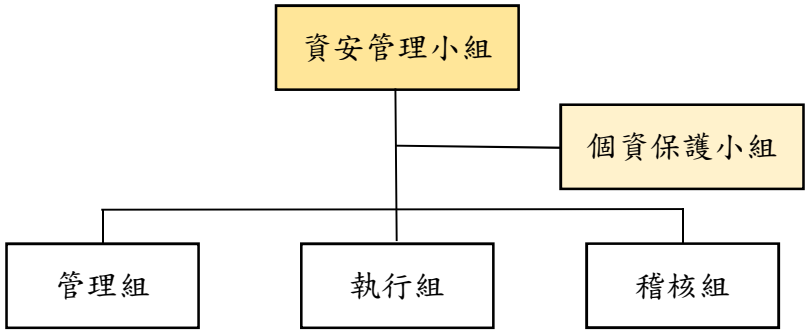
宜進實業‧資通安全治理

宜進實業股份有限公司（以下簡稱本公司）於 94 年成立「資安管理小組」，以統籌辦理本公司資通安全管理事務，目前由總經理室副總經理擔任主管，督導資安政策之落實及資安措施之執行，協調各項資源分配，提升資安之防禦能力及抗擊韌性，建立同仁安全的資訊作業觀念，降低整體之資安威脅及風險，並定期向董事會提報年度之執行情形。

資通安全管理組織架構

本公司設置「資安管理小組」，以資訊安全政策為規範，其職責在強化資訊安全管理，保護本公司資訊資產，防範本公司內部或外部以及來自人為、蓄意或意外之破壞；其組織架構如下說明。



1. 資安管理小組：其下由管理、執行、稽核三個常務單位組成，並得視任務之需要，設置次級之功能性單位；主管由小組中最高層職級之副總經理以上人員擔任，負責核定各項事務；組織權責包括審查/制定資訊安全政策、個人資料保護管理辦法，規劃/推動各項資訊安全措施之實施，督導/稽查執行措施之可行性及有效性，評估整體之資安威脅及風險，以使資訊安全管理循 P.計畫-D.執行-C.檢核-A.改善行動 持續的良性運作。
2. 管理組：由總經理室經(副)理級以上主管組成，負責管理、協調、核定，目前 1 名專責人員並擔任資安主管。
3. 執行組：由資訊單位人員組成，負責聯絡及執行資安之相關措施，目前 1 名專責人員。
4. 稽核組：由稽核單位人員組成，負責定期稽查資安之相關執行成效，目前 1 名專責人員。
5. 個資保護小組：設置召集人及執行幹事各一人，得由資安管理小組之成員兼任；組員由本公司個人資料之承辦人員或經指定之專人兼任之，辦理個資保護之相關業務，目前 4 名專責人員。

資訊安全政策

目的	為強化資訊安全管理，保護本公司資訊資產，免於遭受來自於本公司內部或外部以及來自人為、蓄意或意外之破壞。
目標	確保本公司業務相關電腦資訊資料、系統、設備及網路之安全，避免因人為疏失、蓄意破壞或自然災害等風險，使資訊資產遭不當使用、洩漏、竄改、破壞等情事，而影響電腦作業系統正常運轉或損及公司權益。

實施範圍	1.資訊安全政策制定及評估 2.資訊安全組織及權責 3.人員安全管理及教育訓練 4.資訊資產之控管 5.實體及環境安全管理	6.通訊與操作管理 7.系統存取控制 8.系統開發及維護之安全管理 9.永續運作計畫 10.內部稽查及其他
審查	本政策每年進行一次獨立及客觀的評估，並視評估結果及必要性，做適當修訂，以反映本公司資訊安全管理政策、相關法令規範、資訊技術環境及業務之最新狀況；需修訂內容經資安管理小組成員共同審定後，由資安管理小組主管核定實施。	

資安風險管理運作

本公司資訊安全管理以內部控制為根基，謹慎衡量公司發展的需要與期望，依據經營管理階層對營運宗旨與企業價值之共識，針對核心業務流程及重要工作項目，界定各項資通安全之作業方針，並據以實施運作，對已知之威脅採取適當之處理方法，對潛藏之威脅盡可能予以事前分析及鑑別，以提升本公司承受外部攻擊之防護能力及容忍底線,減緩衝擊等級及降低可能造成的損害,妥善因應風險。

項次	資安管理分類	重要管控措施	執行頻率
1	資訊安全政策	‧明定資安組織、權責及事件之通報、處理綱要。	檢視1次/年
		‧定期審查、修訂資訊安全政策。	
		‧資通安全治理執行成效及風險評估，並向董事會提報。	彙編1次/年
		‧配合政府法規及國際相關準則，研議資訊安全管理相關辦法，規範內部執行事項。	不定期
2	建立資訊安全組織	‧設資安管理小組及個人資料保護小組，定期開會討論資安相關事宜。	至少1次/半年
		‧訂立資安事件之緊急應變處理及回報程序，由資安管理小組統籌管控。	不定期
		‧派員參與資訊安全之研討會及相關課程。	
3	人員安全與管理	‧內部控制制度定義資訊人員、使用者之作業權限劃分，及人員異動、離職之作業準則。	檢視1次/年
		‧定期執行作業權限複核。	至少1次/半年
		‧資訊管理系統的密碼實施複雜性原則檢查，定期要求變更。	變更1次/半年
		‧定期普查個人電腦，防止公器私用。	執行1次/年
4	資產分類與控管	‧核心業務之資訊軟、硬體資產定期盤點及列冊管理。	執行1次/年
		‧重要的伺服器、資訊系統每年簽訂委外維護合約，確保持續運作。	1次/年
5	實體及環境安全管理	‧專用電腦機房具獨立空調、溫度自動控管及消防設施。	每日檢視
		‧使用不斷電系統保障電源之緊急供應，並定期保養、檢測。	保檢1次/年
		‧伺服器及個人電腦安裝防毒軟體，重要職務之電腦，每日定時備份，其備份份數至少二代。	每日、每週執行
		‧營運資料庫採雙主機即時備援，每半年定期模擬事故演練後輪替運作。	切換1次/半年
		‧對重要伺服器或網路設備定期弱點掃瞄。	執行1次/週
6	通訊與操作管理	‧電子郵件主機具自我防護及保存稽核之功能，並在雲端使用Hinet郵件守門員過濾可疑、惡意郵件。	每日執行

		・設置閘道防火牆並分析紀錄，並使用趨勢雲端防護軟體分析、記錄上網行為，即時防堵內、外部異常行為。	每日檢視
		・使用 Hinet 資安艦隊之防駭守門員、先進網路防禦等服務，擴展防禦的廣、深度，防堵內、外之攻擊。	每日執行
		・DDOS 分散式阻斷防護機制，過濾、清洗電路流量。[Hinet，必要時用]	連續 3 天/年
		・電子郵件社交工程演練，模擬釣魚郵件，訓練可疑郵件之察覺能力。	1 次/半年
		・即時宣導資安事件、通告或案例，提升防護意識。	至少 1 次/季
7	存取控制	・電子檔資料依部門、個人設定存取權限。	每日執行
		・對外連線作業申請需經部門主管同意及副總級以上主管核准。	有需求時執行
		・電子郵件區分權限，不須對外連絡者僅能內部寄信。	有需求時執行
		・人力資源系統於讀取個資時，自動記錄存取軌跡。	每次存取時執行
8	系統開發與維護	・自行開發、維護的資訊管理系統，在規劃分析時主動將安全需求納入設計考量，防範外部的侵入篡改，並限制特權帳號之使用對象。	有需求時執行
		・資訊管理系統的程式在修改前留存備份，於程式開頭註記修改資訊；修改後，經權責主管複核後上線。	
		・系統開發文件限制存取權限，非開發人員不得編輯。	
9	永續運作之計畫管理	・營運資料庫主機每半年定期模擬事故演練、測試。	1 次/半年
		・重要設備訂立緊急應變計劃，供發生重大資安事件時遵循及應變。	需要時執行
		・各項防護措施之數據指標化，供評估運作之風險及研討因應措施。	每日
10	內部稽查及其它	・每年電腦普查時公告公司軟體所授權之範圍，授權以外之軟體則要求移除或提供授權證明；由平日異動及普查結果，更新核心業務之資產狀況	普查 1 次/年 資料隨時更新
		・資訊單位定期自評資訊作業環境安全。	自評 1 次/年
		・配合稽核單位定期自評資訊控制作業。	自評 1 次/年
		・內部稽核人員及會計師團隊每年定期稽查資訊控制作業之執行情形。	每年至少一次

2023 年執行摘要及投入資源

本公司從系統面、技術面、程序面建立端點、閘道到網際網路的多層資安管控措施，持續導入資安防禦技術，將資安控管機制整合於軟硬體維運、作業流程、系統監控及查核改善，以維護公司資訊財產的安全性及完整性；本年度執行及投入資源重點列示如下：

- 資通安全治理暨風險評估報告於 1 月完成，並於 2/22 董事會提報。
- 資安管理小組於 2、9 月共召開 2 次會議，討論資訊控制作業制度之修訂、資安防護措施之實施和補強、資訊安全政策之審視等相關事宜。
- 委託資安廠商於 6、12 月進行電子郵件社交工程演練及教育訓練，強化員工對不明來源郵件的警覺性和判斷力，並了解近期之資安事件，提醒加強防範。
- 資安防護服務、安全認證及系統/軟硬體保全之年度支出共約 44 萬元。
- 使用者帳號之作業權限複核於 6、12 月共審查 2 次。
- 加強員工對於資訊作業威脅之判斷與警覺性的資訊安全教育宣導，全年共 8 次。
- 執行營運資料庫伺服器模擬緊急事故之演練、輪替切換 2 次，資料庫之運作檢測共 4 次。
- 於 10 月會計師事務所針對資訊系統之自動分錄風險進行評估，11 月資訊控制作業之內部稽查及自評，12 月進行資訊作業環境安全自評。