資訊安全風險管理

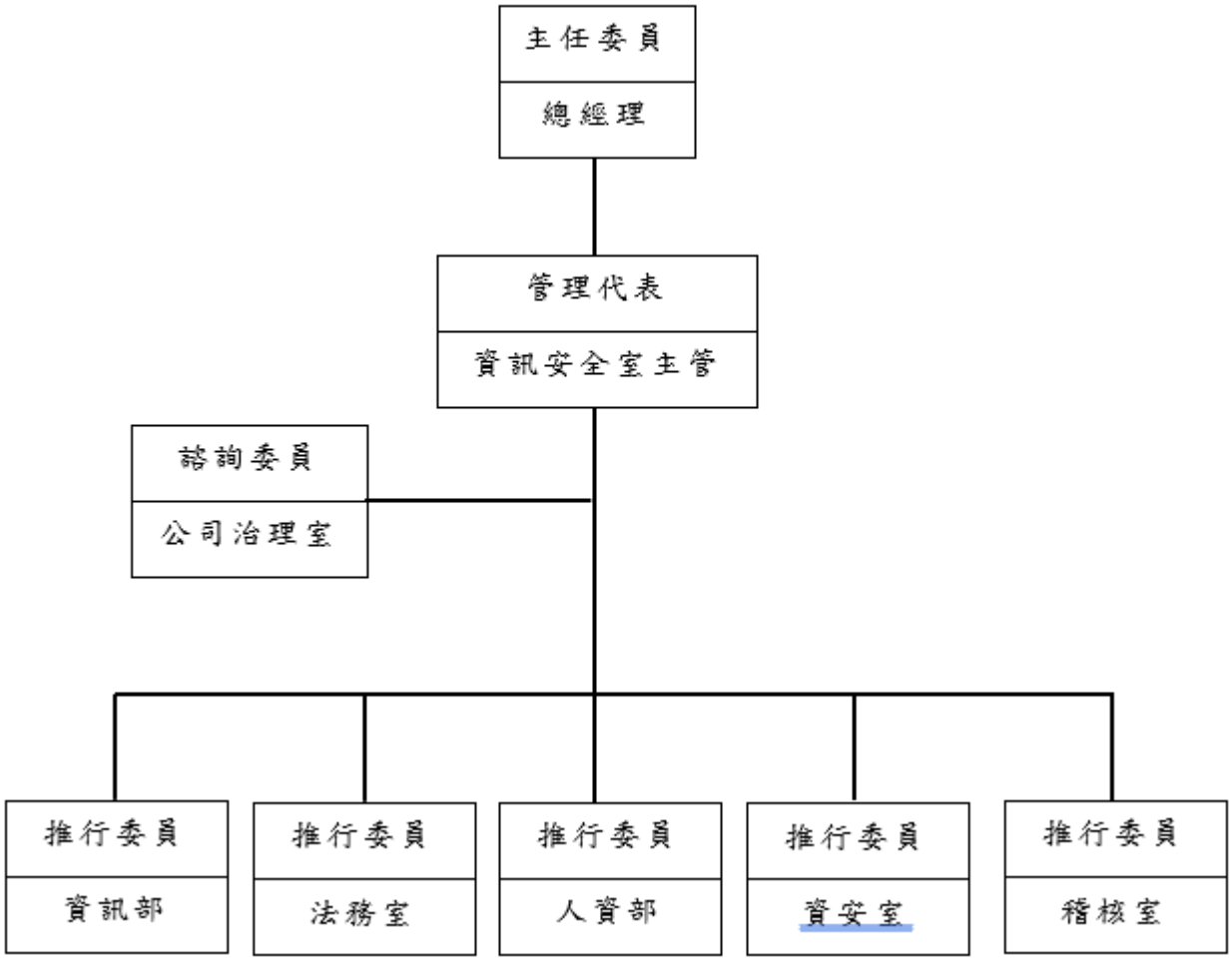
一、資訊安全目的與範圍：

對象：員工，客戶，供應商和股東以及營運相關資訊軟硬體設備。

範圍：為確保本公司資訊安全，訂定本公司「資訊安全政策」，及資訊安全相關程序文件制定應用技術和數據安全標準，並納入資訊安全管理運作體系，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與資訊安全維護。

二、資訊安全風險管理架構

資訊安全委員會組織圖



1.105 年 3 月起成立**「台燿科技資訊安全管理委員會」**，每年定期召開一次或視實際需要不定期召開「資訊安全管理委員會議」，負責審視公司資安治理政策、監督本公司資安管理運作情形。

110 年度「資訊安全管理委員會議」於 110 年 8 月 20 日召開。

111 年度「資訊安全管理委員會議」於 111 年 9 月 1 日召開。

112 年度「資訊安全管理委員會議」於 112 年 9 月 1 日召開。

113 年度「資訊安全管理委員會議」於 113 年 9 月 3 日召開。

114 年度「資訊安全管理審查會議」於 114 年 8 月 15 日召開。

2.112 年 12 月 13 日董事會決議通過，設置資訊安全室為公司資訊安全專責單位，指派總經理擔任資訊安全專責主管及周孝勇資深工程師擔任資訊安全專責人員，進行資訊安全制度之規劃、監控及執行資訊安全管理作業。

三、資訊安全政策

資訊安全政策:

維護公司資訊之機密性、完整性、可用性與適法性，避免發生人為疏失、蓄意破壞與自然災害時，資訊與資產遭致不當使用、洩漏、竄改、毀損、消失等，影響本公司作業，並導致公司權益損害。

四、具體管理方案

1.規劃導入 ISO 27001 資訊安全管理系統，預計 114 年度取得第三方驗證，規劃透過 ISO27001 資通安全管理系統之導入，強化資通安全事件之應變處理能力，保護公司與客戶之資產安全。

2.113 年 2 月加入台灣 CERT/CSIRT 聯盟，獲取國際資訊安全情資、資安聯防。

3.公司不斷提升資訊網路安全防護能力，並保證將網路攻擊入侵之發生機率降至最低，並且資訊系統架構依其風險等級建立高可用性之異地主機備援及資料備份機制，以確保服務不中斷，並將備份媒體上傳至受國際機構認證之雲端資料庫保管存放，加強機房各項模擬測試與緊急應變等演練以確保資訊系統之正常運作及資料保全，可降低無預警天災及人為疏失造成之系統中斷風險，確保符合預期系統復原目標時間。

4.辦理營運持續管理(Business Continuity Management)，透過營運衝擊分析，由內部單位鑑別出各項業務關鍵流程與對應支援的資訊系統服務，評估其交易量、業務功能重要性，以及對財務面、法令規章、客戶等層面之營運風險與衝擊，計算出風險值，並依據風險等級，規劃設計與提升適當軟硬體設備 資源、改善作業流程等因應措施。

5.針對員工定期辦理資訊安全教育訓練(每年至少一次)及不定期網路安全宣導。

110 年度資訊安全教育訓練舉辦時間:110 年 12 月 受訓人數:739 人

111 年度資訊安全教育訓練舉辦時間:111 年 12 月 受訓人數:709 人

112 年度資訊安全教育訓練舉辦時間:112 年 12 月 受訓人數:683 人

113 年度資訊安全教育訓練舉辦時間:113 年 12 月 受訓人數:689 人

114 年度資訊安全教育訓練舉辦時間:114 年 8 月 受訓人數:686 人

五、最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施

113 年度及 114 年度，本公司並未發生任何重大的網絡攻擊或事件，已經或可能將對公司業務及營運產生重大不利影響，也未曾涉入任何與此有關的法律案件或監管調查。