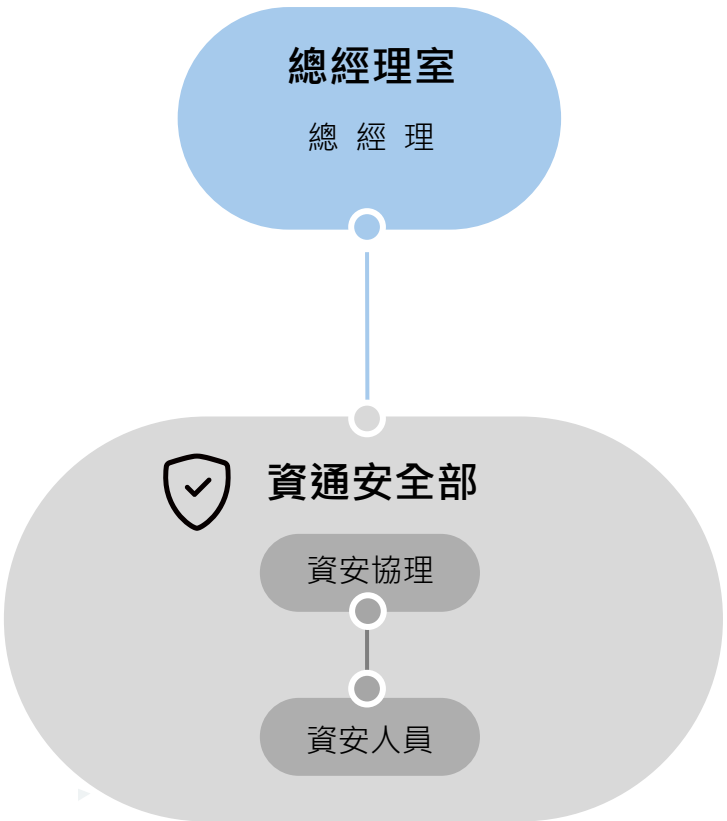
* 資通安全

資通安全，指的是保護資訊和通訊系統，使其免受未經授權的訪問、使用、洩漏、破壞或干擾的措施和實踐，確保資訊的機密性、完整性和可用性，防止資料被竊取、竄改或無法使用。本公司已制定資安政策，規範資通安全相關的措施和策略，以確保公司的運營穩定、合規並抵禦各類潛在的安全威脅。

* 資訊安全政策

資訊資產，舉凡實體資產、軟體資產、服務資產、文件、人員、企業形象等皆是，利用主動或被動的各種方法，來保護或保存一個環境，使其活動的進行不受干擾。其主要為了避免因人為疏失、蓄意洩漏、竄改、竊取、破壞或自然災害等風險，運用一整套適當的控制措施，包括政策、實踐、步驟、組織結構和軟體功能等，來確保資訊資產受到妥善的保護。

* 組職



資訊安全目標

建立安全及可信賴之電腦化作業環境，以確保電腦資料、系統、設備及網路安全。

* 資訊安全事件通報應變

- 訂定資訊安全事件通報及應變作業辦法。
- 如發生重大資訊安全事件，應依相關規定辦理。

* 資訊安全持續精進及績效管理

- 資訊安全組織相關人員定期向管理階層報告資訊安全執行情形，確保運作之適切性及有效性。
- 內部稽核：依年度稽核計畫執行資安稽核，並就發現事項擬定改善措施，且定期追蹤改善情形。
- 必要時，辦理委外廠商之資安稽核。

* 風險管理

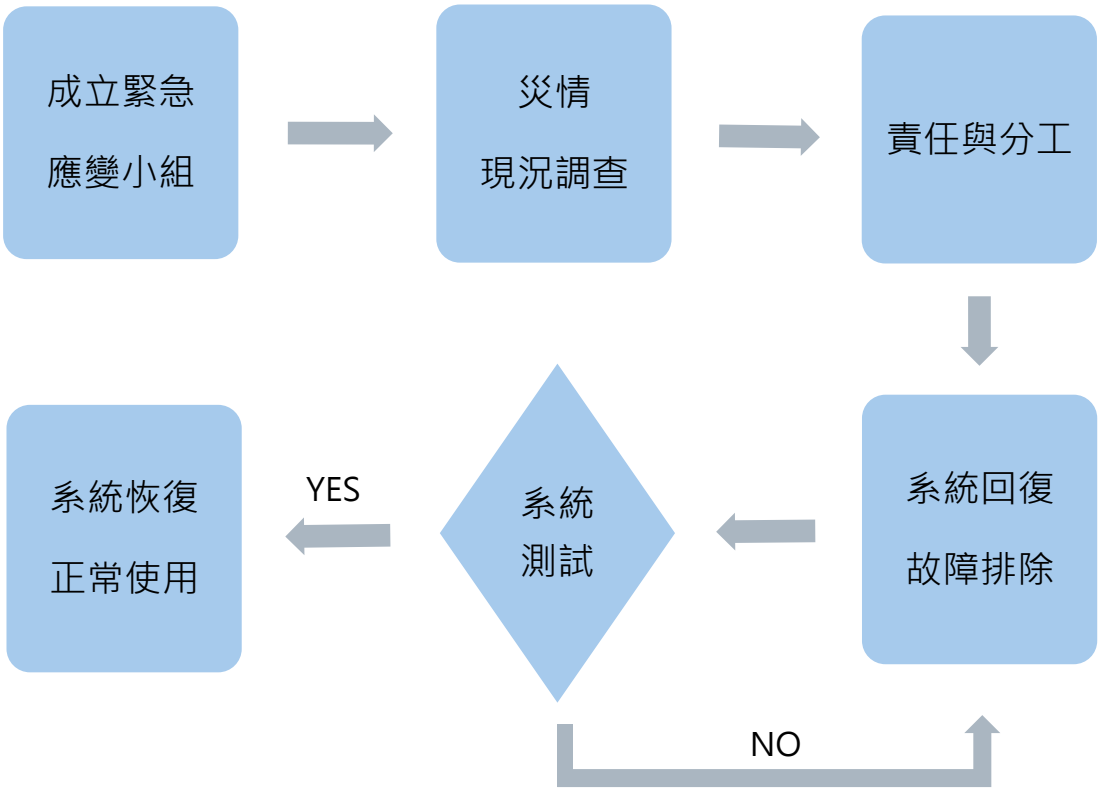
- 定期進行資安風險評估，識別能的安全威脅和漏洞並進行改善。
- 根據資安風險評估結果，針對各類風險制定相對應計劃和措施，降低風險的影響。

* 系統復原計劃

系統復原計劃每年至少測試一次，並將測試結果做成報告，依報告修改計劃。

* 應變程序

因應各項重大災變，或是電腦相關機器設備損壞，電腦機房或設備因不可抗拒因素，造成軟硬體毀損，於重大災變後一小時內成立緊急應變小組，或配合緊急應變防災體系，以儘速切斷災變來源，減少災變範圍之擴大，儘速恢復設備之運轉，並預先備份設備或媒體進行災變回復，以期資訊作業不致中斷。



* 備份作業與管制

公司重要的應用系統或程式之各項作業文件，於正式作業前或修撰後均應備份乙套，與原始文件異地保存，並責成專人妥善保存並行維護。

* 合規與審計

法規遵循

- 確保資通安全措施符合相關法律法規和行業標準。
- 定期進行內部審計稽核，檢查資通安全措施的合規性和有效性。必要時，辦理委外廠商之資安稽核。

外部審計

- 聘請第三方機構進行資通安全審計，評估並改進現有的資通安全措施。
- 根據審計結果，制定改進計劃和措施，持續提升資通安全水平。

* 2025資安教育訓練統計

資訊教育訓練課程名稱	對象	參與人數	訓練時數	參與率
社交工程演練課程	各部門(共89人)	75	1	84%
資訊安全教育訓練	各部門(共89人)	75	2	84%
ISO 27001強化企業防禦體系	資訊部(共5人)	4	1	80%
備份與災難復原演練的關鍵差異	資訊部(共5人)	2	1	40%
資安事件的緊急應變處理	資訊部(共5人)	2	3	40%
無線網路的使用與安全意識	資訊部(共5人)	2	3	40%