天剛資訊股份有限公司
資通安全檢查辦法

一、目的：

為落實本公司資訊安全政策，強化並提昇本公司資訊作業之安全水準，特制定此辦法。

二、資訊安全定義：

所謂資訊安全係採行與資訊資產價值相稱及具成本效益之管理、作業及技術等安全防護手段、措施或機制，以確實掌握本公司各項資訊資產免遭不當使用、洩漏、竄改、竊取、破壞等情事，倘不幸遭受惡意攻擊、破壞或不當使用等緊急事故發生時，亦能迅速作必要之應變處置，並在最短時間內回復正常運作，以降低事故可能影響及危害本公司業務運作之損害程度。

三、資訊安全目標：

建立安全及可信賴之電腦化作業環境，確保本公司電腦資料、系統、設備及網路安全，以保障本公司業務永續運作。

四、資訊安全範疇：

包括本公司資訊安全及政策、建立資訊安全組織、人員安全與管理、資產分類與控管、實體及環境安全管理、通訊與操作管理、存取控制、系統開發與維護、永續經營管理、內部稽查及其他等十大工作項目。

五、資訊安全管理作業規定：

（一）資訊安全政策

1.管理階層應瞭解資訊安全目的並予支持。

2.應訂定資訊安全政策的的說明文件及資料（如作業程序、資訊安全控管文件、使用者應遵守的安全規則）。

3.資訊安全政策應定期評估。

4.定期對單位人員及資訊設備進行安全評估，確定其遵守資訊安全政策及相關規定。

5.於委外契約中有關安全需求內容應包含法律需求（如電腦處理個人資料法保護法）、界定雙方有關人員權責、使用何種實體與邏輯安全控管措施、對委外廠商稽核權、得依實際需要隨時修改安全控管措施及作業程序等。

（二）建立資訊安全組織

1.指定高級主管人員負責推動、協調及監督資訊安全管理事項。

2.指定單位辦理風險評估、安全分級、系統安全控管措施。

3.單位內若開放給外單位作資料存取，應訂定控管程序。

（三）人員安全與管理

1.依員工職務層級進行適當的資訊安全講習。

2.對員工的私人資訊設備作必要之安全控管程序。

（四）資產分類及控制

1.資產清冊應隨時更新。

2.公司應建置資訊安全等級分類標準(如資訊分級，區分機密性、敏感性及一般性)。

（五）實體及環境安全管理

1.公司對攜帶型的資訊財產應訂有安全之攜出管理規則及嚴謹的保護措施(如設通行碼、檔案加密、專人看管)並落實執行。

（六）通訊與操作管理

1.公司應與業者簽訂適當的資訊安全協定，賦與相關的安全管理責任，並納入契約條款。

2.公司應使用網路防火牆(Fire Wall)並定期檢討電腦網路安全控管事項之執行。

3.公司對於敏感性資訊之傳送應採取資料加密等保護措施。

4.公司對於輸出及輸入機密性、敏感性資料應有處理程序及標示。

（七）存取控制

1.公司應依網路型態訂定適當的存取權限管理方式。

2.公司應規範於不使用時用上鎖或密碼等管制措施以不讓電腦或終端機遭非法使用。

3.公司資訊及應用系統應設有作業結束後或在一定期間未操作時即自動登出或中斷連線之保護機制，若需再登入需重新取得授權。

4.公司應依環境或業務需要於網路防火牆作適當之設定。

5.公司應管制使用者的連線功能（如網路通訊閘道所設定的規則），並針對電子郵件、單雙向檔案傳輸、互動式存取與存取時段做通盤連線控管考量。

6.公司應指定專人管理應用程式原始碼、資料庫及執行檔。

7.公司的機密及敏感性資料的處理應於獨立或專屬的電腦作業環境中執行。

（八）系統開發與維護

1.定期對使用軟體實施病毒偵測。

（九）永續經營管理

1.辨識關鍵性業務及執行其風險評估、衝擊影響、優先順序。

2.定期作風險估並調整永續經營政策。

（十）內部稽查及其他

1.單位應使用合法軟體。

2.軟體之使用及資料之儲存、處理和報廢，應有適當之控制。

六、組織職掌及分工：

以常態任務編組方式設「資訊安全處理小組」，辦理本公司資訊安全預防及危機處理相關事項。惟為因應緊急突發安全事故或辦理安全政策評估修正時，除向上級單位要求技術或人力支援外，得另委請專家學者或民間專業組織及團體，提供資訊安全顧問諮詢服務。

（一）由資訊管理處經理擔任「資訊安全處理小組」召集人，負責推動、協調及督導下列資訊安全管理事項：

1.資訊安全責任之分配及協調。

2.資訊資產保護事項之監督。

3.資訊安全事件之檢討及監督。

4.其他資訊安全事項之核定。

（二）由資訊管理處人員負責資料及資訊系統之安全需求研議、使用管理及保護等事項，同時指派稽核室一人擔任資訊安全稽核員，並依其專長任務分組，定期辦理本公司資訊安全稽核事項。

七、資訊安全事故處理程序：

（一）依據資通安全等級判斷事故等級依影響業務運作程度區分為下列三級：

1.『A』級：電腦系統完全停頓，業務無法運作者。

2.『B』級：業務中斷，影響系統效率者。

3.『C』級：業務短暫停頓，可立即修復者。

（二）本公司所有同仁均負資訊安全事故通報之責任，狀況發生時先通知資訊室同仁，經判斷確為資訊安全事故，可即時因應或處理者，則先予處置；倘個人能力無法處理則通報資訊室會診處理，安

（三）資訊安全緊急處理作業程序應定期演練及測試。

八、評估與修正：

本辦法訂於每年十二月由「資訊安全處理小組」召開資訊安全顧問會議，以獨立公正客觀原則，辦理本公司資訊作業安全事項重行評估與修正事宜，以反映相關法令、資訊技術及本公司業務發展現況，俾使本辦法確實符合安全需求。

九、訓練與宣導：

本辦法公佈於本公司內部網站內供同仁上網查閱，新進人員則於報到時由資訊室同仁負責相關訓練與宣導課程，或自行上網研習網路教學相關課程。

十、實施：

本辦法自總經理核可後生效實施，並於本公司網站公告週知，修正時亦同。