加捷生醫股份有限公司
JIA JIE Biomedical Co.,LTD

資 通 安 全 政 策

一、資通安全管理之目的：

Version 1131225

1. 確保公司主機、網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資通安全管理規範。

2. 確保公司業務資訊之機密性、完整性與可用性。

    ※ 機密性：確保被授權之人員才可使用資訊。

    ※ 完整性：確保使用之資訊正確無誤、未遭竄改。

    ※ 可用性：確保被授權之人員能取得所需資訊。

二、資通安全政策內容：

1. 本公司各項資通安全管理規定必須遵守政府相關法規

    (如：資通安全管理法、刑法、國家機密保護法、公平交易法、多層次傳銷管理法、商標法、著作權法、個人資料保護法等）之規定。

2. 成立資通安全管理專職單位，負責資通安全制度之建立及推動事宜。

3. 定期實施資通安全教育訓練，宣導資通安全政策及相關實施規定。

4. 建立主機及網路使用之管理機制，以統籌分配、運用資源。

5. 新系統及設備建置上線前，須將風險、安全因素納入考量，防範危害資通安全之情況發生。

6. 建立資訊機房實體及環境安全防護措施，並定期施以相關維護及保養。

7. 明確規範網路系統之使用權限，防止未經授權之存取動作。

8. 訂定資通安全管理制度內部稽核計畫，定期檢視資通安全管理制度範圍內所有人員及設備使用情形，依稽核報告擬訂及執行矯正預防措施。

9. 訂定營運持續管理備援/備份還原之演練，確保公司業務持續運作。

10. 本公司所有人員，均有維持資通安全之責任，且應遵守公司相關之資通安全管理規範。

11. 委外廠商在執行本公司委外業務時若有複委託之需求，應評估複委託業務相關之資安風險。並要求委外廠商依資通安全相關規定對複委託廠商進行適當之監督與管理。

12. 對內部及外部專案管理的過程中，應明訂及陳述與專案相關之各項資通安全要求，確保內部及外部專案資訊之機密性、完整性及可用性，降低機敏資訊(含個人資料)外洩及違反法令之風險。

13. 資安政策之評估與審查應至少每年評估及審查一次，以反映管理政策、政府法令、新科技技術及公司業務等之最新發展現況，確保資通安全管理制度的可行性及有效性，以維持營運和提供適當服務的能力。

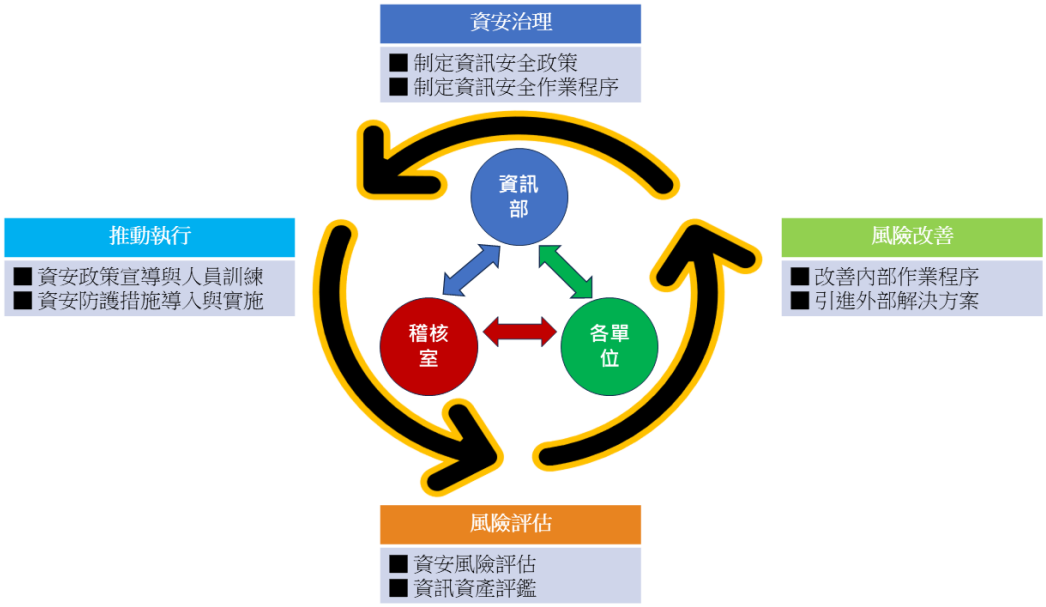
三、資通安全風險管理架構：

1. 本公司資通安全之權責單位為資訊部，該部設置資訊主管，與專業資訊人員，負責訂定企業內部資通安全政策、規劃暨執行資通安全防護與資安政策推動與落實，並定期公佈公司資安治理概況。

2. 本公司稽核室為資通安全監理之督導單位，該室設置稽核主管，與專職稽核人員，負責督導內部資安執行狀況，若有查核發現缺失，旋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，以降低內部資安風險。

3. 組織運作模式採定期稽核與循環式管理，確保可靠度目標之達成且持續改善。



四、資通安全政策具體管理方案：

本公司資訊安全管理機制，包含以下四個面向：

- 資訊政策的制定：訂定公司資訊安全作業管理辦法，明確訂定人員對於資訊作業的行為。
- 資訊科技的運用：建置資訊安全管理設施，並持續提升與汰換軟體、硬體資訊設施，以符合當前資安風險控管。
- 資安宣導與訓練：持續對人員進行資訊安全宣導與教育訓練，提昇全體同仁資安意識。
- 資安稽核與改善：本公司稽核部門定時稽核資訊安全單位，針對資安與網路風險以風險評估之流程進行風險評估，適切提出控制點建議，資訊部門依此作調整與改善。

本公司實施之資通安全政策與管理措施，包含如下：

類別	說明	相關措施
權限管理	人員帳號, 權限管理, 系統操作	人員帳號權限管理與審核 人員帳號權限定期盤點
存取管制	人員存取內外部系統, 資料傳輸管道安全措施	內/外部存取管控 資料外洩管控 操作行為軌跡紀錄
外部威脅	內部系統潛在弱點, 防毒防駭的保護措施	主機電腦弱點檢測與更新措施 防毒防駭, 垃圾與惡意程式偵測
系統可用	系統可用狀態與服務中斷時的處置措施	系統/網路可用狀態監控及通報機制 服務中斷之應變措施 資料備份與系統備援機制 定期災害還原演練

五、本公司資通安全通報程序如下，資安事件之通報與處理，皆遵守該程序之規範進行