中国平安 PING AN
专业 · 价值

专业 让生活更简单

平安集团
信息安全管理政策声明

2024 年 3 月

随着平安集团深入推进全面数字化转型，数字化业务场景日趋丰富、业务真实数据量高速增长，信息安全已成为平安实现可持续发展的重要基石。平安承诺以高标准体系管理信息安全风险，确保全集团信息系统的安全与可靠运作，为各项业务向客户提供多样化的产品和便捷的服务提供坚实保障。

适用范围

本政策声明适用于平安集团、所有成员公司、所有部门、员工，以及能接触到信息资产的第三方人员（包括但不限于外包公司人员、代理人、厂商工程师、咨询公司顾问等），覆盖平安所有业务板块。

承诺

平安承诺以高标准开展信息安全管理，具体包括：

- 严格遵守国家法律、监管机构法规及行业规范和守则的信息安全要求，并以最高标准作为规范原则；
- 确保信息受到适当的保护，保证信息的保密性、完整性、可用性；
- 构建信息及信息系统安全控制是以深度防御及默认安全为实施原则；
- 信息及信息系统所建立的保护与其敏感度、价值及重要性相匹配。

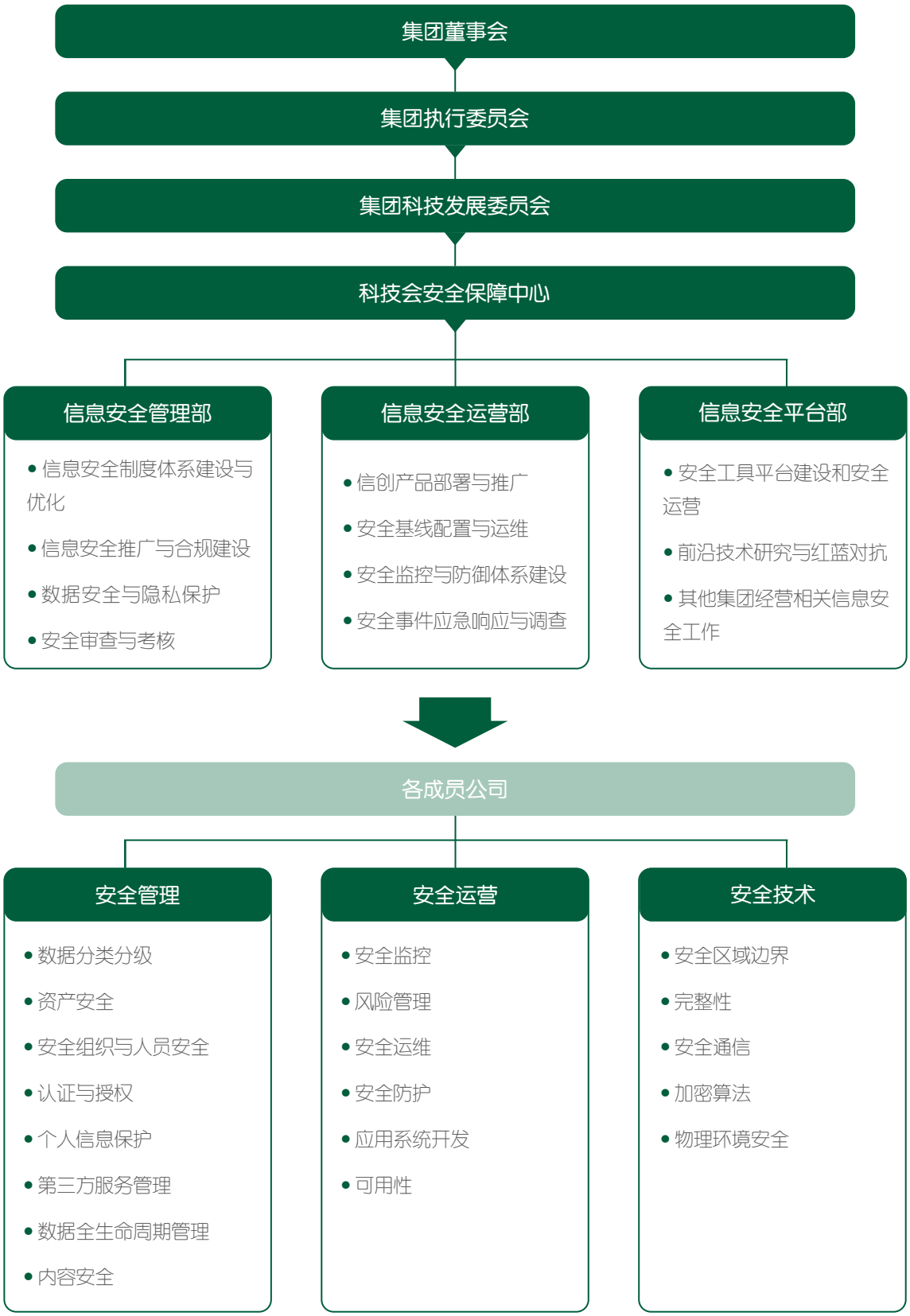
信息安全管理架构

集团董事会负责监督及监察本集团信息安全事宜的管理表现，以及监督、评估及确保信息安全管理体系运行的有效性，对集团信息安全风险管理承担最终责任。

集团执行委员会下设集团科技发展委员会（以下简称集团科技会）是本集团信息安全工作的领导机构，监督集团信息安全管理措施有效且持续执行。集团科技会下设安全保障中心统筹网络安全、数据安全和个人信息保护工作，主要从集团层面，整体负责统筹、规划、构建、推动、组织协调开展信息安全工作。

各成员公司已明确网络安全负责人、数据安全负责人和个人信息保护负责人，落实网络安全、数据安全、个人信息保护责任。履行信息安全义务，落地具体的管控策略，确保数据机密性、完整性、可用性。

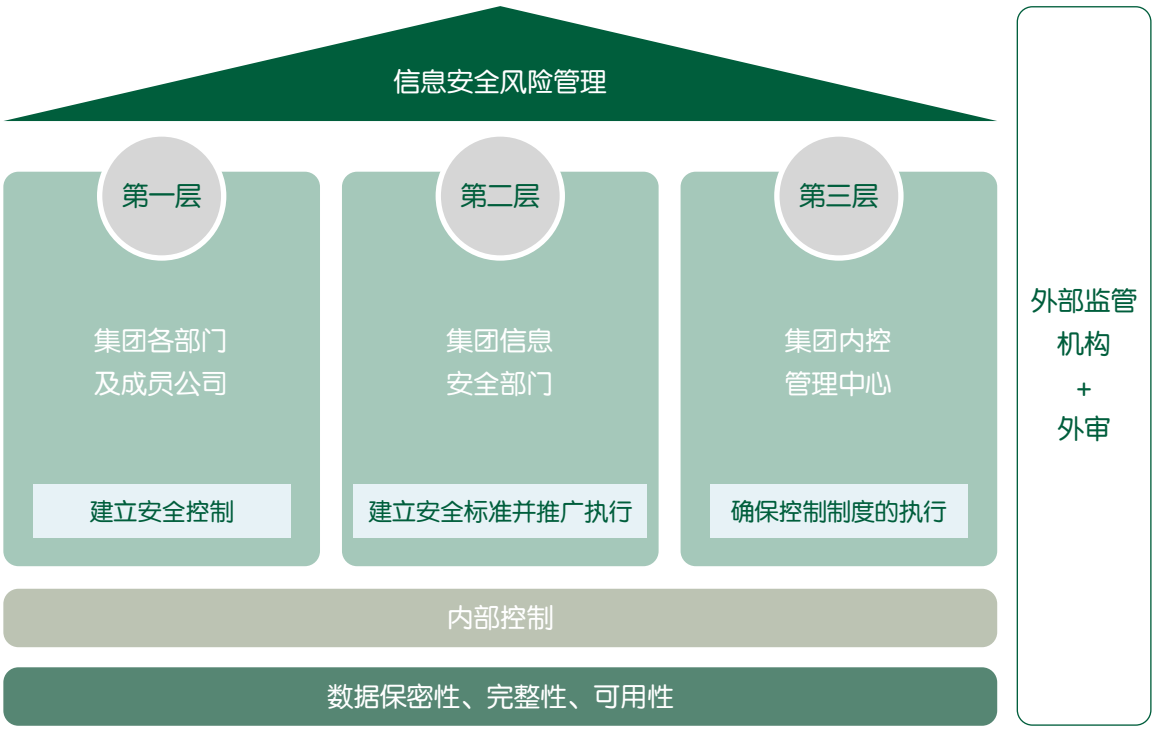
平安信息安全管理架构及主要工作范畴展示如下。



信息安全管理体系

信息安全风险管理是就信息安全风险对公司进行指导和控制的协调活动，包括评估准备、风险识别、风险定级、风险评价、风险分析、风险处置、风险监控、风险审批、风险报告等。识别和评估信息安全风险，确保信息安全风险被全面识别，并将信息安全风险控制在可接受范围，降低其对组织的影响。

平安的信息安全管理体系由三道防线构成，各层承担不同的信息安全角色及责任，共同执行保护信息资产的工作。平安的每一位人员，都有共同的责任，做好保护信息资产的工作。



第一道防线

第一层为集团各部门及成员公司，主要负责安全控制，通过建立安全防控及事件响应与处置措施，保护信息资产的保密性、完整性及可用性。

第二道防线

第二层为集团信息安全部，主要负责建立安全规范并推广执行，通过构建信息安全体系，落实合规审查与培训考核，完善信息安全管理工作。

第三道防线

第三层为集团内控管理中心，主要负责确保控制制度的执行，通过对集团各部门及成员公司进行独立审查，评审信息安全工作的执行情况。

信息安全原则与措施

平安依据法律法规及行业标准，确立了信息保护的原则和措施的方向，围绕安全管理、安全运营和安全技术形成 12 个工作重点：

资产安全与数据分类分级

- 所有信息资产，包括著述、口述及电子信息，都应该根据其敏感性、重要程度以及业务所要求的访问限制原则进行分类和标识。

- 所有与信息相关的重要资产都应该在资产清单中标出，并及时维护更新。

- 根据数据分类分级原则、规则对数据进行分类分级，对不同级别数据实施保密保护要求。

安全组织与人员

- 所有工作岗位必须有安全职责描述，并且说明岗位的敏感性。

- 员工在入职前必须通过品格审查，并签订保密协议，人员岗位发生变化或离司时，必须执行相关程序，确保信息资产保护不受影响。

- 任何违反平安信息安全制度的人员均会按照最新的《“红、黄、蓝”牌处罚制度》进行处罚，对于特别严重的行为平安将会追究法律责任。

- 在信息安全意识宣导上，所有新入职人员在新入职期的首三个月内会完成入职信息安全培训。同时，平安每年都对所有员工及第三方人员开展信息安全相关主题培训，覆盖数据安全、个人信息保护、终端安全等安全领域内容，全面加强员工的信息安全保护意识及技能。各成员公司也在集团的指导下，根据业务实践针对性地开展信息安全主题培训。

认证与授权

认证

用户在访问信息和信息系统之前，需要进行身份认证，认证方式与信息的敏感性及风险程度相适应。

授权

遵循权限最小化原则、知悉需要原则，只开通必要的权限。

职责分离

任何人员不容许单独一人进行整个业务交易或者操作程序。高风险的功能必须采取有效的监控措施，例如分拆工序、工序轮流、强制执行审查及审批程序。

系统开发及维护

• 在应用系统开发、发布、更新过程中，实施安全守则。电子商务应用系统的开发要确保客户信息在公共网络环境中的保密性及完整性，并确保交易的不可否认性。

• 所使用的加密算法必须达到数据保护的原则，包括：达到保护数据的机密性、完整性、认证性及不可抵赖性的要求；选用的加密运算必须公开论证；加密密钥在整个密钥生命周期中必须妥善管理。

• 对重要业务系统采用如双因素认证等强身份认证手段，严格遵行“最小权限、知悉需要”的权限管理原则防止内部数据窃取行为的发生；同时，采用先进的技术手段加强系统日志审计，追踪、发现数据泄露行为。

• 在运维过程中必须确保执行相关变更流程，防止恶意或意外的非授权篡改或删除信息。

安全监控与防护

• 平安采取主动与被动防御相结合的措施维护系统信息安全，对信息活动进行监控和记录及对信息安全事件进行全流程操作管理，确保所有对平安信息系统的重要访问和操作都被记录，保证在系统中的敏感行为都有迹可查，能够准确追溯至负责的执行者。同时，及时响应和处理信息安全事件，保障信息资产和数据安全以及各项业务的安全稳定运行。

• 在网络入侵方面，根据网络安全风险态势，部署 DDOS、IPS、WAF 等网络安全设备，部署 APT 态势感知防御系统、蜜罐系统等安全平台 / 工具，从外到内覆盖安全监控、分析、预警、响应的纵深防御。

• 在威胁情报方面，搭建安全应急响应平台和部署威胁情报系统，收集与信息安全有关威胁的信息，进行分析和排查，发出安全预警并跟踪修复整改完毕。

区域边界与通信安全

• 根据网络区域的不同，在网络边界部署相应的访问控制机制，并设置访问控制规则。

• 通对网络的性能、流量、非法接入等进行监控，异常情况应及时处理或上报。

• 建立适当的防范，防止信息资产受到恶意或意外的非授权篡改或删除。

• 所有连接到平安网络的线路，必须采取适当的安全措施，以保护内部网络、信息和信息系统，尤其是与公共网络及非平安管理的网络的连接控制更为重要。

• 重大的网络及操作系统必须在适当的时间内进行重要的补丁；新构建的操作系统必须配置最新的补丁。

• 所有服务器、工作台及合适的设备必须安装防病毒、防侦察软件，并及时升级防病毒系统、更新病毒库，防止被恶意代码攻击。

业务连续性计划

• 平安建立适当防范，确保信息能够提供给授权的使用方。当原始信息破坏或者丢失时，提取最近的备份信息以实现业务的连续性。

信息安全合规

• 平安严格遵循法律、监管机构、行业常规和守则的信息安全要求，以最高规范为实施原则。按照法律、法规、合同要求，保护客户信息及隐私。

• 严格履行等级保护、关键信息基础设施保护、商用密码应用安全性评估和网络安全审查等义务。

• 网站、APP、小程序、快应用等应依法向监管部门申请互联网信息服务域名备案或者许可手续，在网站主页或 APP 的显著位置标明备案编号或者电信业务经营许可证编号。

信息安全审计与认证

• 平安至少每年开展一次信息安全管理体系的内部审计，审计结果呈报集团董事会、执行委员会和风险管理委员会。

• 平安至少每年开展一次信息安全独立外部审计，并按照监管机构的管理规定及要求开展具体的专项审计与检视工作。

• 平安积极推进业务适用的信息安全相关管理体系标准认证，包括但不限于 ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 等。

供应商及第三方信息安全管理

• 平安以高标准管理供应商及第三方服务信息安全事宜。供应商指采购业务中直接、间接向平安提供产品或服务资源的合法市场主体或其他组织。第三方服务人员包括但不限于外包公司人员、代理人、厂商工程师、咨询公司顾问等。平安以“敏感数据不出平安”为核心原则，根据相关法律法规，结合业务实际情况，制定并执行《集团第三方服务安全管理规范》《集团供应商信息安全管理制度》等管理制度。平安实施采购管理、分类分级、合同条款、监控评价、风险管理、监管报告等管理要求，并通过充分沟通，确保供应商及第三方知悉并执行平安的管理要求，切实降低与供应商及第三方合作带来的信息安全风险。

• 平安定期对合作供应商及第三方进行信息安全和隐私保护合规性评估，评估内容包括但不限于数据储存、管理制度、技术措施保障、访问权限、灾难恢复设施和应急管理体系等。同时，平安每年还将通过问卷等方式对供应商进行尽职调查，并对其中的重要供应商进行现场审计。

内容安全

• 平安建立信息内容安全审核管理机制，遵循“先审后发”原则，针对信息内容违法和不良行为采取过滤监控，主动阻断违法不良信息，确保信息内容合法性、准确性、真实性，维护网络传播良好秩序。

物理及环境安全

• 平安采取了严格的物理安全防范措施，以防止信息资产与信息系统在未经授权下收到物理访问、破坏或者干扰。同时，针对火灾、水灾、骚乱等天灾、意外或者人为灾难对信息设备的影响，平安设计并实施了相对应的物理环境保护措施。