黑松股份有限公司 資訊系統安全實施管理要點

規章編號：C-0083-AD
109 年 12 月 28 日起適用

第 一 條：目的

為維護本公司整體資訊系統安全，強化人員、設備、系統、資訊、資料及網路等資訊資產之安全管理，免於因外在威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，特訂定資訊系統安全實施管理要點，以供相關人員共同遵循。

第 二 條：適用範圍

一、適用於本公司各項資訊資產及資訊使用者。

二、資訊使用者包含正式員工、聘僱人員、建置維護廠商及其他經授權使用資訊資產之人員。

第 三 條：法令要求

一、資訊使用者應確實遵守個人資料保護法、著作權法等法規要求，如有違反者，依相關法令辦理。

二、本公司另訂有「個人資料檔案安全維護計畫實施要點」及「營業秘密管理辦法」，同仁使用資料時應遵循相關規定。

第 四 條：組織

一、資訊系統安全管理計劃及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。

二、資訊機密維護及使用稽核管理事項，由稽核室執行。

三、資料及資訊系統之使用管理及保護等事項，由使用單位負責辦理。

第 五 條：資產管理

一、電腦硬體驗收後資產歸屬各使用部門，各使用部門負責該項資產保管責任。

二、資訊單位應依設備異動狀況，適時更新電腦設備管理清冊，並列表存查。

三、資訊單位針對資訊設備應設置適當之防護，以避免遭受損壞以致影響業務之持續運作。

四、針對行動裝置採用安全措施，以管理使用行動裝置所導致之風險。

五、資訊單位為全公司軟體管理部門，軟體版權正本皆統一存放於總公司。

六、所有機台皆有軟體授權控管，並宣導員工合法使用軟體。

七、資訊單位應定期清查電腦安裝之軟體，以確保遵循智慧財產權之規定。

八、每年與廠商簽署軟/硬體維護合約，並明訂備機/備援條款，以確保使用故障時可快速恢復正常。

九、員工應簽署「員工使用電腦約定書」，依規範使用電腦軟硬體資源。

十、個人存放於主機上之檔案應定期檢視是否需要留存，並定期清理刪除；資訊設備移交或汰換時應確認已刪除非關業務需要之檔案及相關授權軟體。

十一、委外處理的電腦設備、媒體蒐集及委外處理資料，應慎選具有足夠安全管理能力及經驗的機構作為委辦對象。

第 六 條：人員安全

一、資訊單位應以書面、電子或其他方式正式發布且告知所有同仁，並向員工與

協力廠商宣導遵守資訊系統安全管理要求，以提高人員對資訊系統安全之認知。

三、辦理各項資訊業務作業，應事先將資訊系統安全納入評估，並對廠商進行審慎評核，明訂廠商之資訊系統安全責任及保密規定，並列入合約要求廠商遵守。

第 七 條：設備安全

一、電腦機房門禁鑰匙應由機房管理者保管，機房門亦維持常鎖門禁。

二、進入機房須脫鞋，並禁止攜帶飲食進入。

三、人員須經權責主管同意後始得進出機房。

四、為防瞬間斷電造成系統毀損或資料遺失，電腦機房配置有不斷電系統，因應斷電時有足夠時間進行存檔與正常的關機程序。

五、伺服器、核心網路設備等應設置於具有門禁管理、空調、電源供應穩定、防火等安全區域內，以避免非法存取或破壞行為。

六、各種作業系統環境配置、資料庫管理、資訊資源控管、換版作業管理及系統結構變更管理等，應依系統特性建立相關之控管流程。

七、為確保資訊系統或設備正常運作，應建立電腦病毒、挖礦等其他惡意程式預防及控制措施。

八、應取得資訊系統或設備供應商已公布之技術脆弱性資訊，定期執行伺服器弱點掃瞄，評估應採取的適當管控措施，以處理所面臨之風險。

九、公司訂有「電腦使用政策說明書」、「員工使用電腦約定書」，明訂軟硬體及網路等使用權責規範。

十、初次申請登錄公司網路帳號者，應簽署「員工使用電腦約定書」，在帳戶啟用時設定密碼，並妥善保管密碼不得外洩。

十一、員工負有保護登錄公司網路帳號密碼之責任，確保登錄帳號之機密性。

十二、人員到/調/停/離職前，皆須填寫「電腦使用申請交接單」變更各項資訊資源使用權限，以維護公司網路資源的安全。

第 八 條：網路安全

一、網路架構規劃或調整時，應對是否滿足營運需求及資訊系統安全進行考量。

二、因業務或營運需要新增之設備，須遵照各網段使用之用途設計，未經授權不可任意交叉混用或串接。重要網段應施予適當防護及監控機制，例如：安裝防火牆或入侵偵測系統，定期檢視稽核紀錄等，且稽核紀錄不得被新增、刪除、修改。

三、應建立防火牆及其他必要安全設施，加強網路安全管理，以確保網路傳輸資料與資源存取之安全性。

四、防火牆設有網路安全稽核規則，阻擋不當之網路存取及駭客攻擊行為。

五、所有人員不得私自串接外部網路與內部網路，並應設置必要之安全設施以保護內外部網路。

六、與外點營運單位進行連線時，皆經由防火牆管控，並予以加密保護，確保人員登錄及資料傳輸之安全。

七、使用者或廠商以遠端登錄方式進入內部網路，應加強控管，採取特別的安全

控管機制，如使用帳號密碼或其它認證機制。

八、禁止收發不當電子郵件，包括內含風險或危害網路安全之信件、公司機密文件、垃圾郵件等。

第 九 條：應用系統安全

一、應用系統程式原始碼應進行適當管理。

二、對委外廠商應規範及限制可接觸之應用系統與資料範圍。

三、開發或維護應用系統、新購應用軟體於正式上線前，須經妥善之測試。系統開發及測試不可使用真實資料，如果測試作業必須使用真實資料，應評估控制措施來保護資料的機密性。

四、電子商務服務應依主管機關規定，應用系統開發人員應考量交易之特性及需求後，採取相關防護措施。

五、應用系統應有專人負責維護工作，並設立代理人。

六、應用系統軟體之變更，應由使用部門填具「電腦作業變更申請單」經權責主管核准，並依程式開發及設計程序辦理。

七、委外軟體之開發及導入，應有控制程序以確保其品質。

八、系統測試時所發生之問題應做成紀錄並保存之。

九、使用應用系統應依使用人提出申請做為授權之依據，僅提供予使用者存取其已被特定授權使用之網路、系統及服務之存取，並防止未經授權之存取。

十、人員到/調/停/離職前，應填寫「電腦使用申請交接單」變更各項資訊資源使用權限。

十一、為加強應用系統控管，除受限於系統特性外，任何使用者帳號均需輸入密碼，以進行使用者身分識別與鑑別之作業。

十二、應建立通行密碼管理，如密碼原則及變更週期。

十三、爲確保對存取資料和資訊服務進行有效控制，應定期進行授權帳號權限之審視作業。

第 十 條：災害復原管理

一、公司主機資料皆定期執行必要的資料、軟體備份及備援演練作業，並將備份媒體異地存放保管，以於發生災害或是儲存媒體失效時，可迅速回復正常作業。

二、因公務需要須回復歷史資料或檔案之使用者，申請單位應填具「檔案複製移轉或回存單」，由備份伺服器管理者協助執行還原作業。

三、應訂定資訊系統災害復原計畫，評估各種人為及天然災害對正常業務運作之影響，並定期演練及調整更新計畫。

四、應建立資訊系統安全事件緊急處理機制，在發生資訊系統安全事件時，立即依其處理程序進行通報與處理。

第十一條：本要點內容經總經理核定後公布施行，修正時亦同。