勝品電通股份有限公司
Topview Optronics Corp.
資訊安全風險管理架構

一、資訊安全政策

資訊安全管理制度遵循說明：

1. 本公司依「公開發行公司建立內部控制度處理準則」第九條「電腦化資訊系統處理」之規定制定相關內部作業規定，以降低新興資訊科技應用以及環境變遷所帶來未知的資安風險。

2. 勝品電通持續對資訊安全完備其治理制度與提升防禦能力，各項資訊作業不僅須符合資安標準流程外，更要符合資訊安全法令法規。

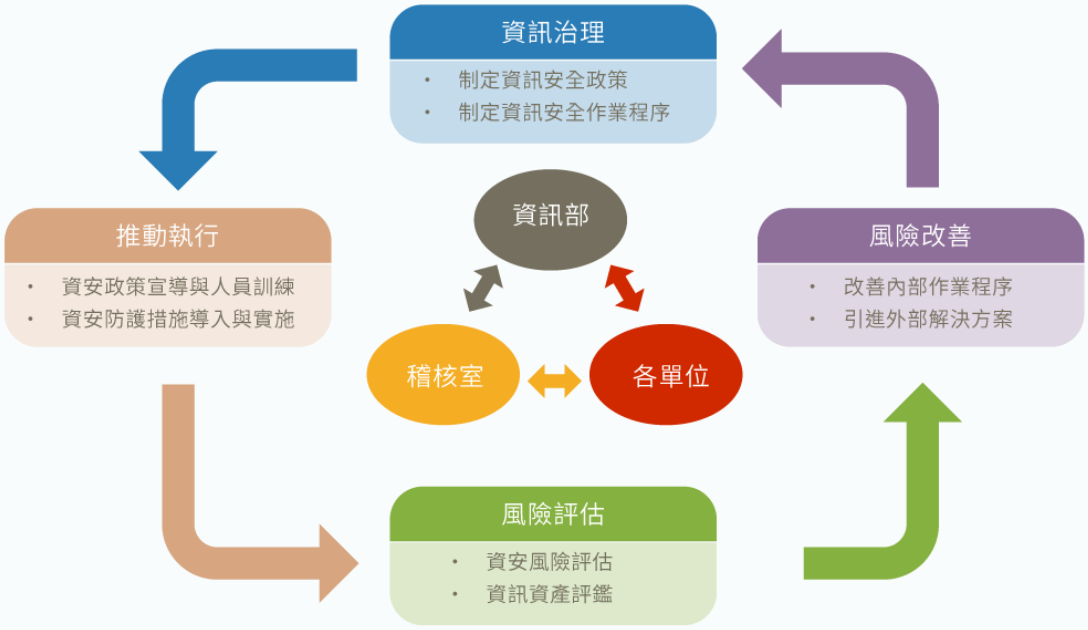
二、資訊安全管理策略組織

組織運作模式-採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。

1. 本公司資訊安全之權責單位為資訊部，該部設置資訊主管乙名，與專業資訊人員數名，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實，並定期向公司管理階層報告公司資安治理概況。

2. 本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管乙名，與專職稽核人員數名，負責督導內部資安執行狀況，若有查核發現缺失，旋即要求受查單位提出相關改善 計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。

3. 自 2017 年起依循公司【資訊安全發展藍圖】逐步精進，深刻落實資訊安全風險管理。



三、資訊安全風險管理架構

為掌握資訊安全風險管理，勝品電通自三方面向來對應及預防風險事件發生：

【資訊安全發展藍圖】

註 1 綠色為已執行項目

註 2 藍色為進行中項目

短中期【2017~2025】

1.端點安全-強化電腦權限管理
2.Web 安全-強化上網瀏覽器安全管理
3.網路安全-強化內網合規存取
4.網路安全-骨幹網路安全確保
5.員工資安意識-實施社交安全訓練演練
6.身分識別機制-擴充高風險系統雙重認證機制
7.資料外洩保護-納管企業內通訊系統
8.資料外洩保護-增加文件分級分權管理機制

長期【2025~2030】

1.定期進行系統安全檢測
2.定期強化員工資安意識
3.持續增強 IT 基礎架構
4.擴充異地機房備援
5.優化災害復原流程與演練
6.增加資安作業檢核機制(ISMS/ISO)

短期原則 優先處理緊急威脅 → 中期策略 優化重要資安環節 → 長期發展 持續滾動式檢討與因應

1. 未發生前：定期自主盤點檢驗，從流程與技術多方面著手，主動預防資安事故。

   a)防入侵：主動防禦來自內外網攻擊，侵入資訊系統造成破壞。

   b)防外洩：主動防範公司機敏資訊及營業秘密遭外流外洩，影響勝品電通永續經營。

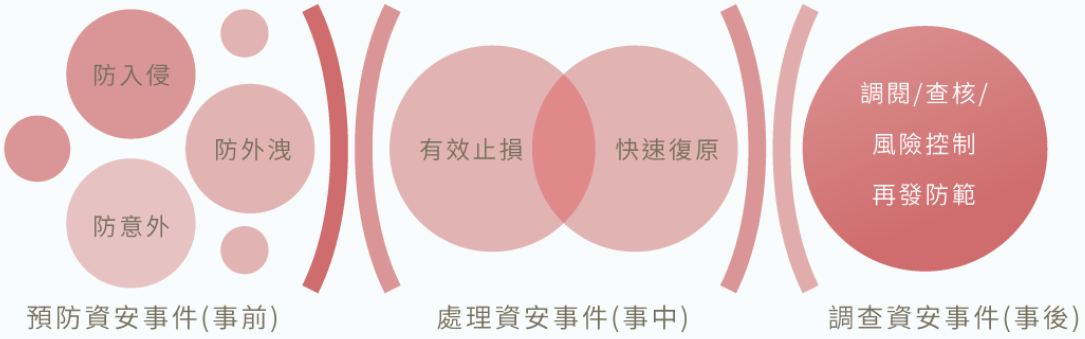
   c)防意外：主動預防環境內因素（故障/跳電/病毒/設備遺失）造成的生產損失。

2. 事件發生時：損害控制緊急應變
   a)完善機制：建立有效的災害應變機制，迅速將損害控制止血。

   b)落實演練：運用演練經驗，在最短時間內恢復正常，維持企業體持續營運。

3. 發生以後：追查並列入預防
   a)避免問題發生：調閱系統紀錄追蹤問題原因，擬定對策成新預防措施。

   b)查核方法再強化：引入外部顧問/弱點檢測團隊，低減查核盲點提高內控機制可靠性。



四、資訊安全具體管理方案

資訊安全規劃勝品電通為強化整體資訊安全,2018 年起即進行具體多項資訊安全強化專案，範圍包含:

1.【內/外網路安全】 2.【員工資安意識提升】 3.【Internet 上網安全】

4.【身份識別機制強化】 5.【資料外洩保護 DLP 】 6.【增強 IT 基礎架構】

目前資訊安全規劃『資訊風險內控管理措施』，穩健推展中長期整體資安、持續優化，包含:

1. 資安人員配置：
   - 資訊部組織組織設置資安主管 1 名及資安執行人員 1 名。
2. 資安會議：每半年召開 1 次。
3. 基礎資訊建設：
   - 機房消防設施與機房供電系統優化提昇
   - 汰換未達現代資安要求之設備及設施
   - 建構新世代資安防禦設備

4. 智慧製造防護：
   - 監控應用系統及網路節點裝置異常徵兆(預知管理)
   - 運用先進加密技術，增強機敏資料傳輸保障
5. 落實資安訓練(提升一般同仁對資安素養)：
   - 新進人員教育訓練中加入資訊安全說明
   - 每年執行 2 次資訊安全宣導郵件
   - 每年執行 2 次社交郵件模擬通知
   - 每年定期執行資訊人員資安系統教育訓練。

五、資安事件通報程序

本公司資訊安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行