一、目的

本安全政策係以本公司核心之「本 ISMS 涵蓋本公司執行之 ERP、MES、CRM、BPM 與 BI 系統維運活動，包括系統監控、事件處理、帳號管理、資料備份、異常回復與協力廠商管理流程」業務為主，並依據 ISO 27001:2022 為標準，由本公司所制定，並作為發展本公司資通安全管理制度之承諾。為達到資通安全之管理需求，本公司由系統發展組之作業範圍，開始依據本安全政策規劃及推動資通安全管理制度，並視實施成效做為進一步擴展之參考。冀望資通安全管理制度之實施，可促使本公司各項電子化作業之設計開發、使用管理及營運維護等工作的安全性，以及保障本公司資訊之機密性、完整性、可用性及遵循性。

二、資通安全政策聲明

「善用資訊，提昇效率」

「嚴密管理，確保安全」

說明如下：

（一）本公司係資訊技術之核心研發及管制單位，同仁應妥善使用資訊系統，提昇工作效率，並確保資訊之機密性、完整性、可用性及遵循性。

（二）本公司同仁應降低資通安全事故之發生機率，以確保本公司業務能永續經營。

（三）資通安全乃本公司所有員工之共同責任，各單位主管均應督促所屬同仁，遵守本公司資通安全管理制度之相關規定。

（四）資訊安全管理之日常作業程序及規定均應符合國家相關法律、行政法規、本公司規定及相關合約之要求。

三、資通安全目標

資通安全管理制度推動委員會應訂定本公司之年度資通安全目標，並每年檢視審查，促使資通安全程度之日益精進。資通安全目標詳細內容參考資通安全管理制度推動委員會之管理審查會議記錄。

四、實施範圍

本公司建置資通安全管理系統之實施範圍，涵蓋本公司「本 ISMS 涵蓋本公司執行之 ERP、MES、CRM、BPM 與 BI 系統維運活動，包括系統監控、事件處理、帳號管理、資料備份、異常回復與協力廠商管理流程」所管理之系統和設備的日常操作、機房實體環境管理、應用軟體開發、資料儲存管理、人員安全管理等各種層面。範圍內之資訊資產泛指相關之資料紀錄和文件、電腦主機與相關資訊設備、實體運作環境（電腦機房內部）、所屬之人員及各種應用軟體系統等。

五、管理責任

本公司組織架構為總經理，下轄系統發展組及業務組；為達成上述之資通安全目標，本公司單位主管和所有同仁應負起責任，全力遵循及施行資通安全管理制度：

（一）責任分工、切實遵循：資通安全管理為本公司最重要政策之一，各單位主管均應全力支持和參與，並持續要求所有員工、委外廠商人員切實遵循資通安全管理制度。

（二）建立資通安全管理制度：本公司應依據 ISO 27001:2022 標準，訂定符合標準要求之資通安全管理制度文件，彙整成冊公布施行。

（三）符合法規及契約要求：本公司資通安全管理程序制定與實施，應符合國家法規、行政院(財政部)所屬各機關學校資通安全管理要點等法令，及本公司與其他機構所簽訂契約之要求。

（四）制定作業安全政策：應將資訊管理之作業安全政策與操作標準，制定為管理程序文件並發行公告，以利相關人員遵循實施。

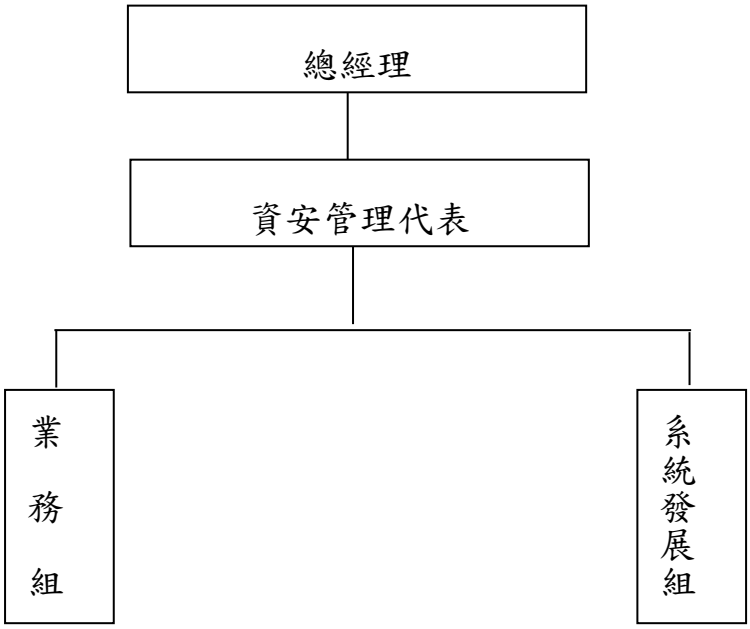
（五）教育訓練：定期辦理資通安全教育訓練及宣導，建立員工資通安全認知；同仁必須充分了解資通安全管理制度的重要性以積極推動。

（六）定期稽核、即時改善：透過稽核程序，發現資安問題並研商對策，提出改善建議，任何危及資通安全的行為都應訴諸適當的懲處程序，以落實資通安全管理制度的要求。

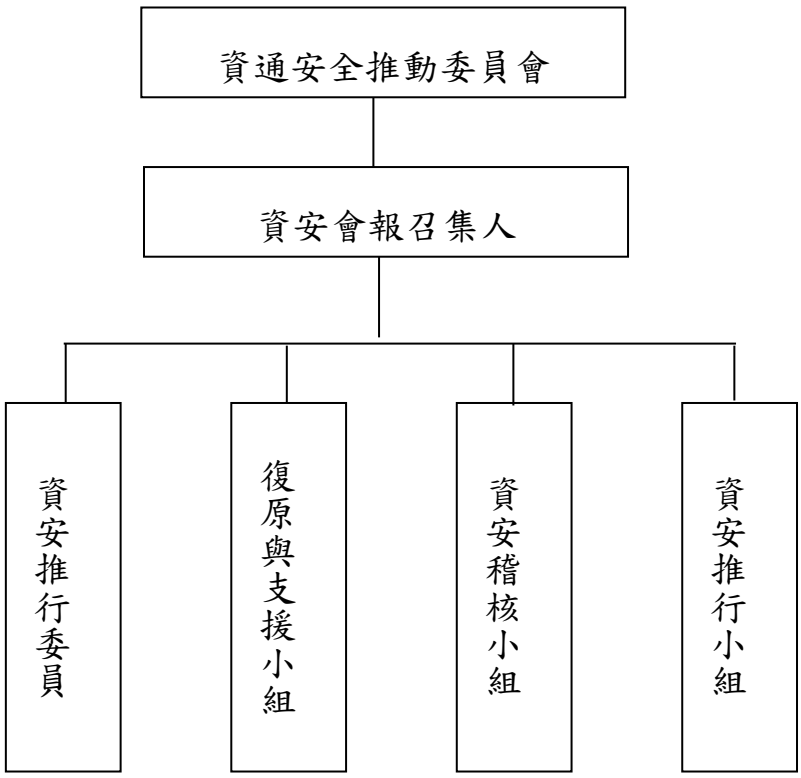
六、安全組織

資通安全管理制度推動委員會

(一) 組織架構：



(二) 資安推動委員會功能架構：



（三）工作職掌及成員：資通安全會報管理程序

組織名稱	工作職掌	相關人員
管理審查會議	1. 核定及審查第一階文件。 2. 安全風險審查及建議。 3. 本公司資訊安全措施整體提昇討論。 4. 宣導資訊安全觀念及管制措施。 5. 審核稽核報告與執行成果。	主席(總經理)
安全管理代表	1. 推廣既定之資訊安全政策與資訊安全手冊。 2. 不定期於管理審核會議報告執行狀況及改善建議。 3. 每年或不定期修訂資訊安全政策與手冊。	資安管理代表(系統發展組主管)
稽核小組	1. 每半年提出稽核報告及建議事項。 2. 安控機制執行狀況稽查及報告撰寫。	各組至少一名
資安推行委員/執行小組	1. 鑑別潛在風險及應有之安控機制。 2. 鑑別與盤點資訊資產價值。 3. 文件制定、修訂與廢止之申請。 4. 執行本系統資訊安全管理制度與發展安控機制。 5. 定期執行安全檢查，提供檢查報告或建議事項。 6. 推展宣導資訊安全觀念與安控機制。 7. 遵循相關監控作業程序。 8. 核定之文件登錄、傳遞及保管等相關管理工作。	程序書權責人員 機房管理人員 網路管理相關應用系統管理及執行相關人員
復原與支援小組 (緊急應變組)	1. 負責系統緊急應變處理程序。 2. 資安事件之通報及技術支援	系統管理與支援人員

七、資通安全管理系統之建立

本公司資通安全管理系統之建立和實施，依據 27001:2022 標準指引，依照 Plan – Do – Check – Action 標準流程進行操作：

(一)計畫

1. 標準與法規：依據資通安全管理標準：27001:2022，做為推動與建置制度的規範。
2. 資安教育與認知：透過資安教育訓練，使相關同仁充分了解資通安全管理制度的重要性，積極協助制度的實施。
3. 資通安全政策訂定及評估：資通安全政策必須由高階主管審查及核准，並要求本公司同仁切實遵守，以期資通安全管理成果和組織目標一致。
4. 資通安全組織及權責：組成資通安全管理組織，應涵蓋本公司內部相關組織共同運作。
5. 風險評鑑：應用風險評鑑技術來鑑別資訊資產價值，釐清面對的威脅與漏洞、法令規章的要求，據以採取相對應之風險處理和控制措施，確保應受保護資訊的機密性、完整性及可用性。

(二)執行：

1. 風險管理：資通安全管理制度推動委員會對於風險評鑑之結果，應訂定風險可接受程度，並要求相關人員擬定風險處理計畫，限期處理。
2. 資訊資產安全管理：資訊資產應依據安全等級分類，並指定專責管理人員。
3. 人員安全管理及訓練：資訊使用人員之任用、在職及解職過程應有適當之管理機制。
4. 設備之安全管理：資訊處理設備應妥善保管，避免作業環境導致之安全風險。
5. 網路通訊與操作管理：網路通訊應有標準作業程序，明定使用者及委外服務人員之責任。管理程序書應訂定系統規劃及驗收、電腦病毒及惡意軟體防範、備份管理、電腦媒體管制、資訊交換之安全管理、系統安全監控等作業規範。
6. 系統存取控制：依據本公司對「本 ISMS 涵蓋本公司執行之 ERP、MES、CRM、BPM 與 BI 系統維運活動，包括系統監控、事件處理、帳號管理、資料備份、異常回復與協力廠商管理流程」系統存取之需求，訂定使用者存取管理機制，賦予適當責任和權限，建立網路、作業系統、應用系統之存取控制措施，以及行動式電腦與電信通訊等管理機制。
7. 應用系統委外開發及操作維護：建置或採購應用系統應事先評估安全需求，系統上線後，管理人員必須遵照標準作業程序操作，並注意資料保密措施、主機日常運作及維護作業之安全性。
8. 資通安全事件管理：凡遇資通安全事件或發現系統弱點，應立即循規定管道通報主管，以即時管理和矯正資通安全事件。
9. 營運持續性管理：應訂定營運持續性管理計畫，定期演練和更新，維持緊急應變之能力。

(三)檢查：

1. 符合性：資通安全制度必須符合法規要求，管理程序和規範應依據本政策及技術符合性進行審查，並定期實施稽核，確保施行結果切合制度之要求。
2. 定期稽核：應定期進行稽核作業，稽核成果應擬具報告，由推動委員會決議後執行改善行動。
3. 懲處與責任：凡本管理制度所規範之範圍內，各相關人員未能依循制度執行業務，因而影響本公司資通安全者，將依照本公司相關人事規定追究責任及懲處。
4. 獎勵措施：凡本公司同仁對於資通安全管理系統之實施據有良好績效者，或能提出創新積極之改善建議者，得呈報上級給予獎勵。

(四)行動：

1. 持續改善：資通安全管理為永久性之政策，全體同仁應持續執行既定的管理程序。
2. 矯正措施：應訂定矯正及改善措施之作業程序，依據稽核審查的結果，採取矯正及預防措施，以持續改善資通安全管理作業。
3. 工作會議：資通安全代表應不定期召集各工作小組成員，舉行資通安全管理制度之工作會議，經常性檢視及討論資通安全制度之執行狀況，並適時引進管理技術，以保持資通安全制度與時代同步。

八、審查與評估

（一）本政策應由資通安全管理制度推動委員會討論及核准後公布實施，修訂亦然。

（二）當適用範圍內之資訊環境變化或資訊風險變更，必要時應對資通安全政策內容重新審查。

（三）本政策之審查應考慮下列事項：

1. 已發生的安全事件性質、次數及衝擊，檢查政策的適切性與有效性。
2. 控制措施對「本 ISMS 涵蓋本公司執行之 ERP、MES、CRM、BPM 與 BI 系統維運活動，包括系統監控、事件處理、帳號管理、資料備份、異常回復與協力廠商管理流程」業務運作效率上的負面影響。
3. 對技術變化的影響。