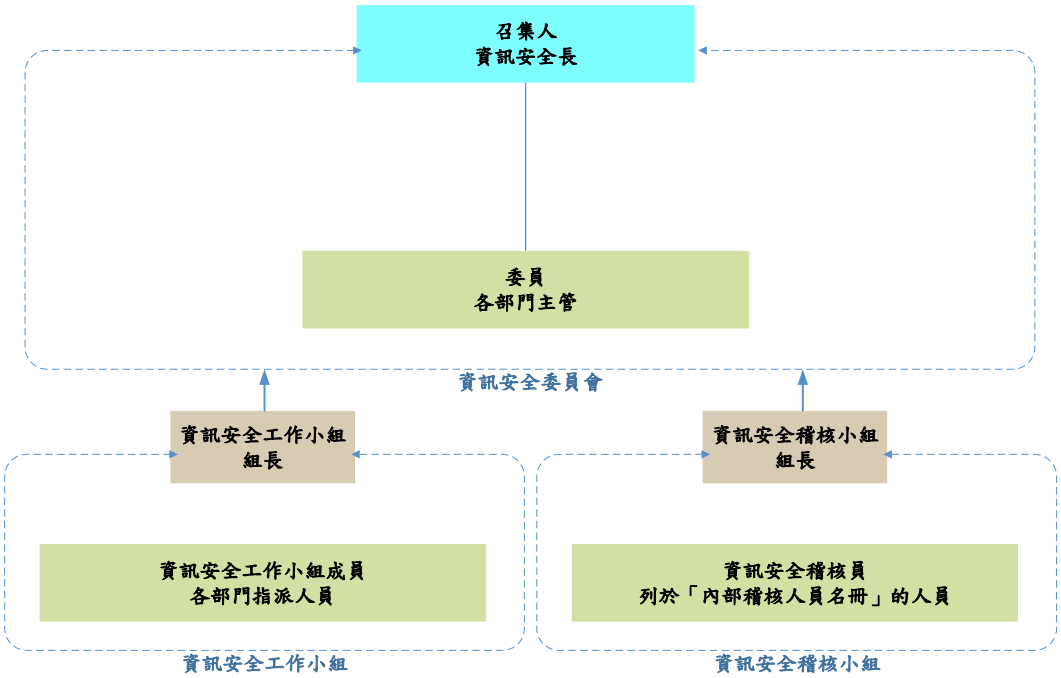
萬潤科技股份有限公司

資訊安全風險管理架構

(一)本公司於 113 年 12 月依據 ISO/IEC 27001:2022 國際標準之要求導入資訊安全管理制度，並於 114 年 3 月發布實施。為推動與治理本公司資訊安全管理制度之各項工作，設立管理制度運行組織，並明訂管理制度組織運作方式與工作職責，以確保管理制度之各項作業活動能持續、有效地運作。說明如下:

1. 資訊安全管理組織



2. 資訊安全管理組織權責說明

2-1　資訊安全長，由董事長特助擔任，權責如下:

2-1-2　核准管理制度政策及目標。

2-1-3　整合管理制度需求和組織流程。

2-1-3　確保管理制度所需資源之可用性。

2-1-4　溝通有效的資訊安全管理和符合管理制度需求之重要性。

2-1-5　確保管理制度達成預期之結果。

2-1-6　指導與支持人員對管理制度之有效性做出貢獻。

2-1-7　倡導持續改善。

2-1-8　支援其他相關管理制度角色，以展現他們之領導，符合所負責之

領域。

2-2　資訊安全管理委員會，由本公司各單位主管共同組成，權責如下:

2-2-1 管理及監督資訊安全工作小組於管理制度推行之狀況與績效。

2-2-2 審查管理制度政策與目標。

2-2-3 召開管理審查會議，瞭解管理制度之績效。

2-3 資訊安全工作小組組長，資訊部主管擔任，負責管理制度活動之執行。

2-4 資訊安全工作小組，由各單位主管指派人員共同組成，負責執行資訊安全管理制度之各項作業活動。

2-5 資訊安全稽核小組組長，由資安長指派，負責規劃資訊安全稽核作業及追蹤資訊安全稽核發現之改善。

2-6 資訊安全稽核小組，小組成員由稽核小組組長於資訊安全內部稽核活動執行前，選擇各單位符合資訊安全內部稽核資格之人員組成，負責執行資訊安全稽核作業。

3. 資通安全政策

本公司之資訊安全管理政策為「提供持續運作之資訊服務，確保資訊服務及資訊之機密性、完整性及可用性，符合法令、法規、合約及客戶需求，達成本公司營運之目標。」。

資訊安全管理政策經資訊安全長審查核准後，發佈實施。資訊安全政策之發佈更新，應讓本公司同仁知悉，並依據需求，讓關注方了解本公司資訊安全管理政策之要求。

4.具體管理方案：

依據資訊安全管理制度之要求，執行各項資訊安全作業。為符合資安政策與管理制度各項績效指標之要求，建立全面性的資安防護，113-114 年度推行的管理事項及具體管理方案如下：

① 採用新世代防火牆，內/外網採取分級制，人員僅能存取一般服務，特殊服務需申請權限，並將記錄留存。

② 郵件伺服器加裝垃圾郵件閘道器，及選購社交工程防護、防詐騙、防毒模組，過濾有害郵件。

③ 導入端點安全防護系統，落實外接設備管控，對可攜式儲存媒體訂有管制標準，記錄使用者上網、檔案存取行為，資訊設備資產盤點並導入 MDR 防駭軟體，24 小時監控及防護。

④ 機房端使用一般防毒並導入進階 MDR 防駭軟體，並 24 小時監控及防護。

⑤ 獨立備份區域，搭配備份軟/硬體，將資訊機房電腦資料定期備份，僅有備份服務能存取該區域，降低駭客風險。

⑥ 帳號分權管理，一般人僅有最小權限，如需特殊權限須經申請核准備查，帳號均強制要求定期變更密碼，密碼強度拉到最高，降低風險。

⑦ 定期進行資安教育訓練，內化資安防護警覺性，提升人員資安意識。

⑧ 加入科學園區資安資訊分享與分析中心(SP-ISAC)，掌握可能的資安威脅與弱點資訊，以利管理和及早因應。

⑨ 導入資安監控中心/SOC，提供 24 小時威脅偵測及防護。

4.投入資通安全管理之資源：

資訊安全已為公司營運重要議題，對應資安管理事項及投入之資源方案如下：

① 專責人力：設有資訊安全專責主管及資安專責人員，負責公司資訊安全規劃、技術導入與相關的稽核事項，並由內部稽核定期查核，若發生缺失，旋即要求受查單位改善並追蹤改善結果，以降低內部資安風險。已完成上市櫃公司資安專責人力申報作業。

② 資訊管理體系導入：自民國 113 年決定投入 ISO27001 資訊安全管理體系的認證，預定於 114 年底前通過第 3 方稽核驗證。使資訊系統皆能在標準的管理規範下運作，降低因人為疏失所造成的安全漏洞及生產異常，也透過年度的複審作業，不斷持續改善。

③ 客戶滿意：無重大資安事件，無違反客戶資料遺失之投訴案件。

④ 資安公告及宣導：對所有員工及新進員工，公告傳達資安防護相關規定與注意事項。

⑤ 資訊安全設備與服務:預定建置及導入資訊安全設備與服務，如:DLP、MDR、SOC、EMM 等，使資訊安全作業之執行更有效率及效度。

5.資安教育：

① 113 年 11 月，執行 ISO/IEC 27001:2022 條文說明，使同仁了解國際標準之要求。

② 114 年 1 月，執行組織全景分析、資訊資產盤點、風險評鑑作業訓練，使同仁了解全景分析、資訊資產盤點及風險評鑑作業之執行，以識別重要之資產及需要改善之風險。

③ 114 年 1 月，執行 ISMS 活動實施之彙整說明，使同仁了解 ISMS 各項作業活動之執行內容及活動紀錄之產出。

④ 114 年 3 月，執行資訊安全內部稽核訓練，使同仁了解資訊安全內部稽核活動之執行，以利於了解 ISMS 活動之落實程度。

(二)列明最近二年度及截至公開說明書刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：

於 114 年 4 月 20 日發現部份主機與電腦，遭受駭客網路及病毒攻擊。事發當下已立即啟動防禦機制及備援機制，封鎖內部網路與外部網路的連接，重建受駭主機，全面佈署 MDR 與資安防護軟體。