# 厚生股份有限公司

民國 112 年 12 月 22 日訂定

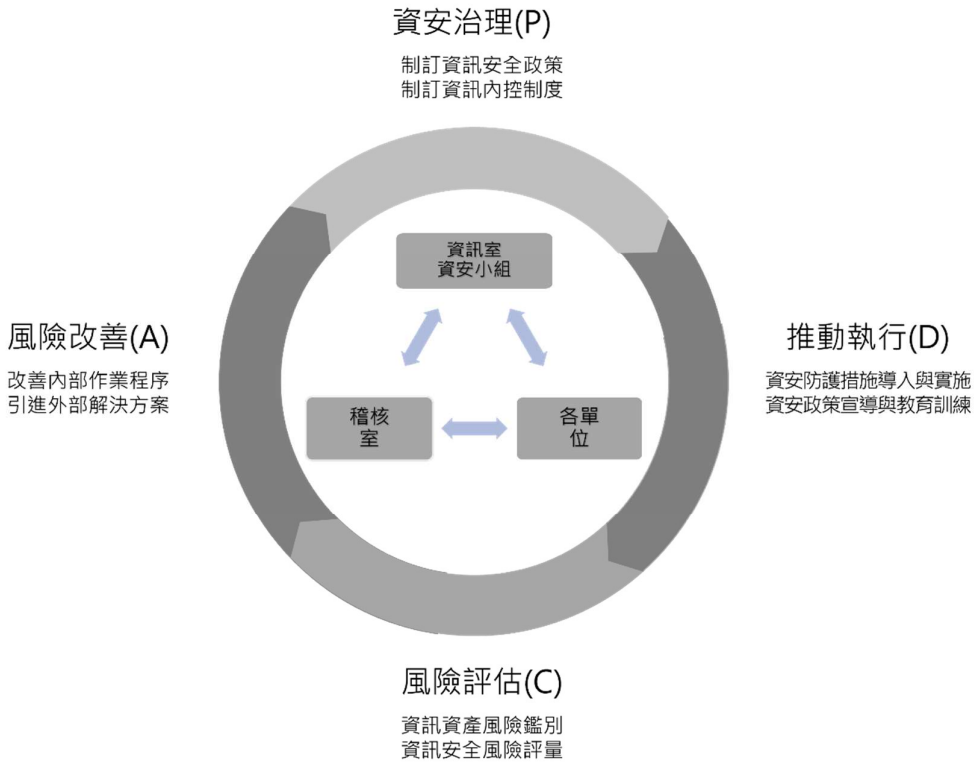
## 資 訊 安 全 管 理

壹、 資訊安全風險管理架構

一、依本公司風險管理政策，本公司設置三級風險管理組織，由權責部門→稽核室→董事會組成。遵此，本公司資訊安全之權責單位為資訊室，設置資訊安全主管 1 名與資訊安全專責人員 1 名組成資安小組，負責訂定企業內部資通安全政策、規劃暨執行資訊安全防護與資訊安全政策推動與落實，並定期公佈公司資訊安全治理概況。

二、本公司稽核室為資訊安全監理之督導單位，負責督導內部資訊安全執行狀況。若有查核發現缺失，立即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資訊安全風險。

三、運作模式採取定期稽核與循環式管理(Plan -> Do-> Check-> Action)，確保可靠度目標之達成且持續改善。



貳、 資訊安全政策

一、目的：

為使本公司業務持續順利穩定運作，防止資訊系統或網路通訊系統受到未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性、完整性及可用性。特制定本政策如下，作為本公司資訊安全管理作業的指導方針。

二、適用性：

本政策所規範之事項，其適用之對象為本公司董事、顧問、員工、約聘人員、委外服務廠商及與本公司連線作業之機關，其涉及本公司資訊安全管理之資產範圍者，皆有責任遵循此一政策。

三、目標：

(一). 確保本公司業務相關資訊之機密性，保障本公司業務機密與個人資料之安全。

(二). 確保本公司業務相關資訊之完整性及可用性，提高工作效能與品質。

(三). 提升本公司資訊安全防護能力。

(四). 達成本公司業務持續運作之目標。

四、策略：

(一). 應遵守政府相關法律如資通安全管理辦法及考量企業營運要求，評估資訊作業安全需求，建立相關程序，以確保資訊資產之機密性、完整性及可用性。

(二). 建立本公司資訊安全風險管理架構並訂定分工權責，俾利後續資通安全作業之推行。

(三). 參照政府所頒布資訊安全責任等級分級辦法之規定，執行各項應辦事項。

(四). 建立資訊安全事件通報應變機制，以確保資訊安全事件被妥善回應、控制及處理。

(五). 定期執行資通安全稽核作業，以確保資通安全管理落實執行。

五、涵蓋範圍：

(一). 本資訊安全政策之範圍涵蓋下列事項：

1. 資訊部門之功能及職責劃分。
2. 系統開發及程式修改作業。
3. 編制系統文書之控制作業。
4. 程式及資料存取控制作業。
5. 資料輸入、處理及輸出控制作業。
6. 檔案及設備之安全控制作業。
7. 電腦硬體及系統軟體之購置、使用及維護之控制作業。
8. 系統復原計畫制度及測試程序之控制作業。
9. 資通安全檢查之控制。
10. 公開資訊申報相關作業之控制。

(二). 以上涵蓋範圍，皆於本公司「內部控制制度」規範其相關作業準則並執行之，同時接受稽核審查。

六、 事件之通報及處理

(一). 當各單位發現資訊資產受到安全性威脅、侵犯或攻擊時，應由發現者立即向資訊室反應，在經資訊室資安小組初步研判及過濾後，若情節嚴重足以影響營運者，應依核決權限逐級向上通報，並運用相關資源儘速處理；最後資訊安全小組應將處理結果，適時向董事會提報受影響之範圍及最後處理情形，若遭明確之權益損害時，得循法律途徑求償。

(二). 資訊安全小組於接獲資訊安全事件之訊息後，應做第一線之防範及回復處理，無法自行解決時，應儘快尋求外部廠商的技術支援，以縮小損害程度至最低為目標；過程中，應保留受害之具體事實，以做為日後查證時之證據。

七、 審查與修訂：

本政策由資訊室每年至少評估一次，或於組織有重大變更時重新評估。 依評估結果、相關法令、技術及業務等最新發展現況，予以適當修訂，並於董事會審議通過後公告實施。