宜特科技股份有限公司
資通安全檢查管理辦法

1. 目的 Purpose：

為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

2. 範圍 Scope：

本政策之範圍如下，有關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效：

2.1 人員管理及資訊安全教育訓練。
2.2 電腦系統安全管理。
2.3 網路安全管理。
2.4 系統存取控制。
2.5 系統發展及維護安全管理。
2.6 資訊資產安全管理。
2.7 實體及環境安全管理。
2.8 業務永續運作計畫之規劃與管理。

3. 名詞定義 Definition：

3.1 資訊資產：
3.1.1 係指為維持本公司資訊業務正常運作之硬體、軟體、服務、文件及人員。
3.1.2 保護對象不僅限於本公司自有，亦包含自顧客端取得，及將提供予顧客者。
3.2 業務持續運作之資訊環境：
3.2.1 係指為維持本公司各項業務正常運作所需之電腦作業環境。

4. 權責 Responsibility：

4.1 此政策規範由最高管理階層擬定，藉有效的系統運作，包含各流程持續改善，以預防不符合事項，以達到資訊安全之目的。
4.2 為統一資訊安全管理等事項之協調、規劃、稽核及推動，由本公司資訊處擔任負責幕僚作業。
4.3 依下列分項原則，配賦適當之人員其權責：
4.3.1 資訊安全政策、計畫及技術規範之研議、建置及評估等事項。
4.3.2 資料及資訊系統之安全需求研議、管理及保護等事項。
4.3.3 資訊機密維護及安全稽核等事項。
4.4 全員應負之相關責任：
4.4.1 資訊安全管理者透過適當的標準和程序以實施此政策。
4.4.2 所有人員和委外服務廠商均須依照相關安全管理程序以維護資訊安全政策。
4.4.3 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
4.4.4 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司.之相關規定進行懲處。

5. 作業內容 Procedure：

5.1 人員管理及資訊安全教育訓練

5.1.1 對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。各業務主管人員，應負責督導所屬員工之資訊作業安全，防範不法及不當行為。

5.1.2 針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升資訊安全水準。

5.2 電腦系統安全管理

5.2.1 辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定 期考核。

5.2.2 依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。

5.2.3 採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

5.2.4 對各種系統變更作業，應建立控管制度，並建立紀錄，以備查考。

5.2.5 採購資訊軟硬體設施，應依公司標準或權責主管訂定之政府資訊安全規範，研提資訊安全需求，並列入採購規格。

5.3 網路安全管理

5.3.1 開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵 測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

5.3.2 與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。

5.3.3 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未同意之個人隱私資料及文件，不得上網公布。

5.3.4 訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。

5.3.5 為避免網路使用者不慎違反本公司相關網路安全規定，網路管理人員可考慮以相關網路技術以不干擾正常網路使用為原則下， 主動管制違反本公司相關網路規定之使用者。

5.4 系統存取控制

5.4.1 訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。

5.4.2 離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取 授權規定，限期調整其權限。

5.4.3 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過六個月為原則。

5.4.4 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

5.4.5 建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

5.5 系統發展及維護安全管理

5.5.1 自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本 異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

5.5.2 對廠商之軟硬體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，並嚴禁核發長期性之系統辨識碼及通行密碼。如基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

5.5.3 委託廠商建置及維護重要之軟硬體設施，應在本公司相關人員監督及陪同下始得為之。

5.6 資訊資產安全管理

5.6.1 建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等。

5.6.2 依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施。

5.6.3 已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

5.7 實體及環境安全管理

5.7.1 就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。

5.8 業務永續運作計畫之規劃與管理

5.8.1 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定 期演練及調整更新計畫。

5.8.2 建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

5.8.3 當發生資訊安全事件，若有損及顧客權益疑慮時，經資訊安全主管裁決，透過業務單位人員通報相關內容。

5.8.4 依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及充足之資訊安全措施。