欣巴巴事業股份有限公司

113 年資通安全管理執行情形報告

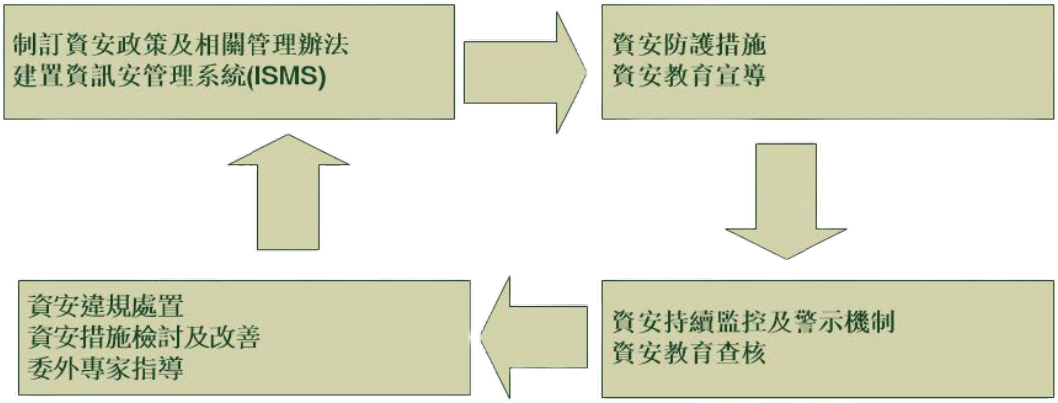
一、資訊安全架構

(一)資訊安全組織架構

本公司依規定設有資計安全專責主管及資訊安全專責人員，統籌資訊安全相關政策制定，並定期與相關單位主管人員討論推動機制及工作重點。

(二)企業資訊安全風險管理政策架構

為有效落實資訊安全管理，以資訊安全管理系統(ISMS)準則，進行循環式品質管理(PDCA)持續改善流程架構。



二、資訊安全政策

為強化資訊安全，依資訊安全管理系統(ISMS)區分四大面向

1. 規範辦法：依內控作業循環及相關辦法之電腦化資訊作業，增訂資訊安全政策，強化資訊作業。
2. 硬體建置：建置完善資訊安全設備，落實資訊安全管理。
3. 人員教育：定期及遇有重大資訊安全事件進行知會，以提昇全體同仁資訊安全意識。
4. 政策檢討：推動資訊安全持續改善，確保企業永續經營。

以上述四大面向進行執行政策：

1. 資訊安全政策訂定與評估。
2. 資訊安全組織建立及運作。
3. 資訊安全小組定期分享及研議資訊安全議題。
4. 資訊分類、分級，定期盤點及檢視運作效能。
5. 人員安全管理及教育訓練。
6. 權限存取控制安全及查核。
7. 定期宣導教育使用者資訊安全知識，推廣使用者對資訊安全認知提升。
8. 軟體定期升級修補資訊漏洞。

9. 評估硬體設備運行效能，並制定更新計畫。

10. 加強備份機制，檢測備份完整性及備份存取安全。

三、資訊安全管理方案

管理項目	說明	具體作業
權限管理作業	帳號、系統權限管制措施	●帳號申請、異動、刪除管理。 ●權限分級控管、盤點與查核。 ●不同職務別的網路存取控制。
資料管理作業	人員存取系統及資料之管理與控制措施	●資料及系統之存取權限控管。 ●存取使用軌跡之紀錄。 ●文件加密系統的佈署。
外部威脅管理	檢視所有可登入的管道，進行封阻及建置相關預防措施	●建置防火牆設備及主動式端點滲透攻擊偵測系統，防堵入侵伺機器主機及使用者電腦，有效阻絕目前各式各樣的網路攻擊，強化駭客入侵預防。 ●垃圾郵件篩選及隔離機制，以防止收到夾帶病毒之電子郵件。 ●伺服器與使用者電腦皆安裝防毒軟體，定期掃毒，防範病毒攻擊。 ●伺服器、使用者電腦定期漏洞更新。
系統穩定管理	建立相關預防措施，減少因系統中斷所造成的損失	●系統及網路可用狀態監控與通報機制。 ●系統中斷之應變措施。 ●系統復原管理措施。
備份機制建立	備份作業建立及審查備份完整性	●定期檢視備份效率及備份完成度。 ●備份空間檢討，估算備份資料使用容量。 ●備份目的多樣性檢討，調整排程作業。 ●定期進行系統復原測試，達成如遇災難時可快速回復運行。
教育訓練機制	內部訓練及外部交流	●每月定期分享或宣導資訊安全潛在風險。 ●針對資訊安全發生因應流程作業。 ●外部加入資訊安全相關組織共享資訊。 ●參與技術研討會議評估改善流程或設備升級。

四、資安管理資源及執行情形

公司定期審視內部資訊安全規範執行資訊安全作業，提升整體資訊安全及提供可信賴的資訊安全環境，確保資訊系統之機密性、完整性及可用性。

具體執行作業項目如下表：

項目	113 年執行情況
資安宣導	定期於每月例會進行各種資安全議題宣導
查核作業	每季進行抽查離職人員權限查核 每季查核軟體授權作業 每半盤點年硬體資訊設備 每年查核軟、硬體及人員整體 每年會計師進行資訊作業項目審查
備份演練	每年進行資訊安全發生災難時，針對 ERP 系統還原演練，並檢測備份作業完整性
聯防組織	加入資安聯盟會員(TWCERT)
設備升級	防火牆版本升級 ERP 系統升級，包含作業系統及資料庫系統
硬體監控	GGS3.0 系統監測伺服器硬體底層連線
資訊會議	每月內部資安會議
研討會議	參加中華電信主辦：南部資安防治應用研討會 參加晉泰科技主辦：高雄區資訊安全防護系統說明會

五、資安事件

資安指標	資安客訴事件	外部破壞、竊取資料或病毒威脅事件	資訊系統異常或設備異常影響營運事件
113 年事件統計(件)	0	0	0