

文件名稱	資通訊安全管理政策	文件編號	AE-006	版本/版次	1.1
制訂部門	資訊部	頁次	1/3	制訂日期	114/10/01

# 資通訊安全管理政策

修訂記錄	日期	版本	總頁數	核准	審查	製作
第一次制訂	113/11/01	1.0	3			
第一次修訂	114/10/01	1.1	3			
第二次修訂						
第三次修訂						
第四次修訂						
第五次修訂						

文件名稱	資通訊安全管理政策	文件編號	AE-006	版本/版次	1.1
制訂部門	資訊部	頁次	2/3	制訂日期	114/10/01

### 1.目的：

確保公司所有主機、網路通訊、應用系統之安全，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、竄改或破壞等風險以確保公司業務資訊之機密性、完整性與可用性。

1.1 機密性：確保被授權之人員才可使用資訊。

1.2 完整性：確保使用之資訊正確無誤、未遭竄改。

1.3 可用性：確保被授權之人員能取得所需資訊。

### 2.範圍：

實際營運控制權之轄下分公司、子公司、辦事處等皆受此政策規範。

### 3.內容

- 3.1 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、專利法、商標法、著作權法、個人資料保護法等之規定。
- 3.2 資訊部門為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。
- 3.3 不定期對全體員工實施資通安全教育、宣導資通訊安全政策及相關實施規定。
- 3.4 建立主機及網路使用之管理機制，以統籌分配、運用資源。
- 3.5 資訊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。
- 3.6 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。
- 3.7 依業務需求設置相關之應用及網路系統使用權限，防止未經授權之存取動作。
- 3.8 訂有資通安全管理相關之內部控制及稽核制度，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。
- 3.9 訂有營運持續管理備援及備份還原之辦法及演練，確保資訊系統支持公司業務持續運作。
- 3.10 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通訊安全管理規範，若有違反相關規範，依公司相關規範處理。
- 3.11 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通訊安全風險；並要求委外廠商依資通訊安全相關規定對複委託廠商進行適當之監督與管理。
- 3.12 對內部或外部專案管理的過程中應包含與專案相關之各項資通安全要求，確保專案資訊之機密性、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。
- 3.13 資通訊安全管理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、新技術及公司業務等最新發展現況，確保資通訊安全管理相關制度的適切性及有效性，以維持營運和提供適當服務的能力。

文件名稱	資通訊安全管理政策	文件編號	AE-006	版本/版次	1.1
制訂部門	資訊部	頁次	3/3	制訂日期	114/10/01

3.1.4 資訊存取之控制管理應與組織核決權限一致或業務需求適當配置。

#### 4.組織與職掌

- 4.1 資通訊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，負責制定資通訊安全管理政策、規劃暨執行資通訊安全相關制度推動、維護及檢討。
- 4.2 稽核單位為資通訊安全之監理稽核單位，該單位設置稽核主管或稽核人員，負責查核內部資通訊安全執行狀況，若有發現缺失，立即要求受查核單位提出相關矯正措施，且追蹤改善成效，以降低內部資訊安全風險。
- 4.3 組織運作模式採定期稽核與循環式管理，確保資通訊安全相關制度確實執行且持續改善。

#### 5.管理機制

公司資通訊安全管理機制，包含制度規範、系統防護及人員訓練三個面向：

- 5.1 制度規範：訂定公司資訊安全管理制度或相關辦法，規範人員作業行為。
- 5.2 系統防護：建置資通訊安全管理系統，落實資通訊安全防護管理措施。
- 5.3 人員訓練：進行資通訊安全教育訓練或宣導，提昇全體同仁資通訊安全意識。
- 5.4 資通訊安全政策有重大變更或發生重大資通訊安全事件應立即採取應對措施並依核決權限通報。

#### 6.發佈

本資通訊安全政策經總經理核准後發佈實施，修正時亦同。