招商银行股份有限公司
信息安全管理制度要点
（2025 年版）

一、目的

招商银行股份有限公司（以下简称“招商银行”“我行”）高度重视信息安全管理，致力于维护网络安全和数据安全。

我行严格遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》等法律法规及监管规定，制定《招商银行网络安全管理规定》《招商银行数据安全管理规定（第二版）》等制度规范，确保信息系统和信息安全的机密性、完整性和可用性，保障我行运营所需的硬件设备、信息系统和数据的可靠性。

二、适用范围

本制度适用于我行全部业务条线，涵盖所有业务板块的产品和服务。我行全体员工、供应商均应遵守本制度要求。

三、管理架构

网络安全方面，招商银行行长是全行网络安全第一责任人，负责网络安全的全面工作。招商银行信息安全管理委员会负责统筹管理网络安全和数据安全工作，信息安全管理委员会由行长担任主任委员，首席信息官担任执行副主任委员。总行信息技术部作为网络安全工作的牵头管理部门，在信息安全管理委员会的领导下，开展全集团网络安全管理工作。全行网络安全工作遵循“谁主管谁负责，谁运行谁负责，谁

使用谁负责”的原则，明确责任分工，逐级落实责任，确保有效执行。

数据安全方面，招商银行行长是全行数据安全第一责任人，首席信息官是全行数据安全的直接责任人。董事会听取数据安全相关汇报，督促高级管理层提升数据安全管理有效性。信息安全管理委员会下设数据安全工作组，由总行信息技术部牵头组织，统筹推进全行数据安全管理工作。各分行和各附属子公司参考总行治理架构，成立分行或子公司数据安全工作组，由信息科技部门牵头组织，严格按履职清单要求落实总行布置的各项数据安全工作。

我行建立网络和数据安全管理的三道防线：第一道防线由总行信息技术部牵头组织，总行各部门、各分行和子公司落实所辖业务领域的各项数据和网络安全管理要求；第二道防线为总行风险管理部和法律合规部，负责将网络和数据安全纳入全面风险管理体系和内控合规管理体系；第三道防线为各级内部审计部门，负责对第一、二道防线履职情况及有效性进行监督评价。

四、数据安全管理

数据收集与使用方面，招商银行坚持“合法、正当、必要、诚信”原则，明确数据收集和处理的目的、方式、范围、规则，保障收集过程的数据安全性、数据来源可追溯。敏感

级及以上数据传输应当采用安全的传输方式和存储措施，保证数据完整性、保密性、可用性，防止勒索病毒、木马后门等攻击。我行严格实施对敏感级及以上数据的管理，制定用户对数据的访问策略，采取有效的用户认证和访问控制技术措施，规范数据操作行为，用户对数据的访问应当符合业务开展的必要要求并与数据安全级别相匹配。

数据备份方面，我行加强数据备份管理，制定备份策略，备份数据和生产数据隔离分开保存，严格管理备份数据的访问权限；制定备份验证计划，确保备份数据完整有效、业务可恢复。

数据安全监测方面，我行对数据安全威胁进行有效监测，实施监督检查，主动评估风险，防止数据篡改、破坏、泄露、非法利用等安全事件发生。

五、网络安全管理

招商银行总行信息技术部牵头落实网络安全法律法规和监管要求，制定全行网络安全的主要目标、基本要求、工作任务、保护措施，每年组织开展一次全行网络安全风险评估。同时，我行建立漏洞扫描和渗透机制、漏洞修复机制，明确漏洞分类、漏洞修复流程、漏洞修复时长等要求，动态调整网络安全管理策略。

六、网络和数据安全监控与应对

网络安全方面，招商银行持续监测全行网络安全事件，识别网络安全威胁。我行将网络安全应急管理纳入全行信息安全事件应急处置统一管理，建立网络安全应急管理组织和协调联动机制，及时处置网络安全事件。根据网络安全事件造成的影响范围和程度，划定不同事件级别，并制定网络安全事件的应急响应和处置预案，定期开展应急演练。

数据安全方面，我行建立数据安全技术应急管理机制，组织开展数据安全风险技术监测、预警、通报与处置，防范外部攻击、内外部破坏等危害数据安全活动。

七、第三方管理要求

对于非驻场的第三方服务供应商，招商银行在供应商引入前开展供应商风险评估，确保供应商具备符合要求的网络安全保障能力；在供应商提供服务期间，至少每年开展一次对供应商的网络安全检查。在第三方产品和服务的采购合同中明确供应商的网络安全责任，包括但不限于：为我行提供服务的信息系统应满足我行网络安全要求；一旦发现第三方产品的漏洞或发生安全事件应及时处置并告知我行。

对于涉及第三方数据委托处理的情况，由业务主管部门负责，开展数据安全评估，形成评估报告。我行将数据委托处理纳入信息科技外包管理范围，以合同协议方式约定双方

的数据安全责任和义务，对数据处理活动进行记录和检查。我行与合作方约定，不得转委托其他主体处理数据，发生数据安全事件立即通知我行并及时做好处置，要求合作方配合我行开展各项数据安全监督检查工作。委托数据处理终止时，应当要求服务提供商及时删除数据，并采取现场检查等有效监督措施，确保数据被销毁、不可恢复。

八、检视与更新

本制度由招商银行负责制定、解释和修订。我行将根据国家政策、监管要求、行业发展和内部管理需要，适时对本制度进行检视和更新。