中信银行隐私与数据安全管理政策要点

中信银行根据《中华人民共和国个人信息保护法》《中华人民共和国消费者权益保护法》《中华人民共和国数据安全法》等法律法规，制定发布《中信银行数据安全管理办法》《中信银行消费者金融信息保护管理办法》等规章制度，明确数据安全管理要求，健全管理机制，有效防范数据泄露风险，充分保障客户信息安全。

一、适用范围

中信银行已建立适用于全行的数据安全管理制度，指导全体员工遵守数据安全与客户信息保护要求、落实保护措施，具体包括《中信银行数据安全管理办法》《中信银行消费者金融信息保护管理办法》；政策涵盖行内所有通过提供金融产品和服务或者其他渠道（包括但不限于柜面、自助设备、网站、App、公众号、H5 页面等）获取、加工和保存的个人客户信息和公司客户信息等。

二、主要内容

（一）组织架构

中信银行已建立结构较完整的数据安全管理组织架构，在相关管理制度中明确董事会将数据安全相关内容纳入公司治理、企业文化建设和经营发展战略中，指导和督促相关工作有效执行和落实；高级管理层负责审定数据安全管理目标及策略，决策和审批相关规划和重大事项等工作；各部门对所辖数据落实数据安全

保护管理要求，并按照合法、正当、必要、诚信原则，采取与处理目的直接相关、对客户权益影响最小的方式开展客户信息处理活动，切实保障客户对其信息的控制权利。

（二）管控机制

中信银行已建立较完善的信息安全管理体系，涵盖物理安全、通信管理、访问控制等多方面，并采取加密、脱敏、权限管理、访问控制、日志审计等措施，实现数据和客户信息处理全周期的安全管控。一是严格落实信息系统在需求、设计、开发、测试、发布等环节的数据安全保护措施，持续开展安全测试、安全评估等，确保数据安全与客户信息保护贯穿于信息系统开发全流程。二是明确数据收集、存储、使用、加工、传输、提供、公开和清理等处理环节的安全要求与管控措施。三是严格实施数据权限管控，按照最小必要原则开展处理活动。四是采取技术措施保证数据的真实性、完整性、保密性，防止客户数据其被未授权的第三方获取。五是制定数据泄露事件的应急处置、报告流程与管理机制，保障事件处理的及时性和有效性。六是通过员工签署保密协议或劳动合同中设置保密条款的方式，确保相关员工履行数据保护责任和义务。

（三）隐私保护举措

中信银行严格履行客户信息处理前的“告知-同意”流程，定期重检和优化隐私政策内容，保障客户合法权益。一是明确告知客户信息处理的目的、方式、范围等，仅采集和使用提供业务服

务所必须的客户信息，涉及处理敏感个人信息的，均告知处理必要性及对个人权益的影响；依法保障消费者对其个人数据的控制权，明确个人数据的访问、修正和删除等权利。二是仅在法律法规、监管要求期限内，以及为实现业务服务所必须的最短时限内保留客户信息。三是除因监管要求、案件分析、客户纠纷处理等情况需归档外，其余确认不再使用的客户信息立即清理，原则上禁止长期留存。四是在获得客户授权同意、法律或行政法规允许的前提下，按照“最小必要”原则向第三方提供客户信息，并履行对应风险评估等责任。五是通过建立管理制度、执行评估检查、开展应急演练等方式，防控外包活动过程中的数据安全和客户信息泄露风险。

三、执行情况

中信银行注重对隐私与数据安全保护，严格落实数据安全管理、客户信息保护、消费者金融信息保护相关要求，并通过检查评估确保相关要求执行到位。一是每年度开展一次信息科技审计，每三年实现对分支机构及子公司审计全覆盖，重点关注数据处理过程的安全技术防护措施，并对信息安全管理环节执行针对性审计程序。二是聘请外部第三方机构每两年对电子银行相关业务系统开展一次安全评估，评估范围包括安全策略、内控制度、风险管理、系统安全、客户信息保护等多方面。三是强化员工行为管理，对违反相关规定的员工，按照《中信银行员工违规行为处理办法》进行处分或处理。

四、培训宣贯

中信银行持续开展覆盖不同群体、形式多样的信息安全培训及宣贯活动。一是针对科技条线专业人员，开展合规警示教育培训和专项技术培训，培训内容覆盖网络安全、人员行为规范、IT连续性和生产运行维护安全等方面，提高专业人员安全工作技能。二是面向全员（包含合同工及外包员工等），通过案例宣传、仿真演练等形式，开展安全意识教育，内容涉及数据安全与隐私保护管理工作要求、具体流程等，不断提升人员安全防范能力，此外，要求供应商对配置人员加强宣导培训，规范人员行为和办公安全管理等方面要求。三是面向分支附属机构，开展网络安全有关培训，提升分支附属机构安全防御和实战对抗水平。四是面向社会公众，宣导普及网络安全知识，举办线上、线下网络安全宣传活动，帮助社会公众提高防范网络诈骗、保护个人金融信息的安全意识。

五、外部认证

中信银行积极参与外部信息安全有关测评认证，持续提升信息安全防护水平。一是根据《中华人民共和国网络安全法》及国家网络安全等级保护要求（以下简称“等保”），对核心业务系统、网上银行系统等重要信息系统向有关部门进行等级保护定级备案，并每年按照等保测评要求，围绕物理、网络、应用等多领域开展安全测评，全面提升系统安全防护能力，降低网络攻击风险。二是手机银行、动卡空间等 App 通过北京国家金融科技认证

中心“金融科技产品认证（客户端软件）”，以及中国互联网金融协会“移动金融客户端应用软件”备案，标志着行内自主研发的移动金融 App 获得权威机构认可，在客户端软件安全、条码支付安全、客户个人信息保护等方面实现质量达标可控。三是信用卡业务通过 ISO 27001 信息安全管理体系认证，认证业务范围包含征信发卡、授权、账务账单、催收调扣，以及系统开发、系统运行和信息科技规划等方面。