

## 資訊安全管理

### ➤ 資訊安全風險架構

本公司資安小組隸屬於資訊部門，負責審視公司資安政策、監督資安管理運作情形，確認本公司資訊安全管理運作之有效性，並建立同仁良好的資訊安全意識。每年定期由內部稽核單位執行資訊安全管理作業查核，出具稽核報告，並定期於審計委員會及董事會做稽核結果業務報告。

### ➤ 資訊安全政策

#### ● 目的

為確保本公司營運業務提供流程中之資訊機密性、完整性及可用性，並符合相關法規之要求，降低本公司面臨之內外部資訊安全風險，制定相關政策規範。

#### ● 範圍及管理措施

資訊安全範圍共包含以下管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竊改、破壞等情事發生，對本公司帶來各種可能之風險及危害。

項目	相關作業或控制措施
資安治理	制定完整管理制度，定期檢視及修訂相關作業規範 強化資安教育訓練 資訊安全政策遵循性管理
資訊資產及系統管理	定期盤整資訊資產清單，落實各項管控措施 實體與環境安全 通訊與作業安全 資訊系統開發與維護之安全 資料備份管理
權限管理	同仁帳號、密碼及必要業務之使用權限設定管理、並定期更換 資料存取控制
外部威脅	個人電腦安裝防毒軟體且定期更新病毒碼 禁止使用未經授權軟體 資訊安全事件暨事故管理

#### ● 目標

透過上述資訊安全範圍管理與管制，結合預防與復原控制措施及程序，落實本公司企業持續營運之目標，預防營運活動中斷，將可能造成營運中斷之風險降低到可接

受的等級。

持續辦理資訊安全教育訓練與宣導，提高員工資安意識與強化其對相關責任的認知，確保資訊之機密性及完整性，並保障員工、業務及客戶資料之隱私無虞。

建立資訊業務永續運作計畫，執行符合相關法令或法規要求之資訊業務活動運作。

➤ 執行情形

本公司於 112 年 3 月 20 日向審計委員會及董事會報告資訊系統管理制度執行情形及資通安全檢查結果。

經檢討各部門資安管理之執行情形，112 年度並無發生危害資安之事件。