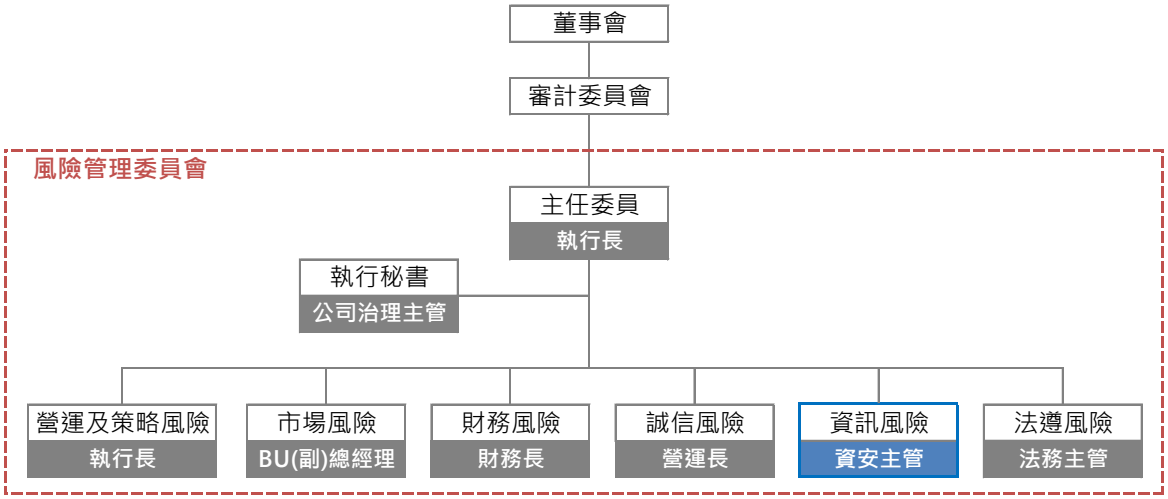
日揚科技股份有限公司
112 年資通安全管理執行情形報告

一、資訊安全管理架構

（一）資安組織架構

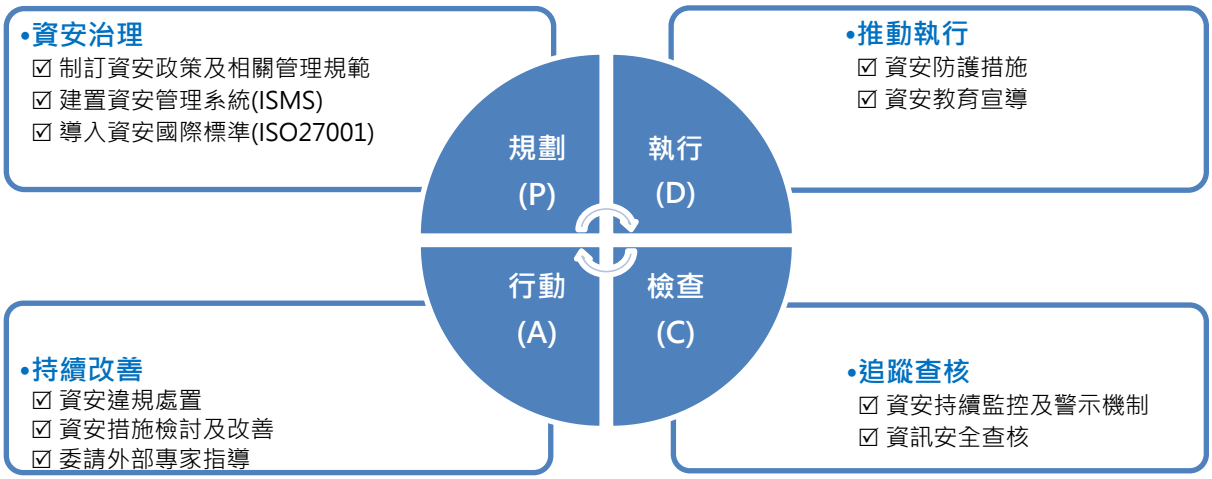
本公司於111/11/10設置風險管理委員會，由執行長擔任主任委員，並建立資訊風險小組，為資訊安全專責管理單位，定期每年至少一次向董事會報告資通安全管理執行情形（112年於112/11/9向董事會報告）。

本公司依規定於112/12/19設置1位資訊安全專責主管及1位資訊安全專責人員，統籌資訊安全及保護相關政策制定，並定期與相關單位主管人員召開會議討論推動機制及工作重點（初期規劃定期每月召開會議，後續依管理需求調整開會頻率）。



（二）企業資通安全風險管理與持續改善架構

為有效落實資安管理，依據規劃、執行、查核與行動（PDCA）的管理循環機制為資安持續改善架構。



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」，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

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：

<table>
<tr><th>項目</th><th colspan="3">112年執行情形</th></tr>
<tr><td>資安宣導</td><td colspan="3">於公告系統發布，執行全員資安宣導：
☑ 網路安全5招基本功（112/3/28）
☑ 普發6000 慎防釣魚網站（112/4/7）
☑ 個資三惡意行為(112/10/6)</td></tr>
<tr><td>查核作業</td><td colspan="3">資通安全檢查作業查核（112/1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">經申請核可為TWCERT資安聯盟會員（111已加入）</td></tr>
<tr><td>資安會議</td><td colspan="3">112召開2次風險管理委員會，於第1次會議（112/4/27）報告資安議題，重點事項：
☑ 112年主管機關對上市櫃的資安要求。
☑ 資訊安全框架 / 導入流程 / 管制方法及應用資訊產品評估。
☑ 依ISO27001架構建立資安管理系統。</td></tr>
<tr><td rowspan="10">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>111/7/12</td><td>工控資安環境認知課程</td><td>3小時, 1人</td></tr>
<tr><td>111/8/5</td><td>中堅企業及產業資安-資安管理與維運班</td><td>24小時, 1人</td></tr>
<tr><td>111/9/7</td><td>ISO 27001:2013資訊安全管理系統- 初階訓練課程</td><td>14小時, 1人</td></tr>
<tr><td>112/4/19</td><td>智慧製造企業資安實務研討會</td><td>3小時, 1人</td></tr>
<tr><td>112/6 月</td><td>iPAS 經濟部產業人才能力鑑定：資訊安全工程師-初級能力</td><td>鑑定合格</td></tr>
<tr><td>112/8 月</td><td>EC-Council CCT 網路安全認證技師課程</td><td>40小時, 1人</td></tr>
<tr><td>112/8/25</td><td>資安實務案例教育宣導-詐欺防治</td><td>1.5小時, 15人</td></tr>
<tr><td>112/8/30</td><td>資安領域專班-網路安全分析與防護課程</td><td>12小時, 1人</td></tr>
<tr><td>112/10/26</td><td>SEMI E187:半導體產線設備資安標準規範</td><td>3小時, 23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
112年事件統計(件)	0件	0件	0件