寒舍餐旅管理顧問股份有限公司
資訊安全風險之管理

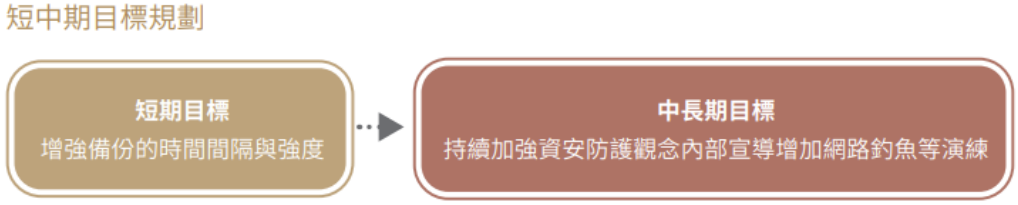
（一） 資通安全風險管理架構

1. 企業資訊安全治理組織

本公司設有「資訊安全委員會」，由各館飯店總經理與資訊安全召集人資訊處，統籌寒舍集團旗下各飯店資訊安全及保護相關政策制定、執行、 風險管理與遵循度查核，並由各部門一階主管級實際執行各部門資訊安全及資料保護相關政策,並由集團資訊處最高主管每年向董事會彙報資安管理成效、資安相關議題及方向。本年度資訊安全管理情形，資訊主管業已於 112/11/9 向董事會報告。

（二） 資通安全政策

除設置「資訊安全委員會」為權責單位，寒舍餐旅已建置資安管理機制，以防範電腦網路犯罪與 危機，另通過「資訊系統中斷服務之緊急應變計劃」並規劃定期演練、優化，當發生資安事件或 系統毀損時，也能於最短時間恢復運行到持續營運不中斷。為降低網路安全風險及維護公司和客戶資料安全，除制定規範，我們也持續透過跨部門的協力幫助，定期辦理教育訓練宣導資安觀念及應用資安工具，在尋找合作廠商時也會特別重視信譽良好 並具專業能力之廠商，並於各飯店官網首頁均有防詐騙提醒資訊，平日亦不定期發送簡訊提醒賓客，除了以上措施外並增加第三方複審稽核，由資安廠商進行核心系統弱點掃描及網站滲透測試，以提升資安防護能力。



（三） 具體管理方案

寒舍餐旅針對資訊安全透過以下方針，持續精進集團資訊安全管理：

寒舍餐旅管理顧問股份有限公司
資訊安全風險之管理

• 建立電腦網路系統的安全控管機制：確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取造成機密資料外洩。

• 對於跨公司之電腦網路系統，加強網路安全管理：對內安裝防毒軟體，設置對外之網路防火 牆，以防止電腦病毒、攻擊性之惡意軟體入侵，而造成公司網路系統癱瘓。

• 教育員工正確概念：確保員工正確認知電腦病毒的威脅，並使用合法軟體，提升員工的資訊 安全警覺。關於使用者之帳號及密碼，叮嚀員工避免使用容易被識破及猜測的密碼，密碼不 可為空白及外流，並且定期更改密碼。

• 離職員工帳號：充分檢查是否予以停用，確實預防資料外洩。

• 建置 WAF 防護：為因應各種新型態網路攻擊，我們每季實施弱點掃描，預先找出公司網站缺 失加強防護。

• 建置 DLP 資料外洩保護監控系統：為全方位防止資料外洩，透過此系統我們持續保護資料安 全性。

• 外部第三方定期檢測：委託專業網路安全公司每季針對公司的 IT 基礎架構進行檢視，進行弱 點掃描以持續優化。

• 定期內控自評網站弱點、實行災難演練：為強化公司的資安韌性，我們制訂各種情況的應對 SOP，推動所有系統完整備份資料及系統主機備份工作，並每日檢查備份記錄。關於 IT 基礎 架構每季由專業網路安全公司每季定期檢視，持續優化。

（四） 投入資通安全管理之資源

資訊安全已為公司營運重要議題，對應資安管理事項及投入之資源方案如下：設有專職之企業組織「資訊安全委員會」，負責公司 資訊安全規劃、技術導入與相關的稽核事項並有 7 名資安管制人員，以維護及持續強化資訊安。

- 設備更新 : 持續不斷更新系統主機 ,及增購新備份機制 , 提升系統可靠性及縮短系統故障時停機由 24 小時提升至 4 小時之內。
- 客戶滿意：無重大資安事件，無違反客戶資料遺失之投訴案件。
- 教育訓練：所有新進員工到職前皆完成資訊安全教育訓練課程執行率 100%；112 年執行社交工程釣魚郵件測試 470 帳號有 96%符合資安標準 4% 使用者持續加強資安教育。
- 資安公告：不定期發送資安公告，提醒使用者新資安風險及攻擊手法及新防護規定與注意事項。