電腦設備暨網路資訊安全管理

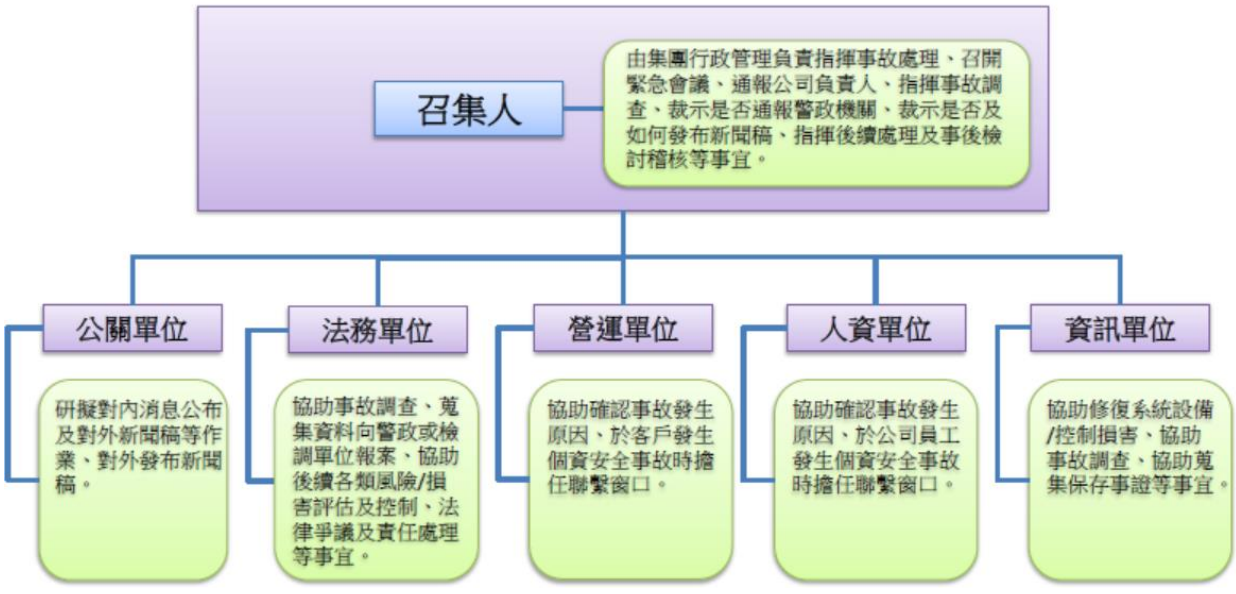
資通安全政策與目的

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

- 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，經權責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預防。 ✓資安宣導與提醒。 ✓主被動蒐集網路威脅及整理情資並予以更新網路系統，優化網路設定避免可能性風險以確保各單位內部系統主機與資料的安全性。

資安管理執行-系統軟體及資料維護管理

- 目的：
  - 避免因內部不當操作作業或被外部攻擊而影響軟系統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。
資料維護管理	• 資料依其機密特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權責主管核准後，依申請內容設定相符的系統權限。 ✓資訊系統管理者將依據授權原則，提供各帳號資料授權內容，以確保各個系統帳號在資訊存取過程中的安全性。 • 建立及資料保護及保存的機制： ✓321備份原則：3份資料(至少3代)、2種儲存媒介(不同儲存媒體)、1份在異地(異地備份)。 ✓備份機制：透過定期自動排程或臨時性手動的操作，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。 • 具個資機敏資料之程式資料庫需提供加密機制。

資安管理執行-設備及網路安全管理

- 目的：
  - 強化資訊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確保機房不過熱。
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部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 ✓ 長度應達一定字數以上，並由大寫、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。

2024年度新投入資安管理優化內容

- 資安優化內容：
  - 資訊安全已為公司營運重要議題，2024年度對資安新投入之優化方案如下：。

汰換六福萬怡暨六福村核心網路設備	• 核心網路設備包含防火牆及Core-Switch。汰換後將優化底下功能: 1. 新增SSLVPN功能及MFA(多因子認證)功能: 提升外部跨平台設備使用更安全連線方式進入企業內網. 2. 提升防火牆本身防毒與防駭攻擊的過濾機制，並支援 site to site VPN policy管控: 可在防火牆內進行網段Policy 管理，減少駭客橫向移動感染攻擊風險。
執行企業內部管理之個資資料庫加密	• 針對企業內部”員工入口網站系統”內，具有個資資料之系統資料庫進行加密，減少個資機敏資料外洩風險。
優化連線傳輸加密方式	• 針對企業內外部網站連線方式由舊有的”Http”連線方式全面改為”Https”的加密連線方式，以減少在連線傳輸的過程中被竊取資料。

113年度購買防毒軟體支出250千元，113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113年12月27日。