必應創造股份有限公司
B'IN LIVE CO., LTD.

資通安全政策

一、目的

本政策規範本公司資訊安全管理制度，以確保本公司管轄資訊資產之機密性、完整性、可用性及符合相關規範及法規之要求。

二、適用範圍

本公司員工、接觸本公司業務資料之外機關人員、委外廠商及訪客。

三、要求事項

資訊安全目標為確保本公司資訊資產、資料之安全及各項公司營運相關資訊作業之執行順利，制定本公司之資訊安全政策，以提供全體人員遵循。

1.各項資訊安全防護及管理規定。應符合政府之資訊安全相關政策及法令要求。

2.所有資訊作業相關措施，應確保業務資料完整性、可用性及機密性，防止敏感性資料與個人資料外洩與遺失。

3.資訊資產（包括軟體、硬體、網路通訊設備及資料庫等）應予適當保護，採行合宜之備份回復措施及作業，防止未經授權或因作業疏失對資產所造成之損害。

4.本政策及各項資訊安全規定應每年定期評估檢討，以符合政府法令、技術發展及業務需求等，以落實資訊安全作業及管理。

四、管理方案

1. 存取控制管理：控管同仁與第三方人員對服務營運相關之資產、網路、系統、應用程式及其資訊之存取防止任何未經授權之存取行為，及保護機敏性資料或設備免於竊取或破壞之風險。

2.實體與環境安全管理：保護本公司之設備及周邊設施，降低因環境安全、設備操作、維護與管理疏失或不當，造成資產遭受失竊、破壞、遺失之機會，以達成安全控管的目的。

3.資訊系統開發管理：系統購置或開發前應進行安全功能需求之評估，開發過程須確保開發人員於原始碼及敏感資料之存取權限適切地劃分，並確保資訊系統於資料處理過程中的正確性及系統開發環境之安全。

4.系統主機管理：導入虛擬化容錯移轉之備援架構，以避免故障影響，同時定期完整備份資料及執行異地保存等。

5. 委外廠商管理：委外廠商在執行委託之需求，應評估相關之資安風險。並要求委外廠商依本公司資安相關規定對委外商進行適當之監督與管理。

6.加入 TWCERT/CC 等資安聯防組織，強化資安聯防體系與威脅情資共享。

7.持續社交工程演練及教育訓練提升員工資訊安全意識。

8.持續提升資安人員專業培訓，確保作業人員皆符合資通安全標準。

9.弱點掃描系統隨時掌握系統漏洞並持續追蹤及改善。

五、管理階層審查修訂

確保「資訊安全管理系統」實務運作之可用性、安全性及有效性。本政策每年依業務變動、技術發展及風險評鑑的結果或配合政府及關注方資訊安全管理要求、法令、技術及最新業務發展現況至少評估或修訂一次。

六、施行

本政策須經執行長審核，核定後公告或傳達給本公司各單位人員與相關外部單位實施，修訂時亦同。