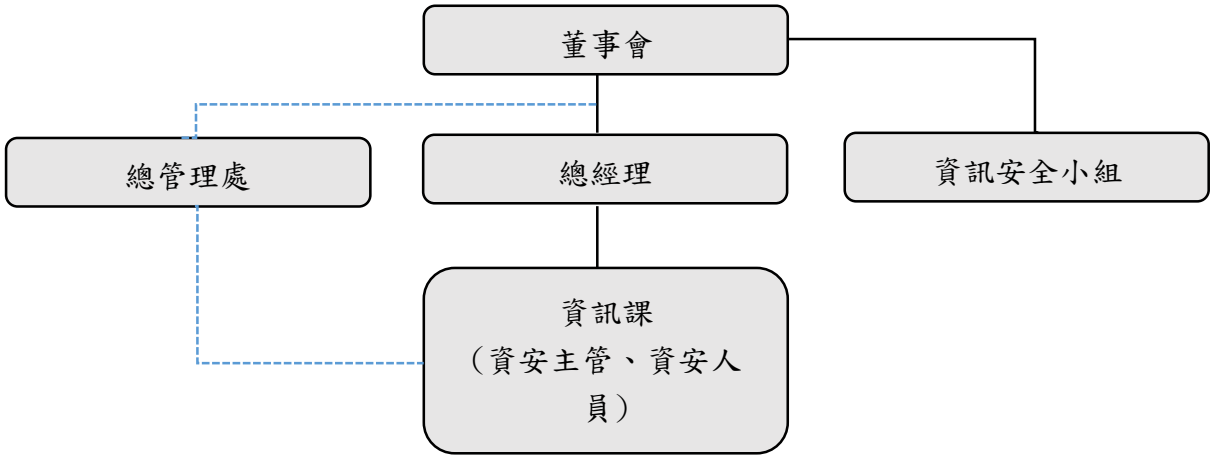
114 年資通安全管理情形

1. 和勤公司針對資訊安全防護採取適當的管理，訂定「012-B-34 資訊安全管理辦法」避免網路攻擊、設備故障等因素所造成資訊安全事件。並設置資訊安全主管與資訊專責人員，統籌資訊安全保護相關規範制定與執行。

2. 本公司董事會於 112 年 2 月 23 日決議通過設置資安專責主管 1 位及資安專責人員 1 位，並單獨建置新部門單位「資訊課」，由專責單位負責處理公司之資通安全管理，本公司建置之資通安全風險管理架構如下：



3. 資通安全政策：

(1)資訊安全方針「構築安全資訊環境，提升服務與營運效能」。

(2)各項資訊安全管理規章必須遵守政府相關法規（如：刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等）之規定，由資訊課負責資訊安全制度建立及推動事宜。

(3)新資訊系統應於建置前納入資訊安全風險評估，防範危害系統安全之情況發生。

(4)依職務職責明確規範資訊系統及網路服務之使用權限，防止未經授權之存取動作，跨職務之權限皆需透過申請始得存取。

(5)應遵守網路安全政策規定，如有違反網路安全之情事，應依資訊安全規定，限制或撤消其網路資源存取權利，並依規定及相關法規處理。

(6)建立資訊軟、硬體之管理機制，採取相應措施以降低及解決資訊處理相關風險。

(7)為維持在伺服器硬體設備正常運作，與廠商簽署硬體維護合約，發生損壞時快速進廠維修。

(8)確保復原計劃於緊急發生時能有效的運作，每半年執行系統復原測試。

4.具體管理方案：

推行措施	說　　明	
	推動原因	推行方式
軟體安全、禁止使用盜版軟體	資訊工具取得方便，員工因作業方便會自行下載盜版軟體使用。	廠區內的電腦裝置，皆由資訊單位管控，不得安裝盜版軟體，並管制安裝權限。員工有需求的作業系統或應用程式，皆由公司取得正版授權，並由資訊單位進行安裝使用。
社交工程	使用免費的社交通訊軟體，如 line、skype 等，來傳送檔案、快速 聯繫、或發布公告，皆是使用原本私人帳號，作為公務使用，因此會潛藏眾多資安風險，容易機密外洩，例如將公務情事傳到私人群組。	採用企業型通訊軟體，區隔公務 / 私用訊息平台，由公司內部認證登入，成員皆為公司員工，防止機密外洩，並有紀錄備查。
自攜設備管理	對於員工能使用自己裝置，快速進入工作狀態，且不受地域限制，隨時都與工作進度接軌，提升團隊作業效率；對於公司則能降低企業的資訊採購成本，滿足移動商務需求，可大幅降低設備的折舊與維運管理支出。	設立自帶資訊設備管理辦法，明確規定自帶設備之申請及使用，並接受公司資安政策管控，簽立自帶資訊設備使用同意書，以防範外部的盜取或員工的洩漏。
垃圾信管理	垃圾信包含無害的廣告信及惡意的釣魚	透過防火牆、防毒軟體、垃圾信過濾軟體，層層把關，

	信、病毒信，惡意信件將危害公司資訊系統運作，嚴重將造成公司財產損失。	將惡意信件阻擋在外，不定時宣導惡意信件的資安觀念。
系統備份	勒索病毒惡意危害公司資訊系統或相關營密資料	透過系統備份及還原，提升資料完整性。

5.定期資通安全檢討：

114 年 3 月辦理資通安全檢查自我檢核，透過自我檢核表逐一檢查系統安全是否存有可用性、機密性與完整性並進行確認，以落實資通安全相關要求。

6.每年定期檢討次年度應投入之資通安全管理預算，113 年度及 114 年分別編列預算 1,628 仟元、1,470 仟元，執行改善相關資安設備，如：檔案加密系統、強化防火牆防護功能、遠端桌面系統，提高資訊安全性，達成資訊不落地目標。115 年度編列預算 1,015 仟元，預定執行伺服器儲存設備、更新防火牆防護功能、防毒軟體及郵件防護系統更新等。

7.資訊教育訓練及安全宣導執行情形：

114 年 4 月 1 日資安主管及人員參加資安事件說明及預防措施、資通安全管控指引、資訊安全必備知識與責任等課程，114 年 12 月 3 日資安主管採電子郵件對公司全體員工宣導如何判斷是否為「詐騙釣魚信件」。

8.114 年度並無發生任何資安事件或洩漏客戶隱私之相關情事。