電腦設備暨網路資訊安全管理

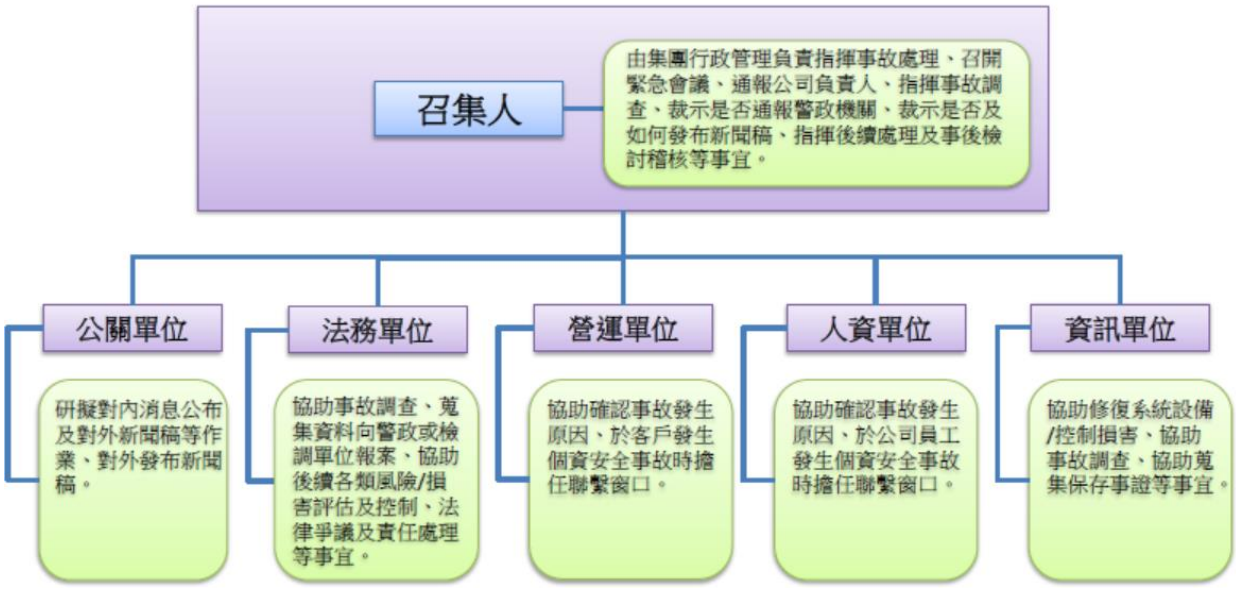
資通安全政策與目的

LEOFOO 六福旅遊集團 TOURISM GROUP

- **法規政策**
  - 為強化資通安全防護及管理機制，同時符合「公開發行公司建立內部控制制度處理準則」第九條使用電腦化資訊系統處理者相關控制作業，必需訂定資安政策並成立推動組織。
  - 資安推動組織
    - 需配置適當的人力、物人與財力資源，並指派專責資安主管及人員，以推動並協調監督資安管理事項。
    - 資訊安全之主管及人員，每年接受資訊安全專業課程訓練。
    - 訂定資通安全作業程序。
- **目的**
  - 為確保資訊網路安全及電腦設備之穩定運作(包含使用設備軟硬體、儲存資料、以及網路系統時)，必須注意相關控管的安全事項，以防止公司資訊系統及其資料遭致不當使用、洩漏、竄改、破壞等營運風險與危害資訊安全。
  - 執行面向: 為達成上述目的，分別以底下三個面向建構出全方位的資安防護能力，包含:
    - 使用者人員管理
    - 軟體資料管理
    - 電腦設備及網路管理

資通安全管理架構

LEOFOO 六福旅遊集團 TOURISM GROUP



資安管理執行-人員權責管理

LEOFOO
六福旅遊集團
TOURISM GROUP

- **目的：**
  - 對於與資訊系統有接觸的人員，依照不同角色，規定其對資訊系統的使用權限和責任。
- **對象：**

一般使用人員	• 帳號申請(為執行所屬部門及業務的工作內容) ✓填寫資訊需求單申請相關帳號及權限，經部門主管簽核同意與資訊處審核通後，使用人員才能取得帳號。 • 人員離職或職務異動 ✓離職：取消其所使用相關資訊系統帳號。 ✓職務異動：調整帳號權限及取消已不需使用之帳號；若需其它系統帳號，則需另外填寫資訊需求單申請相關帳號及權限。 • 一人一帳號 ✓禁止分享帳號及密碼供他人使用，防止系統無法追蹤實際操作者行為及權限被濫用的情況。
網路系統管理人員	• 管理個別使用者的帳號及權限 ✓負責系統帳號的建立、停用、刪除以及權限的編輯設定等相關管理作業。 ✓定期列出使用者帳號清冊，供各單位檢視帳號是否有繼續使用的必要性。 • 執行各系統及網路的資安風險偵測及。 ✓資安宣導與提醒。 ✓檢視系統設定是否適當，並優化設定與操作以規避風險。 ✓蒐集網路威脅及整理情資，並即早制定因應策略，確保各單位內部系統主機與資料的安全及完整。

資安管理執行-系統軟體及資料維護管理

LEOFOO
六福旅遊集團
TOURISM GROUP

- **目的：**
  - 避免被外部攻擊而影響軟體程式正常運作，及確保資料保全完整性。
- **對象：**

軟體程式維護管理	• 系統軟體設定變更管理 ✓設定變更須經過權責單位主管核定後執行，並做變更管理紀錄。 • 電腦及伺服器主機全面安裝防毒軟體。 ✓當電腦偵測到病毒入侵時應立即將網路離線以避免病毒擴散，並馬上通知網路管理者，直到網路管理者確認病毒已移除，才可重新與網路連線。 • 建構備援機制 ✓當系統軟硬體及資料在毀損或操受破壞時，能迅速切換至備援系統，以降低服務障礙時間。 • 資訊設備禁止下載及安裝非法或未經資訊處確認的軟體。 • 應用軟體使用之資料庫需提供加密機制。
資料維護管理	• 資料依其特性及機密性區分成不同的存取權限(讀取、建檔、修改、刪除)。 ✓使用者填寫資訊需求單並取得部門主管核准後，依申請內容設定相符的系統權限。 ✓資訊系統管理者將依據各授權原則提供各資料保護方式，以確保各個系統在資訊存取過程中的安全性。 • 建立及管理資料保護及保存的機制： ✓備份機制：透過定期自動排程或手動的操作，確保資料因故損壞時能有複本可進行系統回復(Recovery)，以降低資料損毀所造成系統無法正常運作的衝擊。 ✓321備份原則：3份資料、2個儲存媒介、1份在異地。

資安管理執行-設備及網路安全管理

- **目的：**
  - 強化電腦設備及網路連線安全性。
- **對象：**

電腦設備管理	• 電腦設備放置於指定的場所，並有對應保管單位與保管人負責。 • 公司核心設備均放置於資訊機房，並有專人負責管理機房，一般人員進出機房均需有管制並由機房人員陪同。 • 機房基礎設備(包含電力與空調)需提供不同電源迴路與不斷電系統，以及裝設溫度感知器。
網路連線作業管理	• 公司內部網域與外部網際網路之間需設置防火牆 ✓外部電腦或伺服器連線到內網中的各系統進行資料存取作業時，均需受到防火牆適當的管控。 • 外部遠端連線 ✓員工因業務需要必需經由外部遠端登入公司內部系統時，除了系統帳密驗證，也需搭配安全連線機制。 ✓遠端登入的安全連線機制需要先經申請審核，通過後才能於公司電腦上設定及使用。
系統帳號密碼管理	• 操作資訊系統必需使用個人帳號與密碼。個人帳號須經由申請程序審核通過後取得。 • 密碼設定具備複雜度及規則 ✓長度應達一定字數，且由大寫、小寫英文字母及數字三者順序交錯構成。 ✓密碼皆需強制定期更改，以提高安全性。 • 密碼登入數次失敗後，系統會“鎖定”該帳號，以防止有心人士嘗試重複猜測密碼。 • 使用者若因異動(離職或調職)不再使用，將由系統管理者將之取消或調整權限。

資安具體方案與未來預計提升項目

- **系統裝置安全**

1. 伺服器與個人電腦更新

伺服器與個人電腦作業系統與軟體更新，避免過舊的系統漏洞被駭客利用入侵。

2. 郵件系統更新

郵件主機從地端上到雲端Exchange Online ，無需定期更新系統。

3. 防毒程式

雲端版本，隨時隨地自動更新與偵測並封鎖病毒、木馬、蠕蟲等已知威脅 。

4. 端點防護(EDR\MDR)系統

導入可主動偵測並告警，阻擋來自網站、電子郵件、即時通訊和社群網站、惡意網址中的詐騙與漏洞掃瞄，防範網路詐騙等惡意未知的威脅入侵。

5. 社交工程演練

定期執行釣魚郵件防禦演練，加強員工對郵件社交工程攻擊的警覺性。

112年度購買防毒軟體支出250千元，112年度召開2次會議討論資訊安全。

基於資訊安全的重要性，權責單位每年定期向董事會報告公司資訊安全治理與執行狀況，近期報告日期為112年12月29日。