大學光學科技股份有限公司
Universal Vision Biotechnology Co., Ltd.

資通安全

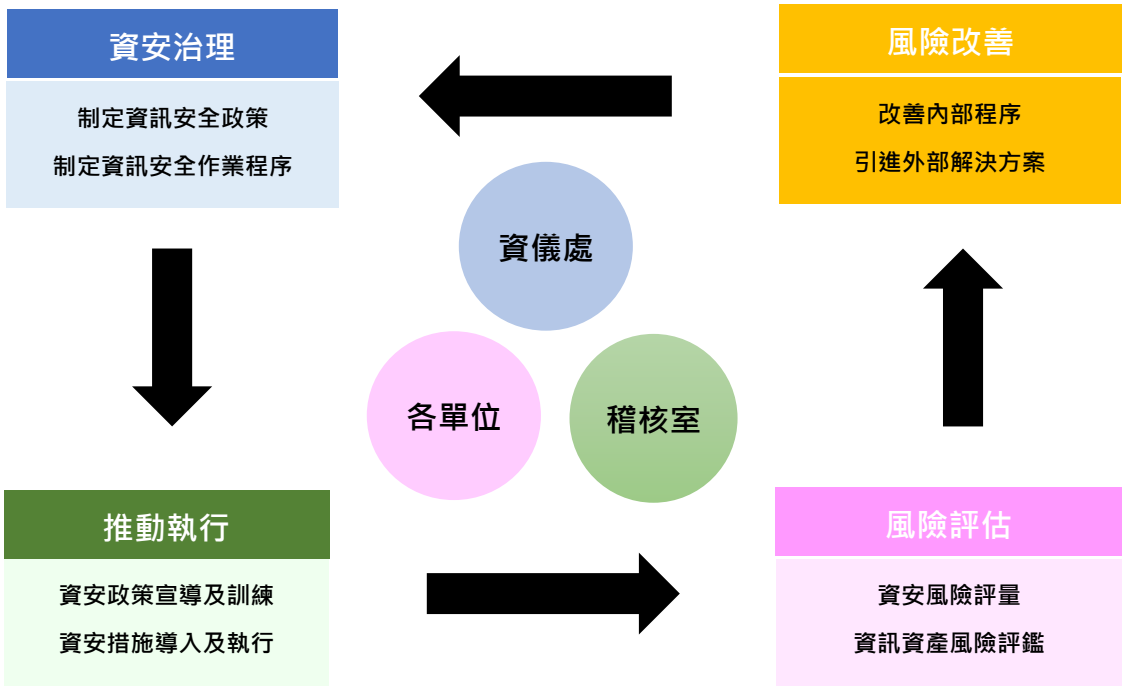
（一）資通安全管理策略與架構、資通安全政策、具體管理方案、投入資通安全管理之資源：

1. 資通安全管理策略與架構

本公司資訊安全權責單位為資訊暨儀器處，該處設置主管乙名，及專業資訊人員數名。負責訂定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，並向審計委員會報告公司資安治理概況。

本公司資訊安全監理查核單位為稽核室，該室設置稽核主管乙名，與專職稽核人員數名。負責督導及查核內部資安事項執行狀況，若查核發現相關缺失，即要求受查單位提出相關改善計畫與具體作為，並追蹤改善成效，以降低內部資安風險。

組織運作模式-採用 PDCA 循環式管理，確保可靠度目標之達成且持續改善。



2. 資通安全政策

為貫徹本公司各項資訊管理制度能有效運作執行，維護重要資訊系統的機密性、完整性、可用性，以確保資訊系統、設備網路之安全維運。

本公司定訂資訊安全管理機制，包含以下三大項：

（一）制度規範：制定公司資訊安全管理制度及辦法，規範同仁資訊相關作業行為。

（二）新科技運用：導入、建置資訊安全管理相關軟、硬體，落實資安管理措施。

（三）人員訓練：定期進行資訊安全教育訓練，提昇全體同仁資訊安全觀念及落實資訊安全各項措施。

說明如下：

- 制度規範：本公司內部訂定多項資安管理辦法與制度，以規範本公司人員資訊安全行為，每年定期檢視相關制度是否符合營運環境變遷，並依需求適時調整。
- 新科技運用：本公司為防範各種內、外部資安威脅，除採多層式網路架構設計外，更建置各式資安防護系統、機制，例如:高可用性之高可靠度架構(HA)、主機環境備份、資料備份(交易紀錄、差異備份、完整備份)、異地備分機制等以提昇整體資訊環境之安全性。此外，為確保內部人員之作業行為符合公司制度規範，亦導入資產管理系統工具，落實設備及人員資訊安全管理措施。
- 人員訓練：本公司定期舉辦資訊安全教育訓練課程，並建置線上學習 (E-Learining)系統，藉以提昇內部人員資安知識與專業技能。

3. 具體管理方案

資訊安全管理措施		
類型	**說明**	**相關作業**
權限管理	人員帳號、權限管理與系統操作行為之管理措施	人員帳號權限申請管理與審核 定期人員帳號權限盤點
存取管控	人員存取內外部系統及資料傳輸管道之控制措施	內/外部存取管控措施 操作行為軌跡記錄
外部威脅	內部潛在弱點、中毒管道與防護措施	主機/電腦弱點檢測及更新措施 病毒防護與惡意程式檢測 防止惡意攻擊設備
系統可用性	系統可用狀態與服務中斷時之處置措施	機房例行檢查 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、本/異地備份機制、定期資料還原測試 主機還原測試 定期災害復原演練

4. 投入資通安全管理之資源: 投入兩名兼職人員負責資訊安全發展事宜，並編列 600 萬元以上之資訊安全軟、硬體更新預算。

（二）最近年度及截至公司年報刊印日止，因重大資通安全事件所遭受之損失、可能影響(例如：營運或商譽的影響)及因應措施，如無法合理估計者，應說明其無法合理估計之事實：無。