中国平安 PING AN
专业 · 价值

專業 讓生活更簡單

平安集團
信息安全管理政策聲明

2024年3月

隨着平安集團深入推進全面數字化轉型，數字化業務場景日趨豐富、業務眞實數據量高速增長，信息安全已成爲平安實現可持續發展的重要基石。平安承諾以高標準體系管理信息安全風險，確保全集團信息系統的安全與可靠運作，爲各項業務向客戶提供多樣化的產品和便捷的服務提供堅實保障。

適用範圍

本政策聲明適用於平安集團、所有成員公司、所有部門、員工，以及能接觸到信息資產的第三方人員（包括但不限於外包公司人員、代理人、廠商工程師、咨詢公司顧問等），覆蓋平安所有業務板塊。

承諾

平安承諾以高標準開展信息安全管理，具體包括：

- 嚴格遵守國家法律、監管機構法規及行業規範和守則的信息安全要求，並以最高標準作爲規範原則；
- 確保信息受到適當的保護，保證信息的保密性、完整性、可用性；
- 構建信息及信息系統安全控制是以深度防御及默認安全爲實施原則；
- 信息及信息系統所建立的保護與其敏感度、價值及重要性相匹配。

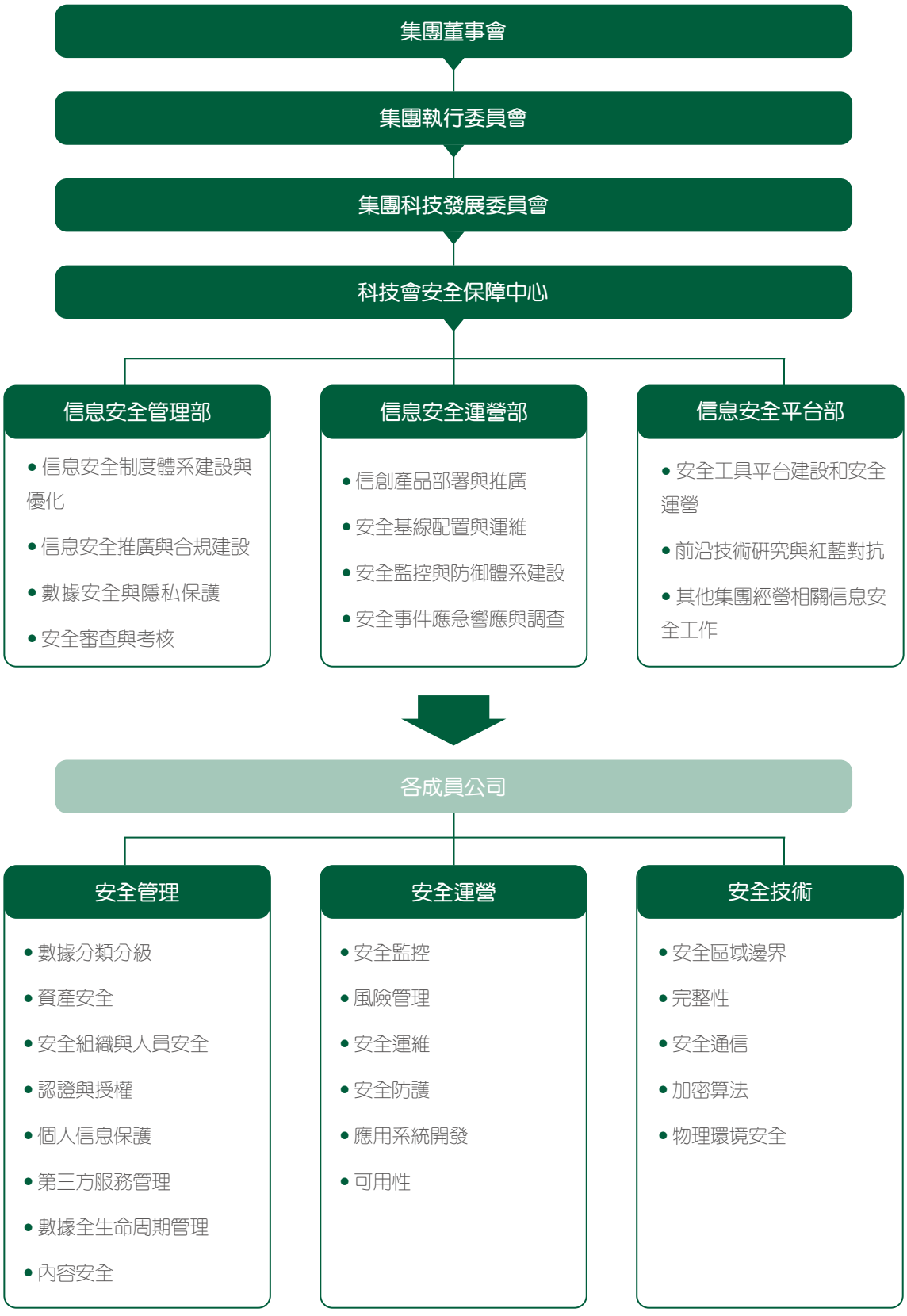
信息安全管理架構

集團董事會負責監督及監察本集團信息安全事宜的管理表現，以及監督、評估及確保信息安全管理體系運行的有效性，對集團信息安全風險管理承擔最終責任。

集團執行委員會下設集團科技發展委員會（以下簡稱集團科技會）是本集團信息安全工作的領導機構，監督集團信息安全管理措施有效且持續執行。集團科技會下設安全保障中心統籌網絡安全、數據安全和個人信息保護工作，主要從集團層面，整體負責統籌、規劃、構建、推動、組織協調開展信息安全工作。

各成員公司已明確網絡安全負責人、數據安全負責人和個人信息保護負責人，落實網絡安全、數據安全、個人信息保護責任。履行信息安全義務，落地具體的管控策略，確保數據機密性、完整性、可用性。

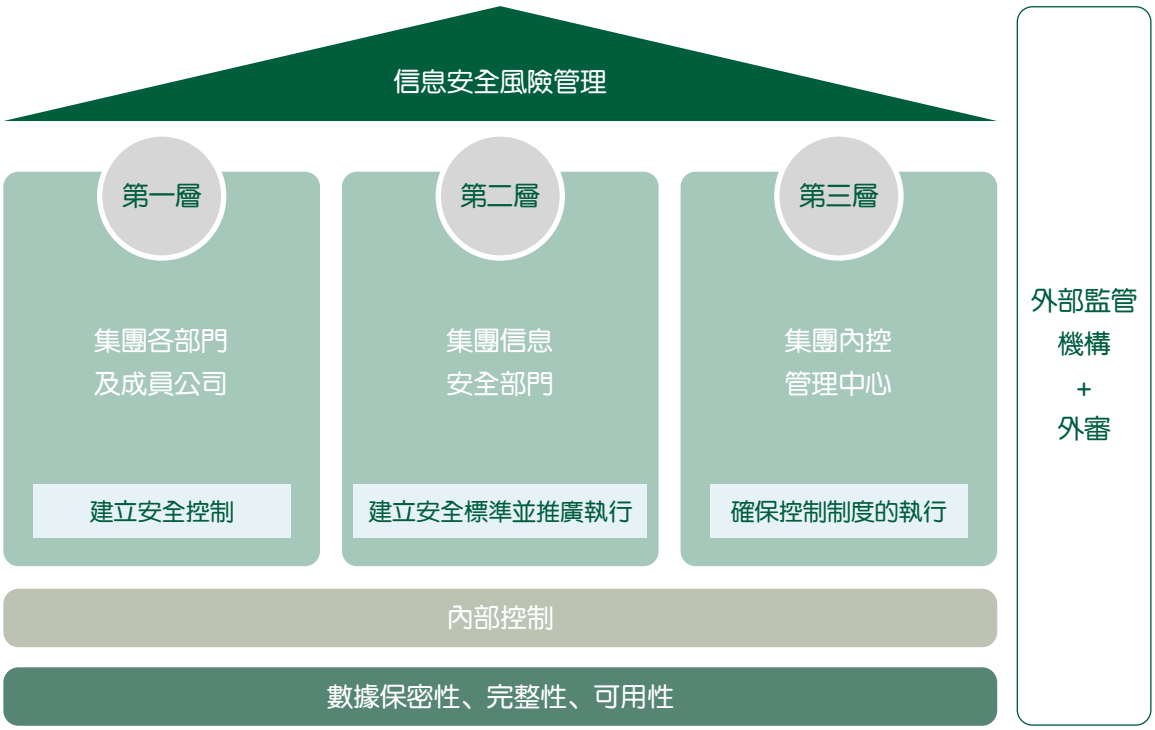
平安信息安全管理架構及主要工作範疇展示如下。



信息安全管理體系

信息安全風險管理是就信息安全風險對公司進行指導和控制的協調活動，包括評估準備、風險識別、風險定級、風險評價、風險分析、風險處置、風險監控、風險審批、風險報告等。識別和評估信息安全風險，確保信息安全風險被全面識別，並將信息安全風險控制在可接受範圍，降低其對組織的影響。

平安的信息安全管理體系由三道防線構成，各層承擔不同的信息安全角色及責任，共同執行保護信息資產的工作。平安的每一位人員，都有共同的責任，做好保護信息資產的工作。



第一道防線

第一層爲集團各部門及成員公司，主要負責安全控制，通過建立安全防控及事件響應與處置措施，保護信息資產的保密性、完整性及可用性。

第二道防線

第二層爲集團信息安全部，主要負責建立安全規範並推廣執行，通過構建信息安全體系，落實合規審查與培訓考核，完善信息安全管理工作。

第三道防線

第三層爲集團內控管理中心，主要負責確保控制制度的執行，通過對集團各部門及成員公司進行獨立審查，評審信息安全工作的執行情況。

信息安全原則與措施

平安依據法律法規及行業標準，確立了信息保護的原則和措施的方向，圍繞安全管理、安全運營和安全技術形成 12 個工作重點：

資產安全與數據分類分級

- 所有信息資產，包括著述、口述及電子信息，都應該根據其敏感性、重要程度以及業務所要求的訪問限制原則進行分類和標識。

- 所有與信息相關的重要資產都應該在資產清單中標出，並及時維護更新。

- 根據數據分類分級原則、規則對數據進行分類分級，對不同級別數據實施保密保護要求。

安全組織與人員

- 所有工作崗位必須有安全職責描述，並且說明崗位的敏感性。

- 員工在入職前必須通過品格審查，並簽訂保密協議，人員崗位發生變化或離司時，必須執行相關程序，確保信息資產保護不受影響。

- 任何違反平安信息安全制度的人員均會按照最新的《「紅、黃、藍」牌處罰制度》進行處罰，對於特別嚴重的行爲平安將會追究法律責任。

- 在信息安全意識宣導上，所有新入職人員在新入職期的首三個月內會完成入職信息安全培訓。同時，平安每年都對所有員工及第三方人員開展信息安全相關主題培訓，覆蓋數據安全、個人信息保護、終端安全等安全領域內容，全面加強員工的信息安全保護意識及技能。各成員公司也在集團的指導下，根據業務實踐針對性地開展信息安全主題培訓。

認證與授權

認證

用戶在訪問信息和信息系統之前，需要進行身份認證，認證方式與信息的敏感性及風險程度相適應。

授權

遵循權限最小化原則、知悉需要原則，祇開通必要的權限。

職責分離

任何人員不容許單獨一人進行整個業務交易或者操作程序。高風險的功能必須採取有效的監控措施，例如分拆工序、工序輪流、強制執行審查及審批程序。

系統開發及維護

• 在應用系統開發、發布、更新過程中，實施安全守則。電子商務應用系統的開發要確保客戶信息在公共網絡環境中的保密性及完整性，並確保交易的不可否認性。

• 所使用的加密算法必須達到數據保護的原則，包括：達到保護數據的機密性、完整性、認證性及不可抵賴性的要求；選用的加密運算必須公開論證；加密密鑰在整個密鑰生命周期中必須妥善管理。

• 對重要業務系統採用如雙因素認證等強身份認證手段，嚴格遵行「最小權限、知悉需要」的權限管理原則防止內部數據竊取行爲的發生；同時，採用先進的技術手段加強系統日志審計，追踪、發現數據泄露行爲。

• 在運維過程中必須確保執行相關變更流程，防止惡意或意外的非授權篡改或刪除信息。

安全監控與防護

• 平安採取主動與被動防御相結合的措施維護系統信息安全，對信息活動進行監控和記錄及對信息安全事件進行全流程操作管理，確保所有對平安信息系統的重要訪問和操作都被記錄，保證在系統中的敏感行爲都有迹可查，能夠準確追溯至負責的執行者。同時，及時響應和處理信息安全事件，保障信息資產和數據安全以及各項業務的安全穩定運行。

• 在網絡入侵方面，根據網絡安全風險態勢，部署 DDOS、IPS、WAF 等網絡安全設備，部署 APT 態勢感知防御系統、蜜罐系統等安全平台 / 工具，從外到內覆蓋安全監控、分析、預警、響應的縱深防御。

• 在威脅情報方面，搭建安全應急響應平台和部署威脅情報系統，收集與信息安全有關威脅的信息，進行分析和排查，發出安全預警並跟踪修復整改完畢。

區域邊界與通信安全

• 根據網絡區域的不同，在網絡邊界部署相應的訪問控制機制，並設置訪問控制規則。

• 通對網絡的性能、流量、非法接入等進行監控，異常情況應及時處理或上報。

• 建立適當的防範，防止信息資產受到惡意或意外的非授權篡改或刪除。

• 所有連接到平安網絡的線路，必須採取適當的安全措施，以保護內部網絡、信息和信息系統，尤其是與公共網絡及非平安管理的網絡的連接控制更爲重要。

• 重大的網絡及操作系統必須在適當的時間內進行重要的補丁；新構建的操作系統必須配置最新的補丁。

• 所有服務器、工作臺及合適的設備必須安裝防病毒、防偵察軟件，並及時升級防病毒系統、更新病毒庫，防止被惡意代碼攻擊。

業務連續性計劃

• 平安建立適當防範，確保信息能夠提供給授權的使用方。當原始信息破壞或者丟失時，提取最近的備份信息以實現業務的連續性。

信息安全合規

• 平安嚴格遵循法律、監管機構、行業常規和守則的信息安全要求，以最高規範爲實施原則。按照法律、法規、合同要求，保護客戶信息及隱私。

• 嚴格履行等級保護、關鍵信息基礎設施保護、商用密碼應用安全性評估和網絡安全審查等義務。

• 網站、APP、小程序、快應用等應依法向監管部門申請互聯網信息服務域名備案或者許可手續，在網站主頁或 APP 的顯著位置標明備案編號或者電信業務經營許可證編號。

信息安全審計與認證

• 平安至少每年開展一次信息安全管理體系的內部審計，審計結果呈報集團董事會、執行委員會和風險管理委員會。

• 平安至少每年開展一次信息安全獨立外部審計，並按照監管機構的管理規定及要求開展具體的專項審計與檢視工作。

• 平安積極推進業務適用的信息安全相關管理體系標準認證，包括但不限於 ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 等。

供應商及第三方信息安全管理

• 平安以高標準管理供應商及第三方服務信息安全事宜。供應商指採購業務中直接、間接向平安提供產品或服務資源的合法市場主體或其他組織。第三方服務人員包括但不限於外包公司人員、代理人、廠商工程師、咨詢公司顧問等。平安以「敏感數據不出平安」爲核心原則，根據相關法律法規，結合業務實際情況，制定並執行《集團第三方服務安全管理規範》《集團供應商信息安全管理制度》等管理制度。平安實施採購管理、分類分級、合同條款、監控評價、風險管理、監管報告等管理要求，並通過充分溝通，確保供應商及第三方知悉並執行平安的管理要求，切實降低與供應商及第三方合作帶來的信息安全風險。

• 平安定期對合作供應商及第三方進行信息安全和隱私保護合規性評估，評估內容包括但不限於數據儲存、管理制度、技術措施保障、訪問權限、災難恢復設施和應急管理體系等。同時，平安每年還將通過問卷等方式對供應商進行盡職調查，並對其中的重要供應商進行現場審計。

內容安全

• 平安建立信息內容安全審核管理機制，遵循「先審後發」原則，針對信息內容違法和不良行爲採取過濾監控，主動阻斷違法不良信息，確保信息內容合法性、準確性、眞實性，維護網絡傳播良好秩序。

物理及環境安全

• 平安採取了嚴格的物理安全防範措施，以防止信息資產與信息系統在未經授權下收到物理訪問、破壞或者幹擾。同時，針對火災、水災、騷亂等天災、意外或者人爲災難對信息設備的影響，平安設計並實施了相對應的物理環境保護措施。

該政策聲明由平安集團解釋和修訂，集團會適時根據國家政策、監管要求和行業發展進行更新。