

## 一、目的

為保護公司資訊資產，免於遭受破壞，不論這些破壞是來自於內部或外部人為、蓄意或意外，而制定集團資訊安全管理辦法，以作為實施各項資訊安全措施之標準。

## 二、適用範圍

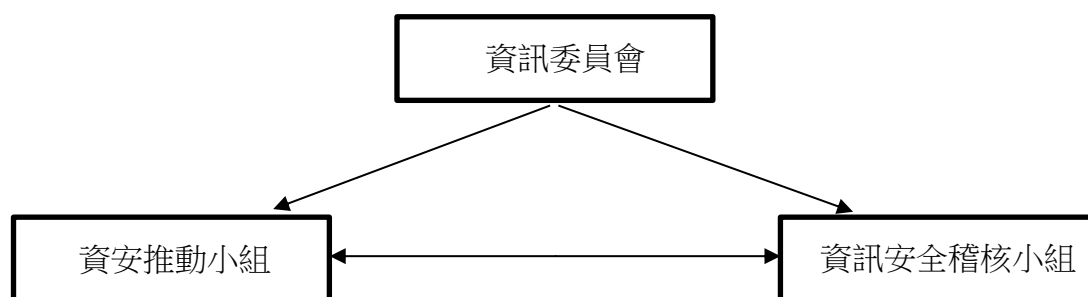
(一) 本政策適用範圍為本公司全體同仁、委外服務廠商與訪客等。

(二) 資訊安全管理事項如下：

1. 資訊安全政策評估。
2. 資訊安全組織與管理。
3. 資產管理。
4. 人力資源安全。
5. 實體與環境安全。
6. 通訊與作業管理。
7. 存取控制。
8. 資訊系統取得、發展及維護。
9. 資訊安全事故管理。
10. 企業持續運作管理。

## 三、資訊安全組織

為提升集團資訊安全管理與資訊安全相關政策執行與推動，由「資訊委員會」負責審視各子公司資安治理政策，並監督資安管理運作情形。



資訊委員會	為任務編組方式組成，由管理部主管擔任召集人、各部級主管為委員，負責資訊政策制定及資訊管理事項之協調，如因職務調動即刻指派遞補人員與辦理交接。
資安推動小組	由資訊委員會執行幹事擔任組長並指派組員，負責規劃及執行各項資訊安全作業。
資訊安全稽核小組	由資訊委員會指派小組成員(含內部稽核人員)；負責評估與檢視資訊安全管理制度及執行情形。

#### 四、實體與環境安全

各資訊資產管理者應妥善地維護設備，以確保設備的完整性及可以持續使用，資訊單位就系統伺服器主機設備安置於主機房，並由資訊單位專責管理，並管制非相關資訊、維修人員隨意進出，並於每次進出填寫管制紀錄表。

#### 五、通訊與作業管理

(1)為確保系統、連網設備安全以及軟體安裝審核，任何異動，皆應獲得權責管理人員的同意並由資訊單位進行處理。

(2)定期評估網路系統安全及電腦病毒及惡意軟體的防範。

#### 六、存取控制

(1)公司資料應放在網路磁碟機公檔中，並依據管理辦法歸列檔案。

(2)公司敏感性資料如有需要被讀取或交流時，需經核決權限通過後始可開放。

(3)於工作場所使用之公司資產的可攜式儲存媒體及設備需經過登記並註明用途後始可借用。

(4)非公司既有資產之可攜式設備，須登記後並由資訊單位確認後才能至公司使用。

(5)如有長期外借電腦設備需求時，經核決權限通過後方可外借，並簽收保管單。

#### 七、資訊系統取得、發展及維護

(1)與公司往來資訊服務提供者，依採購辦法進行採購並由資訊單位評核委外服務合約與維持適當的互動管道，即時解決相關突發性的資訊安全問題。

(2)外部連線(供應商)至內部主機進行更新或異常排除時，應填寫維護紀錄表，留存主機系統更動紀錄。

#### 八、企業持續運作管理

(1)為因應各種人為及天然災害造成業務運作受影響，資訊單位須定期進行資料備份。

(2)發生資訊安全事件時，應立即向權責主管通報，由資訊單位聯繫檢警調單位偵查。

(3)為保障企業營運秘密安全，資訊單位得對電子資料通訊做必要的監控與資料保存。