和椿科技股份有限公司

資訊安全政策及施行管理方案

114年度投入資訊安全、資通安全管理之資源暨115年執行計劃

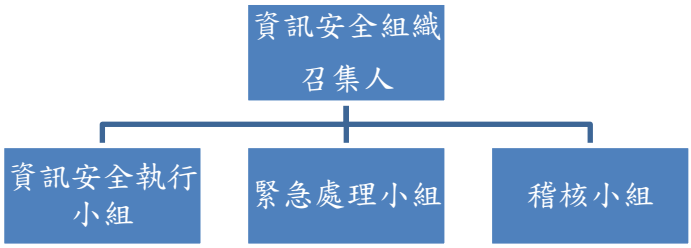
董事會報告日期：114.11.06

一、 資訊安全風險管理架構

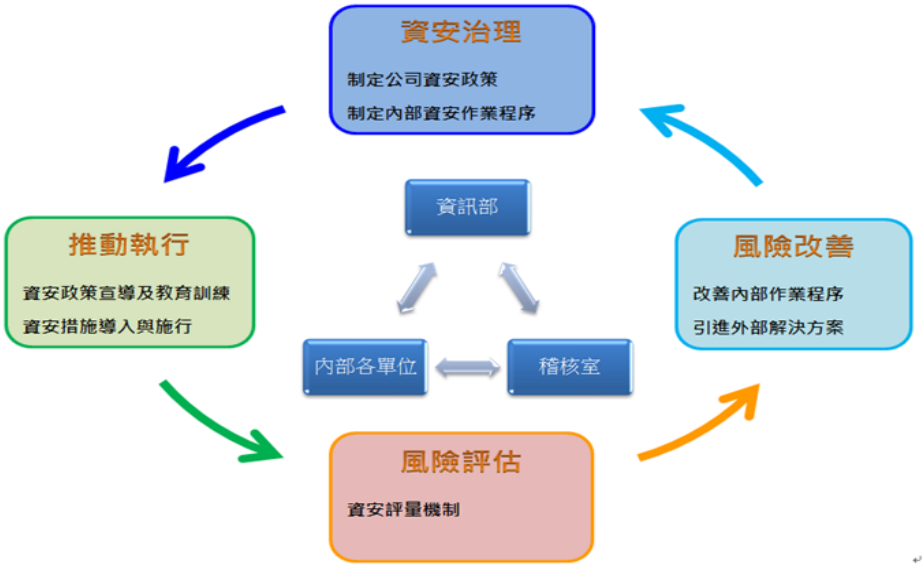
本公司資訊安全之權責單位為資訊部，負責規劃、執行及推動資訊安全管理事項，並推展資訊安全意識。

本公司稽核室為資訊安全監理之查核單位，若查核發現缺失，旋即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。

a. 資訊安全組織



b. 組織運作模式-採用P D C A（Plan-Do-Check-Action）循環式管理，確保可靠度目標之達成且持續改善。



二、資訊安全政策及管理方案

（一）本公司資訊安全管理機制，包含以下三個面向：

1、制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

2、科技運用：建置監控軟體，落實資訊安全管理措施。

3、人員訓練：進行資訊安全教育訓練，提昇全體同仁資訊安全意識。

（二）本公司資訊安全政策：

1、遵守國家法令訂定相關資訊安全管理規章，對本公司資訊資產提供適當的保護措施，以確保其機密性、完整性、可用性及法律遵循性。

2、定期評估人為及天然災害對本公司資訊資產之影響，並訂定重要資訊資產及關鍵性業務資訊之防災對策及應變復原計畫，定期演練災害復原計劃，以確保資訊資產之穩定運行，保持本公司業務持續運行。

3、督導公司同仁落實公司資訊安全防護及配合資訊安全管理措施，確保同仁對資訊安全的防護及認知。

4、除要求本公司同仁確實遵守公司的資訊安全規定外，亦要求有使用到本公司資訊系統的往來廠商，恪守本公司資訊安全規定，如有違反或造成本公司損失時，將依相關法律追訴究責。

三、 資訊安全管理措施

對象	管控類型	相關作業	頻率	說明
員工	權限管理	人員帳號權限管理與審核 人員帳號權限定期盤點	不定期 至少1次/年	人員帳號、權限管理與系統操作行為之管理措施 密碼長度修正
員工	存取管控	內/外部存取管控措施 操作行為軌跡記錄 外寄郵件過濾 限定裝置權限管理(包含USB) 遇到較大檔案時公司內部有私有雲提供	即時 即時 即時 即時 即時	人員存取內外部系統及資料傳輸管道之控制措施
系統	外部威脅	主機防火牆沙箱及IPS更新措施 病毒防護與惡意程式檢測 各據點網路以SD-WAN加上EdgeShield連接	即時 即時 即時	內部防火牆、中毒管道與防護措施 確保各據點威脅防禦功能的虛擬安全網關，方便集中部署及管理
系統	系統可用性	系統/網路可用狀態監控及通報機制 服務中斷之應變措施 資訊備份措施、本/異地備份機制 定期災害復原演練 個人重要資料空間擴大	即時 即時 每天備份，桃園與台北異地1次/年 即時同步	系統可用狀態與服務中斷時之處置措施
系統	深化資料保全	每日備份外，運用儲存設備再進行系統即時鏡射備份	每小時1次24份+7天4*7=28份，總計52份	系統可用狀態與服務中斷時之處置措施

四、114年度投入資訊安全、資通安全管理之資源

資訊安全已為公司營運重要議題，對應資安管理事項及投入之資源方案如下：

（一） 專責人力：

本公司於112年8月10日經董事會任命張曜燦先生為本公司資訊安全主管，112年11月8日指派史宗平先生為資訊安全專責人員。

資訊部共六名：

(1)資訊部-經理一名。

(2)資訊部-軟體課三名。

(3)資訊部-網管課二名。

（二） 無重大資安事件、無重大資通安全事件所遭受之損失、無違反資料遺失之投訴案件。

（三） 教育訓練：所有新進員工皆完成資訊安全教育訓練課程，114 年度共辦 2 場教育訓練。

（四） 資安公告:114 年度共製作 1 份資安公告,傳達資安防護重要規定與注意事項。

（五） 資訊安全管理：

管控類型	投入工時	投入資源
權限管理	38.8	IPguard軟體
存取管控	39	Fileserver、Safesync雲端
外部威脅	6.2	防火牆整
系統可用性	806.4	軟硬體升級及維護
合計	890.4小時	

（六）投入資源：

1. 資安防毒，每年18萬元
2. 郵件安全，每年18萬元
3. 資料保存，每年25萬元
4. 社交演練及弱點掃描，每年20萬元
5. MDR，快速應對勒索病毒、DDoS 等威脅，每年81.6萬元
6. 各據點網路連線，每年85萬元
7. 因應微軟產品資安問題，執行作業系統升級及更新設備，175萬元
8. 因應微軟產品資安問題，主機系統軟體升級，105萬元
9. 防火牆更新，48.5萬
10. 集團整體無線網路更新，80萬元

（七）資訊設計服務滿意度調查表：

114年度截至10月共統計741份，共投入890.4工時。

項目	非常滿意	滿意	尚可	非常不滿意
處理效率	641	92	6	1
回覆效率	646	88	6	0
服務態度	648	84	7	1
合計	共741份			

五、115年資訊預計執行項目如下：

（一） 持續強化資安等級：

1. 持續執行系統合規：預計投入費用每年200萬
2. 公司ERP系統升級，符合法遵要求，預計投入費用600萬
3. 資安防毒/郵件安全/資料保存/社交演練及弱點掃描/MDR，預計投入費用200萬
4. 資安軌跡紀錄與稽核：預計投入費用100萬

（二） 計畫執行取得ISO27001：預計投入費用200萬

1. 提升管理效率：透過清楚的資訊安全範圍定義與權責區分，能夠使組織內部更清楚資訊安全管理的相關負責人與各自權責，面臨事件時更能即時找到對的人進行應對。
2. 遵循法律規定：許多國家都有針對資訊安全訂出法律規定，例如台灣《個資法》，而ISO27001內容足以建立起一定資安制度，確保企業蒐集、使用、保存資料時符合法律規範。
3. 降低營運成本：導入ISO27001能夠事前評估資安風險，以降低資料外洩造成的營運損失，變相降低了營運成本。
4. 增加客戶信任：對於重視資訊安全的客戶，ISO27001能夠消除不信任感，增進個人及企業客戶商務往來的意願與相互信任，協助業績蓬勃發展。
5. 維持公司信譽：當企業守法且資安能力足以讓客戶信賴，長久經營下來，公司信譽也會連帶提升。
6. 進軍國際市場：因ISO27001為全球認可的資安標準，對於有意擴展國際市場的企業，能夠做好事前部屬，讓國外客戶了解企業能力，提升企業競爭力。

（三） 資訊機房整建：內湖機房重整預計投入費用200萬元