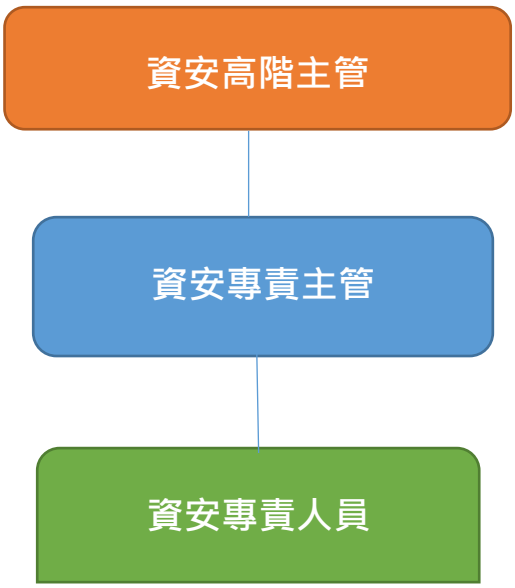
漢唐集成股份有限公司

資訊安全管理辦法

壹、資訊安全風險管理架構



本公司由管理高層主導，成立資訊安全中心為資安專責單位，任命資訊室主管為資安專責主管，並指派一名資安專責人員，進行資訊安全制度之規劃、監控及執行資訊安全管理作業。

貳、資訊安全政策

一、目的：

為遵循資訊安全相關法令，增進本公司資安作業安全及穩定之運作，確保資訊資產之機密性、完整性及可用性，並順利推展本公司各項業務，以符合客戶資訊安全需求，特制定此資訊安全政策做為本公司資安管理最高指導原則與方針。

二、範圍：

本政策適用於總公司、海外分公司、駐外辦公室、及使用或連結本公司資訊環境、接觸業務資訊或提供服務之廠商及第三方人員。

三、目標：

I. 確保公司業務相關資訊之機密性，保障本公司業務機密與個人資料。
II. 確保本公司業務相關資訊之完整性及可用性，提高工作效能與品質。
III. 提昇本公司資訊安全防護能力。
IV. 達成客戶要求之資安標準。

參、資訊安全管理作業

一、目的：

為維護公司資訊系統安全及強化資訊安全防護機制，訂定相關規範，作為公司資安政策執行之依據。

二、管理辦法：

◆ **系統存取控制管理**

i. 視作業系統及安全管理需求訂定個人密碼核發及變更程序並作成記錄。
ii. 登入各作業系統時，依各級人員執行任務所必要之系統存取權限，由資訊室系統管理人員設定賦予權限之帳號與密碼，並定期更新。
iii. 經遭破解之個人密碼，立即將帳號進行封鎖，並要求使用者設立與前次不同之密碼，才可繼續使用。

◆ **網路安全管理**

i. 與外界網路連接之網點，設立防火牆控管外界與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。
ii. 機密性及敏感性的資料或文件，不存放在對外開放的資料系統中，機密性文件不以電子郵件傳送。
iii. 對內部網路資料夾進行控管，非內部電腦之網卡序號，無法存取內部雲端硬碟之資料。
iv. 對部門 IP 進行控管，非相關部門 IP，無法存取該部門機密資料。
v. 對電子郵件嚴格控管，寄出之郵件均經過郵件主機掃毒，且確保郵件無法夾帶病毒檔。

vi. 將機密性高之文件存放於『文件管理系統』統一控管，並對文件進行加密、浮水印、可存取人員、存取次數...等等嚴格加密。

◆ **資訊安全作業與保護**

i. 建立處理資訊安全事件之作業程序，並賦予相關人員必要的責任，以便迅速有效處理資訊安全事件。
ii. 建立資訊設施及系統的變更管理通報機制，以免造成系統安全上的漏洞。
iii. 依據個人資料保護法之相關規定，審慎處理及保護個人資訊。
iv. 建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以便發生災害或儲存媒體失效時，可迅速回復正常作業。
v. 嚴格控管同仁電腦是否已安裝公司防毒軟體、使用軟體是否為正版。
vi. 定期對同仁進行宣導釣魚郵件之特性與可能危害，落實資訊安全防護工作，建立相關業務之資訊安全的責任、觀念與行為規範。

◆ **資訊安全權責與教育訓練**

i. 對處理敏感性、機密性資料之人員及因工作需要須賦予系統管理權限之人員，妥適分工，分散權責並建立評估及考核制度，及視需要建立人員相互支援制度。
ii. 對離(休、停)職人員，依據人員離(休、停)職之處理程序辦理，並立即取消使用各項系統資源所有權限。
iii. 依角色及職能為基礎，針對不同層級人員，視實際需要辦理資訊安全教育訓練及宣導，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。
iv. 不定期以郵件宣導公司同仁，宣導使用者設定及操作作業系統之安全機制，目前可能流行的網路病毒、木馬、後門、蠕蟲等，及常見釣魚手段，增加使用者防護知識，以防止同仁被騙取密碼造成公司損害。
v. 非資訊處理人員，機房未經核准不得隨意進入，進出時需填寫進出登記簿。
vi. 機房內不得擺置易燃物品，並擺放符合標準之滅火器與濕度計。

資訊安全管理具體方案

- 使用者權限管理：使用者需按照安全等級區分給予不同之使用權限。
- 作業系統使用權限安全管理：依公司規定安裝作業系統，並加入公司網域，進行集中管理。作業系統定時安全更新，並於公司內之主機及電腦，安裝防毒軟體，並每日自動下載、更新掃描引擎及病毒碼。使用者帳號之密碼定期更新設定措施。
- 應用軟體安全管理:除安裝資訊作業所需的應用軟體以及工具軟體、套裝軟體外，如需安裝其他特殊軟體須另行申請經核准後始得安裝。
- 於防火牆設定禁用軟體、網址之隔絕過濾機制，阻絕通行，以避免影響網路品質及安全。
- 網路通訊安全管理：外部 VPN(遠端)存取及內部存取(檔案傳輸(FTP)、即時傳訊(MSN)、特殊連線(HTTPS)等網路應用)均須經資安中心審查與權限主管核准始得使用。
- 應用系統安全管理：資安中心須限定只能由授權的處理人員才可執行原始程式碼之存取更新；依業務之需求而設定使用者不同之程式執行權限。
- 備援管理：設有系統災難復原、資料庫之備份管理相關措施
- 資產管理：針對機房設備及個人電腦進行資產編號管理並定期盤點。
- 以線上訓練方式，宣導使用者設定及操作作業系統之安全機制；以及現行病毒(木馬、後門、蠕蟲...等)來源途徑、感染方式，增加使用者防護知識。

評估 2022 年度企業資安事件頻傳，漢唐全面強化資訊安全管理，2022 年度資安資源投入包括如下:

- ✓ 電腦(含筆電)汰舊換新計 5,991仟元。
- ✓ 網路設備(NAS & SWITCH) 建置304仟元。
- ✓ 軟體租賃費用(AutoCAD & 機電) 1,226仟元。
- ✓ 防毒軟體(趨勢 Apex One)續約費用 533仟元。

綜整 2022 年度投入資安維護相關經費達 8,054 仟元。

本公司 2022 年度未發生重大資安事件，符合資訊安全管理目標。

緊急通報程序

當發生資訊安全事件時，發生單位通報資安中心，判斷事件類型並找出問題點，即時處理並留下紀錄。