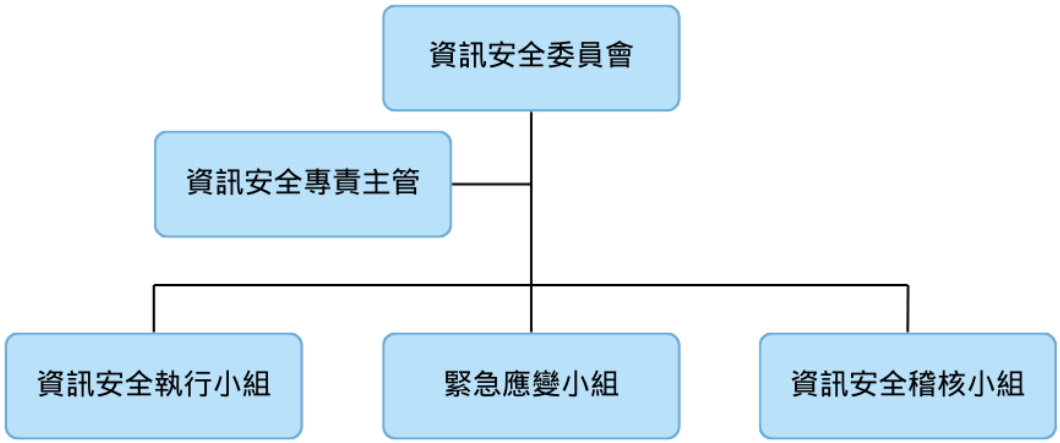
連騰科技股份有限公司
資訊安全政策

資通安全管理

一、資通安全管理策略與架構：

連騰科技股份有限公司為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部蓄意或意外之威脅，業已訂定「資訊安全政策」、「資訊安全管理內部控制制度」及「安全事件管理程序書」等辦法，並組成「資訊安全委員會」，確保資訊安全管理制度執行之有效性，以增進業務運作之安全。

連騰科技股份有限公司已於 114 年 7 月 5 日取得 ISO/IEC 27001:2022 證書，此證書的有效期自 114 年 07 月 05 日至 117 年 7 月 05 日且其有效性應繫於持續符合的定期稽核，從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求、最高規格的機密資訊保護服務。資訊安全委員會架構工作執掌:



資訊安全委員會：為任務編組方式組成，資訊安全專責主管擔任召集人由本公司資訊部部門主管擔任，如因職務調動應即刻指派遞補人員與辦理交接。

資訊安全執行小組：資訊安全委員會指派人員組成，負責規劃及執行各項資訊安全作業。

緊急處理小組：由公司各關鍵業務流程負責人組成。

資訊安全稽核小組：由資訊安全委員會指派，負責評估資訊安全管理制度之執行情形。

二、資通安全政策

(一)資訊安全政策願景：

1.強化人員認知、避免資料外洩。

2.落實日常維運、確保服務可用。

(二)依據資訊安全政策願景，擬定資訊安全目標如下：

1.辦理資訊安全教育訓練，推廣員工資訊安全意識與強化相關責任之認知。

2.保護本公司業務活動資訊，避免未經授權的存取與修改，確保其正確完整。

3.每年定期進行稽核作業，確保相關規定皆能落實執行。

4.確保本公司關鍵核心業務維持一定水準的系統可用性。

針對上述資訊安全目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間、評估方式與執行結果，相關監督與量測程序，應遵循本公司「監督與量測管理程序書」辦理。資訊安全執行小組應於管理審查會議中，針對資訊安全目標有效性量測結果，向資訊安全委員會召集人進行報告。

(三)企業資訊安全風險管理與持續改善架構

系統運作過程中發生之缺失及潛在之風險，採取相關的矯正及持續改善措施，以防止類似事件發生，進而達成持續改善之目標。

資訊安全委員會：負責矯正與持續改善措施之管理審查。

缺失權責單位　：負責稽核所發現缺失、資訊安全事件（含重大異常事件）或自行發現缺失之原因分析，決定優先順序與處理時限，提出矯正或持續改善措施並實施。

(四)具體管理方案

1.安裝防毒軟體，定期執行電腦掃瞄與 Windows 系統的漏洞更新。

2.導入應用層防火牆，管控內部和外部網路的流量，強化網路安全。

3.導入電信公司的網路線路入侵防護服務，提高資安防護。

4.導入檔案加解密系統，保護研發圖檔，避免公司的智慧財產遭受損害。

5.每年舉辦資訊安全教育訓練，提昇員工資安意識。

6.要求與公司合作的資訊系統廠商簽訂保密切結書。

7.加入 TWCERT(台灣電腦網路危機處理暨協調中心), 獲取資安情資與參加資安宣導活動，厚植企業資安認知。

三、資通安全風險與因應措施：

資訊安全的威脅與攻擊不斷的推陳出新，連騰科技股份有限公司雖然已建立全面的網路與電腦相關資安防護措施，仍無法保證資訊安全相關的控管措施能完全避免來自任何第三方癱瘓系統的網路攻擊。為確保營運持續運作，並降低關鍵性業務流程受重大故障或災害之影響，訂定「營運持續運作管理程序書」。

(一)營運持續運作管理

連騰科技股份有限公司實施營運持續運作管理作業，結合預防和復原控制措施，將業務災害或故障（如自然災害、意外、設備故障和蓄意行為等）造成的中斷情形降低到可接受的範圍。

連騰科技股份有限公司分析業務災害或故障對公司之衝擊，並發展和實施「營運持續運作計畫」，確保能在所需時間內恢復業務運作。

營運持續運作程序須每年測試演練，以確保計畫之有效性，並使相關人員確實瞭解計畫之最新狀態。測試計畫得以定期測試個別計畫之方式進行。

「營運持續運作計畫」應視業務、本公司及人員的調整需求而定期更新，以確保計畫之有效性。

(二)災害現場蒐證與清理

災害現場搶救完成後，緊急處理小組需指派相關人員進行災害現場鑑識與蒐證工作，以做為日後訴訟索賠之依據。鑑識蒐證工作如有需要，應配合相關單位（如消防單位、警察單位等）進行。鑑識蒐證完成後，始可進行現場清理。

(三)事件處理檢討

事件處理完成後，緊急處理小組須召開檢討會議。檢討事件通報、應變處理與復原作業各階段運作是否達成本程序預定目標，並依據「矯正及持續改善管理程序書」辦理。檢討結果呈報資訊安全委員會，並做為修訂「營運持續運作管理程序書」的重要依據。

四、 投入資通安全管理之資源

資訊安全為公司治理與營運的重要議題，本公司於資訊安全管理事項及投入之資源方案如下：

1.專責人力：

(1) 設立資訊安全委員會，負責公司資訊安全管理與規劃、資訊安全系統導入與相關的稽核事項，以維護及強化資訊安全。

(2)資訊安全專責主管 1 名，資訊安全執行小組成員 3 名，資訊安全稽核小組成員 3 名，緊急處理小組成員 3 名。

2.投保資安險金額:無

3.113 年 2 月 16 日執行資訊安全管理制度內部稽核(每年執行 1 次)，無重大缺失。

4.113 年 2 月 23 日執行資訊安全管理審查會議(每年執行 1 次)，無重大異常，要求持續落實資訊安全措施。

5.認證：114 年 7 月 5 日取得 ISO/IEC 27001:2022 證書，此證書的有效期自 114 年 7 月 05 日至 117 年 7 月 05 日且其有效性應繫於持續符合的定期稽核。

6.客戶滿意：

(1)無重大資安事件，無違反客戶相關資料遺失之投訴案件。

(2)要求與公司合作的資訊系統廠商簽訂保密切結書。

7.教育訓練：每年舉辦資訊安全教育訓練，提昇員工資安意識。

8.資訊系統:

(1)安裝防毒軟體，定期執行電腦掃瞄與 Windows 系統的漏洞更新。

(2)導入應用層防火牆，管控內部和外部網路的流量，強化網路安全。

(3)導入電信公司的網路線路入侵防護服務，提高資安防護。

(4)導入檔案加解密系統，保護研發圖檔，避免公司的智慧財產遭受損害。