AIBEST · 愛貝斯網路

資訊安全政策

愛貝斯設計有限公司

愛貝斯設計有限公司
資訊安全政策

2024 年 5 月總經理核定訂定｜2025 年 6 月修訂（配合 ISO/IEC 27001:2022）

第一章　目的與範圍

第一條　本公司為確保所屬資訊資產之機密性、完整性與可用性，保護公司、客戶及網站使用者之資料免於遭受內外部之蓄意或意外威脅，並符合相關法令及契約要求，特訂定本政策。

第二條　本政策適用於本公司全體員工、外包人員、供應商及所有可存取本公司資訊資產之人員。資訊資產包括硬體設備、軟體、雲端服務、網路、資料、文件及人員。

第三條　本公司資訊安全管理系統（ISMS）之範圍，涵蓋台中總部之網站設計開發、主機維運與 AI 服務，並依 ISO/IEC 27001:2022 建置及持續改善。

第二章　資訊安全目標

第四條　本公司資訊安全目標如下：一、每年重大資安事件為零件。二、全體員工每年完成資安教育訓練比率達百分之百。三、核心服務系統年度可用率達百分之九十九點九以上。四、客戶網站高風險弱點於七日內修補完成。五、社交工程演練全年平均點擊率低於百分之五。

第五條　資訊安全目標應每年由資訊安全委員會檢討，並依風險評鑑結果、營運需求及外部威脅變化調整之。

第三章　組織與權責

第六條　本公司設置資訊安全委員會，由總經理擔任召集人，成員包括營運副總、技術長及各部門主管，負責核定資訊安全政策、目標及資源配置，並每季召開會議。

第七條　本公司設置資訊安全室，負責資訊安全管理制度之規劃、執行、監控、事件應變、教育訓練及社交工程演練。

第八條　各部門主管應督導所屬人員遵循資訊安全規範，並指派資安聯絡窗口協助推動相關事務。

第四章　管理原則

第九條　存取控制：資訊系統之存取應依業務需要及最小權限原則授權，重要系統應採多重驗證，並定期覆核權限。人員離職或職務異動時，應即時停用或調整權限。

第十條　資產管理：資訊資產應建立清冊並指定負責人，依機密等級予以標示、保護及處理。

第十一條　實體與環境安全：辦公區域及機房應設置門禁管制，重要設備應有適當之電力與環境防護。

第十二條　營運安全：系統應定期更新及修補弱點，並執行惡意程式防護、日誌監控與備份。備份應依三二一原則辦理並定期進行還原測試。

第十三條　開發安全：網站及系統開發應遵循安全程式開發規範，並於上線前執行程式碼審查及弱點掃描。

第十四條　供應商管理：委外廠商及雲端服務商應簽署保密協議，並依本公司資訊安全要求提供服務；可接觸客戶資料者，應接受本公司之評鑑與稽核。

第十五條　事件管理：發現資訊安全事件時，應依資安事件通報及應變程序立即通報，並採取必要之控制措施、通知受影響之客戶及進行根因分析。

第十六條　營運持續：本公司應訂定營運持續計畫，並每年至少演練一次，確保重大事故發生時核心服務得以持續或及時恢復。

第五章　教育訓練與附則

第十七條　全體員工每年應完成至少三小時之資訊安全教育訓練；新進人員應於到職一週內完成。本公司並定期辦理社交工程演練，以提升人員警覺。

第十八條　違反本政策者，依本公司相關規定懲處；情節重大或涉及法律責任者，依法處理。

第十九條　本政策每年至少檢討一次，經總經理核定後公告實施，並告知全體員工及相關外部單位。