

《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	91460000348086474N-2021-0001	
	创新应用名称	基于人工智能技术的风险交易预警服务	
	创新应用类型	金融服务	
	机构信息	统一社会信用代码	91460000348086474N
		全球法人识别编码	300300C1309246000041
		机构名称	海南银行股份有限公司
		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：B0729H246010001 发证机关：中国银行业监督管理委员会 海南监管局
	拟正式运营时间	2022 年 01 月 15 日	
	技术应用	1. 运用大数据技术，在客户授权的前提下，海南银行对客户历史交易信息和来源合法合规的涉案人员信息、司法涉诉信息、电信网络诈骗黑名单等数据进行清洗处理，分析挖掘风险交易特征，为识别可疑交易及潜在电信诈骗风险客户提供多维度数据支撑。 2. 采用机器学习等人工智能技术，通过对银行客户历史交易信息和涉案人员信息等数据进行特征学习和样本训练，构建风险交易监测模型，对客户的消费、提现等交易行为进行实时监测，辅助海南银行识别电信网络诈骗行为，提升电信网络诈骗等交易欺诈风险的识别效率。 3. 采用流式计算技术，对交易产生的信息实时进行分析处理，及时甄别、发现潜在风险交易，提高风险交易预警的时效性。	
	功能服务	本项目运用大数据、人工智能等技术构建风险交易监测模型，辅助海南银行识别电信网络诈骗等交易欺诈行为。对识别为存在风险的交易，海南银行进行分级分类处理：涉嫌电信网络诈骗的，在充分保护个人隐私的前提下通过短信、电话等方式向客户进行及时预警；风险较高的，在人工确认核实基础上，依法向公安机关进行举报。 本项目由海南银行股份有限公司负责系统研发、运维并提供金融应用场景，此外无其他第三方机构参与。	
创新性说明	1. 数据应用方面，在海南银行行内数据基础上，引入行外电信网络诈骗黑名单、司法涉诉等数据，丰富银行对风险交易的评价维度。		

		2. 数据处理效率方面，运用流式计算技术提升银行对海量数据的分析与并发处理能力，有效缩短数据分析处理时间。 3. 风险识别能力方面，通过风险交易监测模型实时识别交易风险，较以往全人工进行风险分析的工作方式，提高银行风险交易识别的效率和准确性。
	预期效果	提升海南银行的风险交易识别能力，充分保障客户资金安全。
	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，预计服务海南银行客户约 100 万户。
创新应用 服务信息	服务渠道	线上渠道：通过 PC 端和移动端 App 提供服务 线下渠道：银行网点
	服务时间	线上渠道：7×24 小时 线下渠道：9:00 至 17:00（工作日）
	服务用户	海南银行客户
	服务协议书	《服务协议书-基于人工智能技术的风险交易预警服务》 （见附件 1-1）
合法合规 性评估	评估机构	海南银行股份有限公司法律合规部
	评估时间	2021 年 11 月 04 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》、《中华人民共和国反洗钱法》、《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》、《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）、《金融机构大额交易和可疑交易报告管理办法》（中国人民银行令（2016）第 3 号发布）、《中国人民银行关于落实个人银行账户分类管理制度的通知》（银发〔2016〕302 号）、《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号）、《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2019〕85 号）、《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》（中国人民银行、银监会、证监会、保监会令〔2007〕第 2 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，可依法合规地开展业务应用。

	评估材料	《合法合规性评估报告-基于人工智能技术的风险交易预警服务》（见附件 1-2）		
技术安全性评估	评估机构	海南银行股份有限公司信息科技部		
	评估时间	2021 年 11 月 04 日		
	有效期限	1 年		
	评估结论	本项目严格按照《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）、《基于大数据的支付风险智能防控技术规范》（JR/T 0202—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）等相关金融行业技术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行业标准要求。		
	评估材料	《技术安全性评估报告-基于人工智能技术的风险交易预警服务》（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，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，借助标记化等技术，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	创新应用上线运行后，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	在项目实施过程中，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

			施	行，保护金融消费者合法权益。
			风险点	本项目风险交易监测模型可能因数据质量问题或其他突发情况导致模型效果产生偏差。
		3	防范措施	一是加强人工监控，设置模型管理专岗，建立模型监控预警机制。依托自动监控预警程序，实时发现数据及模型异常指标，并通知工作人员进行人工干预，及时进行模型迭代，避免模型准确性问题影响风险识别效果。二是对客户可能造成的影响做好解释工作，有效保障客户合法权益的前提下，完成风险交易的核查处置。
	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，由金融场景提供方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. 客服电话 致电海南银行全国客户服务热线	

			(0898-96566)，选择人工服务联系客服代表。 2. 在线客服 通过海南银行手机银行和网上银行等渠道，选择“在线交谈”或“即时留言”，随时与银行客户服务代表进行在线沟通。 3. 微信公众号 关注“海南银行”微信公众号，以文字、图片、语音等形式发送投诉内容。 4. 营业网点 向海南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。
		投诉受理与处理机制	受理部门：海南银行营运管理部 受理时间：接到投诉后的 24 小时内 受理流程：海南银行营运管理部受理投诉后，开展调查工作，并联合相关业务、技术等部门进行投诉处理，并与客户联系沟通处理进展和结果。 受理时限：5 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项目的争议、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，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12月28日（盖章）



附件 1-1

基于人工智能技术的风险交易预警服务 服务协议书



本项目服务协议书包括《海南电子银行服务协议》《海南银行股份有限公司隐私政策》，具体内容如下：

海南电子银行服务协议

为明确双方的权利和义务，规范双方业务行为，改善客户服务，本着平等互利的原则，电子银行个人客户服务申请人（以下简称“甲方”）与海南银行股份有限公司（以下简称“乙方”）就海南银行电子银行服务的相关事宜达成本协议，协议双方应予遵守。

第一条 定义

如无特别说明，下列用语在本协议中的含义为：

电子银行：指乙方通过面向社会公众开放的通讯通道或开放型公众网络，以及为特定自助服务设施或客户建立的专用网络，为甲方提供的离柜金融服务。根据服务渠道的不同，可分为网上银行服务、电话银行服务、手机银行服务、短信服务、自助设备服务等。

身份认证要素：指在电子银行交易中乙方用于识别甲方身份的要素，如客户 ID（用户昵称、证件号码等）、密码、椰盾、动态口令、预留手机号等。

密码：指客户自行设定并用于验证客户身份的字符信息，如登录密码、交易密码、账户密码等。

动态口令：指按照特定规则动态产生并用于识别客户身份的字符组合，乙方动态口令的载体是手机。

客户证书：指用于存放客户身份标识，并对客户发送的电子银行交易信息进行数字签名的电子文件。

椰盾：乙方为甲方提供的客户证书存放介质。

椰信：乙方为甲方提供的短信服务信息。

电子银行业务指令：指甲方通过电子银行渠道向乙方发出的查询、转账、购买金融资产等指示。

第二条 甲方权利、义务

一、权利

（一）甲方自愿申请注册乙方电子银行，经乙方同意后，将有权根据注册项目的不同享受不同的服务，申请方式：

1. 甲方在乙方网点柜面签约，能够获得乙方提供的电子银行各项服务；

2. 甲方自助注册网上银行、手机银行，并按照系统提示完成操作后，就成为乙方网上银行或手机银行客户，能够获得乙方提供的包括查询、转账在内的部分电子银行服务。

（二）甲方有权在本协议生效期间根据乙方相关业务规则对本协议项下电子银行服务提出变更或终止申请。

（三）甲方通过电子银行渠道办理相关交易后，有权在规定时限内到乙方营业网点补登存折。

（四）因网络、通讯故障等原因，甲方不能通过乙方电子银行系统办理业务时，甲方可到乙方营业网点办理相应银行业务。

（五）甲方对乙方电子银行服务如有疑问、建议或意见时，有权通过拨打电话“96566”（省外拨打 0898-96566）或到乙方各营业网点进行咨询和投诉。

二、义务

（一）甲方办理电子银行业务，应遵守《海南银行电子银行章程》以及乙方不定期通过营业

网点、官方网站或电子银行等渠道公布的相关交易规则，否则由此发生的风险和损失由甲方承担。

(二) 甲方到乙方营业网点办理电子银行注册、注销、变更等手续，应按乙方要求提供相关申请资料，甲方应对所申请事项签章确认。甲方签章确认的业务申请资料是本协议不可分割的组成部分。甲方应保证所提供资料真实、准确、完整、有效，对于因甲方提供信息不真实、不准确、不完整等原因而发生的风险和损失由甲方承担。

(三) 甲方办理网上银行业务应直接登录乙方网站(网址：<http://www.hnbankchina.com.cn>)，而不要通过邮件或其他网站提供的链接登录；甲方办理电话银行业务，应直接拨打乙方服务电话“96566”(省外拨打 0898-96566)；甲方使用通过客户端登录的电子银行，客户端软件应从乙方网站或设备指定软件下载网站下载。

(四) 甲方必须妥善保管本人注册卡号(账号、登录 ID 或注册手机号码)、密码、椰盾及接收短信认证的手机，不得交给任何第三方(包括乙方工作人员)使用。使用上述介质和要素所完成的一切交易操作均视为甲方本人所为，甲方应对由此产生的后果负责。乙方执行通过安全程序的交易指令后，甲方不得要求变更或撤销交易指令。

(五) 甲方应按照机密的原则设置和保管密码：避免使用姓名、生日、电话号码等与本人明显相关的信息作为密码；不得将本人自设密码提供给任何第三方(包括乙方工作人员)；通过手机银行办理业务后，须将自设密码从手机上删除；采取其他合理措施，防止本人密码被窃取。因甲方有意泄漏交易密码，或者未按照服务协议尽到应尽的安全防范与保密义务造成损失的，乙方不承担责任。

(六) 甲方应该妥善保管预留验证信息，除在乙方办理业务时使用外，不要向任何其他人、其他网站、电话或短信的问询提供预留验证信息内容。因甲方有意泄漏预留验证信息，或者未按照服务协议尽到应尽的安全防范与保密义务造成损失的，乙方不承担责任。

(七) 甲方使用短信认证功能，应在交易过程中认真核对收方账号和交易金额等信息是否与正在进行的交易事项一致，因甲方未认真核对信息而造成的一切损失，乙方不承担责任。因不可抗力或其他非乙方原因(如：甲方办理电子银行业务时提供的手机号码错误或无效、手机关机、停机、没有信号、短信延迟、丢失等)造成交易无法正常完成以及由此导致的一切后果，乙方不承担责任。

(八) 发生以下情况时，甲方应及时到乙方营业网点办理相应手续，否则可能产生甲方无法正常使用乙方电子银行功能或甲方账户资金安全性降低等风险。甲方应承担办妥手续之前所产生的一切后果。

1. 甲方的密码泄露、遗忘，应办理密码修改、重置手续。
2. 甲方领取的椰盾序列号与申请表上银行打印的序列号不一致，应当场办理更换手续。
3. 甲方领取的客户证书及椰盾在有效期内损毁、遗失或证书密码遗忘，应办理证书更换、挂失解挂或密码重置手续。
4. 甲方输错密码、动态口令超过乙方规定的次数，其交易可能被限制，甲方应及时与乙方办理相应解除限制的手续。
5. 甲方手机号遗失或变更，应及时取消或变更手机银行、椰信绑定的手机号码。

(九) 甲方在使用电子银行服务过程中，所提供的注册信息如有更改，应及时办理有关手续，办妥上述手续之前所产生的一切后果由甲方承担。

(十) 甲方不得有意诋毁、损害乙方声誉或恶意攻击、损坏乙方电子银行系统。

(十一) 甲方办理电子银行业务时，如其使用的服务功能涉及到乙方其他业务规定或规则的需同时遵守。

(十二) 甲方应采取安装防病毒软件、及时安装电脑系统安全补丁等合理措施、防止电子银行相关信息被盗或泄露；甲方同时应尽到合理注意义务，在安全的环境使用电子银行。

(十三) 甲方长期不使用电子银行，应主动申请办理注销手续。

(十四) 甲方使用乙方电子银行服务的, 应按照乙方制定并公布的电子银行个人客户服务收费项目及相应收费标准支付电子银行相关服务费用, 并同意乙方从其约定账户主动扣收。

第三条 乙方主要权利与义务

一、权利

(一) 乙方有权根据甲方资信情况, 决定是否受理甲方的注册申请。

(二) 乙方有权制定电子银行业务收费标准, 并在乙方官方网站及营业网点进行公布; 同时乙方有权按照所公布的收费项目及标准从甲方在乙方开立的账户中扣收相关费用。因甲方原因导致本协议或本服务中止或提前终止的, 乙方有权要求甲方承担违约责任并不退还甲方已支付的所有费用; 非因甲方原因导致本协议或本服务中止或提前终止的, 乙方退回甲方未使用服务所涉及的剩余费用。

(三) 乙方具有对电子银行系统进行维护、升级、改造的权利。(四) 甲方存在未按时支付有关费用、不遵守乙方有关业务规定或存在恶意操作、诋毁、损害乙方声誉等行为的, 乙方有权单方终止对甲方提供电子银行服务, 并保留追究甲方责任的权利。甲方利用乙方电子银行从事违反国家法律法规活动的, 乙方将按照有关部门的要求停止为其办理电子银行业务。

(五) 乙方根据甲方的电子银行业务指令办理业务, 对所有使用甲方在乙方设定的身份识别信息(包括账户账号、卡号、客户编号、电话或手机号码、客户名称、终端设备信息等), 并按照甲方在乙方设定的身份认证要素通过身份验证的操作均视为甲方所为, 该操作所产生的电子信息记录均为乙方处理电子银行业务的有效凭据。

(六) 乙方因以下情况没有正确执行甲方提交的电子银行业务指令, 乙方不承担任何责任:

1. 乙方接收到的指令信息不明、存在乱码、不完整等。
2. 甲方账户存款余额或信用额度不足。
3. 甲方账户内资金被依法冻结或扣划。
4. 甲方未能按照乙方的有关业务规定正确操作。
5. 甲方的行为出于欺诈或其他非法目的。

6. 由于不可抗力、计算机黑客袭击、系统故障、通讯故障、网络拥堵、供电系统故障、电脑病毒、恶意程序攻击及其它不可归因于乙方的原因, 导致甲方未收到或延迟收到乙方发出的与交易相关的认证信息, 或导致乙方无法正常处理甲方的电子银行业务指令。

(七) 乙方有权以公告方式修改本协议条款和章程、相关业务规定、业务规则, 甲方如拒绝此修改, 应在公告规定的合理期限内注销乙方电子银行服务, 若甲方于生效日期后仍使用乙方电子银行服务, 即视为接纳相关修改。如造成损失, 由甲方负责。

(八) 如甲方因乙方电子银行系统差错、故障或其他原因获得不当得利的, 乙方有权从甲方账户中扣划甲方的不当得利所得或暂停对甲方的电子银行服务。

二、义务

(一) 在乙方系统正常运行情况下, 乙方负责及时准确地处理甲方发送的电子银行业务指令, 并及时向甲方提供查询交易记录、资金余额、账户状态等服务。

(二) 乙方对于电子银行所使用的相关软件的合法性承担责任。

(三) 乙方负责及时为甲方办理电子银行注册手续, 并按甲方注册功能的不同为甲方提供相应的电子银行服务。

(四) 乙方负责向甲方提供电子银行业务咨询服务, 并在乙方网站公布功能介绍。

(五) 乙方在法律法规许可和甲方授权的范围内使用甲方的资料和交易记录。乙方对甲方提供的申请资料和其他信息有保密的义务, 但法律法规另有规定的除外。

(六) 因乙方工作过失导致甲方支付指令处理延误的, 乙方按中国人民银行《支付结算办法》

的有关规定赔偿。

第四条 差错和争议的解决

甲方发现自身未按规定操作，或由于自身其他原因造成电子银行业务指令未执行、未适当执行、延迟执行的，应及时通过拨打“96566”（省外拨打“0898-96566”）或到营业网点通知乙方。乙方应积极调查并告知甲方调查结果。

双方在履行本协议的过程中，如发生争议，应协商解决。协商不成的，任何一方均可向乙方所在地人民法院提起诉讼。

第五条 协议的生效、变更、中止和终止

本协议自乙方在电子银行系统为甲方完成注册起生效。

若甲方注册电子银行后又办理银行卡卡片更换，与原卡相关的电子银行服务事项自动转至新卡，本协议继续有效。

甲方变更或终止电子银行服务，须根据乙方相关业务规定通过乙方营业网点、相关电子银行渠道办理。甲方终止电子银行服务前应偿清所有应付款项。

因挂失、冻结等原因导致账户暂不能使用的，相关电子银行服务亦相应中止，待账户可以正常使用后恢复相关电子银行服务。账户销户的，该账户相关的电子银行服务以及本协议中的相关内容亦相应终止。

甲方电子银行注销手续办理完毕，本协议即为终止。

在甲方违反本协议规定或其他乙方业务规定的情况下，乙方有权中止或终止本协议。协议终止并不意味着终止前所发生的未完成电子银行业务指令的撤销，也不能消除因终止前的交易所带来的任何法律后果。

第六条 法律适用条款及其他约定事项

本协议的成立、生效、履行和解释，均适用中华人民共和国法律。

本协议是乙方的其他既有协议和约定的补充而非替代文件，如本协议与其他既有协议和约定有冲突，涉及电子银行业务的，应以本协议为准。

除有相反证据证明外，电子银行服务中产生的凭证和银行交易记录是确定交易真实有效和交易具体内容的依据。

本协议的任何条款如因任何原因而被确认无效，都不影响本协议其他条款的效力。

本协议中未尽事宜应依照国家法律法规、规章、金融惯例以及乙方相关业务规定办理。

海南银行股份有限公司隐私政策 (2018 年 12 月版)

海南银行股份有限公司（以下简称“我行”）非常重视用户的隐私和个人信息保护。您在使用我行的产品与/或服务时，我行可能会收集和使用您的相关信息。我行希望通过《海南银行股份有限公司隐私政策》（以下简称《隐私政策》）向您说明我行在您使用我行的产品与（或服务）时如何收集、使用、保存、共享和转让这些信息，以及我行为您提供的访问、更新、删除和保护这些信息的方式。同时，我行将承诺依法采取相应的安全措施来保护您的个人信息。

您在注册或使用我行产品（或服务）前，请仔细阅读并确认本《隐私政策》。本《隐私政策》是我行统一使用的一般性隐私条款，适用于我行所有个人业务产品（或服务）。我行收集和使用您的信息的目的、方式和范围将通过相应的产品（或服务）协议、授权书等方式向您明示，并取得您的授权或同意。上述文件与本《隐私政策》共同构成我行与您之间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 及相关技术
- 3、我行如何存储和共享您的个人信息
- 4、我行如何保护和保存您的个人信息
- 5、您控制个人信息的权利
- 6、未成年人用户信息保护
- 7、通知和修订
- 8、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。本隐私政策中涉及的个人信息包括：个人姓名、生日、性别、住址、个人电话号码、身份证件号码、账户信息、财产状况等。

个人敏感信息是指一旦泄露、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个人信息，本隐私政策中涉及的敏感信息包括：身份证件号、银行账号、征信信息、财产信息、交易信息等。

（一）我行收集和使用个人信息的原则

我行收集使用您的个人信息将遵循合法、正当、必要的原则，按照法律法规要求以及业务需求收集您的个人信息，不会收集与业务无关的信息或采取不正当方式收集信息。

（二）我行收集和使用个人信息的目的

我行收集您的个人信息，目的在于依法合规的为您提供优质的产品和服务，该等信息对于充分履行您和我行之间的合约很有必要，并使得我行能够遵守相关法律义务，具体可能包括：

- 1、为保护您的账户安全，对您身份进行识别、验证等；
- 2、为评估您的履约能力及履约状况，用于义务准入和防控风险；
- 3、为您提供产品和服务所必须；
- 4、为保护您的资金安全；
- 5、为改善产品和服务、提升客户体验；
- 6、为履行法定义务；
- 7、经您允许的其他用途。

（三）我行收集个人信息的方式

1、我行为您提供金融服务时，您主动向我行提供的个人信息，如您的个人姓名、生日、性别、住址、个人电话号码、身份证件号码等；

2、我行为您提供金融服务过程中形成的与服务相关的信息，如您的设备信息、软件信息、IP 信息、服务日志、通讯日志、位置信息等；

3、按国家有关规定向征信机构、信用管理公司、资信评估机构或有关法律、监管机构许可的类似机构采集您的信用信息和行为信息，如您的个人征信报告等；

4、按国家有关规定向政府机构、司法机关及公共事业单位（如人民银行、公安部、人力资源和社会保障部门、公积金管理中心、中国互联网金融协会等机构）采集和服务相关的必要信息，如您的身份证件信息、工商信息、税务信息、诉讼信息、社保信息等；

5、经您授权，向合法留存您信息的自然人、法人以及其他组织收集与我行提供的服务相关的必要信息；

6、经您许可的其他方式。

（四）我行对您个人信息使用的规则

1、我行会根据本隐私政策的约定并为实现我行的产品与服务功能对所收集的个人信息进行使用。

2、请您注意，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。如您仅在手机设备或个人计算机中删除海南银行相关 App 或网页访问链接时，我行不会停止使用您的个人信息。只有在您完全注销账户服务后，我行才会停止使用您的个人信息，但我行会在业务资料归档、审计、监管协查等领域会继续使用此前收集的您的相关个人信息。

3、我行会对产品与服务使用情况进行汇总、统计分析、加工，并可能会与公众或第三方共享这些统计信息，以展示我行的产品与服务的使用趋势。但这些统计信息不包含您的任何身份识别信息。

4、为了您知悉使用我行金融产品和服务的情况，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。如您不希望接收商业性信息，您有权要求我行停止为此项用途使用您信息。

5、当我行要将您的个人信息用于本政策未载明的其它用途时，或基于特定目的收集而来的信息用于其他目的时，会通过您主动做出勾选的形式事先征求您的同意。

6. 将您的个人信息用于法律允许的其它用途。

二、我行如何使用 Cookie 及相关技术

我行的电子银行相关系统使用了 cookie 技术，该项技术仅用于系统维护用户正常的登录会话状态，确保用户安全、正常的使用我行提供的电子银行相关服务，并未收集用户相关个人信息。

若我行需要通过 cookie 及相关技术收集用户的个人信息时，我行会依据国家相关法律法规开展工作，并及时以邮件、信函、电话、推送通知等方式告知您，确保您的个人信息安全。

三、我行如何存储和共享您的个人信息

（一）存储

1、您的个人信息将全被存储于中华人民共和国境内。如您使用跨境交易服务，且需要向境外传输您的个人信息完成交易的，我行会在获得您的授权同意后，可能将您的个人信息转移到境外，并要求接收方按照我们的说明、本隐私政策以及其他任何相关的保密和安全措施来处理这些个人信息。

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必须的期限内，确定单个用户数据的最长储存期限以及用户日志的储存期限。

（二）共享

我行不会与其他的任何公司、组织和个人共享您的个人信息，但以下情况除外：

1、事先获得您明确的同意或授权；

2、根据适用的法律法规、法律程序的要求、强制性的行政或司法要求所必须进行提供；

3、在法律法规允许的范围内，为实现隐私政策声明的目的，或为向您提供服务之必须，我行会与有关联公司、合作伙伴共享您的某些个人信息。我行只会共享必要的个人信息，且我行合作伙伴和关联公司无权将共享的个人信息用于任何其他用途；

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、该组织重新向您征求授权同意；

5、应您需求为您处理您与他人的纠纷或争议；

6、符合与您签署的相关协议（包括在线签署的电子协议）或其他的法律文件约定所提供；

7、基于学术研究而使用；

8、基于符合法律法规的社会公共利益而使用。

（三）公开披露

我行仅会在以下情况下，且采取符合业界标准的安全防护措施的前提下，才会公开披露您的个人信息：

1、根据您的请求，在您明确同意的披露方式下披露您所指定的个人信息；

2、根据法律法规的要求，或按照强制性的行政执法或司法要求所必须提供您个人信息的情况下，我行可能会依据所要求的个人信息类型和披露方式公开披露您的个人信息。

四、我行如何保护和保存您的个人信息

我行已使用符合业界标准的安全防护措施以及加密技术、匿名化处理等手段保护、保存您的个人信息，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。我行已建立专门的管理制度与管理流程确保信息安全，并将采取合理有效的措施，保护您的个人信息。

请您理解，由于互联网环境并非百分之百安全，我行将尽力确保您发送给我们的任何信息的安全性。但有可能出现我行无法预见的物理、技术、或管理防护设施遭到破坏，导致信息被非授权访问、公开披露、篡改、或毁坏，导致您的合法权益受损。互联网环境极为复杂，因此请您务必提高安全意识，注意防止泄密，协助我行保证您的账号安全。

如发生个人信息安全事件，我行将按照我国相关法律法规，及时向您告知：安全事件的基本情况和可能的影响、我行已采取或将要采取的处置措施、我行对您已采取或将要采取的补救措施等。我行将及时以邮件、信函、电话、推送通知等方式告知您事件的处置情况，难以逐一告知个人信息主体时，我行会采取合理、有效的方式发布公告。同时，我行还将按照监管部门要求，主动上报个人信息安全事件的处置情况。

五、您控制个人信息的权利

我行非常重视您控制个人信息的权利，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

您有权通过我行网点、网上银行、手机银行等渠道访问及更正、更新您的个人信息，法律法规另外规定除外，您有责任及时更新您的个人信息。

（二）删除您的个人信息

在以下情形中，您可以向我们提出删除个人信息的请求：

1、如果我们处理个人信息的行为违反法律法规；

2、如果我们收集、使用您的个人信息，却未征得您的同意；

3、如果我们处理个人信息的行为违反了与您的约定；

（三）拒绝我行商业广告

您有权拒绝接受或退订我行基于个人信息向您推送的商业广告。

（四）响应您的上述要求

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，然后再处理您的要求。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，我行可能会给予拒绝。

在以下情形中，按照法律法规要求，我行将无法响应您的请求：

1、与国家安全、国防安全有关的；

- 2、与公共安全、公共卫生、重大公共利益有关的；
- 3、与犯罪侦查、起诉和审判等有关的；
- 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、涉及到我行商业秘密的。

六、未成年人用户信息保护

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们的产品（或服务）或向我们提供信息。我行将在法律法规及监管要求允许内或保护未成年人所必要的情况下，对外提供此信息。

七、通知和修订

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定时进行修订。修订后我行会通过官网、网上银行、手机银行等渠道公布，公布后即生效，并取代此前相关内容。您应不时关注我行的相关公告，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的服务，并注销相关用户，我行将停止收集您的相关信息；如您继续使用服务，即视为同意接受变动内容。

八、如何联系我行

如您对本隐私政策有任何疑问、意见，请联系我行客服热线：0898-96566。

请您在勾选“同意”之前仔细阅读本隐私政策，确保对其内容特别是字体加黑内容的含义及相应法律后果已全部知晓并充分理解。您勾选“同意”并完成注册程序即视为您接受本隐私政策，我行将按照相关法律法规及本政策来合法使用和保护您的个人信息。

附件 1-2

基于人工智能技术的风险交易预警服务 合法合规性评估报告

经评估，本项目严格按照《中华人民共和国网络安全法》、《中华人民共和国反洗钱法》、《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》、《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）、《金融机构大额交易和可疑交易报告管理办法》（中国人民银行令〔2016〕第3号发布）、《中国人民银行关于落实个人银行账户分类管理制度的通知》（银发〔2016〕302号）、《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261号）、《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2019〕85号）、《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》（中国人民银行、银监会、证监会、保监会令〔2007〕第2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。

综上所述，本项目所提供金融服务符合相关法律法规要求，可依法合规地开展业务应用。

海南银行股份有限公司法律合规部

2021年11月04日

附件 1-3

基于人工智能技术的风险交易预警服务 技术安全性评估报告

经评估，本项目严格按照《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）、《基于大数据的支付风险智能防控技术规范》（JR/T 0202—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）等相关金融行业技术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行业标准要求。

海南银行股份有限公司信息科技部

2021 年 11 月 04 日

基于人工智能技术的风险交易预警服务 风险补偿机制

本项目按照风险补偿方案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，由海南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。

具体机制如下：

1. 建立客户投诉快速响应机制，客户可通过营业网点、24小时服务热线等渠道提出投诉意见，为确保客户投诉及时高效处理，建立项目专项联系人机制，做好各类客户投诉问题的核查及支持保障，及时发现问题，提升客户服务水平。

2. 在项目运营过程中所产生的风险并对于客户合法的权益造成损失时，积极协助客户通过仲裁、诉讼等相关法律途径取得合理的补偿。

3. 在出现风险并造成用户资金损失时，明确责任认定后，按照相关用户投诉及赔付处理机制赔付用户，切实保障用户合法权益。



基于人工智能技术的风险交易预警服务 退出机制

本项目按照退出机制，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。

具体机制如下：

一、业务层面

1、客户告知

通过银行门户网站、直销银行、手机银行等多个渠道发布业务下线公告，并以短信方式主动通知业务所涉及的所有客户，24小时服务热线统一做好客户解释工作。

2、协议解除

按照退出方案终止有关服务，约定在服务终止日提前与客户解除服务协议。

本项目遵循海南银行消费者保护相关制度规定，客户可通过营业网点、24小时服务热线 0898-96566 等渠道提出投诉意见和

赔付要求。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。

二、技术层面

本项目涉及的应用系统将按照海南银行系统管理制度要求做应用下线处理，相关操作在信息技术部门的支持下完成。

1、服务关停

由信息技术部门关停金融业务风控平台服务，关闭服务接口，并将相关数据、模型做下线处理。

2、应用下线

由信息技术部门进行应用系统下线处理，卸载部署在服务器上的程序，并删除配置文件。

3、数据清理

本项目涉及数据的，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。其中，涉及客户数据的，在应用服务下线的同时将该部分数据直接做销毁清除处理；涉及系统数据的，由海南银行有权操作人员依照人民银行关于数据生命周期及会计档案保管的有关规定做好数据备份、保管和清理。

4、硬件资源回收

应用系统下线后，可将服务器等硬件资源进行回收，将应用服务器所在虚拟机回收，物理机操作系统重做，物理机硬盘格式化。

基于人工智能技术的风险交易预警服务 应急预案

本项目按照应急处置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，妥善处置受影响的存量业务，切实保障用户资金和信息安全。

具体应急预案如下：

一、目的

为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，提高对突发危机事件的应变能力，并在最大限度范围内减少因事故的发生所带来的损失，特制定本应急预案。

二、适用范围

本应急预案适用于海南银行相关系统、应用程序、网络、算法模型等发生异常故障，短时间内无法恢复，需要启动应急响应措施，保障故障快速恢复的应急管理处置。

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。

三、处理原则

快速处置原则：发生重大系统安全事件应按相关规定，迅速响应，协同应对和处置。

协调一致原则：按照统一指挥、各司其职原则，充分发挥各专业部门的作用，统一组织实施。

及时性原则：突发事件的报告应遵循快速及时、客观真实、全面的原则，不得迟报、隐瞒不报或漏报。

业务连续性原则：应急响应时，应采取积极有效的措施，保障本项目的连续性处理。

最小损失原则：应急响应中应基于现实条件，在最短时间内用最小代价将损失降到最低。

四、突发事件等级

根据突发事件造成的严重程度、影响范围，对突发事件实行3级分类：

特别重大突发事件（Ⅰ级）。因业务系统发生严重突发事件，导致本项目无法正常运营，影响全部客户，且持续时间可能超过4小时以上的事件。

重大突发事件（Ⅱ级）。因业务系统发生重大突发事件，波及本项目正常运营，影响部分客户，且持续时间可能超过1小时以上的事件。

一般突发事件（III级）。因局部的服务器、存储设备、安全设备、通讯线路等的功能、安装或配置方面存在问题或局部的系统程序、系统参数设置存在问题但尚未影响客户的事件。

上述 I、II、III 级突发事件描述，只是一个基本定义。应根据不同等级的突发事件，采取有针对性的措施，并依据突发事件的性质、分类、影响范围和停机时间等因素，来灵活制定响应启动流程。

当突发事件等级指标有所交叉而难以判定级别时，应按相对较高一级突发事件处理。突发事件在处置过程中，如事态和影响进一步扩大，且达到上一级标准的，则应作升级处理。

五、应急预案及处理措施

1、事前预防措施

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。

2、事中预警措施

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、算法模型、硬件资源等的异常情况进行告警，到早发现、早准备。

3、事后应急响应措施

突发事件发生后，启动相应等级的应急保障预案进行全力处置，及时控制事态，同时向海南银行应急管理部门报告先期处理情况。应急管理部门相关负责人应赶赴现场，指挥有关的应急保

障工作，控制事态的发展，努力减少损失，同时组织力量和有关技术人员对事件的性质、类别、危害程度、影响范围进行评估。

分级响应突发事件发生时，按照快速、机动、灵活的原则，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。

I级响应。当出现I级突发事件，启动I级保障应急预案，及时向海南银行项目管理部门报告，关闭增量业务渠道，并组织专人紧急进行故障排除与处理，同时通过门户网站、手机银行、直销银行、短信等渠道及时向客户进行公告。

II级响应。当出现II级突发事件，启动II级保障应急预案，及时向项目管理部门报告，经统一沟通协商决定是否需要关闭增量业务渠道，并组织专人紧急进行故障排除与处理，同时通过短信通知方式对受影响客户及时进行告知。

III级响应。当出现III级突发事件，启动III级保障应急预案，及时向项目管理部门报告，并组织专人紧急进行故障排除与处理。

4、应急程序终止

突发事件处理完毕，系统恢复正常服务并消除了不良影响，经项目管理部门商议同意后，应急响应措施同时终止。

5、应急预案培训与演练

在建立7 X 24小时事中监控预警的基础之上，加强对突发事件应急处置预案的培训工作。对项目涉及的应急问题，明确应急处置的联系人和处理流程、响应机制。每年至少开展一次应急响

应演练，并事后对应急预案与实际演练的有效性、完备性进行再评估。通过定期实行系统环境巡检与系统切换演练，不断总结、完善预案，保证突发事件应急处理机制的持续性与有效性。