資訊安全政策及管理方案

1.資訊安全風險管理架構

資訊處為負責資訊安全的主管單位、負責訂定並實施資訊安全政策，每三個月向管理階層報告資訊安全執行計畫與執行情形, 以確保內部資安管理機制持續有效運作。

稽核處為資訊安全監理之查核單位,若查核發現缺失,即要求受查單位提出相關改善計畫，且定期追蹤改善成效，以降低內部資安風險。

組織運作模式採用 PDCA（Plan-Do-Check-Act）循環式管理，建構完整的資安管理系統，以有效防範資訊安全事件發生，確保達成資訊安全目標，並持續優化改善。

2.資訊安全政策

本政策為保護晶豪科技股份有限公司所有的資訊資產安全，預防內部或外部、蓄意或意外之各威脅與破壞，致使業務無法正常運作或資訊遭受竄改、取、破壞或破壞，以達永續經營目的。

一、資訊安全定義

為保護公司資訊及資訊系統免受未經授權的進入、使用、披露、破壞、修改、檢視、記錄及銷毀，並維持現有資訊系統的可用性。

二、資訊安全目標

1.確保業務相關資訊之機密性，保障公司機密。
2.確保業務相關資訊之完整性及可用性。
3.提昇資訊安全防護能力。

三、資訊安全範疇

本政策適用於公司內部各項資訊系統、內部同仁以及接觸業務資訊或提供服務之廠商及第三方人員。

3.資訊安全管理方案

本公司針對營連類資產如資訊系統、網路設備等資訊設備，已投備硬体設備電子保險並透過保全監控作業避免設備被竊或是惡意損毀情事發生。鑒於資安保險為新興保險種類，考量保險範圍、理賠範圍、理賠鑑識、鑑識機構資格等議題綜效，本公司經評估後暫不投保

資安險。但因應資訊安全所面臨的挑戰，如 APT 進階持續性攻擊、DDos 攻擊、勒索軟体、社交工程、竊取資等資安議題，已採取以下策略：每年依公司資訊安全政策持續關注資訊環境變化趨勢，並參考技術文刊資料，擬訂資訊安全防護機制與方案。加入 ISAC，取得最新攻擊情資，並採取適當防御對策。定期執行安全性檢測、資通安全健診、社交安全及資安事件演練、強化公司同仁資安危機意識及資安處理人員應變能力，以期能事先防範及第一時間有效偵測並阻絕擴散。

4.資訊安全管理措施，包含如下：

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	● 人員帳號權限管理與審核 ● 人員帳號權限定期盤點
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 ● 機敏資料外洩管控 ● 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/電腦弱點防護及更新措施 ● 病毒防護與惡意程式檢測 ● 網路威脅監控
系統可用性	系統可用狀態與服務中斷時之處置措施	● 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