

金融科技创新应用声明书

创新应用 基本信息	创新应用编号	91640200228070689F-2025-0001	
	创新应用名称	基于移动应用环境监测技术的安全风险评估与防控服务	
	创新应用类型	☒ 金融服务 ☐ 科技产品	
	机构信息	统一社会信用代码	91640200228070689F
		全球法人识别编码	300300C1088064000053
		机构名称	石嘴山银行股份有限公司
		持有金融牌照信息	牌照名称：中华人民共和国金融许可证 机构编码：B1009H364020001 发证机关：国家金融监督管理总局石嘴山监管分局
	正式运营时间	2025 年 04 月 25 日	
技术应用	1. 运用数据分析等大数据技术，将移动应用前端风险监测及服务端业务流量风险分析相结合，打造移动感知平台。通过植入威胁情报 SDK 收集移动应用运行过程中的设备、系统、应用、行为四个维度数据，结合后端大数据分析平台的各种模型规则，实时监测移动应用面临的各种运行时攻击，并支持定位溯源攻击设备、攻击方式、攻击手段、攻击者。通过事前定制的各类安全控制策略，第一时间处理各类安全攻击行为，提高风险发现能力。 2. 采用崩溃采集技术，实时收集移动应用运行过程中的崩溃信息，采集终端用户群体机型分布特征，有效组织兼容性测试，及时根据崩溃信息进行修复。 3. 采用全流量数据关联分析技术，能够清楚掌握应用上线后的运营推广状况，用户启动、安装、日活分布状况。同时，平台内置智能搜索功能，支持搜索目标设备的安全事件、威胁分析、环境安全、运行情况、崩溃情况、设备详情、应用安装列表等多维度信息，用于事后追溯审计。提高对于安全事件追溯的完整性。		
功能服务	本应用使用大数据、崩溃采集、全流量数据关联分析等技术打造了移动感知平台，由移动端 SDK 和服务平台组成。		

创新应用		其中，移动端 SDK 负责数据采集、上送和最终策略执行。服务平台负责业务数据分析，采用大数据分析引擎对数据进行清洗、处理、分析和响应，并最终完成移动应用的威胁数据和运营数据分析。平台还提供了资产发现、终端环境监测、终端风险识别、终端异常访问监测、终端风险处置、终端风险溯源等功能，能有效应对各种终端动态安全风险事件。 本应用由石嘴山银行负责系统研发、运维并提供金融应用场景，此外无其他机构参与。
	创新性说明	1. 在资产梳理方面，采用了流量解析还原技术，自动化分析接入的流量，自动聚合分析到的应用业务平台站点，可高效梳理出应用资产台账。 2. 在终端安全方面，采用终端环境采集技术，可有效发现来自终端应用运行过程中的环境风险，可发现自动化工具、设备造假检测、自动化攻击检测等，有效防止来自终端的安全威胁。 3. 在风险处置方面，可提供平台直接处置、告警、通过 kafka 或 syslog 以及 API 等方式提供给第三方由第三方进行处置等多种风险处置方式，提高对于风险的处置效率。 4. 风险溯源方面，平台记录全量的流量访问记录，可通过 IP、UA、设备、用户等多维度进行风险溯源，提升了风险溯源效率。 5. 在反诈协同联动方面，当平台识别到风险模型中定义的高风险行为时，将同步触发反诈信息共享机制，自动向宁夏回族自治区公安厅反诈中心推送风险用户联系方式、风险行为特征、操作场景等关键信息，为反诈中心及时开展预警拦截、精准劝阻等工作提供信息，从源头遏制电信网络诈骗案件发生，最大限度保障客户资金安全。
	预期效果	本项目通过前端监测与后端分析协同，实现移动应用风险的实时发现与精准处置，显著提升风险识别与响应效率，形成“监测-处置-溯源-优化”的闭环防控体系，全面增强移动金融应用的安全性与稳定性，切实保障金融业务连续性与用户合法权益。
	预期规模	按照风险可控原则合理确定用户范围及服务规模，根据石嘴山银行手机银行客户规模，预计服务客户约 75 万人。
创新应用	服务渠道	通过手机客户端 APP 提供服务

服务信息	服务时间	7×24 小时
	服务用户	个人用户
	服务协议书	本应用为个人用户提供金融服务，服务协议书为： 《石嘴山银行 App（微信银行）用户隐私政策》（见附件 1-1）
合法合规性评估	评估机构	石嘴山银行股份有限公司法律合规部
	评估时间	2025 年 04 月 24 日
	有效期限	2 年
	评估结论	本应用严格遵循《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规，聚焦移动金融应用安全风险实时监测与处置。数据采集环节遵循“最小必要”原则，通过威胁情报 SDK 收集设备环境、崩溃日志等必要信息，并采用匿名化处理技术剥离用户身份关联性；安全防护层面，结合加密传输、动态策略阻断及多维度溯源机制，确保攻击行为处置符合《反电信网络诈骗法》要求，日志留存期限满足金融行业监管标准。平台通过隐私协议明示数据用途并提供用户授权管理功能，保障全流程合规。本项目在数据安全、用户权益保护及风险防控机制设计上均符合现行法规要求，可依法合规开展业务应用。
技术安全性评估	评估材料	《基于移动应用环境监测技术的安全风险评估与防控服务合法合规性评估报告》（见附件 1-2）
	评估机构	石嘴山银行股份有限公司信息科技部
	评估时间	2025 年 4 月 24 日
	有效期限	2 年
技术安全性评估	评估结论	本应用严格按照《中华人民共和国个人信息保护法》、《信息安全技术个人信息安全规范》（GB/T 35273-2020）、《移动金融客户端应用软件安全管理规范》（JR/T 0092—2019）、《个人金融信息保护技术规范》（JR/T 0171—2020）、《商业银行应用程序接口安全管理规范》（JR/T 0185—2020）、《金融科技创新安全通用规范》（JR/T 0199—2020）、《金融科技创新风险控规范》（JR/T 0200—2020）、《基于大数据的支付风险智能防控技术规范》（JR/T 0202—2020）、《金融数据安全数据生命周期安全规范》

		(JR/T 0223—2021)、《金融大数据术语》(JR/T 0236—2021)、《金融领域科技伦理指引》(JR/T 0258—2022)等相关金融行业技术标准规范和要求进行设计开发并进行全面安全评估。经评估,本应用符合现有相关金融行业标准要求。		
	评估材料	《基于移动应用环境监测技术的安全风险评估与防控服务技术安全性评估报告》(见附件1-3)		
风险防控	风控措施	1	风险点	在数据采集、存储、传输、使用等过程中,由于技术缺陷或业务管理漏洞可能会造成数据的泄露风险。
			防范措施	遵循“用户授权、最小够用、全程防护”原则,充分评估潜在风险,加强数据全生命周期安全管理,严防用户数据的泄露、篡改和滥用风险。数据采集时,通过隐私政策文件、个人信息授权书等方式明示用户数据采集和使用目的、方式以及范围,获取用户明确授权后方可采集。数据存储时,通过如数据泛化等技术将原始信息进行脱敏,并与关联性较高的敏感信息进行安全隔离、分散存储,严控访问权限,降低数据泄露风险。数据传输时,采用加密通道进行数据传输。数据使用时,借助加密技术,在不归集、不共享原始数据前提下,仅向外提供脱敏后的计算结果。
		2	风险点	移动应用动态安全风险,涵盖系统环境安全、应用运行时攻击、用户异常行为及第三方 SDK 违规等多维度威胁,包括风险设备运行、恶意攻击(如注入、篡改)、异常登录或操作行为(如频繁更换账号/IP)、第三方 SDK 非授权调用等风险。
			防范措施	一是实时监测与拦截:通过威胁情报 SDK 及大数据分析平台,对设备环境、攻击特征、用户行为及 SDK 调用进行实时监测,结合多维度数据(攻击类型、设备信息、行为模式)识别威胁,动态拦截高风险操作及非授权行为。 二是溯源与审计:记录全量日志(IP、设备指纹、操作轨迹),支持攻击溯源与异常行为审

				计，满足《网络安全法》日志留存要求。
		3	风险点	创新应用上线后，可能面临网络攻击、业务连续性中断等方面风险，亟需采取措施加强风险监控预警与处置。
			防范措施	在应用实施过程中，将按照《金融科技创新风险监控规范》（JR/T 0200—2020）建立健全风险防控机制，掌握创新应用风险态势，保障业务安全稳定运行，保护金融消费者合法权益。
	风险补偿机制	本应用按照风险补偿方案（见附件1-4）构建风险补偿机制，确保安全事件快速响应：数据泄露时24小时内启动应急响应，通过脱敏加密恢复系统安全，联合第三方修复漏洞并更新威胁情报；动态安全风险下实时拦截攻击，隔离高风险设备，推送操作指南协助用户降低二次风险；通过全流量分析实现全链路追踪，建立动态熔断机制隔离高危模块防扩散，定期接受安全审计优化策略，符合监管要求，保障服务连续性与用户权益。		
	退出机制	本应用按照退出机制（见附件1-5），严格遵循《网络安全法》《数据安全法》《个人信息保护法》等法规及金融机构移动应用全生命周期管理规范，在触发监管要求、技术缺陷不可修复或业务需求变更等条件时，通过提前30日官方通知用户及合作方、签订终止协议、停止新用户接入并关闭功能模块的业务退出流程，以及完成数据脱敏归档及原始敏感数据删除、回收系统资源、清理流量日志、下线移动端SDK及后台分析平台的技术退出流程，实现数据安全、系统平稳下线及用户权益保障，确保终止服务符合法规要求并妥善处理遗留问题。		
	应急预案	本应用按照应急预案（见附件1-6），构建“预防-监测-响应-优化”全流程机制，依托威胁情报SDK与全流量关联分析技术防范数据泄露、恶意攻击及终端环境风险；系统上线前完成全链路测试、专项验证及应急培训，上线后通过7×24小时监控实时捕捉异常，对恶意攻击、异常登录等触发动态拦截与全量日志溯源，针对数据泄露启动脱敏隔离、关闭非必要传输，对终端威胁定位攻击源并封禁风险设备及SDK非授权调用，按影响分级响应；定期复盘迭代模型、开展对抗演练，落实《网络安全法》保障合规性，预留应急资源池形成长效风控闭环，确保业务连续性。		

		数据安全及合规运营。	
投诉响应机制	机构投诉	投诉渠道	1. 营业网点 向石嘴山银行营业网点大堂经理、网点负责人反映问题或通过客户意见簿留言。 2. 客服电话 致电客户服务热线（96789），选择人工服务联系客服代表。 3. 信件 邮寄投诉信件至石嘴山银行，由总行消费者权益保护部受理。 邮件地址：宁夏石嘴山市大武口区朝阳西街 39 号 邮政编码：753000 收件人：石嘴山银行股份有限公司
		投诉受理与处理机制	受理部门：总行消费者权益保护部 受理时间：7×24 小时 处理流程：各渠道接到客户投诉后，应详细如实记录客户投诉信息，当日内报送至总行消费者权益保护部。总行消费者权益保护部根据投诉属地原则，第一时间将投诉事件转发总行相关部门或所属分行。总行相关部门或分行根据客户投诉情况安排相关调查核实工作通过监控录像调阅、查阅交易记录等手段还原事件并进行分析后，提投诉解决措施及对被投诉人的处理意见，并在规定时限内将调查核情况、投诉处理情况、对相关责任人处理意见等向消费者进行回复。 处理时限：3 个工作日
	自律投诉	投诉渠道	受理机构：中国互联网金融协会投诉网站：https://tousu.nifa.org.cn 投诉电话：400-800-9616 投诉邮箱： fintech_support@nifa.org.cn
		投诉受理与处理机制	中国互联网金融协会是经党中央、国务院同意，按照人民银行、银监会、证监会、

			保监会、工信部、公安部、工商总局等10部委联合发布的《关于促进互联网金融健康发展的指导意见》（银发〔2015〕221号）要求，由中国人民银行会同银监会、证监会、保监会等国家有关部委组织建立的国家级互联网金融行业自律组织。为保护金融消费者合法权益，营造守正、安全、普惠、开放的金融科技创新发展环境，协会按照金融管理部门相关要求建立健全消费者投诉处理机制。对于涉及相关地区的金融科技创新应用的争议、投诉事项，协会接收投诉意见后，由相关部门依程序进行处置，并接受金融管理部门监督审查。 联系方式：400-800-9616 对外办公时间：周一至周五 上午 8:30-11:30 下午 13:30-17:00
备注	无		
承诺声明	本机构承诺所提交的材料真实有效，遵守国家相关法律法规规定和社会公序良俗，严格落实金融管理部门相关监管要求，认真执行行业相关规则规范，强化全流程风控管理体系建设，有效识别、评估、监测和控制风险，并做出以下声明： 1. 守正创新。忠实履行金融天职和使命，着力解决实体经济痛点难点，确保科技创新不偏离正确的发展方向，严防技术滥用，切实通过技术创新满足人民群众对美好生活的期待与向往。 2. 以人为本。始终坚持以人民为中心的发展思想，坚持金融科技创新行为从人民群众实际需求出发，以增进社会共同福祉为目标，尊重并维护人民群众尊严和利益，致力促进社会和谐与文明进步。 3. 诚实守信。恪守社会主义核心价值观，将求真务实作为金融科技从业人员的基本素养，将履约践诺作为从事金融科技活动的基本要求，强化诚信道德自律，积极倡导诚实守信的良好社会风尚。 4. 公开透明。使用简明清晰、通俗易懂的方式，及时、真实、准确、完整地主动对外披露金融科技创新的功能实质和潜在风险，不隐瞒不利信息。		

不“劝诱”销售产品，让社会公众看得到、读得懂、能监督。

5. 权益保护。充分尊重和保障人民群众隐私权、自主选择权、依法求偿权等合法权益，严格履行适当性义务，严防过度采集、违规使用、非法交易和泄露用户隐私数据行为，采取风险拨备资金、保险计划等补偿机制，切实保护用户资金和信息安全。

6. 安全合规。把遵守法律法规和维护金融稳定作为开展金融科技创新活动的前提条件，已通过业务合规性和技术安全性评估审计等措施保障新技术应用风险可控，避免新技术应用带来的数据泄露、算法黑箱、信息茧房等问题，切实防范技术和数据滥用可能导致的人民群众信息与资金失窃风险。

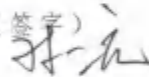
7. 公平普惠。应用新一代信息技术优化金融服务供给结构，持续增强金融服务的普适性、可得性和满意度。重点关注特殊人群、弱势群体需求，努力消除因使用成本、文化程度、地域限制等造成的“数字鸿沟”，不断提升人民群众的获得感、幸福感、安全感。

8. 社会责任。贯彻落实国家战略部署，围绕新时代经济社会发展的战略目标、战略重点，始终把社会效益放在首位，坚持社会效益和经济效益相统一，开展“负责任创新”，打造“值得信赖的技术”，切实服务经济社会健康可持续发展。

本声明书正文与附件表述不一致的，以正文为准。

以上承诺如有违反，愿承担相应责任与后果。

法定代表人或其授权人（签字）



2025年10月23日（盖章）



附件 1-1

石嘴山银行 App（微信银行）用户隐私政策

尊敬的石嘴山银行 App（含微信银行）用户：

我们对《石嘴山银行 APP(微信银行)用户隐私政策》进行了更新。此版本更新内容主要为：对鸿蒙、语音功能、同盾 SDK 采集信息相关内容。

尊敬的石嘴山银行 App（含微信银行）用户（以下简称“您”），石嘴山银行股份有限公司（注册地址：宁夏回族自治区石嘴山市大武口区朝阳西街 39 号、以下简称“我行”）重视用户的隐私，您在使用石嘴山银行 App（含微信银行），以下统称石嘴山银行 App）时，我行将按照《石嘴山银行 App（微信银行）用户隐私政策》（以下简称“隐私政策”）收集、存储、使用及对外共享您的个人信息。为了保证对您的个人隐私信息合法、合理、适度的收集、使用，并在安全、可控的情况下进行存储及传输，我行特制定本政策，请您仔细阅读本并确认了解我行对您个人信息的处理规则。阅读过程中，如您有任何疑问，可联系我行客服热线 0951-96789 咨询。**对本政策中我行认为可能与您的权益存在重大关系的条款和敏感信息，我行采用字体加粗标注。**

如您就本政策点击或勾选“同意”并确认提交，即视为您同意本政策，并同意我行按照本政策来收集、使用、存储和使用您的相

关信息。本《隐私政策》与产品服务相关协议（含石嘴山银行 App 用户服务协议、石嘴山银行个人银行结算账户管理协议、石嘴山银行个人客户电子银行服务协议）产品服务协议，共同构成我行与您达成的完整隐私政策，两者如有不一致之处，以相应的产品（或服务）协议或授权书的约定为准。

本《隐私政策》将帮助您了解以下内容：

- 一、我行如何收集和使用您的个人信息
- 二、我行如何使用 Cookie 和同类技术
- 三、我行如何共享、转让和公开披露您的个人信息
- 四、我行如何存储和保护您的个人信息
- 五、您如何管理您的个人信息
- 六、我行如何保护未成年人信息
- 七、第三方收集和使用您的个人信息情况
- 八、本“隐私政策”如何更新
- 九、如何联系我行

一、我行如何收集和使用您的个人信息

个人信息是指以电子或其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反应特定自然人活动情况的各种信息。个人信息包括姓名、出生日期、身份证件信息（身份证、护照）、

个人生物识别信息、通信通讯联系方式、住址、账户信息、财产状况、位置信息。

个人敏感信息是指一旦泄露或者非法使用，容易导致自然人的¹人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括：生物识别信息、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹信息，以及不满十四周岁未成年人的信息。

（一）我行如何收集您的个人信息

在您使用石嘴山银行 App 服务过程中，我行会收集您在使用服务过程中主动输入或因使用服务而产生的信息：

1. 当您注册成为石嘴山银行 App 用户或使用我行服务时，您需提供您本人的手机号码，我行将通过发送短信验证码的方式来验证您的身份是否有效。您需通过身份基本信息多重交叉验证后方可使用我行的部分服务（包括支付、账户余额购买投资理财金融产品），如果您需使用此类服务，则可能需要提供更多信息（包括姓名、证件、卡号、手机号）以完成身份基本信息多重交叉验证。同时，为了验证您提供信息的准确性和完整性，我行会合法留存并核对您的国家机关、金融机构、企事业单位信息；如在验证核对过程中我行需要向前述验证机构收集您的信息，我行会依照法律法规或监管规定要求相关验证机构说明其个人信息来源，并对其个人信息来源的合法性进行确认。

2. 当您使用石嘴山银行 App 功能或服务时，在下列情形中，您可能需要向我行提供或授权我行收集相应服务所需的个人信息。如

您拒绝提供部分功能或服务所需信息，您可能无法使用部分功能或服务，但这不影响您正常使用石嘴山银行 App 的其他功能或服务。

(1) 您在石嘴山银行 App 内登陆时，我行需要您提供账号、密码，同时可能采集验证指纹、面容（不含鸿蒙系统与安卓系统客户端）、短信验证码和人脸识别手段以便于验证您的身份。为了让您更安全、便捷地使用登陆服务，如您的设备与石嘴山银行 App 版本均支持指纹或面容功能，通过在您的设备上完成指纹或面容验证进行登录。我行仅接收验证结果，并不收集您的指纹或面容信息。如您不想使用指纹或面容验证，仍可通过其他方式进行登录（鸿蒙版没有面容验证）。

(2) 您在使用石嘴山银行 App 开通/使用“电子账户”时，“电子账户”是客户通过我行石嘴山银行 App 开立的个人Ⅱ类银行账户。按照中国人民银行规定，您在申请开通时需提供本人在我行或其他银行开立的同名Ⅰ类银行账户（即储蓄卡账户）作为绑定账户来核验身份信息，包括开户申请人姓名、性别、国籍、职业、住所地或者工作单位地址、联系电话、证件类型、证件号码、证件有效期限、绑定账户账号(卡号)、绑定账户是否为Ⅰ类户或者信用卡账户要素，注册电子账户同时需要人脸认证。同时，为遵守银行账户实名制规定和反洗钱客户身份资料保存制度要求，我们需留存您的身份证件及开户相关影像。如您选择不提供或不同意采集、使用以上个人信息，我行将无法为您提供该服务。



(3) 当您使用石嘴山银行 App“查询添加账户”账户功能时，您需要通过石嘴山银行 App 向我们提供手机号、身份证信息信息，同时采用人脸识别、短信验证方式验证、主账户交易密码来核实您身份的真实性及账户信息查询的申请。如您不提供上述信息，我行将无法向您提供该服务。

(4) 找回登录密码和交易密码，为了保障您的账户和资金安全，在您需要找回密码（包括登录密码和交易密码）时，我们需要重新验证您的身份。在个人石嘴山银行 App，上找回登录密码，您需要向我们提供您的姓名、证件号码、预留手机号码、手机银行登陆密码、手机短信验证码可识别您身份的证明信息，您可根据相关页面的提示输入您的相关信息。

(5) 当您使用石嘴山银行 App 提供的实名认证服务时，我行需要您提供您的姓名、证件类型、证件号码、银行卡号/账号信息，并可能通过验证人脸识别、短信验证码方式对有关信息进行有效性核验。如您不提供上述信息，我行将无法向您提供需完成实名认证后方可使用的产品或服务。

(6) 当您购买我行代销的由基金公司、银行理财子公司、信托或资产管理公司发行的产品时，我行将遵照法律法规、监管要求，并基于您与上述公司的具体交易相应收集您的姓名、性别、国籍、职业、地址、邮政编码、联系方式、证件类型、证件号码、证件有效期、税收居民身份信息、交易账号/投资人理财账户、银行卡号、投资人基金账号、邮箱、年收入、客户风险承受能力级、交易及所购买的产品信息、分红方式、投资者信息、CRS 涉

税信息（如有）、录音录像信息（如有），以便于完成代销产品的购买确认。如您购买私募产品，还将相应收集您最近三年年均收入、个人金融资产、家庭金融资产、两年以上金融产品投资经历、专业投资者信息。如果您不提供本款所列信息，您可能无法购买相关产品。

（7）当您使用石嘴山银行 App 系统手机号转账、石嘴山银行 App 系统话费充值涉及通讯录的功能时，我行仅获取您从通讯录中点选的联系人信息，并进行加密传输以防恶意截取。上述信息属于个人敏感信息。如您不需要使用上述功能，可不提供该信息，将不会影响您正常使用石嘴山银行 App 的其他功能。

（8）当您使用石嘴山银行 App 的转账汇款、扫码支付收付款功能时，您需要提供收款方的姓名、银行账号/手机号、开户银行收款方信息，并需要提供您的姓名、付款卡号、证件类型及证件号码，同时可能采用验证密码、指纹、面容（不含鸿蒙系统与安卓系统客户端）、短信验证码和人脸识别手段以便于验证您的身份。此外，我行还会收集您的收付款交易信息，形成收款人名册，以简化您的转账操作，方便您查询。如您拒绝提供该信息，仅会使您无法使用上述功能。

（9）当您使用公务卡还款相关服务时，您需提供姓名、储蓄卡号、账户交易密码，用于为您提供还款、账户管理服务，如您不提供上述信息，我行将无法向您提供该服务，但不影响您正常使用石嘴山银行 App 的其他功能。

（10）当您使用石嘴山银行 App 消息服务时，我行会收集您的账户信息及交易信息，以便及时向您发送账户资金变动及相关交易通知；我行也可能会向我行的合作伙伴收集其合法留存并经您授权可以共享使用的信息，以便为您提供相应消息通知服务。

（11）您可以通过搜索来精准地找到您所需要的产品或服务。我行会保留或统计您的搜索关键词和点击数据，以方便您重复输入或为您展示与您搜索内容相关联的商品或服务。请您注意，您的搜索关键词信息无法单独识别您的身份，不属于您的个人信息，为了给您和其他用户提供更高效率的搜索服务，我行有权对其进行使用；只有当您的搜索关键词信息与您的其他信息相互结合使用并可以准确识别您的身份时，在结合使用期间，我行会将您的搜索关键词信息作为您的个人信息，与您的搜索历史记录一同按照本隐私政策对其进行处理与保护。

（12）当您使用网点预约、生活基于地理位置的功能时，我行会收集您的位置信息，目的是为了向您提供所在位置的相应服务。如您拒绝提供该信息，您将无法使用上述功能，但这不影响您正常使用石嘴山银行 App 的其他功能。

（13）当您通过石嘴山银行 App 客户端进行支付管理时，如开通扫码支付操作，我行会验证您的交易密码。您可以通过石嘴山银行 App（微信银行）客户端“我的账户”-“密码重置”修改您的交易密码。为保证您的账户资金安全，当您进入安全中心修改交易密码时需要验证您的用户身份。如您拒绝提供该信息，您

将无法使用上述功能，但这不影响您正常使用石嘴山银行 App 的其他功能。

(14) 当您使用石嘴山银行 App 上申请贷款相关服务时，我行可能需要您提供收款账号、还款账号、账号户名、账户开户行、单位信息、单位地址、收入状况、工作年限、住宅地址、车牌号码、企业注册地址、企业名称、企业注册号（统一社会信用代码）、纳税人识别号、法定代表人、联系人姓名、手机号、通讯地址、电子邮箱、证件号、姓名、银行账号、职业、地址、联系方式、工作信息、房产情况、车产、税务、社保、公积金，同时可能采用验证码、短信验证码、人脸识别手段以便于验证您的身份。为了验证您提供信息的准确性和完整性，在经您授权同意的情况下，我行会与合法留存您信息的国家机关、金融信用信息基础数据库、金融机构、企事业单位进行核对。如您拒绝提供该信息，仅会使您无法使用个人贷款服务。

(15) 当您在石嘴山银行 App 参与领奖活动时，我行会收集您的姓名、证件类型及证件号码、手机号码、银行卡号、收件人信息、地址以确保您获得的活动奖品可以正常领取和使用，同时您可能需要根据国家法律法规及监管要求或服务提供方（如有基础电信运营商、移动转手运营商、视频会员、票务销售方、出行服务商、支付服务商）的要求提供您的签署个人信息及活动参与数据。如您不提供本款所列信息，您可能无法正常领取奖品。

(16) 当您在石嘴山银行 App 上参与推荐分享类活动（MGM）时，我行可能需要您提供您的姓名、性别、身份证号、手机号、

位置信息、微信昵称、微信头像、微信唯一用户标识、亲友姓名、亲友手机号。用于确认您和您的亲友可以正常参与推荐分享相关活动，并进行活动记录展示，资格达标判断。如您不提供上述信息，我行将无法向您提供该服务。

（17）当您在石嘴山银行 App 上使用医保电子凭证时，我行需要您提供姓名、身份证号、手机号以便于验证您身份真实性，并将信息经过加密处理后传给相应政府部门用于信息查询。如您不提供上述信息，我行将无法向您提供该服务。

（18）当您在石嘴山银行 App 上使用他行卡转入功能时，我行需要您提供银行卡号（我行或他行）、预留手机号码可识别您身份的证明信息，同时可能采用验证码、短信验证码手段以便于验证您的身份并授权签约第三方支付机构，为了验证您提供信息的准确性和完整性，在经您授权同意的情况下，我行会与相关金融信息数据库对您的信息进行核对。如您拒绝提供该信息，仅会使您无法使用该服务。

（19）当您使用石嘴山银行 App 在商家进行消费时，我行需要按照法律法规及监管规定对商家进行管理，防范套现或欺诈风险，因此，我行将直接收集或向商家收集您的交易信息，包括交易金额、交易对象、交易商品、交易时间、订单信息（如有）。如您不同意我行记录前述信息，则可能无法完成交易。

3. 当您使用石嘴山银行 App 的功能或服务时，在某些特定使用场景下，我行可能会使用具体的相应业务资质及能力的第三方服务

商提供的软件服务工具包（简称“SDK”）来为您提供服务，此时第三方服务商需要收集您的必要信息，具体包括以下几种：

SDK 名称	场景描述	涉及收集的个人信息字段	数据接收方名称
腾讯云 TRTC SDK (鸿蒙版没有该 SDK)	视频营业厅	相机、麦克风、设备生产商 设备型号、操作系统版本号 网络类型、系统语言类型、 屏幕分辨率	飞虎互动科技（北京）有限公司
同盾 SDK	业务安全和风控	OAID、Android ID、IMSI、IMEI、MEID、SIM 卡序列号、国家代码、移动运营商、SIM 卡运营商、手机制式、网络制式、MCC、MNC、设备序列号 (Android 9.0 及以后需要权限)、设备型号、设备类型、无线 IP 地址、无线网络名称、无线 BSSID 无线 Mac 地址、网关地址、WIFI 子网掩码、安装的应用列表、蓝牙 MAC 地址、GPS 定位坐标、广告追踪标示符、当前连接的无线网络名称、当前连接的无线网络的 BSSID、最近一次定位坐标、运行中进行信息、传感器（光传感器、重力传感器、陀螺仪传	同盾科技有限公司

		感器、心率传感器) 相关设备信息	
百度地图 SDK	地图定位、地图	Android ID, IDFA, 操作系统版本, 设备配置, 设备品牌及型号、应用名、经纬度、MAC、GNSS 信息、WiFi 网关地址、BSSID、SSID、WiFi 信号强度、WiFi 状态、WiFi 参数、WiFi 列表、基站 ID 数据信息、运营商信息、设备信号强度信息、IP 地址、蓝牙信息、系统进程信息、传感器信息(加速度、陀螺仪、方向、压力、旋转矢量、光照、磁力计)、移动网络、WiFi 网络、外部存储目录、IDFV、定位、始终允许访问位置信息、跟踪、网络访问、存储、相机、存储。	百度网讯科技有限公司;联系方
小象配网 SDK (鸿蒙版没有该 SDK)	小象存钱罐的配网	用户手机唯一标识 ID 收集客户的 WiFi 的账号密码	广州融至益教育科技有限公司
云从 SDK	人脸识别服务	Android 版本 动作活体:	云从科技集团股份有限公司

		必须权限：相机权限 用到但不采集：设备型号、操作系统版本、网络状态、检查设备是否有风险（是否 Root）、重力传感器、人脸 预览动作视频： 活体验证后返回：主要为最佳人脸图片及 Hack 字符串： iOS 版本 动作活体： 必须权限：相机权限 用到不存储：设备型号、操作系统版本、检查设备是否有风险（是否 Root） 活体验证后返回：主要为最佳人脸图片及 Hack 字符串	
ORC 云从 SDK	OCR 扫描 身份证、 银行卡	Android 版本 身份证 OCR： 必须权限：相机权限 用到但不采集：设备型号、获取操作系统版本、相机权限、重力传感器、	云从科技集团股份有限公司

		身份证预览视频 OCR 识别后返回：抓拍最佳身份证图片（两张：正面背面各一张）、身份证头像图片、姓名、性别、民族、出生日期、住址、身份证号、签发机关、有效期 银行卡 OCR： 必须权限：相机权限 用到但不采集：设备型号、获取操作系统版本、重力传感器、银行卡预览视频 OCR 识别后返回：发卡行、卡号、卡名、卡类型、开始日期、结束日期、抓拍最佳银行卡图片； iOS 版本 身份证 OCR： 必须权限：相机权限 用到不存储：设备型号、获取操作系统版本、相机权限 OCR 识别后返回：抓拍最佳身份证图	
--	--	--	--

		片（两张：正面背面各一张）、身份证头像图片、姓名、性别、民族、出生日期、住址、身份证号、签发机关、有效期 银行卡 OCR： 必须权限：相机权限 用到但不存储：设备型号、获取操作系统版本、重力传感器 OCR 识别后返回：发卡行、卡号、卡名、卡类型、开始日期、结束日期、抓拍最佳银行卡图片	
腾讯移动开放平台 SDK (腾讯 QQ SDK)	一键分享功能	手机终端的电话状态权限、网络通讯权限，来获取该终端的设备信息和网络信息	腾讯科技有限公司及其关联公司
云证通 SDK (鸿蒙版没有该 SDK)	移动电子签名服务，用于下载数字证书，加强交易安	姓名、证件号、设备型号、系统版本号、SE 标识符、应用首次安装时间	中金金融认证中心有限公司

	全性		
安胜华信 sw_security SDK	移动应用 安全监 测，用于 判断当前 App 所运 行的手机 设备的安 全性，防 止恶意的 用户对 App 进行 网络安全 攻击，保 护用户的 财产安全	andriod 版本 Android_ID、MAC 地址、电话状态、 屏幕共享状态、网络状态、系统进程 信息、应用是否安装、设备标识、设 备及系统信息、传感器状态信息 iOS 版本 应用信息、屏幕共享状态、网络状态、 设备及系统信息、设备及系统信息 harmony 版本 应用信息、屏幕共享状态、网络状态、 设备及系统信息、设备及系统信息	北京安胜华信科技有 限公司
Andjni （鸿蒙版没 有该 SDK）	底层功能 支撑	IMEI/MEID、传感器信息、已安装应 用列表、Android_ID、MAC 地址	Jni 基础库

梆梆 SDK (鸿蒙版没有该 SDK)	防止安卓 APP 被破解、反编译、二次打包等威胁	无	北京梆梆安全科技有限公司
科大讯飞语音 SDK (鸿蒙版没有该 SDK)	语音助手	无	科大讯飞股份有限公司

如您不同意上述第三方服务商收集前述信息，可能无法获得相应服务，但不影响您正常使用石嘴山银行 App 的其他功能或服务。

4. 当您使用石嘴山银行 App（微信银行）服务时，为了维护服务的正常运行，降低资金交易风险，我行会收集您的设备型号、设备制造商、操作系统、唯一设备标识符、石嘴山银行 App 软件版本号、登录 IP 地址、接入网络的方式、类型和状态、网络质量数据、与石嘴山银行 App 操作日志及服务日志相关的信息、任务列表、本应用的进程列表、地理位置信息、设备名称、App ID、Android ID、BSSID、MAC、SSID、IDFA、IMSI、IMEI、SIM 卡信息、WIFI 信息、运营商信息、传感器、手机号码、服务日志信息（如您在石嘴山银行 App 搜索、查看的信息、地理位置信息、服务故障信

息、引荐网址信息) 信息, 如您部同意我行收集前述信息, 可能无法完成风控验证, 但不影响您正常使用石嘴山银行 App 的其他功能或服务。

5. 为向您提供更加准确、个性和便捷的服务, 提升服务体验、改进服务质量, 或为防范风险, 我行会收集您反馈意见建议时提供的信息, 收集您使用石嘴山银行 App 功能或服务的类别、方式和操作信息, 我行会对这些信息进行综合统计、加工分析, 并会根据上述信息向您提供相应服务。

6. 当您在石嘴山银行 App 中使用第三方提供的服务时, 第三方可能会通过石嘴山银行 App 获取您的昵称、头像公开信息; 如您已明示同意该第三方可以获取您的地理位置信息, 我行将授予该第三方获得终端地理位置信息接口, 其可以通过该接口获得您的具体位置信息; 在经过您的明示同意后, 第三方可获取您的手机号信息; 对于您在使用第三方提供的服务时主动提供给第三方的相关信息, 我行将视为您允许该第三方获取上述此类信息; 对于您在使用该第三方服务时产生的信息, 应由您与该第三方依法约定上述信息的收集和使用事项。如您拒绝第三方在提供服务时收集、使用或者传递上述信息, 将可能会导致您无法在石嘴山银行 App 中使用第三方的相应服务, 但这不影响您使用石嘴山银行 App 的其他功能。

7. 以下情形中, 您可选择是否授权我行收集、使用您的个人信息。如您拒绝授权部分功能或服务所需信息, 您将无法使用相关功能或服务, 但这不影响您正常使用石嘴山银行 App 的其他功能或服务:

(1) 电话权限（设备状态），用于确定设备识别码，以保证账号登录的安全性。拒绝授权后，我行石嘴山银行 App 将不读取设备状态，同时可能需要通过其他方式进行账号登录的安全验证。

(2) 存储权限，用于缓存您在使用石嘴山银行 App 过程中产生的文本、图像、视频内容，以及用于上传设置您的头像、备注您的交易信息、人脸识别、分享、意见反馈功能。如您拒绝授权后，上述功能可能无法正常使用。

(3) 摄像头，用于身份证识别、银行卡识别、识别二维码、人脸识别、设置头像、录像、拍照，在扫一扫、人脸识别登录/转账/支付/提升认证、头像设置、录像场景、收支图片。拒绝授权后，上述功能将无法使用。

(4) 相册，用户上传照片设置您的头像、备注您的交易信息、电子回单保存、二维码扫描、银行卡及身份证识别服务（我行获得的证件信息，加密后储存于数据库中）。拒绝授权后，上述功能将无法使用。

(5) 手机通讯录，在手机号转账、汇款短信通知、推荐有礼、使用智能助理进行语音转账、话费充值过程中，我行将收集您的手机通讯录用于协助您通过通讯录快速选取电话号码，无需您手动输入。拒绝授权后，上述功能仍可以使用，但需要手工输入手机号码。

(6) 手机短信，用于短信分享链接，及拦截欺诈短信，系统后台不保存短信内容。如您拒绝通讯信息（短信）授权，我行石嘴山银行 App 将不读取短信内容，则您无法享受上述服务。

(7) 地理位置，获取您所在地理位置，主要用于石嘴山银行 App 交易风控、消息推送、分享功能以及展所在城市的服务，包括网点预约、就近生活缴费、开会。我行系统后台保存您交易时的位置信息，拒绝授权后，上述功能可能无法正常使用。

(8) 网络通讯，用于与服务端进行通讯。拒绝授权后，石嘴山银行 App 所有功能无法使用。我行系统后台保存客户交易时所使用设备的网络信息，包括 IP、端口信息。

(9) 应用列表，用于石嘴山银行 App 风控防交易欺诈，我行系统后台不保存您的应用列表信息。如您拒绝授权应用列表权限，我行石嘴山银行 App 将不读取应用列表内容。

(10) 日历，用于预约转账、待办提醒、资金归集场景中使用。如您拒绝授权日历权限，将无法使用日历提醒功能。

(11) 剪切板，用于权益卡密、转账快捷跳转功能，我行系统后台不保存您的剪切板内容。如您拒绝授权剪切板权限，我行石嘴山银行 App 将不读取剪切板内容，则您无法使用上述功能。

(12) 电话，用于一键拨打客服电话、联系我们、幸福版“应急中心”相关服务，如您拒绝授权电话权限，将无法使用上述功能。

(13) 麦克风，用于用于视频营业厅（面对面服务）办理业务时进行语音交互，如您拒绝授权麦克风权限，将无法使用上述功能。

在相应石嘴山银行 App（微信银行）系统使用过程中，上述功能可能需要您在您的设备中向我行开启您的设备、存储、相机（摄像头）、相册、地理位置（位置信息）、手机通讯录、短信、网络

通讯、应用列表、日历、剪切板、电话的访问权限、麦克风，以实现这些功能所涉及的信息的收集和使用。请您注意，您开启这些权限即代表您授权我行可以收集和使用这些信息来实现上述功能，如您取消了这些授权，则我行将不再继续收集和使用您的这些信息，也无法为您提供上述与这些授权所对应的功能。

8. 当您在石嘴山银行 App 上进行人脸识别以核实身份时，我行会采集您的人脸信息，并将加密后存储于系统后台数据库中，用于业务办理过程留存、辅助识别和核实客户身份。对于某些品牌或型号的手机终端自身的本地生物特征认证功能，如人脸识别、面容 ID、指纹功能，其信息由手机终端提供商进行处理，我行不留存您应用手机终端相关功能的信息。

我行在向您提供其他业务功能是，会另行向您说明收集、使用您相关信息的目的、用途、内容和范围，并征得您的同意或授权。我行会按照本政策以及相应的用户协议约定收集、使用、存储、对外提供及保护您的信息。

请您知悉，若您拒绝同意隐私政策，石嘴山银行 App 将无法获取 IP 地址网络信息，您将无法正常使用 App。

（二）我行如何使用您的个人信息

为了遵守国家法律法规及监管要求，以及向您提供服务及提升服务质量，或保障您的账户和资金安全，我行会在以下情形中使用您的信息：

1. 我行会根据本政策的约定并为实现我行的服务或功能对所收集的您的个人信息进行使用。

2. 为了使您知晓使用石嘴山银行 App 服务的状态,我行会向您发送服务提醒。您可以通过手机系统设置中的通知设置关闭服务提醒,也可以通过通知设置重新开启服务提醒。

3. 为了保障服务的稳定性与安全性,我行会将您的信息用于身份验证、安全防范、诈骗监测、预防或禁止非法活动、降低风险、存档和备份用途。

4. 根据法律法规或监管要求向相关部门进行报告。

5. 邀请您参与我行服务、产品或功能有关的客户调研。

6. 为了维护您的合法权益,为您提供完善优质的财富管理、支付结算产品、个人信贷等服务,提升您的用户体验,我行在获取您的授权后,将依法依规收集、使用您的姓名、联系方式、银行账户、交易流水、资产负债情况、位置信息、衍生信息数据。用于如下:

(1) 对您在我行的身份特征、行为偏好、交易习惯及风险等级等特征进行分析;

(2) 向申请人发送用户体验、改进调研、市场调研等信息;

(3) 为很强人提供金融产品及服务的营销推荐、资产配置、客户权益推介等相关内容。

我行服务的方式包括电话、石嘴山银行 APP 消息推送、企业微信、短信、石嘴山银行公众号推送等。我行已采取安全技术措施及管理措施，保护您的个人信息免受丢失、滥用、非授权进入、披露、改变或者破坏。

您不同意接收上述服务或者进入服务信息的，可按照我行提示的方法选择退订：

（1）短信：通过回复 TD 发送。

（2）APP 消息推送/企业微信/公众号推送：通过关闭、取消对应服务或前往石嘴山银行网点进行取消。

请你悉知，当您执行上述操作后，石嘴山银行将无法继续为您提供撤回统一或授权对应的服务，但不会影响此前基于您的授权已开展的个人信息处理。

7. 在收集您的个人信息后，我行在通过技术手段对您的信息数据进行匿名化处理后，该匿名化的信息将无法识别信息主体，有权在不经您同意的情况下直接使用，有权对用户数据库进行分析并予以商业化的利用。

8. 我行会对我行的服务或功能使用情况进行统计，并可能会与公众或第三方共享这些统计信息，以展示我行的服务或功能的整体使用趋势。但这些统计信息不包含您的任何身份识别信息。

9. 当我行展示您的信息时，我行会采用包括内容替换、匿名化处理方式对您的信息进行脱敏，以保护您的信息安全。

10. 因监管要求、业务规则、风控要求需加强身份验证时，我行会应用您在可视柜台和网点柜面办理涉及核实身份业务时留存的现场影像及身份证件人像照进行人脸识别。如您不同意我行应用前述信息，则可能无法完成需利用人脸识别加验的相关业务，但不影响您使用我行提供的其他服务。

11. 为了给您提供更好的使用体验，我行可能会根据您的身份信息、交易信息、资产信息、设备信息、服务日志以及其他取得您授权的信息提取您的偏好特征。特征提取方式包括但不限于：基于个体或群体客户的统计值（如：求和）、向量化处理等。同时，我行可能基于您的偏好特征，使用算法模型预测您的偏好内容，匹配您可能感兴趣的商品、服务或其他信息，向您进行信息推送、商业营销，包括以下场景：

（1）石嘴山银行 App 上的贷款及相关服务的可获得性，以及相关的授信要素（授信金额、授信期限、利率、计息方式、还款方式、担保方式等）均由系统依据收集到的您的个人信息，可能通过自动化决策的方式产生。自动化决策目标主要为您的履约意愿及偿债能力，主要依据以下信息：是否本人真实意愿、贷款用途是否合理、历史履约情况、当前负债情况、金融机构多头借贷情况、当前资产情况、当前收入情况、当前行业/职业稳定性（或经营稳定性）等进行综合判断。若您不接受石嘴山银行 APP 贷款及相关服务的自动化决策结果，我行也提供线下的贷款及相关服务。

（2）石嘴山银行部分理财及先关服务的可获得性，由于系统根据收集到的您的个人信息，通过自动化决策的方式产生。自动化决

策目标主要为您的投资偏好和产品适合度，主要依据以下信息：当前资产情况、当前收入情况、历史交易情况、风险承受能力评级等进行综合判断。若您不愿意接受石嘴山银行 App 上理财及相关服务的自动化决策结果，也可通过我行线下提供的理财服务做进一步咨询。

(3) 石嘴山银行 App 首页 banner、启动页图片、弹窗、公告消息是有系统手机到的您的个人信息，通过自动化决策的方式产生。

此外，为保障您接收信息的自主性，我行也提供了不基于个性推算法的展示内容，您可在石嘴山银行 App 的“我的-消息-消息中心设置”中点击关闭“个性化推荐”选项后，我行不再通过自动化决策发送向您进行信息推送、商业营销。

请注意，单独的设备信息、服务日志信息时无法识别特定自然人身份的信息。如果我行将这类非个人信息与其他信息结合用于识别特定自然人身份，或者将其与个人信息结合使用，则在结合使用期间，这类非个人信息将视为个人信息，除取得您授权或法律法规、监管规定另有规定外，我行会将这类信息做匿名化、去标识化处理。

12. 对于您在石嘴山银行 App 上的贷款及相关服务的可获得性，以及相关的授信要素（授信金额、授信期限、利率、计息方式、还款方式、担保方式）均由系统依据收集到的您的个人信息，可能通过自动化决策的方式产生。自动化决策目标主要为您的履约意愿及偿债能力，主要依据以下信息：是否本人真实意愿、贷款用途是否合理、历史履约情况、当前负债情况、金融机构多头借贷情况、当

前资产情况、当前收入情况、当前行业/职业稳定性（或经营稳定性）进行综合判断。若您不接受石嘴山银行 App 上贷款及相关服务的自动化决策结果，我行也提供线下的贷款及相关服务。

13. 您在石嘴山银行 App 上部分理财及相关服务的可获得性，由系统依据收集到的您的个人信息，通过自动化决策的方式产生。自动化决策目标主要为您的投资偏好和产品适合度，主要依据以下信息：当前资产情况、当前收入情况、历史交易情况、风险承受能力评级进行综合判断。若您不接受石嘴山银行 App 上理财及相关服务的自动化决策结果，也可通过我行线下提供的理财服务做进一步的咨询。

（三）征得授权同意的例外

根据相关法律法规、监管要求及国家标准，以下情形我行会处理您的相关个人信息而无需另行征求您的授权同意：

1. 为履行法定指着或者法定义务所必需；
2. 为订立、履行您作为一方当事人的合同所必需的，或按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需的；
3. 为应对突发公共卫生事件，或情急情况下为保护自然人的生命健康和财产安全所必需。
4. 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息。

5. 依照《个人信息保护法》在合理的范围内处理个人自行公开或者有其他已经合法公开的个人信息。

6. 法律、行政法规规定的其他情形

（四）我行从第三方获得您个人信息的情形

我行可能从第三方（如微信、苹果、华为）获取您授权的共享账户信息（头像、昵称），并在您同意本政策后将您的第三方账户与您的石嘴山银行 App 用户绑定，使您可以通过第三方账户直接登录并使用我行的产品/或服务。

为了给您提供快捷的登录、注册、转账投资支付类的资金交易服务，保障您的交易安全、尽可能防范您的账户被他人不法侵害，我行可能通过依法设立的电信运营商第三方机构（包括但不限于中国电信、中国移动、中国联通外部合作机构）获取您的设备手机号及当前所在城市信息，并依据与上述第三方的约定、对个人信息来源的合法性进行确认后，在符合相关法律法规、监管规定的前提下，使用您的这些个人信息。

二、我行如何使用 Cookie 技术和同类技术

为确保石嘴山银行 App 正常运转，我行会在您移动设备上存储名为 Cookie 的小数据文件。Cookie 是包含标识符、站点名称以及一些号码和字符。借助 Cookie，石嘴山银行 App 能够储存您的偏好数据，我行将不会将 Cookie 用于本政策所属目的之外的任何用途，您进行石嘴山银行 App 退出或关闭时将自动删除设备上保存档次 Cookie 文件。

1. 为了您在使用石嘴山银行 App 期间获得更好的用户体验，我行会在您的移动设备本地保存一些个人用户信息的加密缓存文件，如：登录手机号码、登录证件号码、客群标识、手势密码轨迹路径的加密值以及位置信息相关个人信息。借助于此类缓存文件能够让您更方便快捷的登录和使用石嘴山银行 App。

2. 位置信息是指您开启设备定位功能并使用我们基于位置信息提供的相关服务时，我们收集的有关您地理位置的信息。您可以通过关闭定位功能随时停止我们对您的地理位置信息的收集。

3. 如果您的浏览器允许，您可以通过您的浏览器的设置以管理、（部分/全部）拒绝 Cookie 与/或同类技术；或删除已经储存在您的计算机、移动设备或其他装置内的 Cookie 与/或同类技术，从而实现我们无法全部或部分追踪您的个人信息。您如需详细了解如何更改浏览器设置，请具体查看您使用的浏览器的相关设置页面。您理解并知悉：我们的某些产品/服务只能通过使用 Cookie 或同类技术才可得到实现，我行不会将 Cookie 用于本政策所述目的之外的任何用途。如您可管理或删除除 Cookie（您可以清除移动设备上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能）您可能将无法正常使用我们的相关产品，或无法通过我们的产品与服务获得最佳的服务体验，同时也可能会对您的信息保护和账号安全性造成一定的影响。

三、我行如何共享、转让和公开披露您的个人信息

（一）共享

我行不会向其他公司、组织和个人共享您的个人信息，但以下情况除外：

1. 事先获得您的明确同意。

2. 如业务需要对外共享您的个人信息，我行会向您告知共享个人信息的目的、数据接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得您的单独同意。涉及敏感信息的，除上述之外，我行还会向您告知处理敏感个人信息的必要性以及对您个人权益的影响。

3. 请您理解，我行可能会根据法律法规规定，或按政府主管部门的强制性要求，对外共享您的个人信息。

4. 我行可能会向合作方（主要是推送服务或移动设备厂商）提供您的部分账户信息及交易信息，以便及时向您的移动设备发送账户资金变动及相关交易通知。

5. 当您与石嘴山银行在发生贷款或者担保信用业务时，我行可能会向依法设立的征信机构及其他相关合法机构查询、使用或提供您的信用、资产信息。石嘴山银行依法对您的相关信息承担保密责任，并要求合作机构对您的相关信息承担保密责任。

6. 为了您的账户资金、交易安全，我行可能会与其他银行业金融机构或第三方支付机构相关主体共享您的必要信息，包括收款账号、IMSI（国际移动用户识别码）、IMEI、手机号、设备 SEID（手机 NFC 模块的序列号）信息；同时，在提供开户、登录、注册服务

时，我行可能会向中国支付清算协会提供您的手机号、姓名、证件号码信息，用于验证手机号实名制信息。

（二）转让

我行不会向其他公司、组织和个人转让您的个人信息，但以下情况除外：

1. 事先获得您的明确同意。
2. 根据法律法规或强制性的行政或司法要求。

3. 根据法律法规、监管规定和商业惯例，在合并、收购、资产转让类似交易中，如涉及到个人信息转让，我行会要求新的持有您个人信息的公司、组织继续受本隐私政策的约束，或要求该公司、组织重新向您征求授权同意。

（三）公开披露

1. 我行不会公开披露您的个人信息，如确需披露，我行会获取您的单独同意，并告知您披露个人信息的目的、类型；涉及敏感信息，除上述外，还会告知您敏感信息的内容，处理敏感个人信息的必要性以及对您个人权益的影响，并事先征得您的明示同意。

2. 依据法律、法律程序、诉讼或政府主管部门的要求，我行可能会公开披露您的个人信息。

（四）征得授权同意的例外

根据相关法律法规、监管规定，我行可能会处理您的相关个人信息而无需另行征求您的授权同意：

1. 为履行法定指着或者法定义务所必需；
2. 为订立、履行您作为一方当事人的合同所必需的，或按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需的；
3. 为应对突发公共卫生事件，或情急情况下为保护自然人的生命健康和财产安全所必需。
4. 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息。
5. 依照《个人信息保护法》在合理的范围内处理个人自行公开或者有其他已经合法公开的个人信息。
6. 法律、行政法规规定的其他情形

四、我行如何存储和保护您的个人信息

（一）存储

1. 我行会按照法律法规及监管要求规定，将在境内收集和产生的您的个人信息存储于境内。

2. 我行仅在法律法规要求的期限内，以及为实现本政策声明的目的所必须的最低时限内保留您的个人信息，当超出数据保存期限后，我行会对您的信息进行删除或匿名化处理。例如：

（1）手机号码：当您需要使用石嘴山银行 App 服务时，我行需要一直保存您的手机号码，以保证您正常使用该服务，当您注销石嘴山银行 App 用户后，我行将删除相应的信息；

(2) 用户头像：当您设置了头像以后，我行会一直保存您的头像，用于登录页面展示使用。

(二) 保护

1. 我行已使用符合业界标准的安全防护措施保护您提供的个人信息，我行将尽力防止数据遭到未经授权的访问、公开披露、使用、修改、损坏或丢失。我行会采取一切合理可行的措施，保护您的个人信息。例如：我行会使用加密技术确保数据的保密性；我行会使用受信赖的保护机制防止数据遭到恶意攻击；我行会部署访问控制机制，限定只有授权人员才可访问个人信息。

2. 如我行提供的全部或部分石嘴山银行 App 业务停止运营，我行相关产品或服务将通过公告形式向您进行告知，同时停止相关产品或服务对您个人信息的收集操作，保护您的个人信息安全。如因技术故障、网络攻击、自然灾害及事故、人为因素各种原因造成全部或部分石嘴山银行 App 业务中断，我行将采取应急处置和恢复措施予以应对，尽快恢复服务。

3. 我行已通过国家网络安全级保护的测评和备案。

4. 我行会采取一切合理可行的措施，确保未收集与您所办理业务无关的个人信息。

5. 请您理解，由于各种因素有可能出现我行无法合理预见、防范、避免、控制的意外情况。互联网并非绝对安全的环境，请使用复杂密码，协助我行保证您的账户安全。

6. 如发生个人信息安全事件，我行将按照法律法规的要求，及时采取措施进行化解，同时将事件相关情况以邮件、信函、电话、推送通知方式中的一种或多种告知您。同时，我行还将依据监管规定，上报个人信息安全事件处置情况。

五、您如何管理您的个人信息

按照中国相关的法律法规和监管规定，我行保障您对自己的个人信息行使以下权利：

（一）访问、复制、更正及更新您的个人信息

您有权通过我行柜面、石嘴山银行 App 渠道访问及更正、更新您的个人信息，法律法规、监管政策另有规定的除外。您有责任及时更新您的个人信息。在您修改个人信息之前，我行会验证您的身份。

您登录石嘴山银行 App 后，可以在“我的”中，安全设置、安全中心、个人中心、中修改相应信息。

个人中心—为客户提供个性化的用户昵称设置功能，支持查询个人基本信息及设置头像、个人简介、登录手机号。

安全设置—为客户提供多种增强石嘴山银行 App 使用的安全服务，确保银行账户的安全。主要功能包括：修改登录密码、指纹登录、手势登录

安全中心—为提供转账限额设置、支付设置、授权管理设置。

对于修改个人签约手机号信息，可通过我行柜台或 VTM 办理。

（二）删除您的个人信息

您在我行的产品与/或服务页面中可以直接清除或删除的信息，包括绑定银行卡、消息记录、缓存记录。

在以下情形中，您可以向我行提出删除个人信息的请求：

1. 如果我行处理个人信息的行为违反法律法规。
2. 如果我行收集、使用您的个人信息，不符合本政策所述授权例外情形，却未征得您的同意。
3. 如果我行处理个人信息的行为违反了与您的约定。
4. 如果您不再使用我行的产品或服务，或您注销了我行手机银行 App。
5. 如果我行不再为您提供产品或服务。

如我行决定响应您的删除请求，我行还将同时通知从我行获得您个人信息的实体，要求其及时删除，除非法律法规或监管政策另有规定，或这些实体获得您的独立授权。

当您从我行的服务中删除信息后，我行可能不会立即在备份系统中删除相应的信息，但会在备份更新时删除这些信息。

（三）改变您授权同意的范围或撤回您的授权

您可以通过手机系统权限设置、石嘴山银行 App 的“设置-安全中心-第三方应用授权管理/系统授权管理”方式改变部分您授权我行继续收集个人信息的范围或撤回您的授权。请您注意，您注销石

嘴山银行 App 同时，将视同您撤回了对本政策的同意，我行将不再收集相应的个人信息。但您撤回同意的决定，不会影响此前基于您的授权而开展的个人信息处理活动的效力。

（四）注销用户

如您为我行石嘴山银行 App 注册用户，您可以自主要求通过我行柜面渠道注销您的石嘴山银行 App。注销石嘴山银行 App 后，您的石嘴山银行 App 账号同步注销。如您非我行石嘴山银行 App 注册用户，您可以自主选择卸载或停止使用石嘴山银行 App 客户端，以阻止我行获取您卸载或停止使用后可能产生的交易信息、行为信息个人信息。您注销石嘴山银行 App 账号的行为是不可逆行为，一旦您注销您的石嘴山银行 App，您的石嘴山银行 App 账号会同步注销，我行将不再通过石嘴山银行 App 客户端收集您的个人信息，并将删除有关您石嘴山银行 App 账号的一切信息，法律法规或监管机构对个人信息存储时间另有规定的除外。如您在注销过程中存在任何疑问咨询，我行将在七个工作日内进行处理和反馈。

（五）复制携带副本

如您需要复制或打印您使用石嘴山银行 App 所产生的账户流水，可前往我行柜面渠道办理账户流水打印相关业务。如您在打印复制流水过程中存在任何疑问咨询，我行将在 7 个工作日内进行处理和反馈。

（六）响应您的请求

如果您无法通过上述方式访问、更正或删除您的用户信息，或您需要访问、更正或删除您在使用我行服务或功能时所产生的其他用户信息，或您认为我行存在任何违反法律法规或与您关于用户信息的收集或使用的约定，您均可通过本政策中的联系方式与我行取得联系。为了保障安全，我行可能需要您提供书面请求，或以其他方式证明您的身份，我行将在收到您反馈并验证您的身份后的 15 天内答复您的请求。

此外，根据相关法律法规、监管要求规定，以下情形中遇到国家有权机关或者监管机关要求的，或者存在以下约定其他情形的，我行将可能无法响应您的请求：

1. 与国家安全、国防安全相关的。
2. 与公共安全、公共卫生、重大公共利益相关的。
3. 与犯罪侦查、起诉、审判和判决执行相关的。
4. 有充分证据表明您存在主观恶意或滥用权利的。
5. 响应您的请求将导致您或其他个人、组织的合法权益受到严重损害的。
6. 涉及我行或第三方商业秘密的。

六、我行如何保护未成年人信息

（一）未成年人使用我行服务，必须在其父母或者其他监护人的监护下进行。我行将根据国家相关法律法规的规定保护未成年人的个人信息的保密性及安全性。

（二）如您为未成年人，请您的父母或监护人阅读本政策，并在征得您父母或监护人同意的前提下使用石嘴山银行 App 内（包含我行和第三方）提供的服务或向我行和第三方提供您的信息。对于经父母或监护人同意而使用您的信息的情况，我行只会在受到法律允许、父母或监护人明确同意或者保护您的权益所必要的情况下使用或共享此信息。如您的监护人不同意您按照本政策使用我行的服务或向我行提供信息，请您立即终止使用我行的服务并及时通知我行，以便我行采取相应的措施。

（三）如您为未成年人的父母或监护人，当您对您所监护的未成年人的个人信息处理存在疑问时，请通过本政策中的联系方式联系我行。

（四）如您为 14 周岁以下的儿童，请在征得您父母或监护人同意的前提下使用石嘴山银行 App 内（包含我行和第三方）提供的服务或向我行和第三方提供您的信息。对于经父母或监护人同意而使用您的信息的情况，我行除遵守本隐私政策关于用户个人信息的约定外，还会秉持正当必要、知情同意、目的明确、安全保障、依法利用的原则，严格遵循《儿童个人信息网络保护规定》法律法规的要求进行存储、使用、披露，且不会超过实现收集、使用目的所必须的期限，到期后我们会对儿童个人信息进行删除或匿名化处理。如您的监护人不同意您按照本政策使用我行的服务或向我行提供信息，请您立即终止使用我行的服务并及时通知我行，以便我行采取相应的措施。

七、第三方收集和使用您的个人信息情况

当您在石嘴山银行 App 中使用第三方提供的服务时，第三方可能会从我行获取您的昵称、头像、位置、姓名、证件类型、证件号码、证件有效期、手机号码信息及其他提供第三方服务所必须的信息；在经过您的明示同意后，第三方可获取您的以上信息。在将信息提供给第三方前，我行将尽商业上合理的努力评估该第三方收集信息的合法性、正当性、必要性。我行会与第三方签订相关法律文件并要求第三方处理您的个人信息时遵守法律法规和签署的法律文件，要求第三方对您的信息采取保护措施。如您拒绝第三方在提供服务时收集、使用或者传递上述信息，将可能会导致您无法在石嘴山银行 App 中使用第三方的相应服务，但这不影响您使用石嘴山银行 App 的其他功能。

对于您在使用第三方提供的服务时主动提供给第三方的相关信息，我行将视为您允许该第三方获取上述此类信息；对于您在使用第三方服务时产生的信息，应由您与该第三方依法约定上述信息的收集和使用事项。

您理解，第三方提供的服务由该第三方独立运营并独立承担全部责任。因第三方所提供服务或其使用您的信息产生的纠纷，或其违反相关法律法规或本协议约定，或您在使用其服务过程中遭受的损失，请您与该第三方协商解决。对于需由第三方解决的问题，我行将尽商业上合理的努力推动第三方解决。

八、本政策如何更新

根据国家法律法规、监管政策变化及服务运营需要，我行将对本政策及相关规则不时地进行修改，修改后的内容会通过我行官网（www.szscsb.cn）、石嘴山银行 App 渠道公布，公布后即生效，并取代此前相关内容。您应不时关注相关公告、提示信息及协议、规则相关内容的变动。本政策更新后，石嘴山银行 App 将在首次登录页时通过弹窗进行提示，您需要主动点击勾选确认同意。您知悉并确认，如您不同意更新后的内容，应立即停止使用相应服务，并注销相关的用户，我行将停止收集您的相关个人信息；如您继续使用服务，即视为同意接受更新内容。

九、如何联系我行

如您对本政策存在任何疑问，或任何相关的投诉、意见，请联系客服 0951-96789、官方网站（www.szscsb.cn）、石嘴山银行 App “意见反馈”，以及我行各营业网点进行咨询或反映。受理您的问题后，我行会及时、妥善处理。一般情况下，我行将在 7 个工作日内给予答复。如果您对我们的答复不满意，特别是如果您认为我们的个人信息处理行为损害了您的合法权益，您还可以向网信、电信、公安及市场监管监管部门进行投诉或举报，您还可以通过向被告住所地有管辖权的法院提起诉讼来寻求解决。

附件 1-2

基于移动应用环境监测技术的安全风险评估与防控服务合法合规性评估报告

本应用严格遵循《中华人民共和国网络安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及《移动金融客户端应用软件安全管理规范》（JR/T 0092-2019）等法律法规，聚焦移动金融应用安全风险实时监测与处置。数据采集环节遵循

“最小必要原则”，通过威胁情报 SDK 仅收集设备环境、崩溃日志等必要信息，并采用匿名化处理技术剥离用户身份关联性；安全防护层面，结合加密传输、动态策略阻断及多维度溯源机制，确保攻击行为处置符合《反电信网络诈骗法》要求，日志留存期限满足金融行业监管标准。平台通过隐私协议明示数据用途并提供用户授权管理功能，保障全流程合规。本项目在数据安全、用户权益保护及风险防控机制设计上均符合现行法规要求，可依法合规开展业务应用。

石嘴山银行股份有限公司合规法律部

2025 年 4 月 24 日

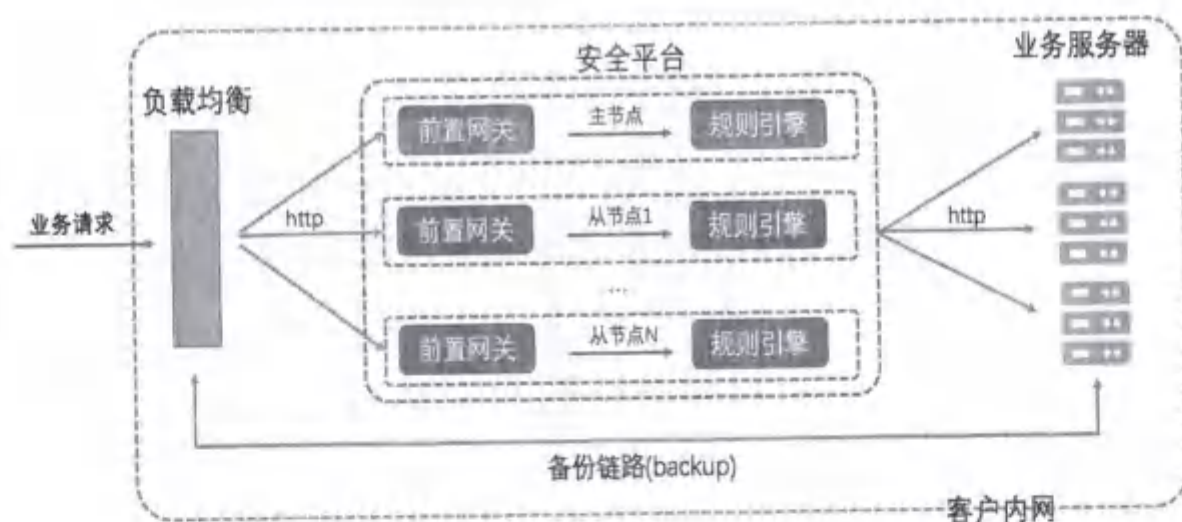


附件 1-3

基于移动应用环境监测技术的安全风险评估与防控服务技术安全性评估报告

一、部署架构安全

系统采用一主多从的集群多活模式运行,使用主节点的 IP 进行日常管理操作。主节点上部署有系统所需的所有组件,并存储有主数据。从节点上只部署前置网关和规则引擎组件,节点运行所依赖的其他信息通过主、从节点间的数据同步来实现。每个节点上最多只能运行一种组件的一个实例,不会出现同一个节点上运行着多个相同组件的情况。主、从节点都参与流量的接受和转发,彼此之间是平级关系,其他组件的离线不会影响到关键组件的请求转发,只会影响安全平台内部一些功能,所以其他组件的离线不会对业务连续性造成影响。通过负载均衡器的链路备份、节点负载、安全平台内部的逻辑 Bypass 等机制来保证安全平台的串联接入不会影响到业务连续性。集群串联架构简易拓扑图如下:



二、数据安全

系统的数据主要来自网络链路中的流量，还有一部分来自客户端 SDK 的采集的数据，传输的方式是将采集到的数据附着在用户的原始请求上报到服务端。安全保障方面，具体如下：

1、客户端 SDK/JS 探针采集数据符合国家 APP 采集个人信息规范，无任何个人隐私数据，具体采集内容见《设备信息采集清单》。

2、客户 SDK 采集的非隐私数据，无主动权限要求，并通过数据使用声明告知用户。

3、服务器端接入流量数据，与路由器，交换机，防火墙等网络设备获取信息相同。

4、接入其他类型数据，均需要与甲方协商对接，系统无强制依赖。

5、数据上报的具体方式是在请求报文的 Header 或 Cookie 中插入设备相关字段，当请求报文到达安全平台时，平台会对其进行自动识别和提取，对业务请求参数没有任何影响。

三、系统安全

本应用严格按照《中华人民共和国个人信息保护法》、GB/T 35273-2020《信息安全技术个人信息安全规范》《移动金融客户端应用软件安全管理规范》（JR/T0092—2019）、《个人金融信息保护技术规范》（JR/T0171—2020）、JR/T 0185—2020《商业银行应用程序接口安全管理规范》、《金融科技创新安全通用规范》（JR/T0199—2020）、《金融科技创新风险防控规范》（JR/T0200—2020）、《基于大数据的支付风险智能防控技术规范》（JR/T0202—2020）、《金融数据安全数据生命周期安全规范》（JR/T0223—2021）、《金融大数据术语》（JR/T0236—2021）、等相关金融行业技术标准规范和要求进行设计开发并进行全面安全评估。经评估，本应用符合现有相关金融行业标准要求。

石嘴山银行股份有限公司信息科技部

2025年4月24日



附件 1-4

基于移动应用环境监测技术的安全风险评估与防控服务风险补偿机制

本应用通过技术手段与流程优化，建立风险补偿机制，确保在安全事件发生时快速响应并降低影响。针对数据安全、动态安全及应用稳定性风险，采用以下措施保障服务连续性 & 用户权益：

1. 针对数据安全风险，开展实时防护，在出现数据泄露时，24 小时内启动应急响应，通过数据脱敏与加密技术恢复系统安全，确保用户数据完整性和服务连续性。另外通过技术溯源，联合第三方安全机构进行漏洞修复，并通过威胁情报更新强化防护策略，防止同类事件再次发生。

2. 针对动态安全风险，实时拦截恶意攻击（如注入、篡改），自动隔离高风险设备或行为，恢复服务正常运行，实现攻击阻断与恢复。同时，对受影响用户推送操作指南，协助其重置密码或调整安全设置，降低二次风险。

通过全流量数据关联分析，实现风险事件的全链路追踪与溯源；建立动态熔断机制，对高危模块或功能快速隔离，防止风险扩散。同时，定期接受第三方安全审计，持续优化

防护策略，确保符合《网络安全法》《数据安全法》等监管要求，实现风险闭环管理。

附件 1-5

基于移动应用环境监测技术的安全风险评估与防控服务退出机制

本应用严格遵循《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》等法律法规要求，结合金融机构移动应用全生命周期管理规范，制定退出机制，确保在终止服务时实现数据安全、系统平稳下线及用户权益保障。

一、退出条件

1. 监管要求触发：因政策调整、监管机构要求或未通过合规性审查需终止服务。
2. 技术缺陷不可修复：经评估，应用存在重大安全隐患或业务功能缺陷且无法有效修复。
3. 业务需求变更：战略调整或市场环境变化导致服务不再必要。

二、退出流程

1. 业务退出

提前通知：提前 30 日通过官方渠道（App 内公告、短信、邮件）通知用户及合作方，明确服务终止时间及后续安排。

协议终止：与用户及合作方签订终止协议，明确数据处理、服务终止后的责任划分及遗留问题处理方式。

服务终止：停止新用户接入，关闭相关功能模块，确保用户原有业务（如数据查询、风险监测）有序退出。

2. 技术退出

数据脱敏与归档：对用户设备、行为、环境等脱敏数据进行归档备份，并删除原始敏感数据。

系统资源回收：关闭移动应用 SDK、后台大数据分析平台及第三方服务接口，清理服务器、数据库资源，确保网络隔离。

流量与日志清理：清除全流量数据关联分析平台中的实时数据，保留合规要求的必要日志以备审计。

系统下线：停止移动端 SDK 数据采集功能，关闭威胁情报分析引擎及实时监测模块。

附件 1-6

基于移动应用环境监测技术的安全风险评估与防控服务应急预案

本预案针对基于移动应用环境监测技术的安全风险评估与防控服务的潜在风险事件，构建“预防-监测-响应-优化”全流程机制，确保业务连续性、用户数据安全及合规运营。依托威胁情报 SDK 与全流量关联分析技术，重点防范数据泄露、恶意攻击及终端环境风险，通过多维度监测、自动化拦截与溯源审计保障系统稳健运行。

一、预防与准备阶段

系统上线前，完成全链路测试及演练，覆盖 SDK 数据采集、服务端流量分析、风险处置等核心环节。针对流量解析还原、终端环境采集等创新技术开展专项验证，确保系统的可靠性。定期组织技术团队开展应急和安全相关培训，模拟实际异常场景，强化实战处置能力。

二、监测与响应机制

建立 7×24 小时生产监控体系，实时捕捉设备环境、用户行为及流量异常。通过威胁情报 SDK 联动数据分析，对恶意攻击、高频异常登录等行为触发动态拦截，并生成全量日志支持溯源审计。针对数据泄露风险，立即启动脱敏隔离机

制，同步触发加密通道关闭非必要数据传输；对终端安全威胁，结合设备指纹与 IP 追踪定位攻击源，自动封禁高风险设备及第三方 SDK 非授权调用。根据事件影响范围实施分级响应，必要时暂停增量业务，优先保障存量业务安全。

三、优化与合规保障

定期复盘应急预案执行效果，迭代威胁情报库与风控模型，优化崩溃采集兼容性测试流程。定期开展对抗演练，验证风险溯源效率及告警通道的冗余可靠性。严格落实《网络安全法》要求，确保用户授权合规性及数据全生命周期安全。预留应急资源池保障高峰时段弹性扩容，形成“技术防御+人工干预+监管协同”的长效风控闭环。