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

2025 年 9 月

本声明适用于中国平安保险（集团）股份有限公司

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和复杂，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，确保公司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

本政策声明适用于中国平安保险（集团）股份有限公司（以下简称“集团”或“公司”），各成员公司可结合本政策声明建立自己的政策声明。

承诺

公司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。
- 以深度防御及默认安全为实施原则，构建信息及信息系统安全控制。
- 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

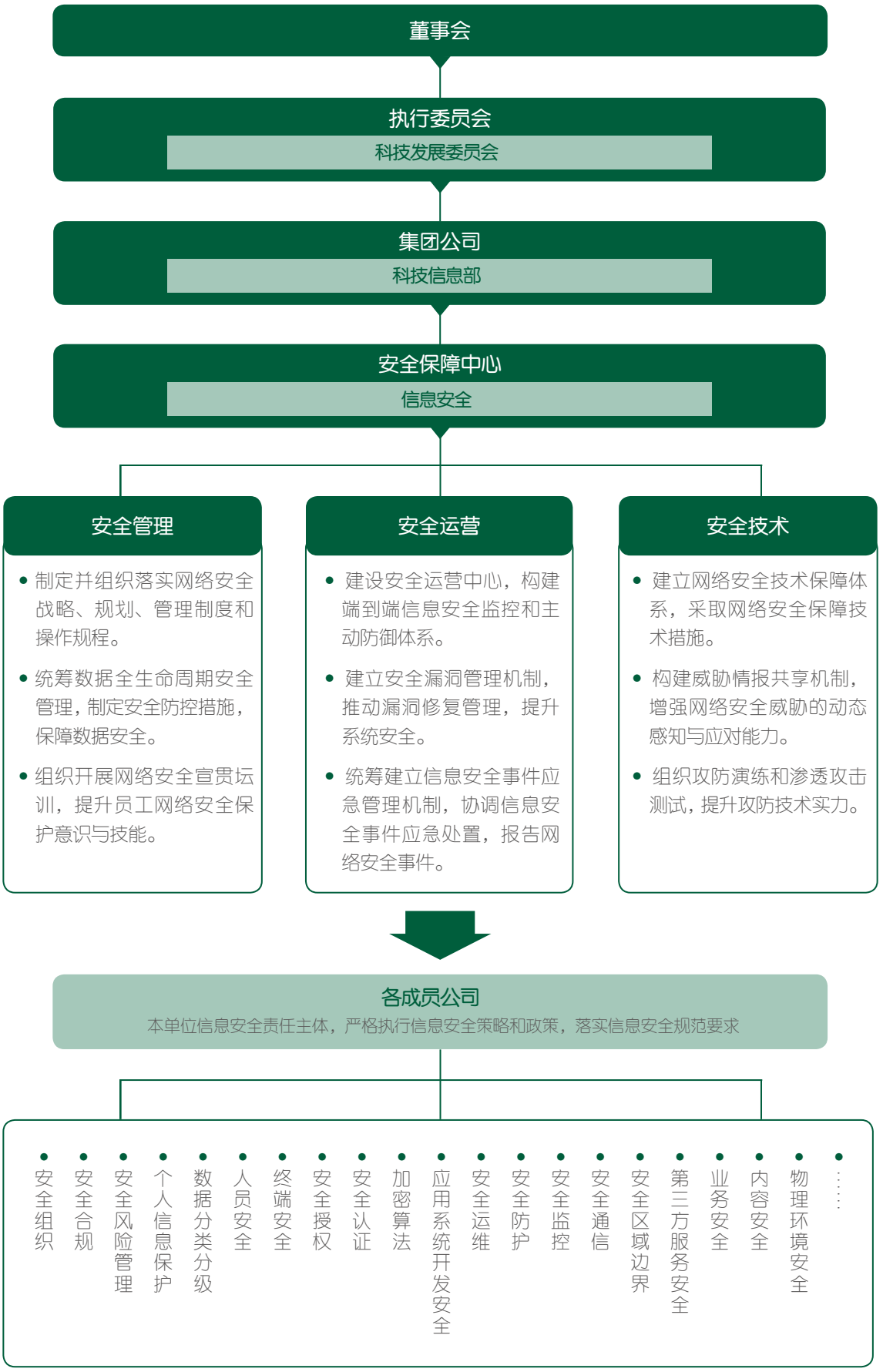
集团建立网络和数据安全责任制，集团董事会对网络和数据安全负主体责任。集团董事会贯彻落实国家关于网络安全的法律法规和政策要求，明确本集团网络安全目标，审议网络安全战略和规划，并对执行情况进行监督。

集团执行委员会下设科技发展委员会，承担集团科技发展战略和科技领域重大方案的统筹职能，负责制定科技领域重大战略、重大制度等，经报执委会审批同意后牵头推动、监督、追踪、指导集团和成员公司相关工作的落实。

集团科技信息部是集团公司的信息安全主管部门，负责从集团层面统筹、规划、组织协调开展信息安全工作，向集团董事会或其授权委员会、高级管理层报告信息安全重要事项。

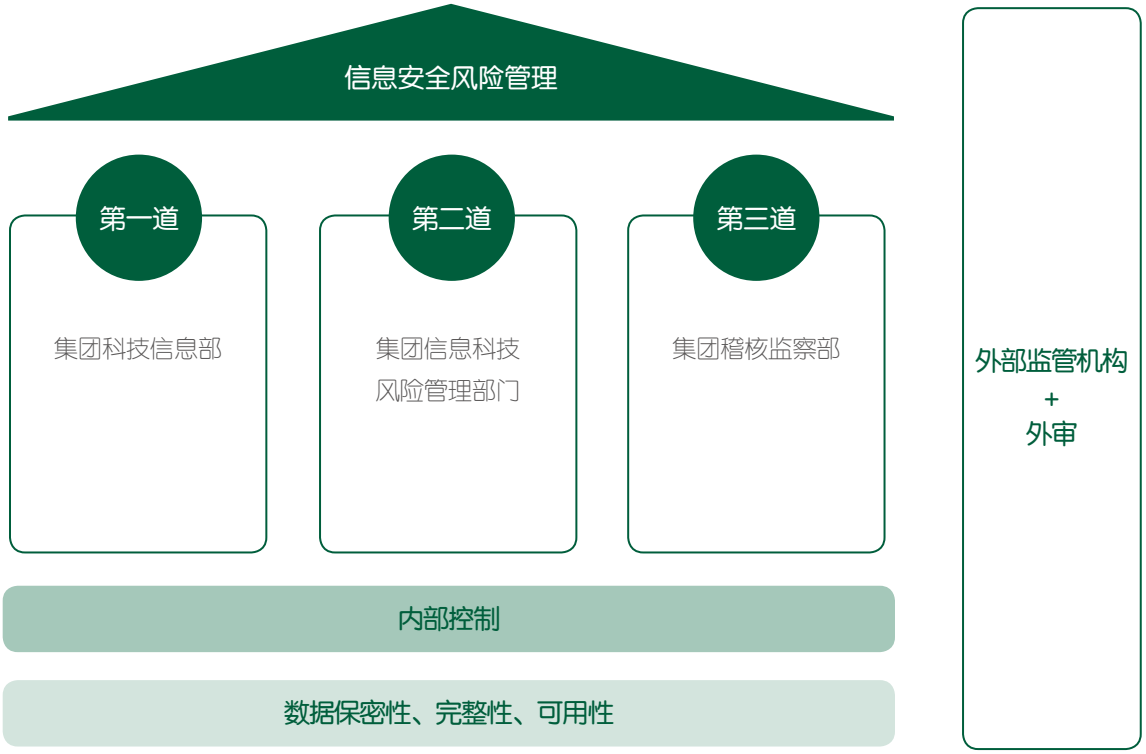
各成员公司是本单位信息安全责任主体，严格执行信息安全策略和政策，落实信息安全规范要求。各成员公司明确网络安全负责人、数据安全负责人和个人信息保护负责人，落实网络安全、数据安全、个人信息保护责任。履行信息安全义务，落地具体的管控策略，确保数据机密性、完整性、可用性。

公司信息安全管理架构及主要工作范畴展示如下。


董事会
执行委员会
科技发展委员会
集团公司
科技信息部
安全保障中心
信息安全
安全管理
制定并组织落实网络安全战略、规划、管理制度和操作规程。
统筹数据全生命周期安全管理，制定安全防控措施，保障数据安全。
组织开展网络安全宣贯培训，提升员工网络安全保护意识与技能。
安全运营
建设安全运营中心，构建端到端信息安全监控和主动防御体系。
建立安全漏洞管理机制，推动漏洞修复管理，提升系统安全。
统筹建立信息安全事件应急管理机制，协调信息安全事件应急处置，报告网络安全事件。
安全技术
建立网络安全技术保障体系，采取网络安全保障技术措施。
构建威胁情报共享机制，增强网络安全威胁的动态感知与应对能力。
组织攻防演练和渗透攻击测试，提升攻防技术实力。
各成员公司
本单位信息安全责任主体，严格执行信息安全策略和政策，落实信息安全规范要求
安全组织
安全合规
安全风险管理
个人信息保护
数据分类分级
人员安全
终端安全
安全授权
安全认证
加密算法
应用系统开发安全
安全运维
安全防护
安全监控
安全通信
安全区域边界
第三方服务安全
业务安全
内容安全
物理环境安全
……

信息安全风险管理

公司的信息安全风险管理由三道防线构成，各道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。公司的每一位人员，都有共同的责任，做好保护信息资产的工作。



第一道

第一道为集团科技信息部及集团各部门，集团科技信息部负责制定并组织落实网络和数据安全规划、管理制度、和操作规程。

第二道

第二道为集团信息科技安全风险管理部门，主要负责建立网络和数据安全风险识别、评估、监测等机制，并组织实施。

第三道

第三道为集团稽核监察部，主要负责组织开展安全专项审计，督促问题整改。

信息安全原则与措施

公司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：

01. 安全组织与人员

- 明确网络和数据安全执行团队，设置专职的网络和数据安全管理和技术岗位，确保相关人员具备必要的专业知识和职业技能。
- 在人员雇佣前、雇佣中和雇佣变更或终止时实施相应网络安全控制，以减少人为的欺诈、偷窃、错误操作等对信息资产造成的危害。
- 每年至少开展一次人员（包括正式员工、第三方人员等）网络安全教育和培训，提高全员网络安全保护意识和水平，要求员工积极识别网络安全风险，及时上报网络安全事件，形成全员共同维护网络安全的良好环境。
- 全体员工遵守本政策与信息安全相关规定，负有维护信息安全及数据保护的责任。任何违反公司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将追究法律责任。

02. 信息安全合规

- 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，维护国家、公民、法人和其他组织的合法权益。
- 严格履行网络安全等级保护、关键信息基础设施保护、商用密码应用安全性评估、网络安全审查等网络安全义务。

03. 安全风险评估与认证

- 每年至少开展一次网络安全风险评估，识别并评估现有风险控制措施的有效性，发现问题及时整改。
- 结合数据处理场景开展数据安全风险评估、监测与处置，每年进行一次全面的数据安全风险评估，保障数据开发利用活动安全稳健开展。
- 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 ISO27701 等。

04. 数据安全全生命周期保护

- 在数据收集、传输、存储、使用、交换、销毁等全生命周期各阶段构建网络安全控制，保证数据相关活动的合法合规、最小必要、可审计和可追溯。

05. 第三方服务安全

- 对第三方服务实施采购管理、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，确保第三方服务的信息安全可控。同时，在与第三方签定合同时，明确信息安全相关条款，包括但不限于数据保护、访问控制、安全事件响应与上报等条款内容。

- 定期对第三方进行信息安全评估，评估内容包括但不限于安全管理制度、人员安全、数据安全、安全防护、应急响应和处置等；每年还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。

06. 安全认证与权限管理

- 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。密码设定有效期，至少每 90 天修改一次，禁止使用弱口令。针对集权系统、外网访问的业务系统等高风险系统，采取白名单访问机制、双因素认证等措施加强安全防护。

- 在权限管理方面遵循权限最小化原则、知悉需要原则，只开通必要的权限。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。

07. 系统开发安全及维护

- 建立覆盖软件开发生命周期的应用安全规范和管控流程，加强安全管理，开展需求分析、安全方案评审、源代码安全检查、组件风险排查和安全测试等工作，安全测试未通过严禁投产。

- 在漏洞管理方面，建立漏洞分级处置闭环机制，明确不同级别漏洞处置时限要求。建立漏洞监测和主动发现机制，通过渗透测试和红蓝对抗等方式，及时发现和修复网络安全漏洞，改进系统的安全性。

- 建立服务器、网络设备、操作系统、数据库、中间件等安全基线，加强管理和维护，对安全基线、安全配置策略的有效性进行验证和更新。

08. 区域边界与通信安全

- 采取隔离技术将网络划为外网、DMZ 及内网。在网络边界部署相应的访问控制机制，设置访问控制规则，防范网络入侵攻击。
- 根据不同网络区域实施不同的安全通信规则。连接到公司网络的线路，采取适当的安全措施，以保护内部网络、信息和信息系统。敏感信息需要经过认可的加密技术加密，方可在互联网上传输。

09. 安全监控与防护

- 实施 7*24 网络安全监控和运营机制，采取主动与被动防御相结合的措施保护信息系统和网络安全，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。
- 制定网络安全事件应急管理制度和覆盖各类网络安全突发事件场景的应急预案，明确应急响应组织架构及机制，落实应急处置相关要求。明确员工报告事件上报流程，采取邮箱一键举报。定期对应急预案进行审查和更新，每年至少组织开展一次网络安全应急演练，提升对各类网络安全突发事件的应急处置能力。发生网络安全事件，按照监管上报时效要求上报，并在必要时向相关方发出通知。
- 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。

10. 终端安全

- 采用终端安全管控技术措施和策略，加强各类违规行为监控、阻断和溯源。

11. 业务与内容安全

- 建立用户注册、密码重置、设备绑定等业务高风险操作的安全控制，确保业务交易身份及设备信息的真实性、抗抵赖性，持续加强异常交易行为监测和处置。
- 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。

12. 物理及环境安全

- 采取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受到物理访问、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，设计并实施了相对应的物理环境保护措施。