LEOFOO
六福旅遊集團
TOURISM GROUP

電腦設備暨網路資訊安全管理

為「維護公司資訊之機密性、完整性、可用性與適法性，避免發生人為疏失、蓄意破壞與自然災害時，遭致資訊與資產遭致不當使用、洩漏、竄改、毀損、消失等，影響本公司作業，並導致公司權益損害」。故制定安全管理制度，強化資訊安全基礎架構設計及保護技術。確保資訊之系統可用性、限制權管及存取管理、抵抗外部威脅及保障員工，供應商和客戶進行業務接洽時之隱私權保護與資訊安全維護。

為確保營運業務持續運作及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，並保障人員資料之隱私。

為達成上述目標，分別以底下三個面向建構出全方位的資安防護能力，包含:

1.使用者人員管理

(1)一般使用人員

- 公司員公電腦均需安裝規定核可之防毒軟體，並需隨時進行病毒碼程式更新。
- 登入公司內部網域均需經由網域認證，並經由核可後的電腦才能連結公司系統存取資料.
- 使用人員因業務之需要,存取對象資訊系統前後台系統之權限,需先進行帳號申請，且存取權限僅限於執行負責部門單位任務之權限,並遵守資訊安全規定之行為(例如密碼修改原則)。
- 使用人員離職時，依規定取消其使用公司內資訊系統之所有帳號權限。
- 一人一帳號，避免使用者將自己的登入帳號與登入密碼供他人使用。
- 禁止以任何方法竊取其他合法使用者的登入帳號與登入密碼，並禁止下載安裝網路上未經許可的檔案程式。
- 嚴禁持有色情或猥褻檔案，並禁止在網路上散播色情文字、圖片、影像、聲音等。

(2)網路系統管理人員

- 執行使用者個別的帳號權限管理，包括其帳號之建立、停用、刪除，權限的編輯設定等。
- 執行系統網路安全相措施,包含資安風險偵測及因應風險規避設定與操作(例如公告提醒員工危險郵件、系統設定防禦攻擊)，以確保各單位內部系統主機與資料的安全與完整。

2.軟體資料管理

(1)軟體程式維護管理

- 每套資訊系統均設有專人負責維持其運作監控管理。

- 系統軟體程式變更須經過權責單位主管核定，並管理變更紀錄。
- 各部門單位使用者禁止使用非法軟體。
- 各部門單位使用者之個人電腦安裝防毒軟體，防止病毒在網路上擴散。使用者如偵測到病毒入侵，須立即與網路離線，避免病毒的擴散，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。
- 應用軟體使用之資料庫需提供加密機制。

(2)資料維護管理

- 各類資料因其特性及內容不同，給予不同的管理與取存權限(例如讀取、建檔、修改、刪除)，須經申請並得部門主管核准後，方可使用。
- 資訊系統管理者將依據各授權原則提供各資料保護方式，以確保各個系統在傳輸資訊時的安全性。此外對於資料本身的保護性也需要一定的管理機制:
  - 備份：透過定期自動排程或手動的操作，將資料備份到”備份資料儲存區”，確保原資料因故損壞時能有複本資料可供系統回復(Recovery)，以降低資料損壞所造成原系統功能運作的衝擊。
  - 備援:透過硬體或軟體的技術，將資料及系統程式完整複製到另一硬體系統上，以確保原系統軟硬體及資料在毀損或操受破壞時，能有另一複製的系統資料能直接提供備援服務，以確保原系統功能運作正常。

3.電腦設備及網路管理

(1)電腦資訊設備保護

- 電腦設備放置於指定適當的場所，並均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。
- 除了系統另有資訊專責管理人員之外，機房基礎設備(包含電力與空調)也都安裝不同迴路與不斷電系統，以及裝設溫度感知機制。

(2)網路連線作業管理

- 公司內部網域與外部網際網路經裝設防火牆做防禦，以減少外部攻擊。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。
- 員工因業務需要必需經由外部電腦遠端登入公司內部系統時，除了系統帳密管理之外，另需有額外的安全連線機制。
- 遠端登入的安全連線機制需要先經申請審核，通過後才能安裝設定使用。

(3)系統帳號密碼管理：

- 使用者登入資訊系統必需要輸入其個人帳號與密碼。帳號的啟用須先經由使用員工經過申請程序審核通過後取得。
- 登入密碼至少須有一定的字數及規則，並由英文字母大寫、英文字母小寫與數字符號構成。

- 密碼皆須強制定期更改，以提高安全性。
- 密碼登入數次失敗後，該帳號會進行“鎖定”，以防止有心人士進行嘗試破解帳號駭入系統。
- 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停用移除。

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2021年12月27日。