資通安全管理：

(一)資通安全管理策略與架構:

1. 資通安全風險管理架構

(1)企業資訊安全治理組織

本公司之企業資訊安全組織，目前由資訊安全委員會組織成員統籌資訊安全及保護相關政策制定、執行、風險管理與遵循落實，本公司稽核處並肩負稽核企業資訊安全之責。

(2)企業資訊安全組織架構

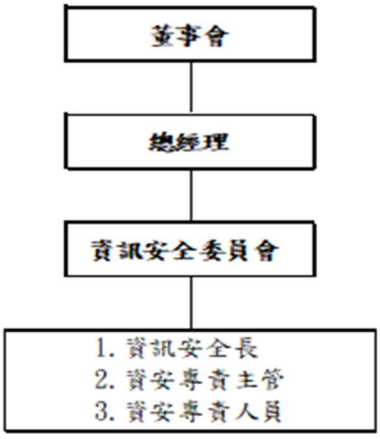
依法設置資通安全專責主管及人員五名，並以資安專責主管為召集人執行審查資安管理政策、擬訂資安管理架構及組織功能，定期檢視公司整體資安管理機制之發展、建置及執行結果。其運作情形如下：

A. 由總經理指派專責主管與人員。

B. 至少每年開會二次(113 年開會次數為 2 次)。

C. 本公司之資訊安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項:

- 資通安全政策及目標之研議。
- 傳達公司資通安全政策與目標。
- 其他資通安全事項之規劃。
- 資通安全相關規章與程序、制度之執行。
- 資訊盤點及風險評估。
- 資料安全防護事項之執行。
- 資通安全事件之通報及應變機制之執行。
- 其他資通安全事項之辦理與推動。



2. 資通安全政策

(1)企業資訊安全管理策略

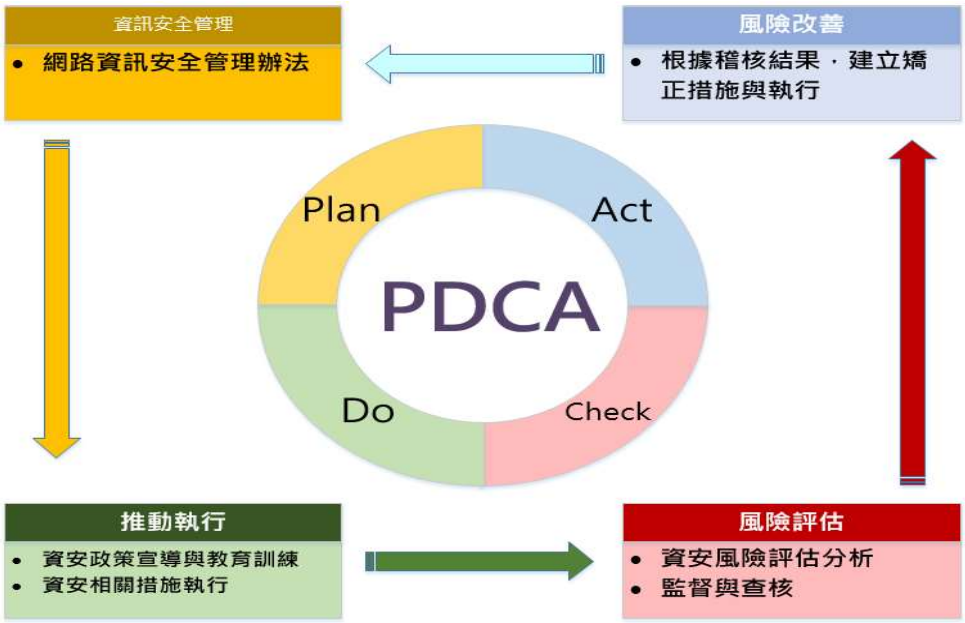
A. 本公司資訊安全之權責單位為資訊安全委員會組織成員，負責規劃內部資訊安全政策、執行資訊安全管理辦法與資安政策推動與落

實。

B. 本公司稽核處為資訊安全監理之查核單位，並依所排定行程進行查核作業，若有發現缺失或風險，即請受查單位進行檢討，並提出具體改善計劃及時程，定期追蹤改善進度，以降低資安風險與落實資訊安全政策。

C. 本公司資訊安全運作模式採用 PDCA（Plan-Do-Check-Act）方式管理，確保目標達成且持續改善。

(2)企業資訊安全風險管理與持續改善架構



(3)資通安全具體管理方案

本公司資訊安全政策，包含以下四個面向：

A. 規範辦法：訂定公司資訊安全管理辦法，規範人員作業行為。

B. 硬體建置：建置完善資訊安全設備，落實資安管理。

C. 人員教育：遇有重大資安事件進行知會，以提昇全體同仁資安意識。

D. 政策檢討：推動資訊安全持續改善，確保企業永續經營。

(二)資通安全風險與因應措施:

資訊技術安全之風險及管理措施

本公司已建立重要性的網路與伺服器相關資安防護措施，為避免來自任何第三方癱瘓系統的網路攻擊，這些網路攻擊可能以非法方式入侵本公司的內部網路系統，進行破壞公司之營運及損及公司商譽等活動或可能會竊取公司重要的機敏資料。因此，本公司將透過持續檢視和評估其網路資訊安全管理辦法，以確保其適當性和有效性，適時增加安全性保護，但此法仍不能完全保證公司在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響，故完善的備份機制也是本公司重要的一環。本公司對未來資

安風險的因應措施如下

1.資訊安全規章及程序:

為落實資訊安全管理,公司制定「資訊安全管理辦法」與相關作業細則,並據以執行資訊工作計畫,嚴格管理資料之利用與安全維護,防火牆政策、申請流程,加以管制,以減少公司資訊安全風險。

2.適時增加安全性保護:

針對重要伺服器佈署端點偵測與回應軟體,對於進階威脅(APT)的防護不足之加強,對於伺服器的最後一道防線偵測,並能快速反應即早做處置,增加本公司資訊安全。

3.備份機制:

本公司資訊系統架構建立資料庫備份機制,並將備份媒體送往異地保管存放,以降低資料損失風險,平時各項模擬測試以確保資訊系統之正常運作及資料保全,可降低無預警天災及人為疏失造成之系統中斷風險,確保符合預期系統復原目標時間。

(三)重大資通安全事件：無