

文件編號	ISMS-A-001	文件類別	資訊安全政策
權責單位	資訊系統部	文件密等	一般
版 本	1.1	發行日期	114.10.07



資訊安全政策

文件編號	ISMS-A-001	文件類別	資訊安全政策
權責單位	資訊系統部	文件密等	一般
版 本	1.1	發行日期	114.10.07

目錄

1. 依據	1
2. 目的	1
3. 適用範圍	1
4. 政策及目標	1
5. 附則	2

文件編號	ISMS-A-001	文件類別	資訊安全政策
權責單位	資訊系統部	文件密等	一般
版 本	1.1	發行日期	114.10.07

1. 依據

- 1.1 『資訊安全管理制度標準』(ISO/IEC 27001)。
- 1.2 資通安全管理法。
- 1.3 資通安全管理法施行細則。
- 1.4 基層醫療院所資安防護參考指引。
- 1.5 個人資料保護法。

2. 目的

「國泰健康管理顧問股份有限公司」(以下簡稱本公司)為維護資訊作業正常且安全穩定的運作,以提供可信賴之資訊服務,並確保資訊之機密性、完整性、可用性,以及符合法令、法規之要求,降低資訊作業風險,特制定本政策為資訊安全管理制度最高指導方針,以供相關人員遵循。

3. 適用範圍

- 3.1 資訊安全管理制度實施範圍為各項資訊作業。
- 3.2 本政策適用於本公司同仁(含正職、約聘僱人員、工讀生、派遣人員、實習生)及其他得接觸本公司業務相關資訊之合作夥伴、委外廠商及第三方人員。

4. 政策及目標

4.1 政策

- 4.1.1 定期考量相關法律規章及營運要求,進行資產風險評估,確認資訊作業安全需求,建立標準作業程序,並採取適當資訊安全控制措施。

文件編號	ISMS-A-001	文件類別	資訊安全政策
權責單位	資訊系統部	文件密等	一般
版 本	1.1	發行日期	114.10.07

- 4.1.2 定期執行資訊安全稽核作業，檢視資訊安全管理制度之落實度。
- 4.1.3 建立資訊安全事故管理程序，以確保事故妥善回應、控制與處理。
- 4.1.4 應訂定營運持續計畫並定期演練，以確保重要業務於災害發生時能於預定時間內恢復作業。
- 4.1.5 同仁依規定接受資訊安全教育訓練與宣導，以加強資訊安全認知。
- 4.1.6 若違反本政策與資訊安全相關規範，應依據本公司獎懲規定辦理懲處；若涉及違反法令法規時，依相關法律規定追究民事、刑事責任。

4.2 目標

- 4.2.1 以「保護資訊資產安全」及「維持業務持續運作，以達企業永續經營」為目標，保護股東權益為基礎，進而達成本公司之使命及願景，維持資訊服務可用性。
- 4.2.2 為確保本公司的協同可發揮最大利益，並善盡社會責任，本公司應以符合法令及風險管理之原則，建立完善之資訊安全管理制度，保護本公司所擁有及使用之資訊與個人資料。
- 4.2.3 保障資訊業務內部使用者權益，維護資料安全性。
- 4.2.4 確保資訊系統存取正當性，防止人為不當使用，遏止駭客入侵行為。
- 4.2.5 建立維運實體與環境安全管理作業規範，避免人為作業疏失，加強資訊安全意識。
- 4.2.6 配合營運策略制定資訊安全目標，於落實資訊安全目標基礎上協助達成營運策略。

5. 附則

- 5.1 資訊安全委員會每年審查政策與資訊安全目標，以符合相關法令、技術、

文件編號	ISMS-A-001	文件類別	資訊安全政策
權責單位	資訊系統部	文件密等	一般
版 本	1.1	發行日期	114.10.07

利害關係者 (Interested Parties) 期待，以及與營運策略連結，依業務變動、技術發展及風險評鑑的結果修訂之。

5.2 本政策經資訊安全委員會審議通過，奉 資訊安全長核定後實施，修正時亦同。