中国平安 PING AN
金融 · 科技

专业 让生活更简单

平安集团
信息安全管理政策声明

2022年1月

本政策适用于中国平安保险（集团）股份有限公司
旗各成员公司及集团职能部门

平安具备丰富的业务场景与海量真实数据，信息安全管理是业务发展中最为关键的一个环节。随着信息系统与数据规模的不断扩大，严格的信息安全管理规范成为平安实现平稳可持续发展的重要保障。

平安集团严格遵循并执行各项法律法规，根据市场监管变化和技术的更新，持续修订更新集团信息安全管理规范。最新版的《信息安全管理规定》，包含信息安全方针、信息安全策略、信息安全标准、信息安全程序、信息安全基线（通常适用于 IT 系统）、指引和守则六大类 22 项规范文档，适用于平安集团、旗下各成员公司的所有部门和员工，以及能够接触信息资产的第三方人员，信息安全制度每两年聘请外部咨询机构进行评估。全集团采取了员工上网行为管理、打印控制、文档加密、硬盘加密、水印跟踪等一系列的行为控制和安全防护手段。

历经十几年的不断完善与实践，平安始终以最高标准执行管理规范，为平安的信息化业务保驾护航。

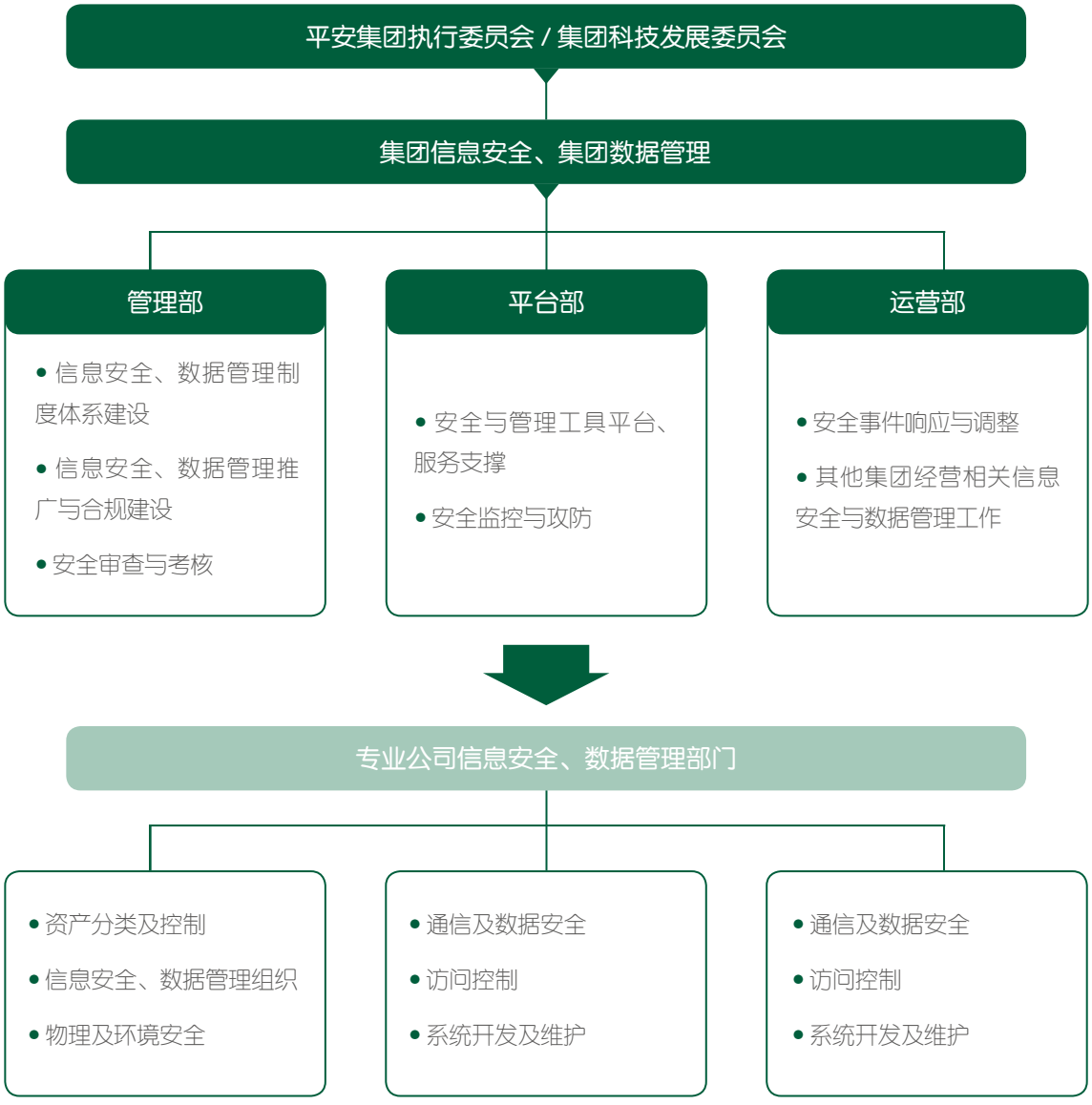
承诺

平安承诺建立并推行高标准的信息安全规范，并：

- 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
- 信息受到适当的保护，确保信息的保密性、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。

管理

平安设有集团科技会信息安全部门统筹开展信息安全工作，下设三个部门实施相关规定并确保有效执行。信息安全管理标准的制定严格遵守国家法律，遵守银保监会、证监会、网信办、公安部等监管机构的法规，执行行业的最高标准。下图展示了集团信息安全管理框架、工作范畴及 9 大工作重点。



在具体管理工作上，平安成立了集团安全应急响应中心，构建业务安全风控等平台，主动感知集团信息安全威胁态势，实现快速响应，为客户提供稳固的信息安全保障。目前，平安的信息安全管理体系已通过 ISO 27001 审计，并定期进行信息安全管理和数据隐私保护的审计，审计结果呈报集团董事会、执委会与风险管理委员会。

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，内容涉及 9 大工作重点：

资产分类及控制

- 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。

信息安全组织

- 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。

- 违反信息安全规范的人员会按处罚规定处理。

在信息安全意识宣导上，平安每年都对所有员工、外包人员开展数据安全、客户隐私等主题培训，全面加强员工的信息与数据安全保护意识及能力。各专业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。

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。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，平安设计和实施了相对应的物理环境保护措施。

通信安全

• 所有与集团网络连接的线路，采取了适当的安全措施以保护内部网络、信息、信息系统以及传输中的信息安全。

• 集团通过网络接入认证、不同密级网络隔离、传输通道加密以及各类常规网络安全防护技术手段坚决杜绝非法入侵和数据外泄。

• 采用 DDoS 防御 (Distributed Denial of Service 分布式拒绝服务攻击)、终端 DLP（Data leakage prevention 数据泄密防护）、邮件 DLP、堡垒机技术等各类安全防护手段减少安全威胁，封堵数据泄露的各种途径。

访问控制

问责
所有行为必须被记录，可追溯至负责的执行者；非授权的行为要进行适当的处理。

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，只开通必要的权限。

保密性
信息资产必须按照信息分类做出合适的保护。绝密、机密信息发放必须有业务需要的依据。

完整性
信息资料必须防止被非授权篡改或者删除。

职责
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：达到保护数据的保密性、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子认证等强身份认证手段，严格遵行“知其必须”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。

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

• 平安严格遵循国家法例、监管机构法规、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。

第三方服务管理

• 在信息领域，平安与合作伙伴有着深入的合作。针对第三方的服务管理，平安制定了明确的管理条例和合作协议以确保采购、合作符合国家相关管理部门的规定。

在信息化、网络化时代，实现信息安全是平安集团落实整体可持续发展目标的重要保障。集团会持续升级相关系统和技术手段，并加强管理与培训等措施，以实现对于信息安全的承诺，提供安全可靠的产品与服务。

该政策由平安集团解释和修订，公司会适时根据国家政策、监管要求和行业发展进行更新。