**xxx银行**

数据安全管理办法

第一章 总 则

第一条 为保证xxx银行（以下简称“本行”）数据在申请、提取、使用以及借阅过程中的数据安全管理，防范数据信息泄露，根据《中华人民共和国计算机信息系统安全保护条例》、《中国人民银行计算机系统安全管理暂行规定》，以及中国银监会、江苏省农村信用社联合社对数据安全管理的相关要求，制订本办法。

第二条 不通过综合业务系统、信贷管理系统等正常途径导出数据，而是通过信息科技部后台取得的信息和数据均适用于本办法。

第三条 业务部门、基层网点、系统开发项目组、查询数据信息的有权机关、客户、客户相关关系人等对数据申请查询、提取、使用、借阅、保管、新增、变更以及销毁等均须遵循本办法。

第四条 查询数据信息的有权机关是指依照法律、行政法规的明确规定，有权查询、冻结、扣划单位或个人在金融机构存款的司法机关、行政机关、军事机关及行使行政职能的事业单位。具体包括：人民法院、税务机关、海关、人民检察院、公安机关、国家安全机关、军队保卫部门、监狱、走私犯罪侦查机关、监察机关（包括军队监察机关）、审计机关、工商行政管理机关、证券监管管理机关等。

第二章 分工与职责

第五条 本办法涉及到的对象包括：业务部门、基层网点、信息科技部、系统开发项目组、公安机关、检察院、法院以及有权在本行进行数据调阅的其他机关或个人等。

第六条 信息科技部主要负责对数据的提取、保管、变更等操作；对数据提出需求进行技术审核；对项目组数据提取、使用、管理进行控制。

第七条 业务部门、基层网点根据自身的业务需要在数据权限范围内对数据申请、提取、借阅以及使用，并对取得数据准确性进行核对与确认；另外业务部门还需对自身牵头的项目组提出的数据需求和使用负责。

第八条 项目组在申请数据时必须向牵头或相关的业务部门提出书面申请，并经信息科技部同意后方可取得和使用数据。

第三章 行内数据使用申请

第九条 行内数据申请使用是指基层网点、部室以及行内员工根据本单位或个人自身的业务工作需要，向信息科技部提出的数据申请需求。

第十条 无特殊情况下，各单位或员工提出数据申请需要经业务部门主管或支行行长签字同意；如果涉及到核心机密数据，必须经过分管领导签字同意；对于需求的申请涉及到费用支出的也必须经分管领导签字确认。

第十一条 各单位申请的数据范围必须在自身的权限范围内。业务部室申请的数据必须是与该部室业务相关的数据，支行仅能申请自身范围内的数据。对查询超出本单位权限范围内的数据，必须经过分管领导的签字确认。

第十二条 各单位内部成员查询数据，可以根据需要设置相应的权限等级。具体的权限等级由各单位自行设定。超出自身权限范围内的，需要经单位负责人签字确认后方可查询申请。

第十三条 各单位对本单位申请的数据安全负责。对于每次申请的数据需要做好登记工作。数据的传输与使用过程中要防止数据的泄露和失密。需要保存留档的必须专人对数据进行管理，防止数据丢失泄露。临时调阅查看的数据，使用完成后立即删除、销毁。处理的过程必须双人进行并做好登记。

第十四条 所有数据的传输必须在本行内部网或经过桌面管理软件认证和杀毒的 U 盘上进行，所有的数据查看必须在桌面安全管理软件管理的电脑上进行操作。需要在未经认证的电脑和设备上操作时，必须经分管领导签字同意并在进行病毒查杀后的电脑上使用。任何人不得在未经允许的情况下，擅自将数据带离本行或泄露给他人。

第四章 有权机关数据查询

第十五条 有权机关在办理协助查询业务时，经办人员应当核实执法人员的工作证件，以及有权机关县市级以上机构签发的协助查询存款通知书。

第十六条 有权机关在办理协助查询业务时必须有两人或两人以上同时在场，并出具相关证件、通知书或其他有效证明。协助查询存款通知书必须详细写明编号、原因、需要查询的数据内容、日期以及有权机关的印章。

第十七条 协助查询的内容必须依据协助查询存款通知书上的内容给予查询，不得超出通知书上的范围。

第十八条 办理协助查询业务时，应当按照内控制度的规定建立和完善协助查询工作的登记制度。在协助有权机关办理查询手续时，应对有权机关名称、执法人员姓名和执法证件号码、经办人员姓名、被查询单位或个人的名称、协助查询的时间和金额、协助查询书文的名称和编号，协助查询结果等进行登记。登记表应当在协助办理查询手续时填写，并由有权机关执法人员和经办人员共同签字确认。经办人员应当妥善保存登记表，并严格执行保密原则。

第十九条 协助有权机关查询的资料包括电子数据和纸质档案资料，经办人员应当如实提供，有权机关根据需要可以抄录、复制、照相，但不得带走纸质档案的原件。

第五章 项目组数据安全管理

第二十条 项目组必须与本行进行签署《xxx银行信息安全保密协议》后方可进入本行开展需求调研、项目开发、测试上线等工作。

第二十一条 项目组作为数据提供方时，需要对信息科技部进行负责，即所有的数据提供必须经过信息科技部的签字同意后方可提供；当作为数据需求方时，需要对牵头的业务部门进行负责，即所有的数据需求必须由牵头部门进行签字确认后方可申请数据资源。

第二十二条 在向项目组进行数据申请时，必须先提供数据需求申请单，申请单中必须注明数据申请内容、范围以及相关业务口径，并由业务部门签字盖章确认；需求申请单必须经信息科技部门进行业务技术评估、数据权限审核并签字确认。

第二十三条 项目组在提供数据时必须检查需求单内容、业务口径要求、申请单位数据权限等事项，不得提供额外的数据信息

第二十四条 项目组提供数据时必须经过内部网或通过桌面安全管理系统认证的 U 盘进行数据传输，不得通过外部网或未经注册的 U 盘进行传输。

第二十五条 项目组必须在本行指定的机器上对数据进行使用和操作；未经允许不得将数据擅自拷贝的个人电脑、移动硬盘等非指定设备上使用与存储；未经允许不得对本行客户数据进行抄录、复制与拍照等；禁止内外网互通，不得将数据放在互联网中进行传输。

第二十六条 项目开发过程中，需要对数据的关键信息进行脱敏处理。开发测试的过程中如必须采用真实数据，需要向信息科技部申请后方可使用，数据使用完毕后必须在本行信息科技部监督下及时销毁。

第二十七条 项目开发过程中，需要对系统生产环境数据进行变更、删除等操作时，项目组必须向信息科技部进行书面申请，并经信息科技部签字盖章确认后方可进行操作。在未经同意的情况下，禁止对生产环境数据进行变更、删除等操作。操作过程中，必须双人操作，双人复合，并做好相应的变更、删除记录。

第二十八条 对系统采用数据备份机制，指定并明确相关责任人定期的检查数据备份文件，以确保数据能够正常顺利的进行恢复工作。

第二十九条 在项目组撤离本行前，必须收回各类开发设备，做好对数据回收、删除、销毁工作；对放在项目组的个人电脑中的数据必须进行删除和销毁，以防止数据泄露。

第六章 其他数据安全

第三十条 重要数据(介质)应设专人负责登记保管，未经批准，不得随意挪用。

第三十一条 在使用重要数据(介质)期间，应严格按保密规定控制转借或复制，需要使用或复制的须经分管领导批准。

第三十二条 对所有重要数据(介质)应定期检查，要考虑介质的安全保存期限，及时更新复制。损坏、废弃或过时的重要数据(介质)应由专人负责消磁处理，机密级以上的重要数据(介质)在过保密期或废弃不用时，要及时销毁载体。

第三十三条 机密数据处理作业结束时，应及时清除存储器、联机磁带、磁盘及其它介质上有关作业的程序和数据。

第三十四条 机密级及其以上的信息存储设备不得并入互联网。重要数据不得外泄，输入及修改信息科技部由专人完成。重要数据的打印输出及外存介质应存放在安全的地方，打印介质及时销毁。

第七章 附 则

第三十五条 本办法由xxx银行信息科技部负责解释和修订。

第三十六条 本办法自发文之日起施行。

附件：xx农商银行信息安全保密协议

附件

xxx银行

信息安全保密协议

项目名称：

甲 方：xxx银行

乙 方：

合同签订地点：江苏xx

根据国家有关信息安全及信息保密相关法律法规，本着平等、自愿、公平、诚信的原则，双方就该项目实施及后续合作过程中有关信息安全保密事项达成以下协议，并由双方共同遵守。

一、保密内容定义

项目实施过程中，由乙方获取的所有与甲方有关保密资料和信息，一切权利归甲方所有。这些信息包括但不限于以下内容：

1．技术秘密：甲方的网络拓扑结构、网络配置协议、安全设备部署结构及详细参数、安全软件及业务平台架构方式、实际部署结构、使用技术参数、系统开发文档、配置文档、业务软件及软件源代码、系统管理手册、知识产权信息及产品专利等。

2．管理秘密：甲方的信息化规划、内部管理规章制度及涉密文件、各类设备及系统的运维账号、密码、密码管理策略、用户手册等。

3.业务秘密：信息化项目方案、信息化项目合同以及乙方在工作中获知的客户对于甲方业务需求的一切数据资料。

二、保密义务

上述保密内容定义范围内，乙方承担以下保密义务：

1.乙方保证从甲方获取的保密信息仅用于与本项目合作有关的用途和目的。

2.乙方保证对甲方提供的保密信息予以妥善保存，并采取与自身保密信息同等级别的措施和审慎程度进行保密。

3.乙方不得刺探与本身业务无关的甲方保密信息。

4.未经甲方授权，乙方不得向任何第三方传递或透露甲方的保密信息，不允许协助第三方使用甲方的保密信息。

5.乙方向其内部提供甲方保密信息的范围应进行严格控制和管理。乙方须向其掌握甲方保密信息的内部人员提示信息的保密性和其应承担的保密义务，并保证上述人员以书面形式同意接受本协议条款的约束。若乙方人员出现岗位调动或离职的情形，乙方有义务立即通知并配合甲方终止其与甲方有关的信息访问权限，收回其所持有的甲方保密资料和涉密介质，并确保该人员在离职后继续履行好保密义务。

6.若乙方与第三方合并、被第三方兼并或被第三方直接或间接控制，在未经甲方书面授权同意的情况下，乙方不得向该第三方披露任何甲方的保密信息。若出现该情况，乙方应立即将甲方的保密资料归还甲方，或根据甲方的要求予以销毁，不得留存任何资料的备份。

7.除履行工作职责需要外，不得向任何第三人或第三方机构披露或泄露甲方所确定的机密信息。

8.不得允许或协助不承担义务的任何第三人或第三方机构使用甲方的客户资料。

9. 如发现甲方信息及所掌握的客户信息被披露或因本人过失造成信息泄露，应当采取有效措施防止信息泄露进一步扩大，并及时向甲方报告。

10.不得在离开甲方后，以在甲方工作期间获得的保密信息为其他企业或个人服务、牟利。

11.乙方在未征得甲方书面同意的情况下，在雇佣期间及雇佣以后任何时间，均不得直接或间接利用或为他人使用在雇佣期间取得或得知的一切甲方保密信息。

三、违约和赔偿

1.乙方应做好内部人员保密管理工作。因乙方在职或离职人员的泄密行为造成的甲方损失，由乙方承担全部责任。

2.乙方有违反本协议的情形，无论故意与过失都应当立即停止侵害，并在第一时间采取一切必要措施防止保密信息扩散，尽最大可能消除影响、减少损失，并及时通知甲方。

3.乙方应承担因违反本协议造成的全部法律责任和对甲方造成的经济、名誉损失。甲方保留向乙方违约行为要求违约赔偿的权利。

四、保密信息的归还

本项目合同终止后，协议所涉及的一切甲方保密信息，无论是书面、电子还是其他具体形式，以及乙方所作的复印件、电子副本均需立即交还甲方或者予以销毁，有关销毁凭证应同时送交甲方。乙方不允许保留任何形式的资料备份。

五、争议的处理

本协议在履行过程中发生的争议，由双方当事人协商解决，也可由有关部门调解；协商或调解不成的，至甲方所在地法院提起诉讼。

六、合同效力

本协议一式贰份，双方各执壹份，自双方法定代表人或其授权代表人签字并加盖公章之日起生效。有效期为 年。

甲 方（盖章）：

授权代表（签字）：

日 期： 年 月 日

乙 方（盖章）：

授权代表：（签字）：

日 期： 年 月 日