子郵件。

2.2 以業務及個人工作需要，對員工電子郵件內容及大小進行規範和限制（以公司實際情況而定）。

2.3 開啟郵件過濾及防毒機制，以過濾垃圾及可能含有病毒的郵件。

3、即時通訊軟體使用安全

3.1 安裝與使用即時通訊軟體（如 MSN、SKYPE）等，必須按業務實際需要進行審慎評估。

3.2 安裝與使用即時通訊軟體，需採取適當的安全控管措施。

4、資料安全與備份

4.1 不定期進行備份資料復原測試，以確保備份資料的有效性。

4.2 任何資料存儲媒體（硬碟、磁片、光碟等）進行報廢時，須徹底將其內資料銷毀，直至無法解讀。

4.3 應用系統的重要資料至少維持 2 套以上的備份。

4.4 實體的機密資料，如紙張檔、重要合約等，宜妥善存放與保管。

5、異常事件處理常式及災害複原計劃

5.1 公司需依實際情況，針對常見的資安事件與異常情況，擬定異常事件處理常式，以增加處理實效，並降低異常事件發生的傷害。

5.2 按企業持續經營的原則，評估並理清重大業務衝擊威脅事件，據以制定災害複原計劃。

六、 人員安全

1、本部分人員安全包含人員安全管理、認知教育與事件通報等，其主要目的為提升企業內部人員的安全意識以及對資安危機的瞭解，將有助於降低因安全意識不足所造成資安事件發生的機會。

2、人員安全管理

2.1 對公司的資訊單位人員的職責進行明確定義。

2.2 公司負責資訊安全相關工作或處理機密資訊的人員，需簽署保密協定。

2.3 各種資訊安全工作，需有 2 人及以上瞭解，以應付緊急情況的需要。

3、安全認知訓練

3.1 資訊安全事件應立即公告公司員工（如最新電腦病毒威脅）

3.2 定期提供員工適當的資通安全認知或教育訓練（依實際情況而定）

3.3 以實際情況，酌情考量將資通安全要求納入員工手冊中。

七、 委外

1、委外的管理需充分注意並儘量降低因委外所造成的資安問題發生的機會。

2、委外管理

2.1 資訊委外（如電腦設備維護、系統開發等）應與委外廠商簽訂契約，並將保密條款納入其中。

2.2 電腦系統資訊委外業務完成後，應要求委外廠商提供詳細的系統檔及手冊。

2.3 委外廠商人員如有派駐公司情況，派駐的委外人員的電腦系統使用權限應予以適當控管。

八、 法令遵循

1、公司應遵循台灣電腦資訊、資訊系統等相關法律法規，避免在資料處理上發生違法的事情。

2、公司對外網站上不得公佈機密檔、敏感性及未經當事人同意的設計個人隱私資料的檔。

3、應確實遵守政府、主管機關等相關資訊安全法令法規。

九、 附則

1、本管理規定由總經理批准後予以施行，一切解釋權歸本公司所有。

2、本管理規定宣導工作由資訊單位負責，視具體情況不定期組織公司各有關部門進行宣導。