資通安全檢查管理辦法

第一條：目的

確保公司資料安全與正確及完整性等事宜並強化資通安全防護及管理機制，特訂定本辦法。

第二條：範圍

本辦法適用於公司有關資訊系統安全相關事項之辦理。

第三條: 辦法制度、修改與廢止

本辦法之制定修改與廢止須經呈董事長核決後實施。

第四條: 作業內容

4.1 公司內部應有專業人員負責處理有關資訊系統安全預防及危機處理相關事宜，以防範電腦網路犯罪與危機，維護資訊系統安全。

4.2 應建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取，造成機密資料之外洩。

4.3 對於跨公司之電腦網路系統，應特別加強網路安全管理，並且對內安裝防毒軟體，設置對外之網路防火牆，以防止電腦病毒、攻擊性之惡意軟體入侵，而造成公司網路系統癱瘓，並定以下作業規範：

1. 網銀密碼與金鑰需分開保管。
2. 員工不得使用未經授權及違法下載、拷貝受著作權法保護之著作之電腦程式。
3. 員工不得無故將帳號借予他人使用，帳號應定期更換密碼。
4. 員工不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。
5. 員工應全面使用防毒軟體並即時更新病毒碼。
6. 每日檢查防火牆 log 檔及流量，是否有異常事項發生。
7. 防火牆之安全控管設定應經常檢討，並作必要之調整，以確定發揮應有的安全控管目標。
8. 機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。

4.4 應教育員工正確使用合法軟體之概念，促使員工正確認知電腦病毒的威脅，進一步提昇員工的資訊安全警覺。

4.5 網路申報系統的最高使用權限，應經權責主管人員審慎評估後，交付可信賴的人員管理，防止非相關人員存取系統資訊。

4.6 最高使用權限人員，應依各業務範圍、權責分別設定使用者之帳號及權限，並且不得私自更換使用，使用者一旦離開原職務，應立即撤銷該使用者之權限。

4.7 使用者之帳號及密碼，應避免使用容易被識破及猜測的密碼，並且應定期更改密碼。

4.8 網路系統管理人員應負責網路安全規範的擬訂，執行網路管理工具之設定與操作，確保系統與資料的安全性與完整性。

4.9 個人電腦及網路系統伺服器，應具備電腦病毒掃瞄工具及入侵偵測與防禦機制，並且定期掃瞄電腦病毒與更新病毒碼。

4.10 個人電腦及網路系統之資料，應每日定期備份重要檔案及資料，以備不時之需。

4.11 申報之資料應儲存於電腦內，並於異地之NAS做儲存備份，同時為便於管理方便，資料應以日期、檔案、部門別分類儲存。

4.12 處理廢棄電腦時，必須徹底確認電腦內的敏感或機密性資料是否有被適當地移除或銷毀。因為不當的資訊揭露可能造成組織的營運危機，包括金錢、信譽等損失，以及犯罪事件，甚至是觸犯法律等結果。為預防這類事件的發生，在電腦或其他資訊設備報廢的過程中，採取以下步驟：

1. 電腦報廢前，針對整個電腦系統或硬碟內含資訊的進行備份。
2. 將上述的備份移轉至新的機器或其他備份裝置中。
3. 執行完整的資訊設備報廢處理程序，包括針對電腦硬碟執行重新格式化、移除相關作業軟體、資料及具有版權之系統軟體；針對磁碟或光碟片等儲存媒體進行實體銷毀，如切碎、折損等。

4.13 保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

4.14 針對可能造成營運中斷事件之發生，須建立完整之備份計畫並制定系統復原辦法，若遭遇偶發事件時，則依照系統復原辦法辦理。於每年五月進行復原測試，並將其結果做成紀錄。

4.15 個人電腦有使用郵件時，針對其外寄之郵件須建立審核機制，機密等級檔案與個資數量超標的往來郵件， 必須經過主管或代理人同意後，才可寄送或加密寄送。