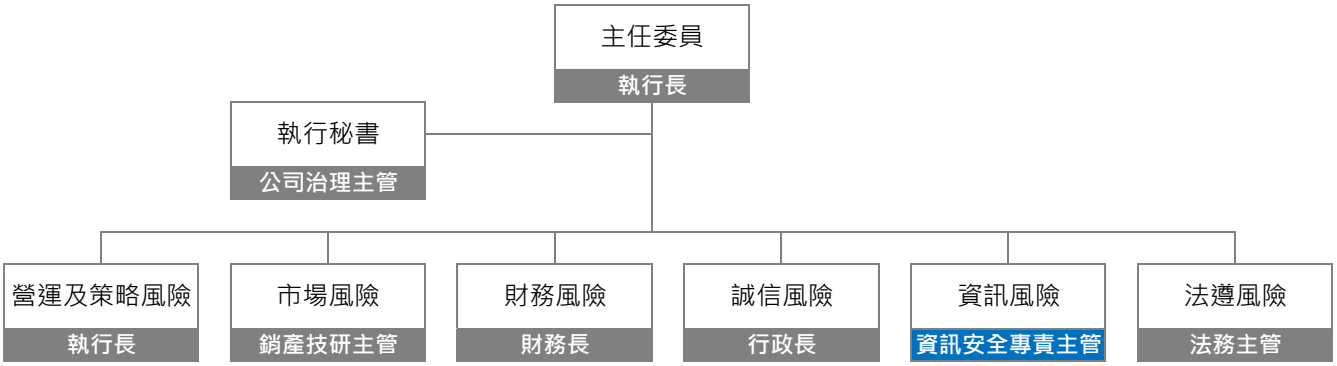
日揚科技股份有限公司
113 年資通安全管理執行情形報告

一、資訊安全管理架構

依據公開發行公司建立內部控制制度處理準則第九條之一第二項規定：公開發行公司應配置適當人力資源及設備，進行資訊安全制度之規劃、監控及執行資訊安全管理作業。符合一定條件者，本會得命令指派綜理資訊安全政策推動及資源調度事務之人兼任資訊安全長，及設置資訊安全專責單位、主管及人員。

本公司目前由智能整合部及資訊部負責資通安全推動，現行資訊管理系統依「公開發行公司建立內部控制制度處理準則」第九條設置內部控制EDP作業制度執行，各項控制作業以ISO 27001、個人資料保護法施行細則、上市上櫃公司資通安全管控指引為參考作業標準，並由資訊單位依組織部門職責負責統籌資訊安全及相關事宜，依據實際管理需求制訂資安政策、訂定管理辦法及策推動與落實。稽核單位依內部控制程序進行內部稽核，定期追蹤改善結果，以降低資安風險。

本公司於111/11/10設置風險管理委員會，由執行長擔任主任委員，並建立資訊風險小組，為資訊安全專責管理單位，並定期每年至少一次向董事會報告資通安全管理執行情形。



二、資訊安全政策

為強化資訊安全，確保所屬之資訊資產的機密性、完整性、可用性與個人資料之要求，以提供本公司之資訊業務持續運作之資訊環境，並符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，本公司於111/9/12制定「資訊安全政策管理辦法」，提供公司全體同仁共同遵循。

為維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。期藉由本公司全體同仁共同努力以達成下列目標：

1. 保護本公司營運活動資訊，避免未經授權的存取，以確保其機密性。
2. 保護本公司營運活動資訊，避免未經授權的修改，以確保其正確性與完整性。
3. 制訂、推動、實施及評估改進資訊安全管理事項，確保本公司具備可供營運持續運作之資訊環境。

4. 辦理資訊安全教育訓練，推廣資訊安全之意識與強化其對相關責任之認知。
5. 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。
6. 實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。
7. 建立本公司營運持續運作計畫，以確保本公司營運服務之持續運作。
8. 本公司之各項營運活動執行須符合相關法令或法規之要求。

三、資訊安全管理方案

為增進本公司資訊安全及穩定之運作，提供可信賴之資訊服務，確保資訊系統之機密性、完整性及可用性，提升用戶端資安意識，實行各項管理作業：

管理事項	作業說明
1. 資訊資產之安全管理	☑ 資產清冊每年定期盤點。 ☑ 重要資產簽訂更新維護保固作業。 ☑ 重要系統及資料進行本地備份、異地備分或雲端備份機制。
2. 人員管理及教育訓練	☑ 持續建立、宣導及推廣員工資訊安全認知，以提升資訊安全 ☑ 新進同仁資訊安全宣導訓練。 ☑ 不定期各類資訊安全宣導。
3. 實體及環境安全管理	☑ 資訊機房安全區域設置有門禁控制，確保只有經過授權人員才許可進入。 ☑ 資訊相關設備，應適當地進行安置、保護、監控，以降低環境威脅所造成的損害，例如環境溫溼度監控。
4. 電腦系統及網路安全管理	☑ 外部及個人電腦網路設備不得私自連接公司網路。 ☑ 企業級無線網路系統，經系統整合驗證機制始能連線。 ☑ 重要資料採檔案加密保護機制。 ☑ 使用專業防毒軟體，並自動更新。 ☑ 設置新世代網路防火牆，設定連線規則，確保使用安全。 ☑ 郵件系統垃圾郵件過戶、病毒威脅防護及主機電腦弱點掃描及重大修補程式更新。
5. 系統存取控制安全	☑ 系統權限依員工職務職能以經權限申請作業後存取。 ☑ 每年定期進行權限覆核作業。 ☑ 設置密碼、鎖定及複雜度等原則。
6. 系統發展、開發及維護之安全管理	☑ 自行開發或委外發展系統，需將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，避免不當危害風險。
7. 營運持續運作	☑ 每年依公司營運持續計畫進行風險評估及災難復原演練規劃，並依計畫進行系統災難復原演練，確保資訊系統之可用性。

四、投入資通訊安全管理資源及執行情形

目前資訊部設置8位人力，負責資訊管理制度、全體公司資訊系統、軟硬體建置，113年各項資安管理作業執行狀況如下：

<table>
<tr><th>項目</th><th colspan="3">執行情形</th></tr>
<tr><td>內部全員資安宣導</td><td colspan="3">☑ 內部EIP公告發布全員資安宣導:
① 網路釣魚陷阱（113/3/27）
② 詐騙郵件提醒（113/7/26）
③ AI軟體與服務可能產生之風險疑慮（113/10/23）
☑ 新進人員資訊安全宣導。
☑ 電子看板常態性資訊安全宣導。
☑ ISO27001 教育訓練（預計113/12進行）</td></tr>
<tr><td>查核作業</td><td colspan="3">☑ 資通安全檢查作業查核（113/1月）</td></tr>
<tr><td>資安演練</td><td colspan="3">☑ 備份系統還原演練（每年至少一次）</td></tr>
<tr><td>聯防組織</td><td colspan="3">☑ 111年已申請核可為TWCERT資安聯盟會員</td></tr>
<tr><td>資安會議</td><td colspan="3">☑ 113年共召開4次資安小組會議，其重點事項：
① 資安風險盤點與監控、建立風險評鑑工作表（113/1/24）
② 外部系統導入資安風險評估（113/04/17、113/8/6）
③ 建立資安架構圖與事件處理流程、第三方資安風險評級（113/7/3）</td></tr>
<tr><td rowspan="6">資安人員教育訓練</td><td>日期</td><td>課程名稱/證書</td><td>時數/人數</td></tr>
<tr><td>113/03/29</td><td>SRAMT資訊安全分析實務-方法、流程與工具</td><td>35H / 1人</td></tr>
<tr><td>113/05/08</td><td>第三方委外與供應鏈資安管理</td><td>3H / 1人</td></tr>
<tr><td>113/06/25</td><td>資訊風險評鑑與風險處理</td><td>3H / 1人</td></tr>
<tr><td>113/09/27</td><td>NSPA 網路安全封包分析</td><td>21H / 1人</td></tr>
<tr><td>113/10/09</td><td>CompTIA Security+ 國際網路資安認證班</td><td>40H / 1人</td></tr>
</table>

五、資安事件

資安指標	資安客訴事件	外部破壞、竊取資料或病毒威脅事件	資訊系統異常或設備異常影響營運事件
113年事件統計	0件	0件	0件