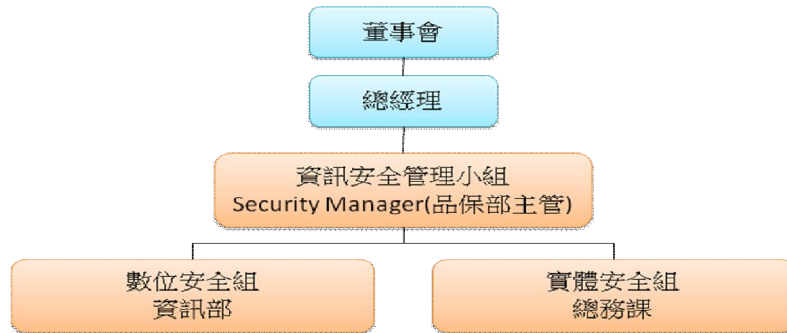


## 鈺德科技股份有限公司 資訊安全政策

本公司重視客戶隱私權及智慧財產權，與客戶簽署保密協定以保護客戶機密資訊，並確保相關業務之同仁確實執行做好保密工作，並已於公司內部管理文件（SA3-200-18 客戶智慧財產保全管理辦法）中規範其管理措施如下：

### 1.1 Security Organization：

為提升資訊安全管理，本公司設有資訊安管理小組由品保部主管擔任 Security manager，負責招集統合數位安全組與實體安全組，進行資訊安全治理、規劃、督導推動及執行。



### 1.2 風險評估(Risk Assessment)：

跨部門檢視所有關鍵流程，對客戶之智慧財產的安全進行風險評估，對有風險疑慮之處驗明並尋求改善之道。風險評估定每年評估一次。

### 1.3 Content security policy：

建立實體及數位內容管控 (Physical & digital controls) 流程，以確保客戶智慧財產完全受到安全保障。

資安策略主軸聚焦資訊安全管理、法令遵循及科技運用，從制度到科技全面提升資安防護能力。

有鑑於資安威脅手法日新月異，本公司全面導入防毒、防駭系統，從點到面全面防禦，並定期實施資訊安全教育訓練，提升同仁資訊安全觀念。

為強化資訊安全管理，確保客戶智財權，本公司除訂定相關管理辦法外，並每年接受 TPN 稽核並取得認證。

### 1.4 Password policy：

- (1) 密碼長度必須6碼以上，重點管制區域PC的密碼組合需8碼以上，需包含英文、數字或特殊符號等組合。
- (2) 密碼更新期限為60天。
- (3) 不可沿用前二次密碼。
- (4) 登錄3次失敗會自動鎖住。

### 1.5 Content transfer policy：

- (1) 實體內容(physical content)傳遞必須點交及記錄。
- (2) 數位內容(digital content)只能在管制下封閉型網路傳遞交換。
- (3) 嚴格管制數位內容轉錄於實體的過程。

#### 1.6 Internet policy :

- (1) 禁止使用 p2p (peer to peer)。
- (2) MSN、Skype 禁止傳檔。
- (3) FTP 需經申請，核准才能使用。
- (4) 有 Mail log。

#### 1.7 Security/Piracy Awareness :

新進人員教育訓練中安排 Security/Piracy Awareness 課程。

#### 1.8 Background Checks :

新聘人員須通過犯罪背景調查。

#### 1.9 保全客戶實體智慧財產之管控：

規範在出入廠管理辦法及廠區安全管理辦法、由部門主管定期檢視其部門人員擁有之權限的適宜性、特別定義母帶管理室、Stamper 儲存室、Server room 為 high value areas，區域隔絕，強化安全防範。

#### 2.0 保全客戶數位的智慧財產(Digital assets)之管控：

本公司使用安全性經驗證過的 Aspera 系統，前處理課據以 Download 客戶授權的母源，並將資料儲存於該電腦 HD；另外，如客戶要求採用加密方式，則須比照要求加密儲存(例如：Disney title)。依流程 Aspera 電腦會將完成 Download 的客戶母源燒錄在 DVD-R or CD-R 上，然後交母帶管理室保存。生產流程中，生管將客戶母源自母帶管理室提領出來，交前處理課工作人員將 Title 的內容資料 Upload 到公司網刻區域網路的 N 槽，刻版部自 N 槽取用資料刻版，而品保部則自 N 槽取用資料檢核。電腦及與 N 槽電腦要有 ID guard 側錄監視電腦動作，由單位主管定期查驗 log，記錄以防不當使用。Log 保存 90 天。