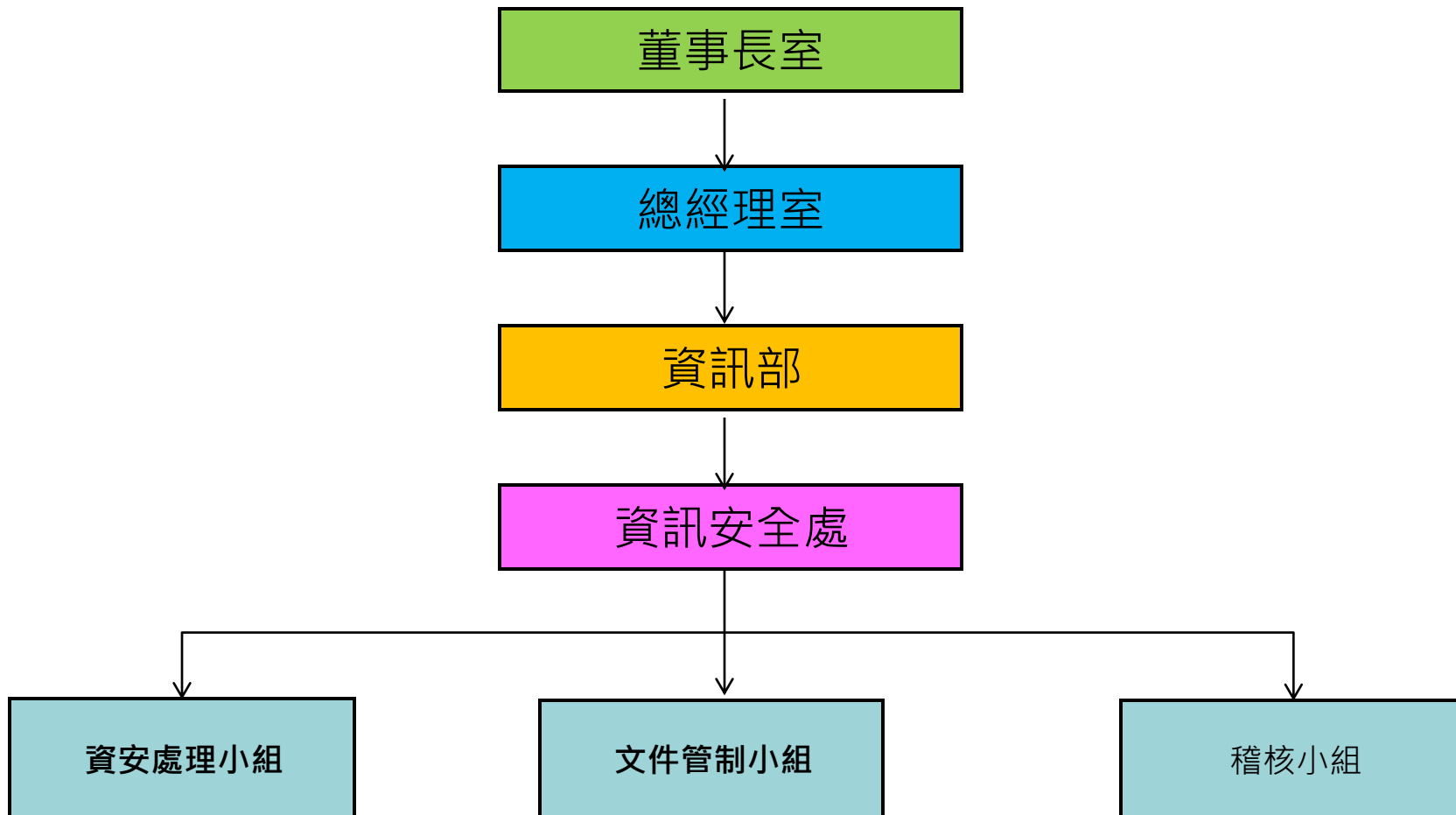


- 設立資訊安全委員會，督導本公司資訊安全管理制度、技術標準及維運作業之推行，由總經理擔任主任委員，作為本公司推動資訊安全之承諾。本公司資訊安全之權責單位為資訊部，設置資訊主管乙名擔任執行秘書，資訊部下成立資訊安全處，指派主管一人擔任資訊安全主管，統籌資訊安全事宜。
- 本公司稽核室執行年度稽核計畫，會將資訊安全列入稽核重點，並將結果報告公司董事會。



資訊安全政策

為貫徹執行本公司資訊安全管理制度、確保其運作有效性並持續監督管理，以維護重要資通系統之機密性、完整性與可用性，特訂定資訊安全管理政策。本政策旨在提供同仁資訊作業之明確指導原則，所有同仁皆有義務積極參與推動，以確保本公司之資料、資訊系統、設備及網路安全維運，達持續營運的目標。

(1)落實資訊安全，強化服務品質

全體同仁應落實執行資訊安全管理制度之所有資訊作業相關措施，確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，而遭受洩密、破壞或遺失等風險，應選擇適切的保護措施，將風險降至可接受程度並持續進行監控、審查及稽核，以強化服務品質，提升服務水準。

(2)加強資安訓練，確保持續營運

應因應資訊安全威脅情勢變化，每年持續進行適當的資訊安全教育訓練，以提高同仁之資訊安全意識，同仁亦應確實參與訓練，建立同仁「資訊安全要做好，風險評估不可少」的觀念，促使同仁了解資訊安全重要性，遵守資訊安全規定，提高資訊安全緊急應變能力，降低資訊安全風險，達持續營運之目標。

(3)做好緊急應變，迅速災害復原

應訂定重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變流程的演練，以確保資通系統失效或重大災害事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。

具體管理方案

- 依個人工作職權需求，設定帳號存取權限，由系統管理人員專責處理。
- 同仁外出時需使用SSLVPN方式連線並啟用MFA，登入密碼定期更換。
- 僅允許合規之電腦可存取公司資源。
- 定期派送Windows作業系統更新程式。
- 公司電腦皆需加入網域、安裝防毒軟體、資產管理、網路存取控制、軟體授權管理。
- 無線網路啟用802.1X身分驗證。
- 檔案伺服器啟用稽核紀錄。
- 定期執行系統備份、備份異地存放及系統還原演練。
- 加入資安情資分享平台，及時更新資安情資。
- 合作廠商皆需簽訂保密合約。

投入資源

本公司雖未投保資訊安全險，但高度重視資訊安全之預防及管理，投入的資源如下：

- 通過ISO27001 2022資訊安全管理系統驗證。
- 建置網路防火牆、雲端管理交換器及無線網路基地台、企業網路存取管制、郵件防毒、垃圾郵件過濾、安裝防毒軟體、員工VPN多因子認證及SSL加密。
- 定期使用弱點掃描工具對系統和網路設備進行檢測，找出所有已知的風險與漏洞，並進行各項Patch修補與弱點修正，縮小系統和網路的受攻擊面範圍，避免遭受惡意入侵、原始碼檢測、重要的系統或服務建置本地端及異地端備援機制。
- 每年定期委託第三方專業單位進行滲透測試，降低人為因素或自然因素之影響對公司營運所造成的衝擊。其目的為瞭解、評估組織網路環境及系統安全狀況，驗證目前資安防護的安全等級與成效，做為漏洞補強、改善方法、加強系統的安全性。
- 定期社交工程演練，模擬駭客的釣魚郵件，檢測員工資安風險意識，輔以資安宣導及教育訓練。
- 定期發布資安電子報，包含最新資安趨勢與近期國內外重大資安事件，藉此提升同仁對於資安的意識及警覺性。
- 每年進行ISO 27001 ISMS內、外部稽核、風險評鑑及營運衝擊分析。
- 執行年度資訊系統災害還原演練。
- 使用SIEM系統來強化資安防護，透過數據蒐集與集中分析、全面性威脅監控及資安事件可視化，來保障網路安全。
- 使用MDR服務快速發現並應對可疑行為及安全事件。
- 導入原始碼掃描工具，定期對開發的程式碼進行檢測。

資訊安全認證(ISO 27001)

- 本公司為強化資訊安全事件之應變處理能力，保護公司與客戶之資產安全，導入ISO 27001資訊管理系統並取得認證(證書如下)，認證效期自2024年11月1日起，至2027年10月31日止。

TÜV NORD

Certificate

Management system as per
ISO/IEC 27001:2022

The Certification Body TÜV NORD CERT GmbH hereby confirms as a result of the audit, assessment and certification decision according to ISO/IEC 27006:2015/Amd.1:2020, that the organization

Senao Networks, Inc.
No. 500, Fusing 3rd RD., Hwa-Ya Technology Park,
Kuei-Shan Dist., Taoyuan City 33383, Taiwan, R.O.C.



operates a management system in accordance with the requirements of ISO/IEC 27001:2022 and will be assessed for conformity within the 3 year term of validity of the certificate.

Scope

Information Security Management activities of IT department including of :

- Information systems infrastructure management, including of Server Room and Networking service.
- System operation, development and maintenance including of ERP, SFCS, EFGP BPM, File Server and Git Server.

As per the Statement of Applicability of 2024-07-09, version 05

Certificate Registration No. 44 12121820004
Audit Report No. IT312-R1

Valid from 2024-11-01
Valid until 2027-10-31
Initial certification 2021-11-01



Visit our database to
verify the validity of
this certificate.

Taipei, 2024-09-23

Lie-Jeng Chang
Certification Body at TÜV NORD CERT GmbH

TÜV NORD CERT GmbH
Am TÜV 1, 45307 Essen
tuv-nord-cert.de



TÜV®