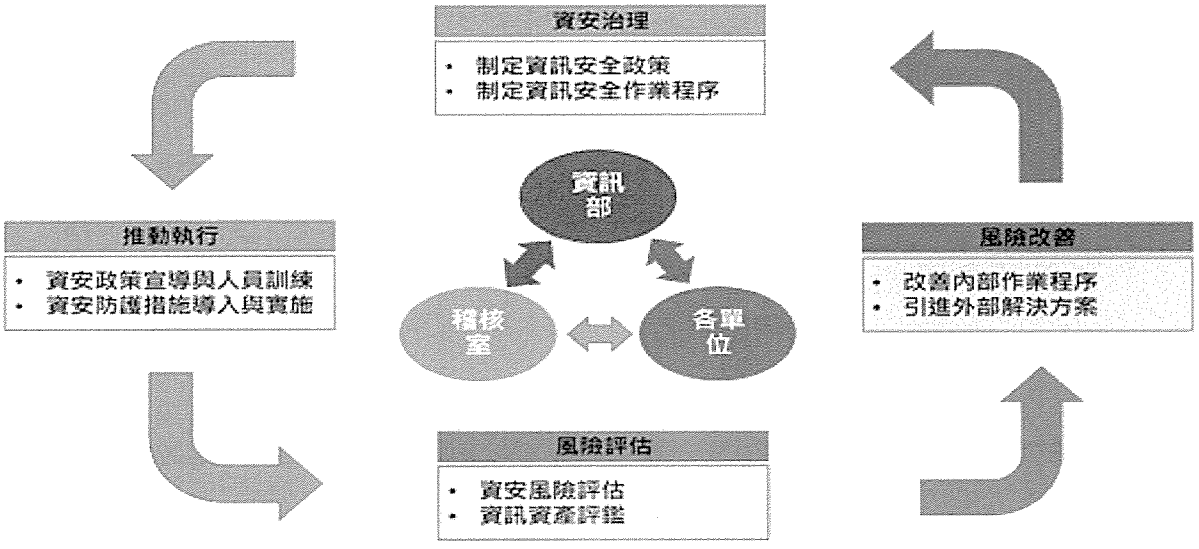
1. 目的:
   1.1. 確保公司主機、網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資訊安全管理規範。
   1.2. 確保公司業務資訊之機密性、完整性與可用性。
      1.2.1. 機密性：確保被授權之人員才可使用資訊。
      1.2.2. 完整性：確保使用之資訊正確無誤、未遭竄改。
      1.2.3. 可用性：確保被授權之人員能取得所需資訊。
2. 資訊安全風險管理架構：
   2.1. 本公司資訊安全之權責單位為資訊部，負責訂定內部資訊安全政策、規劃暨執行資訊安全防護作業與資安政策推動與落實，並定期向董事會報告公司資安治理概況。
   2.2. 本公司稽核室為資訊安全監理之查核單位，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。
   2.3. 組織運作模式採 PDCA 循環式管理，確保可靠度目標之達成且持續改善。



3. 資訊安全管理機制，包含以下三個面向：
   3.1. 制度規範：訂定公司資訊安全管理制度，規範人員作業行為。
   3.2. 系統防護：建置資訊安全管理系統，落實資安防護管理措施。
   3.3. 人員訓練：進行資訊安全教育訓練，提昇全體同仁資安意識。
4. 本公司實施之資訊安全管理措施，包含如下：
   4.1. 本公司各項資訊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、專利法、商標法、著作權法、個人資料保護法等）之規定。
   4.2. 定期實施資訊安全教育訓練，宣導資通安全政策及相關實施規定。
   4.3. 建立主機及網路使用之管理機制，以統籌分配、運用資源。
   4.4. 新系統及設備建置上線前，須將風險、安全因素納入考量，防範危害資訊安全之情況發生。

4.5. 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。

4.6. 明確規範網路系統之使用權限，防止未經授權之存取動作。

4.7. 訂定資訊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。

4.8. 每年定期執行本地、異地備份還原之演練，針對重要主機系統環境與資料建立自動備份機制，確保於災發生時能順利恢復系統運作。

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

4.10. 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。

5. 資安事故之通報與處理，通報程序如下：