國泰建設股份有限公司
資訊安全政策

112.06.20 訂定
112.09.26 修訂
權責單位: 行政管理部

第一條(目的)

為強化國泰建設股份有限公司(以下簡稱本公司)之資訊安全管理，建立安全及可信賴之資訊作業環境，確保資訊資產之機密性、完整性及可用性，並提昇同仁對資訊安全認知，以保障本公司、客戶與員工之權益，特制定本公司資訊安全政策（以下簡稱本政策）。

第二條(政策聲明)

本公司資訊安全管理之政策聲明如下:

一、本公司資訊安全措施，應依「個人資料保護法」及參考相關法令、主管機關規定及本政策之要求。

二、本公司資訊資產，嚴禁未經授權存取與洩露。

三、資訊系統建置應考量有效之資訊安全措施，以降低內部網路及電腦主機系統遭受駭客或內部人士之入侵攻擊或未經授權存取等威脅風險。

四、本公司全體員工(以下含約聘人員、工讀生、派遣人員、實習生)及其他得接觸本公司業務相關資訊之合作夥伴、委外廠商等均有責任及義務保護其所取得或使用之資訊資產，以防止未經授權存取、擅改、破壞或不當揭露。

五、本公司所有員工對於有發生資訊安全事件、弱點及違反本政策與程序之虞者，應隨時保持警戒，並依公司規定程序進行通報。

六、本公司資訊業務委託合約，應規範下列事項：

（一）委託作業事項範圍及受託機構之權責。

（二）受託人員均應善盡責任保護本公司資訊資產，未經授權不得任意存取、擅改、 破壞或不當揭露。

（三）受託人員應遵守本政策與相關管理規範，對於有發生資訊安全事件、弱點及違反本政策與程序之虞者，應隨時保持警戒，並立即通報本公司相關業務負責單位以及資訊單位。

（四）保密條款及查核條款。

（五）合約終止與解約條款。

（六）罰則及損害賠償條款。

（七）其他必要事項。

七、本公司有權管理歸屬於本公司資訊資產，包含但不限於在本公司資訊資產或以本公司名義使用網路資源上所處理、儲存或傳輸交換之資訊。

八、所有員工如違反本政策或相關資訊安全規定者，將衡酌情節追訴其法律責任，併移送人資單位議處。

第三條(資訊安全目標)

一、以「保護資訊資產安全」及「維持業務持續運作，以達企業永續經營」為目標，保護股東權益為基礎，進而達成本公司之使命及願景。

二、為確保本公司的協同可發揮最大利益，並善盡社會責任，本公司應以符合法令及風險管理之原則，建立完善之資訊安全管理制度，保護本公司所擁有及使用之資訊與個人資料。

三、所有資訊作業相關措施，須確保本公司資訊之安全，防止敏感性與機密性資料外洩或遺失。

四、適當保護資訊資產（含軟體、硬體、網路通訊設施及資料庫等），採行合宜之備援或備份回復設施及作業，防止未經授權或因作業疏忽對資訊資產所造成之損害，並定期演練前項備援或備份回復作業。

五、本公司所執行之專案，應有適當之資訊安全管理措施，以確保相關資訊受到適當保護。

六、定期實施資訊安全教育訓練，加強資訊安全政策宣導。

第四條(適用對象及範圍)

本政策適用對象為本公司全體員工(以下含約聘人員、工讀生、派遣人員、實習生)及其他得接觸本公司業務相關資訊之合作夥伴、委外廠商等。

本政策適用範圍如下(以下合稱資訊資產)：

一、本公司所有資料與文件。

二、本公司所有主機、伺服器、個人電腦、終端設備、通訊線路，以及與前述設備相關或是與本公司資訊系統相連等之硬體資訊資產。

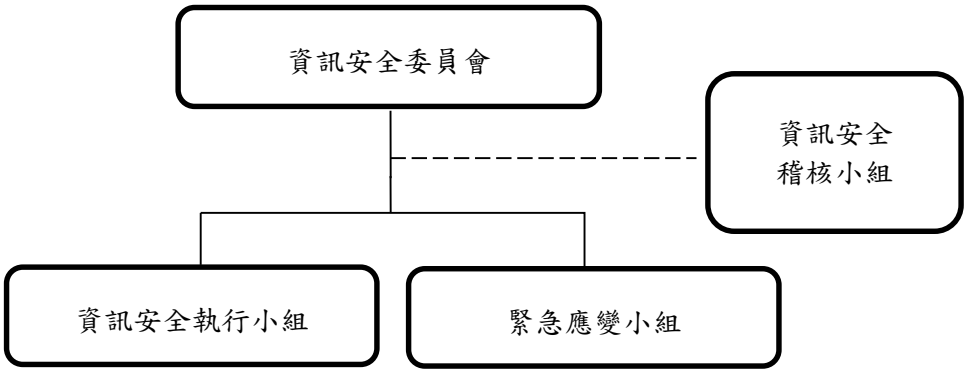
三、本公司所有存放硬體資訊資產之實體環境。

四、本公司所有應用系統，以及與前述應用系統相關或是與本公司資訊系統相連等之軟體資訊資產。

五、其他本公司所有資訊資產，或其他本公司未實際所有，但基於合約、法律及法規所賦予之責任而可支配之資訊資產。

第五條(資訊安全治理架構)

為有效推展本公司整體資訊安全及執行情形，公司資訊安全組織圖如下：



一、資訊安全委員會：

(一) 委員組成：

本會設置指導委員，由本公司董事長、總經理、資深副總經理擔任，主任委員由本公司資訊安全長擔任，其他委員由副總經理、協理、部室主管、資安專責主管擔任之；得視需要邀請指導委員列席指導。

(二) 會議召集：

每年至少召開一次資訊安全管理審查會議，審查組織之資訊安全管理制度，以確保其持續的合宜性、適切性及有效性。並得視需要召開臨時會議。

(三) 組織任務：

1. 資訊安全政策之審核。
2. 資訊安全管理推展、規劃、溝通協調。
3. 資訊安全稽核結果及建議改善事項審核
4. 資訊安全制度執行之各項矯正及預防措施檢討。

二、資訊安全執行小組：

(一) 由本公司資安專責單位及資訊單位共同組成。

(二) 組織任務:

1. 負責資訊安全政策之研擬修訂。
2. 負責規劃及執行各項資訊安全管理制度相關作業。
3. 資訊安全執行情形之彙整報告。
4. 資訊安全稽核結果及建議改善事項規劃。
5. 資訊安全制度執行之各項矯正及預防措施規劃
6. 建立與本資訊安全管理制度相關之「資訊安全組織成員表」及「外部單位聯絡清冊」，並定期維護更新。

三、資訊安全稽核小組：

由本公司稽核室擔任，負責評估資訊安全管理制度之執行情形，必要時可委託外部專業人員協同執行。

四、緊急應變小組：

由本公司資訊安全長擔任召集人，成員包含本公司資訊安全長、資安

專責單位主管及同仁，負責資訊安全事故因應處理，如有需要亦得邀請相關單位主管加入。

第六條(資訊安全管理指標)

本公司將依業務性質，從機密性、完整性、可用性、隱私性及合法性等方面考量，經資訊安全委員會主任委員或其授權人員核可，制訂其資訊安全及個人資料管理有效性量測表，利用量化指標之管理落實本政策。

第七條(資訊安全責任)

一、資訊安全及個人資料保護是本公司全體同仁的責任，應共同維護之。

二、管理階層應支持資訊安全及個人資料管理制度，並積極參與資訊安全及個人資料管理制度活動。

三、為能有效確保本公司之資訊安全，本公司應針對各資訊安全領域訂定資訊安全規範。

四、本公司應定期評估本政策，以反映法令規章、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

五、所有同仁皆應遵循本公司資訊安全事件通報機制，通報所發現之資訊安全事件或資訊安全弱點。

六、本公司每年應規劃並提供人員資訊安全訓練課程，以提昇人員資訊安全認知。

七、本公司委外人員（單位）應簽署保密協議書，並遵守本政策、營業秘密法、個人資料保護法及相關程序之規定。

八、未經授權不得使用本公司之各類資訊資產及個人資料。

九、本公司所有同仁若未遵循資訊安全相關規範或有任何違反資訊安全要求之行為，應依相關規定議處。

第八條 (附則)

本政策應每年配合政府法令、環境、業務與技術之變動評估檢討，其修正經資訊安全委員會審核通過及呈請總經理核定後公告施行。