資訊安全政策宣言

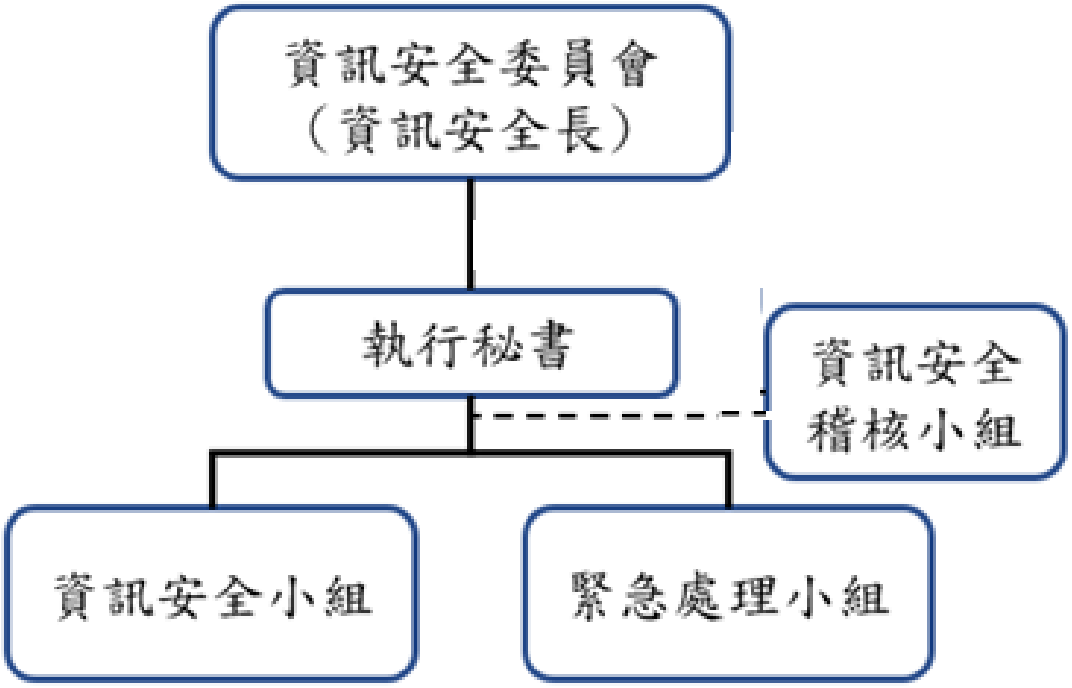
資訊安全與機密資訊保護是思考軟體科技有限公司對客戶、股東及夥伴的承諾。思考軟體科技有限公司為強化資通安全防護及管理機制，設立資訊安全長（CISO）與資訊安全專責組織，配置專業之人力與資源，明訂資訊安全政策、管理程序及規範，發表《資訊安全宣言》，宣示捍衛資訊安全的決心與推動資訊安全的目標—維護思考軟體科技有限公司的市場競爭力及保障客戶與合作夥伴利益。

資訊安全宣言(公司介紹)

思考軟體股份有限公司致力於企業資訊安全、行動裝置管理（MDM/UEM）、電子柵欄、資安管理及資訊系統整合等解決方案，提供企業與政府機關安全、穩定且值得信賴的資訊服務。我們秉持專業、創新與服務的理念，持續提升產品品質及資訊安全管理能力，協助客戶建構安全可靠的資訊環境。

資訊安全治理

思考軟體科技有限公司設有資訊安全委員會(IT Security Committee)並任命總經理擔任思考軟體科技有限公司資訊安全長（CISO），負責資訊安全政策與制度之規劃、監控及管理作業，並與公司資訊技術及相關單位組織協同合作，強化資通安全防護及管理機制。



思考軟體科技有限公司資訊安全組織

資訊安全小組

思考軟體科技有限公司成立「資訊安全小組」，由軟體開發、顧問服務擔任小組成員，定期召開會議檢視及決議重要資訊安全與資訊保護政策與計畫執行，確保實現思考軟體科技有限公司資訊安全政策目標。

資訊安全委員會

思考軟體科技有限公司成立「資訊安全委員會（IT Security Committee）」，由總經理擔任資安長，由各部門推派相關同仁擔任委員會成員，定期召開會議檢視重要資訊安全政策、資訊安全風險評估與強化計畫、資訊安全指標與全球資訊安全態勢與威脅，確保達成思考軟體科技有限公司資訊安全政策與管理目標。

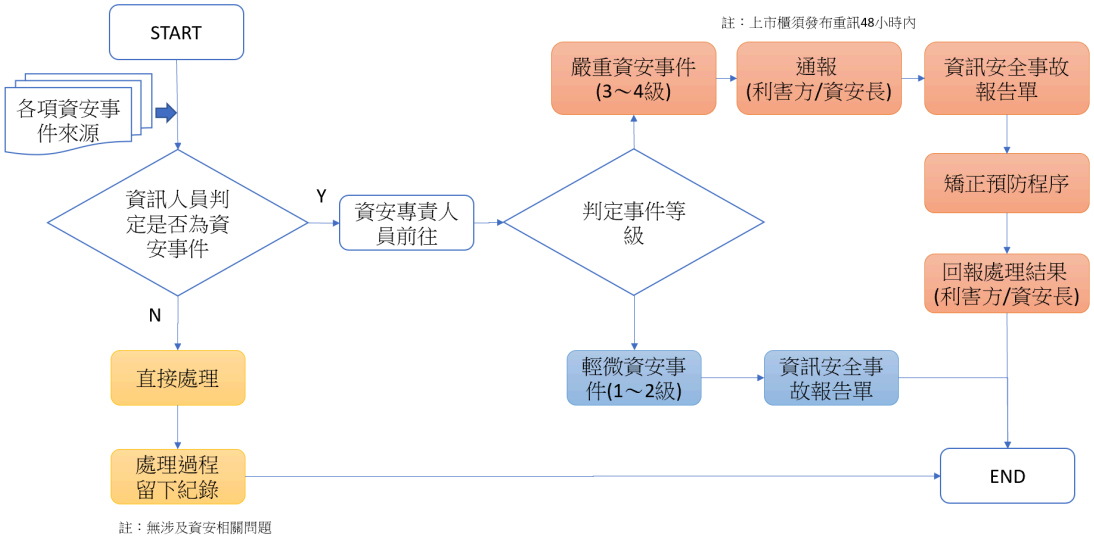
資訊安全管理與執行重點

思考軟體科技有限公司為了預防及降低外部資安風險，落實及持續更新嚴謹的資安措施，例如建置先進的病毒掃描工具，以防止公司所使用之資訊系統遭受病毒感染；強化網路防火牆與網路控管以防止電腦病毒跨廠區擴散；在公司電腦上 建置防毒措施及先進的惡意軟體偵測解決方案；改善資安部署時間以強化資料中心安全。並建立與定期檢討資安績效指標；導入新技術加強資料保護；加強釣魚郵件偵測並定期執行員工警覺性測試；建立一個整合的自動化資安維運平台並強化資安事件偵測與處理自動化；持續演練資安攻擊之處理程序；委託外部專家執行資安評鑑等。每年持續進行的資安執行重點如下：

- 網路安全控管
- 資產管理及資料保護
- 存取控制
- 電腦維運安全管理
- 人員及實體安全
- 應用程式安全
- 資安事件處理(包括威脅監控／應變等)與管理
- 供應鏈安全
- 人員資安管理與教育宣導
- 內/外部資安評測與風險管理

資安事件處理與通報

思考軟體科技有限公司已成立資訊安全應變中心與資訊安全事件管理程序，明訂相關流程與措施，包含資安事件通報程序、指派負責人員處理重大資通安全事件、評估遭受損失及進一步的必要因應措施、評估資安風險可能對公司財務與營運的影響及其因應措施。


START
各項資安事件來源
資訊人員判定是否為資安事件
Y
資安專責人員前往
判定事件等級
嚴重資安事件(3～4級)
通報(利害方/資安長)
資訊安全事故報告單
矯正預防程序
回報處理結果(利害方/資安長)
N
直接處理
輕微資安事件(1～2級)
資訊安全事故報告單
處理過程留下紀錄
END
註：上市櫃須發布重訊48小時內
註：無涉及資安相關問題