亞泰影像科技股份有限公司
資訊安全風險管理辦法

第一章 總則

第一條　本公司資訊安全由管理處負責，訂定內部資通安全政策及目標，規範與制度、規劃暨執行資通安全作業與資通安全政策推動與落實，並依需求適時調整。

第二條　名詞定義：

1. 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
2. 資通服務：指與資訊蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之系統。
3. 核心業務：公司維持營運與發展必要之業務。
4. 核心資通系統：支持核心業務持續運作必要之資通系統。
5. 機敏性資料：依公司業務考量，評估需保密或具敏感性之重要資料。

第二章 資訊安全政策及組織

第三條　本公司由管理處成立資通安全推動組織，配置適當人力及物力資源。指派人員擔任資安專責主管及資安專責人員，辦理風險評估、安全分級、系統安全控管等措施。

第四條　本公司資訊安全政策為遵循資訊安全相關法令，增進本公司資安作業安全及穩定之運作，確保資訊資產之機密性、完整性及可用性，並順利推展本公司各項業務，以符合客戶資訊安全需求。

第五條　本公司資訊安全目標為：

1. 確保本公司業務相關資訊之機密性，保障本公司業務機密。
2. 確保本公司業務相關資訊之完整性及可用性，提高工作效能與品質。
3. 提昇本公司資訊安全防護能力。
4. 達成客戶要求之資安標準。

第六條　本公司資訊安全政策應定期評估及檢討。並定期對單位人員及資訊設備進行安全評估，確定其遵守資訊安全政策及相關規定。

第七條　本公司單位內若開放給外部單位作資料存取，應訂定控管程序。

第八條　本公司所有使用資訊系統之人員，每年接受資訊安全宣導課程；負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練 。

第三章 核心業務安全

第九條　本公司應鑑別並定期檢視公司之核心業務及應保護之機敏性資料。鑑別應遵守法令及契約要求。

第十條　本公司如有資訊核心業務中斷事件，復原時間目標(RTO)為 4 個工時，資料復原時間點目標(RPO)為 8 個工時。

第四章 資通系統盤點

第十一條　本公司資訊系統資產清冊應隨時更新，定期盤點。

第十二條　本公司定期辦理資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施等。

第五章 資通系統發展及安全維護

第十三條　本公司定期對資訊資產設備、系統辦理災害復原演練及弱點掃描、滲透測試。

第十四條　本公司資訊資產及系統上線前應執行源碼掃描安全檢測。

第六章 資通安全防護及控制措施

第十五條　人員安全與管理

1. 訂定人員裝置使用管理規範，如：軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等管控使用規則。
2. 訂定到職、在職及離職管理程序，避免非法使用。
3. 定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。

第十六條　資通安全與操作管理

1. 應使用網路防火牆並定期檢討電腦網路安全控管事項之執行。
2. 對於敏感性資訊之處理應採取資料加密、傳輸加密、人員管理、存取權限、實體隔離、處理規範等保護措施。
3. 對於輸出及輸入機敏性資料應有處理程序及標示。
4. 應依網路型態訂定適當的存取權限管理方式。
5. 應規範資訊設備使用上鎖或密碼等管制措施以防止遭非法使用。
6. 資訊及應用系統應設有作業結束後或在一定期間未操作時即自動登出或中斷連線之保護機制，若需再登入需重新取得授權。
7. 用戶使用者密碼應為八碼以上、二十碼以下之英、數、特殊符號混和之複雜密碼，並每半年更新一次
8. 應管制使用者的公司內外連線功能，並針對電子郵件、加密連線、單雙向檔案傳輸、互動式存取與存取時段做通盤連線控管考量。
9. 應指定專人管理應用程式原始碼、資料庫及執行檔。
10. 機密及敏感性資料的處理應於獨立或專屬的電腦作業環境中執行。
11. 機房建立進出管控及環境安全措施，包含身分驗證存取紀錄、存取資源紀錄與未授權之連線等，並定期檢查。
12. 建立資通系統及相關設備適當之監控措施，並保存相關操作日誌。
13. 每年定期辦理電子郵件社交工程演練，並對誤開信件或連結之人員進行教育訓練、並留存相關紀錄。

第十七條　永續經營管理

1. 本公司辨識關鍵性業務及執行其風險評估、衝擊影響、優先順序。

2. 本公司定期執行風險評估並調整永續經營政策。

第七章 資通安全事件通報應變及因應

第十八條 本公司訂定資安事件應變處置及通報作業程序，包含判定事件影響及損害評估、內外部通報流程、通知其他受影響機關之方式、通報窗口及聯繫方式。

第十九條 本公司評估加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊。

第二十條 本公司如發生符合「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。

第八章 稽核及其他

第二十一條 本公司各單位應使用合法軟體。軟體之使用及資料之儲存、處理和報廢，應有適當之控制。

第二十二條 資訊安全單位應留意安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。

第二十三條 資訊安全單位不定期辦理委外廠商之資安稽核，並就發現事項擬訂改善措施，且定期追蹤改善情形。

第二十四條 內部稽核負責查核內部資安執行狀況，每年稽核一次。

第九章 評估與修正

第二十五條 本辦法訂於每年十二月由「資訊安全小組」召開資訊安全會議，辦理本公司資訊作業安全事項重行評估與修正事宜，以反映相關法令、資訊技術及本公司業務發展現況，俾使本辦法確實符合安全需求。