

《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	91450300198879064G-2021-0001	
	创新应用名称	基于人工智能技术的无障碍金融服务	
	创新应用类型	金融服务	
	机构信息	统一社会信用代码	91450300198879064G
		全球法人识别编码	300300B1105H24503003
		机构名称	桂林银行股份有限公司
		持有金融牌照信息	牌照名称：中华人民共和国金融许可证 机构编号：B1105H245030001 发证机关：中国银行保险监督管理委员会广西监管局
	拟正式运营时间	2021 年 07 月 26 日	
	技术应用	1. 运用人物形象建模技术，以银行真实员工形象为基础，模拟其形态、动作、表情等，塑造虚拟“数字人”，在客户业务办理和咨询过程中提供真实的视觉体验。 2. 运用语音合成技术，将采集的银行真实员工数据进行训练和定制模仿，将“数字人”交互信息实时、准确地转换为流畅语音呈现给客户，增加客户在使用过程中的真实感。 3. 运用语音识别技术，将客户语音指令转化为机器可识别数据，提升“数字人”对客户指令的理解能力，提高业务办理效率。 4. 运用语义理解技术，通过对话管理、情绪识别、上下文理解等方式，从客户输入的语言信息中分析和理解出客户意图，为客户提供更加确的指导与建议。	
	功能服务	本项目基于语音识别、语音合成、语义理解等人工智能技术，依托桂林银行手机 APP 打造虚拟“数字人”，提供填单辅助、交易查询、余额查询、资产负债查询、产品咨询、客服答疑等非动账类服务。尤其为老年人等群体提供语音导航、语音辅助等无障碍金融服务，优化服务体验与流程，提高金融产品的易用性与安全性，更好弥合数字鸿沟。 本项目由桂林银行股份有限公司独立研发和运维，此外无第三方机构参与。	
	创新性说明	1. 在客户服务方面，“数字人”能够实现“面对面”、“一对多”服务，可以更快速地定位到客户所需办理的业务并获取相关信息，帮助客户更高效地完成业务办理。	



		2. 在交互真实性方面，完善虚拟“数字人”的形象展示与声音播报，提供更真实、更自然的交互体验。 3. 在语义理解准确性方面，通过自学习机制持续优化语音识别效果，随着人机交互轮次的增加不断提高识别准确率，提升服务质量，为客户提供更贴心的银行服务。 4. 在无障碍服务方面，通过语音导航、语音辅助等方式，降低老年客户等人群获取金融服务的门槛，提高银行服务能力。
	预期效果	节省人工客服投入成本，为客户提供更加贴心、更有温度的金融服务，提高业务办理效率与客户满意度。
	预期规模	按照风险可控原则合理确定用户范围和服务规模，预计涉及客户数 400 万人。
创新应用 服务信息	服务渠道	线上渠道：桂林银行手机银行 APP
	服务时间	7×24 小时
	服务客户	桂林银行客户
	服务协议书	《服务协议书-基于人工智能技术的无障碍金融服务》（见附件 1-1）
合法合规 性评估	评估机构	桂林银行股份有限公司法律合规部
	评估时间	2021 年 06 月 15 日
	有效期限	3 年
	评估结论	本项目严格按照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国消费者权益保护法》、《中国人民银行金融消费者权益保护实施办法》（中国人民银行令〔2020〕第 5 号发布）等相关国家法律法规及金融行业相关政策文件要求进行设计，在数据收集和使用过程中采取措施保护个人金融信息和用户敏感信息安全，所提供金融服务符合相关法律法规要求，可依法合规开展业务应用。
	评估材料	《合法合规性评估报告-基于人工智能技术的无障碍金融服务》（见附件 1-2）
技术安全 性评估	评估机构	桂林银行股份有限公司信息技术部
信息	评估时间	2021 年 06 月 15 日
	有效期限	1 年
	评估结论	本项目严格按照《移动金融基于声纹识别的安全应用技术规范》（JR/T 0164—2018）、《移动金融客户端应用软件安全管理规范》（JR/T 0092-2019）、《网上银行系统信息安全

		通用规范》（JR/T 0068-2020）、《个人金融信息保护技术规范》（JR/T 0171—2020）、《金融科技创新安全通用规范》（JR/T 0199—2020）、《金融业数据能力建设指引》（JR/T 0218—2021）、《人工智能算法金融应用评价规范》（JR/T 0221—2021）等相关金融行业标准规范要求进行设计开发并进行全面安全评估。经评估，本项目符合现有相关金融行业标准规范要求。		
	评估材料	《技术安全性评估报告-基于人工智能技术的无障碍金融服务》（见附件 1-3）		
风险防控	风控措施	1	风险点	在语音识别、声纹识别的过程中，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，严防用户数据泄露、篡改和滥用风险。数据采集时，通过隐私政策文件等方式明示用户数据采集和使用目的、方式以及范围，获取用户授权后方可采集。数据存储时，通过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，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	创新应用线上运营时，可能面临网络攻击、业务连续性中断等方面风险。
			防范措施	在项目实施过程中，平台运行严格按照《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。
		3	风险点	虚拟“数字人”可能会因为语音识别不够精准出现交互偏差，导致客户满意度降低、投诉次数增多。
			防范措施	设立转人工客服机制，在虚拟“数字人”无法解答客户问题的时候及时切换人工，快速响应客户并安抚客户情绪。
	风险补偿机制	本项目按照风险补偿方案（见附件 1-4）建立健全风险补偿机制，明确风险责任认定方式、制定风险赔付机制、配套风险拨备资金、保险计划等补偿措施，切实保障金融消费者合		



		法权益。在金融消费者因使用金融服务而出现资金损失时，由桂林银行按照风险补偿机制进行赔付。对于非客户自身责任导致的资金损失，提供全额补偿，充分保障消费者合法权益。	
	退出机制	本项目按照退出机制（见附件 1-5），在保障用户资金和信息安全的前提下进行系统平稳退出。 在业务方面，按照退出方案终止有关服务，及时告知客户并与客户解除协议。如遇法律纠纷，按照服务协议约定进行仲裁、诉讼。涉及资金的，按照服务协议约定退还客户，对客户造成资金损失的通过风险补偿机制进行赔偿。 在技术方面，对系统进行下线。涉及数据的，按照国家及金融行业相关规范要求做好数据清理、隐私保护等工作。	
	应急预案	本项目按照应急处置预案（见附件 1-6）妥善处理突发安全事件，切实保障业务稳定运行和用户合法权益。在系统上线前进行全链路压测、容灾演练，对相关操作人员进行应急处置培训；在系统上线后定期开展突发事件处置演练，确保应急预案的全面性、合理性和可操作性。建立日常生产运行监控机制，7×24 小时实时监控运行状况，第一时间对核心链路、接口、功能模块、硬件资源等的异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取有针对性措施进行分级分类处理，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。	
投诉响应机制	机构投诉	投诉渠道	1. 营业网点：向桂林银行股份有限公司各营业网点大堂经理、网点负责人反映问题。 2. 投诉电话：致电客户服务热线（96299）。
		投诉受理与处理机制	接到投诉事件后，桂林银行股份有限公司负责对事件进行了解和分析，在确认投诉原因和相关问题后，协调相关技术部门或业务部门进行解决，并及时将处理进度反馈投诉人员。
	自律投诉	投诉渠道	受理单位：中国支付清算协会 投诉网站：http://cfp.pcac.org.cn/ 投诉电话：010-66001918 投诉邮箱：fintechts@pcac.org.cn
		投诉受理与处理机制	中国支付清算协会是经国务院同意、民政部批准成立的全国性非营利社会团

			体法人。为保护金融消费者合法权益，营造遵守国家宪法、法律、法规和社会道德风尚的良好金融科技创新监管环境，推动金融科技行业健康可持续发展，按金融管理部门工作要求，协会以调解的形式，独立公正地受理、调查以及处理金融科技创新监管工具实施中出现的投诉举报等相关事宜。 对于涉及相关地区的金融科技创新应用项目的投诉举报事项，中国支付清算协会将依照规定的程序进行调解，由协会举报中心对投诉情况进行沟通、记录后，相关业务部门负责进行调查处理。 联系方式：010-66001918 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，严格遵守相关金融管理要求，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“负责任的创新”，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） 2021 年 6 月 23 日（盖章）

附件 1-1

基于人工智能技术的无障碍金融服务
服务协议书

仅供样式参考，填写内容无效

桂林银行股份有限公司电子银行隐私政策

尊敬的桂林银行电子银行用户（以下简称您），桂林银行股份有限公司（以下简称我行）深知个人信息对您的重要性，我行一直致力于维护您对我行的信任，恪守以下原则保护您的个人信息：权责一致原则、目的明确原则、选择同意原则、必要性原则、确保安全原则、公开透明原则等。我行将按照《桂林银行股份有限公司电子银行隐私政策》（以下简称本政策）收集、存储、使用及对外提供您的个人信息。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、可控的情况下进行传输、存储，我行制定了本政策，请您仔细阅读本政策并确定了解我行对您个人信息的处理规则。

本政策将帮助您了解以下内容：

1. 我行如何收集和使用您的个人信息
2. 我行如何使用 Cookie 和同类技术
3. 我行如何共享、转让和公开披露您的个人信息
4. 我行如何存储和保护您的个人信息
5. 您如何管理您的个人信息
6. 我们如何处理未成年人信息
7. 本政策如何更新
8. 如何联系我行

我行强烈建议您在使用/继续使用我行的电子银行服务前，仔细阅读并完全理解本政策中的全部内容，并自主进行适当的选择。对本政策中与您的权益存在重大关系的条款，我行采用粗体字进行标注以提示您注意。如果您不同意本政策的内容，我行将无法为您提供完整的产品和服务，同时您也需要立即停止使用相关的金融服务。您一旦点击“同意”并开始使用我行的产品或服务，则视为您已经充分、完全地阅读并理解了本政策中的全部内容，并且同意我行按照本政策的规定收集、使用、存储及对外提供您的个人信息。

本政策仅适用于我行电子渠道的金融产品或服务，包括手机银行、桂银直销、小能人生活服务平台、微信银行、网上银行、我行官方网站、桂银商户通等。

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者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映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、身份证件号码、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、位置信息等。其中一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的信息为个人敏感信息，主要包括：身份证件号码、个人生物识别信息、银行账号、征信信息、财产信息、交易信息、位置信息、健康生理信息等。

（一）信息如何收集

为向您提供服务并确保您的电子银行服务（手机银行、桂银直销、小能人生活服务平台、微信银行、网上银行、我行官方网站、桂银商户通等服务，下同）安全，在您使用电子银行服务过程中，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. 当您开通电子银行服务时，依据法律法规及监管要求，我行会收集您的个人基本资料、身份信息、财产信息、通信信息、生物识别信息、手机号码信息，以帮助您完成电子银行注册，如果您拒绝提供这些信息，您可能无法开通电子银行或无法正常使用我行电子银行服务。

2. 当您使用电子银行功能或服务时，例如在下列情形中，您可能需要向我行提供或授权我行收集相应服务所需的用户信息。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我行电子银行的其他功能或服务。

（1）在您注册成为我行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/语音验证码或人脸识别的方式来验证您的身份是否有效。根据相关法律法规的规定，您需通过身份基本信息多重交叉验证，需提供更多信息（例如：姓名、证件号码、银行卡号/账号、手机号码等）以完成身份基本信息多重交叉验证。如您拒绝提供上述信息，您将无法使用我行电子银行服务。

（2）当使用转账汇款功能时，您需要提供收款方的姓名、银行账号/手机号、开户银行等收款方信息，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、短信验证码等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。上述信息属于个人敏感信息，如您拒绝提供该信息，仅会使您无法使用上述功能，但不影响您正常使用我行电子银行的其他功能或服务。

（3）如您在使用我行电子银行服务时选择通过指纹、手势密码、人脸识别进行登陆、支付、身份认证，需向我行提供您的指纹、手势密码、人脸图像信息。您可以通过手机银行“安全中心”或者直销银行“登录方式”开启或关闭此功能。我行不会采集您的指纹，您的指纹仅保存在您授权采集指纹设备上。我行征得您的明示同意后采集人脸信息，将加密存储于我行信息系统后台数据库中。如您不提供上述信息，我行将无法向您提供需完成指纹、手势密码、人脸认证后方可使用的产品或服务。

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中的信息。

（4）当您使用我行电子银行提供的实名认证服务时，您可能需提供您的姓名、证件类型、证件号码、银行卡号/账号、设备信息、人脸认证信息，我行还可能通过验证账号/卡密码、短信/语音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。

（5）当您在我行电子银行申请开通一户通账户时，我行需要您提供您的姓名、身份证号、身份证有效期、手机号码、绑定银行卡号，以便验证您的身份的真实性，如您不提供上述信息，我行将无法向您提供该产品或服务。

(6) 当您使用我行电子银行提供的搜索服务时，我行会收集您的搜索关键词信息。当搜索关键词信息无法单独识别您的个人身份时，该信息不属于您的用户信息，我行可以对其加以其他目的使用；当搜索关键词信息与您的其他信息结合可以识别您的个人身份时，我行将在结合期间将您的搜索关键词信息作为您的用户信息，对其加以保护处理。

(7) 当您使用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我行电子银行的其他功能或服务。

(8) 在向您提供手机银行、桂银直销等电子银行服务的过程中，我行还可能使用第三方服务商提供的软件开发工作包（简称“SDK”）来为您提供服务，由第三方服务商收集您的必要信息，如您拒绝提供相关信息或权限，您将无法使用相关功能服务。具体包括：

1) 百度定位 SDK。为了向您提供基于位置的服务，我们使用了百度定位 SDK，该 SDK 需要获取您的手机终端唯一标志信息（IMEI 号）、经纬度信息，用于实现定位功能。

2) 云从 SDK。为了向您提供人脸识别服务，我们使用了云从 SDK，该 SDK 需要获取您的人脸信息，用于实现人脸识别功能。

3) 爱加密 SDK。为了向您提供安全的 App 服务，我们使用了爱加密 SDK，用于防止安卓 App 被破解、反编译、二次打包等威胁。

4) 微信 SDK。为了向您提供微信分享、微信联合登录、微信支付服务，我们使用了微信 SDK、用于实现微信分享、登录、支付。

5) 云证通（中国金融认证中心 CFCA）SDK。为了向您提供云证通电子签名服务，我们使用了云证通（中国金融认证中心 CFCA）SDK，该 SDK 需要获取您的手机终端唯一标志信息（IMEI 号）、MAC 地址，用于实现电子签名功能。

6) 图睿 OCR 识别 SDK：为了向您提供基于图片自动识别服务，我们设备 OCR 设备 SDK 用于界面使用摄像头扫描身份证、银行卡号，实现自动输入功能输入。

7) 微通新成密码键盘 SDK：为了向您提供安全的密码输入方式。我们使用密码键盘 SDK，用于防止木马程序、恶意代码、HOOK、录截屏软件等窃取用户私密数据。

8) 邦盛设备指纹 SDK：为了向您保障登录账号的安全，我们使用设备指纹 SDK，用于获取您的设备 ID 相关信息确定您的账号登录设备的唯一性，该 SDK 需要获取您的手机终端唯一标志信息（IMEI 号/IDFV 号）已确保账号登录设备的唯一性。

9) 平安文字识别 SDK：为了向您提供文字识别(OCR)服务，我行使用了平安文字识别 SDK，需要获取您的身份证图片、存储权限、摄像头权限，用于进行身份证文字识别。

10) 极光推送 SDK：为了向您提供订单状态跟踪等服务，我行使用了极光推送 SDK，需获取通知权限，用于订单状态等信息推送。

11) Mob 一键分享 SDK：为了向您提供快捷分享至社交媒体服务，我行使用了 Mob 一键分享 SDK，无需特殊权限，用于进行社交媒体分享。

(9) 当您使用微信银行服务时，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；我行可能会在经您明示同意后

向我行的合作伙伴提供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和提醒服务。如您不提供上述信息，我行将无法向您提供该产品或服务。

(10) 当您使用信贷服务时，需要向我行提供您的银行账户名称、银行卡号/账号、支付密码、手机号码、家庭住址、收入情况等信息，同时授权我行向依法设立的征信机构及其他合法机构使用、查询、收集您的信息，具体见您与我行在信贷业务中另行签署的授权书。如您不提供上述信息，我行将无法向您提供该产品或服务。

(11) 当您通过我行购买银行发行的理财产品、银行代理销售的其他金融产品或在桂银直销购买直销银行产品时，需要向我行提供姓名、付款账户名称及账号、收款账户名称及账号、联系电话、联系地址、邮编、风险评测等信息。如您不提供上述信息，我行将无法向您提供该产品或服务。

(12) 当您使用我行电子银行服务时，如您选择手机短信验证码认证工具，我行将向您的签约手机号发送手机短信验证码，用以进行电子银行服务交易验证。

(13) 当您使用我行电子银行渠道的水电缴费、话费充值、物业缴费、交通罚款、社保缴费等服务时，我行可能会根据不同的缴费类型收集您的银行账户信息、账户余额、缴费编号、缴费金额、交易时间等必要的缴费信息，上述信息属于个人信息，如您拒绝提供该信息，仅会使您无法使用上述功能，但不影响您使用其他功能或服务。

(14) 当您使用我行电子银行渠道的信用卡申请进度查询、信用卡激活、信用卡还款、账单查询、账单分期等信用卡服务时，根据不同的业务类型可能需要您提供您的信用卡卡号、证件类型、证件号码、CVV2、有效期、卡片密码、预留手机号、还款方式、还款账户等信息，如您拒绝提供上述信息，我行可能无法向您提供相应的服务。

(15) 当您在我行电子银行进行电子账户开户时，依据法律法规及监管要求，我行会收集您的个人基本资料、身份信息、银行卡信息、通信信息、手机号码信息，以帮助您完成直销银行注册及电子账户开户，如果您拒绝提供这些信息，您可能无法开通电子账户或无法正常使用我行的直销银行的功能或服务。

(16) 当您使用小能人生活服务平台时，您可以通过搜索来精准地找到您所需要的商品或服务。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。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识别您的身份时，则在结合使用期间，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。

(17) 当您在电子银行中使用第三方提供的服务时，第三方可能会获取您的昵称、头像、位置、姓名、证件类型、证件号码、手机号码信息；在经过您的明示同意后，第三方可获取您的以上信息；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电子银行中使用第三方的相应服务，但这不影响您使用电子银行的其他功能或服务。

3. 当您使用我行电子银行时，为了维护服务的正常运行，预防交易和资金风险，我行会收集以下基础信息，包括您的设备型号、操作系统、唯一设备标识符、软件版本号、登陆 IP 地址、接入网络的方式、类型和状态、网络质量数据、操作日志、服务日志信息（如您在手机银行搜索、查看的信息、服务故障信息）、地理位置信息，这些信息是为您提供服务必须收集的基础信息，以保障您正常使用我行的服务。

4. 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，我行会收集您反馈的意见、建议或举报时提供的信息，收集您使用电子银行功能或服务的类别、方式和操作信息，及您在我行的用户信息，我行会对这些信息进行统计、分析，并会根据上述信息向您提供相应服务或产品。

5. 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：

（1）摄像头，用于如识别二维码、人脸识别、设置头像，在人脸识别登录/转账/支付/实名认证、扫一扫、头像设置、电子账户开通场景中使用。拒绝授权后，上述功能将无法使用。我行将获取的人脸等数据，加密后存储于系统后台数据库中。

（2）麦克风，用于业务录音、电话银行客服等用途，拒绝授权后，上述功能将无法使用。我行采集的语音数据，加密后存储于系统后台数据库中。

（3）手机通讯录，在转账、支付、话费流量充值过程中，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，向手机号转账、汇款短信通知、话费流量功能仍可以使用，但需要手工输入手机号码。电子银行仅读取并记录指定电话号码，不读取客户全量通讯录。

（4）手机短信，在需要短信验证码的环节可能需要读取验证码短信内容协助您进行验证码填写。如您拒绝通讯信息（短信）授权，我行手机银行将不读取短信内容，系统后台不保存短信内容。

（5）地理位置，获取您所在地理位置，主要用于电子银行交易风控、网点查询等。系统后台保存您交易时的位置信息。拒绝授权后，电子银行相关功能无法使用。

（6）网络通讯，用于与服务端进行通讯。拒绝授权后，手机银行所有功能无法使用。系统后台保存客户交易时所使用设备的网络信息，包括 IP、端口等信息。

如在上述情形之外收集或使用您的信息，我们会事先征求您的同意，并向您充分告知信息收集和使用的目的、方式和范围。

6. 我行在向您提供新增的其他业务功能时，会另行向您说明信息收集的范围与目的，并征求您的同意后方收集提供相应服务所必要的您的信息。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，如您拒绝提供该信息，您将可能无法使用新增的业务功能，但这不影响您正常使用我行电子银行的原业务功能或服务。

（二）信息如何使用

1. 在向您提供我行的金融产品或服务，并为改进这些产品或服务时使用。
2. 在我行向您提供金融服务期间，您授权我行持续收集和使用您的信息。在您注销服务时，我们将停止收集您相关的个人信息，但我行会在业务资料归档、审计、监管协查等领域继续使用此前收集的您的相关个人信息。
3. 为提升您的产品或服务体验，或为防范风险，我行会对服务使用情况进行汇总、统计分析、加工，但这些信息不会包含您的任何身份识别信息。
4. 为了使您知悉使用我行金融产品或服务的情况或使您进一步了解我行服务，我行会向您发送服务状态通知以及相关产品或服务的商业性信息。
5. 您授权同意的以及于法律允许的其它用途。

（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，以下情形中，我行可能会收集、使用您的相关个人信息而无需另行征求您的授权同意：

1. 与国家安全、国防安全直接相关的；
2. 与公共安全、公共卫生、重大公共利益直接相关的；
3. 与犯罪侦查、起诉、审判和判决执行等直接相关的；
4. 与履行国家法律法规及行业主管部门有关规定的义务相关的；
5. 出于维护您或其他个人的生命、财产等重大合法权益但又很难得到您本人同意的；
6. 所收集的个人信息是您自行向社会公众公开的；
7. 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；
8. 根据您要求签订和履行合同所必需的；
9. 用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障；
10. 为开展合法的新闻报道所必需的；
11. 出于公共利益开展统计或学术研究所必需，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；
12. 法律法规及监管要求规定的其它情形。

二、我行如何使用 Cookie 和同类技术

（一）Cookie

为确保网站正常运转，我行会在您的计算机或移动设备上存储名为 Cookie 的小数据文件。通常包含标识符、站点名称以及一些号码和字符。借助于 Cookie，网站能够存储您的偏好或购物车内的商品等数据。我行不会将 Cookie 用于本政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。您可以清除计算机上保存的所有 Cookie，部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要在每一次访问我行的网站时更改用户设置。

（二）Do Not Track（请勿追踪）

很多网络浏览器均设有 Do Not Track 功能，该功能可向网站发布 Do Not Track 请求。目前，主要互联网标准组织尚未设立相关政策来规定网站应如何

应对此类请求。但如果您的浏览器启用了 Do Not Track，那么我行的所有网站都会尊重您的选择。

三、我行如何共享、转让和公开披露您的个人信息

（一）共享和转让

1. 除非获得您的明确同意或授权，我行不会向其他任何公司、组织和个人共享或转让您的个人信息。

2. 如业务需要对外共享或转让您的个人信息，我们会向您告知共享或转让个人信息的目的、数据接收方的类型，并征得您的授权同意。涉及敏感信息的，我们还会告知敏感信息的类型、数据接收方的身份和数据安全能力，并征得您的明示授权同意。

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. 根据法律法规和商业惯例，在合并、收购、资产转让等类似交易中，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，否则我行将要求该公司、组织重新向您征求授权同意。

（二）公开披露

1. 我行不会公开披露您的个人信息，如确需披露，我行会告知您披露个人信息的目的、类型；涉及敏感信息的还会告知敏感信息的内容，并事先征得您的明示同意。

2. 请您理解，在法律、法律程序、诉讼或政府主管部门强制性要求的情况下，我们可能会公开披露您的个人信息。

（三）征得授权同意的例外

根据相关法律法规及监管要求、国家标准，以下情形中，我行可能会共享、转让、公开披露用户信息无需事先征得您授权同意：

1. 与国家安全、国防安全直接相关的；
2. 与公共安全、公共卫生、重大公共利益直接相关的；
3. 与犯罪侦查、起诉、审判和判决执行等直接相关的；
4. 与履行国家法律法规及行业主管部门有关规定的义务相关的；
5. 出于维护您或其他个人的生命、财产、声誉等重大合法权益但又很难得到本人同意的；
6. 您自行向社会公众公开的个人信息；
7. 从合法公开披露的信息中收集的用户信息，如合法的新闻报道、政府信息公开等渠道。

四、我行如何存储和保护您的个人信息

（一）存储

1. 我行在中华人民共和国境内收集和产生的个人信息，将存储在中华人民共和国境内。但为处理跨境业务并在获得您的授权同意后，您的个人信息可能会被转移到境外。此种情况下，我行会采取有效措施保护您的信息安全，例如，在跨境数据转移之前实施数据去标识化等安全措施，或通过协议、核查等措施要求境外机构为您的信息保密。

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时限内保留您的个人信息。例如：

手机号码：当您需要使用电子银行服务时，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，当您注销电子银行账户后，我行将删除相应的信息；

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。当您选择恢复默认为头像后，我行将删除您设置的头像信息。

（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，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，确保只有授权人员才可访问个人信息；以及我行会举办安全和隐私保护培训课程，加强员工对于保护个人信息重要性的认识。

2. 如我行提供的全部或部分电子银行业务停止运营，我行相关产品或服务将通过公告等形式向您进行告知，同时停止相关产品或服务对您个人信息的收集等操作，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、人为因素等各种原因造成全部或部分电子银行业务中断，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等级保护的测评和备案，在信息安全方面数据中心已达到国家 A 级认证标准的要求，并获得相应的认证。

4. 我们会采取一切合理可行的措施，确保未收集无关的个人信息。

5. 请您理解，由于技术水平局限以及可能存在的恶意攻击，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号安全。

6. 如发生个人信息安全事件，我行将按照法律法规的要求，及时将事件相关情况以邮件、信函、电话、推送通知等方式告知您，或采取合理、有效的方式发布公告。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、更正及更新您的个人信息

您有权通过我行电子银行渠道访问及更正、更新您的个人信息，法律法规另有规定的除外。您有责任及时更新您的个人信息。在您修改个人信息之前，我们会验证您的身份。

1. 您登录手机银行后，可以在“我的-安全中心-证件更新”中，查询姓名、证件类型、证件号码、家庭地址、职业等信息；在证件信息维护中，可以修改职业、家庭地址。可在“账户管理”功能中管理绑定的银行卡、II类户、III类户、其他账户服务。可在“安全中心”进行云证通服务开通、关闭、限额修改，管理设备绑定、修改登录密码、指纹登录设置、人脸登录设置、手势密码设置。

2. 您登录网上银行后，可以在“客户服务-个人资料修改”中，查询姓名、证件类型、证件号码、家庭地址等信息；可以修改邮箱、家庭地址。可在“账户管理”功能中管理绑定的银行卡、II类户、III类户、其他账户服务。可在“安全中心”进行证书更新，管理设备绑定、修改登录密码、USBkey 密码设置。

3. 您登录直销银行后，可以在“设置-电子账户信息”及“设置-头像”中，查看个人姓名、证件类型、证件号码、电子账号、开户行、开户时间、身份证有效期等信息，可以进行收货地址新增、修改及删除。可以进行登录手机号修改、登录方式修改等操作。

（二）删除您的个人信息

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，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. 如果你不再使用我们的产品或服务，或您注销了账号；
5. 如果我们不再为您提供产品或服务。

如我行决定响应您的删除请求，还将同时通知从我行获得您的个人信息的实体，要求其及时删除，除非法律法规另有规定，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，但法律法规另有规定或应有权机关要求的除外。

（三）改变您授权同意的范围

每个业务功能需要一些基本的个人信息才能得以完成。对于额外收集的个人信息的收集和使用，您可以根据手机的不同品牌和型号，通过开通或关闭位置服务权限、读取联系人权限、拨打电话权限等，随时给予或收回您的授权同意。

请您注意，您自主注销我行电子银行服务的同时，将视同您撤回了对我行该政策的同意。当您收回同意后，我们将不再处理相应的个人信息。但您收回同意的决定，不会影响此前基于您的授权而开展的个人信息处理。

（四）个人信息主体注销账户

1. 如您为我行电子银行注册用户，您可以到网点通过我行柜面或智能柜台等渠道注销您的电子银行。

2. 如注销手机银行，您可下载我行手机银行客户端，启动客户端，进入“我的-安全中心-自助注册销户”输入登录密码和短信验证码，验证通过后即可注销手机银行。

3. 如取消关注微信银行，在“桂林银行”微信公众号详情页面点击“不再关注”按钮，即可取消“桂林银行”微信公众号的关注。

4. 如注销短信服务，您可通过多种方式注销短信金融服务，包括、手机银行、微信银行和银行网点。

如您非我行电子银行注册用户，您可以自主选择卸载或停止使用手机银行、桂银直销、小能人生活服务平台客户端、网上银行、我行官方网站，以阻止我们获取您的个人信息。您注销电子银行的行为是不可逆行为，一旦您注销您的

电子银行，我们将不再收集您的个人信息，并删除有关您电子银行的一切信息，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。

（五）约束信息系统自动决策

在某些业务功能中，我行可能仅依据信息系统、算法等在内的非人工自动决策机制做出决定。如果这些决定显著影响您的合法权益，您有权要求我行做出解释，我行也将提供适当的救济方式。

（六）响应您的上述请求

为保障安全，您可能需要提供书面请求，或以其他方式证明您的身份。我行可能会先要求您验证自己的身份，然后再处理您的请求。请您理解，对于某些无端重复、需要过多技术手段、给他人合法权益带来风险或者非常不切实际的请求，我行可能会予以拒绝。

尽管有上述约定，但按照法律法规要求，如涉及以下情形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、审判和判决执行等相关的；
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. 涉及我行商业秘密的。

六、我行如何处理未成年人信息

如果没有监护人的同意，未成年人不得创建自己的用户账户。如您为未成年人，请您的监护人仔细阅读本指引，并在征得您的监护人同意的前提下使用我行的服务或向我行提供信息。我行只会在法律法规及监管要求允许或者保护未成年人所必要的情况下使用、对外提供此信息。

七、本政策如何更新

根据国家法律法规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（<https://www.guilinbank.com.cn/>）、手机银行、桂银直销、小能人生活服务平台、微信公众号等渠道公布，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、规则等相关内容的变动。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。

八、如何联系我行

如您对本隐私政策有任何意见或建议以及对您的个人信息的安全存在疑问，可以通过拨打我行客服热线 96299（广西）、400-86-96299（全国），关注“桂林银行”微信公众号或到我行各营业网点反映或投诉。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 15 个工作日内给予答复。

版本号：1.2
版本发布时间：2020 年 12 月 10 日

仅供样式参考，填写内容无效

附件 1-2

基于人工智能技术的无障碍金融服务 合法合规性评估报告

本项目严格按照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国消费者权益保护法》、《中国人民银行金融消费者权益保护实施办法》（中国人民银行令〔2020〕第5号发布）等相关国家法律法规及金融行相关政策文件要求进行设计，在数据收集和使用过程中采取措施保护个人金融信息和用户敏感信息安全，所提供金融服务符合相关法律法规要求，可依法合规开展业务应用。

桂林银行股份有限公司法律合规部

2021年06月15日

附件 1-3

基于人工智能技术的无障碍金融服务 技术安全性评估报告

本项目严格按照《移动金融基于声纹识别的安全应用技术规范》(JR/T 0164—2018)、《移动金融客户端应用软件安全管理规范》(JR/T 0092—2019)、《网上银行系统信息安全通用规范》(JR/T 0068—2020)、《个人金融信息保护技术规范》(JR/T 0171—2020)、《金融科技创新安全通用规范》(JR/T 0199—2020)、《金融业数据能力建设指引》(JR/T 0218—2021)、《人工智能算法金融应用评价规范》(JR/T 0221—2021)等相关金融行业标准规范要求设计开发并进行全面安全评估。经评估,本项目符合现有相关金融行业标准规范要求。

桂林银行股份有限公司信息技术部

2021 年 06 月 15 日

附件 1-4

基于人工智能技术的无障碍金融服务 风险补偿机制

本项目由桂林银行股份有限公司建立健全风险补偿机制，明确风险责任认定方式、制定风险赔付机制、配套风险拨备资金、保险计划等补偿措施，切实保障金融消费者合法权益。在金融消费者因使用金融服务而出现资金损失时，由桂林银行按照风险补偿机制进行赔付。对于非客户自身责任导致的资金损失，提供全额补偿，充分保障消费者合法权益。

仅供样式参考，

附件 1-5

基于人工智能技术的无障碍金融服务 退出机制

本项目由桂林银行股份有限公司制定退出机制，在保障用户资金和信息安全的前提下进行系统平稳退出。

在业务方面，按照退出方案终止有关服务，及时告知客户并与客户解除协议。如遇法律纠纷，按照服务协议约定进行仲裁、诉讼。涉及资金的，按照服务协议约定退还客户，对客户造成资金损失的通过风险补偿机制进行赔偿。

在技术方面，对系统进行下线，涉及数据的，按照国家及金融行业相关规范要求做好数据清理、隐私保护等工作。

仅供样式参考，

基于人工智能技术的无障碍金融服务 应急预案

本项目由桂林银行股份有限公司按照应急预案妥善处理突发安全事件，切实保障业务稳定运行和用户合法权益。在系统上线前进行全链路压测、容灾演练，对相关操作人员进行应急处置培训；在系统上线后定期开展突发事件处置演练，确保应急预案的全面性、合理性和可操作性。建立日常生产运行监控机制，7×24小时实时监控系统运行状况，第一时间对核心链路、接口、功能模块、硬件资源等的异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取有针对性措施进行分级分类处理，视需要及时关闭增量业务，妥善处理受影响的存量业务，切实保障用户资金和信息安全。

具体应急预案如下：

一、应急预案总体目标

总体目标是通过制定和实施应急预案，当桂林银行股份有限公司信息系统发生突发事件时，可以实现应急处置领导小组快速响应、及时报告和高效处置。

二、资源保护策略

1、机房环境

架构策略：关键的环境资源，如UPS、空调等，双机冗余备份。

容量策略：机房承重、空调制冷、UPS容量。

备件策略：厂商7 X 24 X 2小时备件库。

2、网络资源

架构策略：关键网络设备实现双机热备，关键板卡实现双卡热备，关键互联端口实现端口级冗余。

容量策略：带宽容量。

备件策略：厂商7 X 24 X 2小时备件库。

3、系统资源

架构策略：小型机系统资源都实现HA双机热备，PC Server采用集群备份方式，存储、数据。

容量策略：系统容量、存储容量。

备件策略：厂商7 X 24 X 2小时备件库。

4、人力资源

(1) 操作员2名7 X 24小时现场值班。

(2) 负责人、部门经理、关键岗位员工7 X 24小时非现场电话值班。

5、服务资源

产品服务商服务等级为7 X 24小时响应，2小时内现场服务。重要信息系统和特色信息系统备件全部本地保存。

三、应急预案案例

1、路由器故障

处置步骤：

(1) 故障信息收集，若设备可登录，登录设备收集故障信息，确认故障点，判断需要更换的网络设备或配件。

(2) 备份设备替换，断开故障设备网络连接，使备份设备接管业务。

(3) 网络及业务验证，验证设备网络连通性和应用服务是否正常。

(4) 清除应急处置配置，恢复修复后设备网络连接。

2、数据库服务器异常

场景名称	数据库服务异常	场景关键字	数据库故障
故障系统和设备	数据库服务器	受影响系统	
场景简描述	应用连接数据库服务器异常，数据库无法正常服务。		
处置步骤： (1) 优先利用 HA 在备机恢复数据库服务，HA 自动检测切换数据库服务至备机运行，检查备机状态； (2) 通知恢复应用，监控应用运行情况； (3) 通知设备维护厂商现场支持； (4) 更换故障硬件； (5) 启动主机； (6) 检查更换设备后主机的卷组、文件系统和逻辑卷状态，确保主机就绪； (7) 将数据库服务从备机切换回主机（选择业务影响最小的时间）； (8) 检查回切后的主、备机的 HA、卷组、文件系统、数据库及应用状态； (9) 通知恢复应用，监控应用运行情况。			

3、应用服务器异常

场景名称	应用服务器服务异常	场景关键字	应用服务器请求过多
故障系统和设备		受影响信息系统	

场景简描述	特殊时期或特定事件导致的某一时段内系，统吞吐量大幅增加，超过系统设定压力至场景简要描述，停止响应等情况。
处置步骤： (1) netstat -an 检查平台相关端口运行是否正常，查看日志找出交易量突然增大的应用来源。 (2) 如有应用交易量突然增大，可通过修改程序或数据库配置等方式暂时限制该应用接入的交易数量。 (3) 如集群中有服务引擎运行不正常，则用脚本命令重启有关服务。 (4) 查看平台到关联 MongoDB 数据库连接是否正常，如不正常则通知系统科处理。	

四、应急演练机制

在项目上线前进行压力测试和容灾演练，并对相关人员进行培训。上线后定期开展突发事件处置演练，确保应急预案的全面性、合理性和可操作性。建立日常生产运行监控机制，7×24小时实时监控系统运行状况，对异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取有针对性措施进行分级分类处理，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。