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	911200001030702984-2024-0001	
	创新应用名称	基于深度学习和智能安全终端的轻型柜面服务	
	创新应用类型	金融服务	
	机构信息	统一社会信用代码	911200001030702984
		全球法人识别编码	300300C1080312000031
		机构名称	天津银行股份有限公司
		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:B0108H212000001 发证机关:中国银行保险监督管理委员会天津监管局
	机构信息	统一社会信用代码	9111010266753115XC
		全球法人识别编码	300300C1080312000031（总行）
		机构名称	天津银行股份有限公司北京分行
		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:B0108B211000001 发证机关:中国银行保险监督管理委员会北京监管局
	机构信息	统一社会信用代码	91130100MA07QT733T
		全球法人识别编码	300300C1080312000031（总行）
		机构名称	天津银行股份有限公司石家庄分行
		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:B0108B213010001 发证机关:中国银行保险监督管理委员会河北监管局
	拟正式运营时间	2024 年 12 月 1 日	
	技术应用	1.运用计算机视觉技术（CV）、自然语言处理（NLP）、大规模语言模型（LLM）、增强现实（AR）、深度学习等技术，实现客户身份验证、金融咨询服务、交易处理、客户服务、风险评估、跨语言服务、无障碍服务等多种金融业务场景，	

		快速响应客户需求，提升国际化服务能力，提高金融服务的可获得性。 2.运用活体采集技术，准确捕捉人脸图像，提取和分析人脸的生物特征，判断用户做出的特定动作是否符合要求，确保金融业务办理为客户意愿，防范非法操作风险，提升柜员和客户的身份识别能力。 3.运用北斗定位、时间同步、差分定位、多模接收等技术，实现对设备实时无间断定位、轨迹监控，设备断电后，支持24小时内持续上传位置坐标信息，硬件模块上传北斗坐标，后台监控系统在此基础上可提供电子围栏等功能，具备更广泛的定位区域覆盖、更强的抗干扰能力，附带救援通信功能，提升设备智慧管理水平。 4.运用数据加密技术，基于设备板载TCM安全芯片、提供可信安全启动和数据完整性验证，支持加密通信、防篡改保护、隐私保护，确保系统从启动到操作系统加载的整个过程未被篡改，加大对柜面终端数据的保密力度，全面提升设备的安全性和可靠性。
	功能服务	本项目综合运用深度学习、活体采集技术、北斗定位、数据加密等技术搭建轻型柜面高集成度终端设备，结合远程柜员业务，支持全委托远程业务办理，满足复杂的业务需求，推动网点向轻量化、交互化、数字化转型。同时兼顾老年人需求，增加放大镜，配备眼动仪，增加扶手功能，构建适老化服务生态。本项目创新数字技术在乡村振兴金融服务中的运用，提供多维度、跨行业的便捷金融服务供给。具体提供业务主要包括六大类，分别是金融咨询类、产品信息查询类、账户交易明细查询类、便民服务类、风险提示类和账户管理类；具体为金融知识普及、养老服务、反电诈、投资理财咨询、存款产品查询、理财产品查询、账户信息查询、社保联动查询、横联电子纳税银行端缴税、非税收入缴费、社保费税缴查询缴费、维修资金补缴、灵活就业社保查询缴费、综合签约类　　个人综合签解约、个人客户信息建立/维护/查询、个人账户挂失、个人账户密码管理（密码重置、账户激活）、个人转账（行内转账、跨行转账）以及个人开卡等业务。 本应用由天津银行股份有限公司负责研发及运维，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.在服务方式方面，通过整合轻型设备、智能柜员、远程视频及全委托业务办理模式，实现多元化服务渠道的综合应用。轻型设备可部署至养老院、社区、园区场地，实现多生态跨界合作，拓展了服务范围。 2.在业务效率方面，简化业务流程，为客户节省办理业务的时间和精力成本；依托智能设备和先进技术，大幅提高业务处理速度和整体业务办理效率。 3.在服务范围方面，重点聚焦老年人、特殊客户群体，精准

		满足其特殊需求，有效提高金融服务的可获得性。同时，覆盖无网点地区及无法到达网点的客群，为乡村振兴和普惠金融贡献力量。 4.在安全防范方面，从多个维度构建安全防范体系，包括物理安全、信息安全、网络安全和身份安全等，确保安全终端不受外部破坏或非法入侵，并运用数据加密技术加强信息安全保护，防止客户信息泄露和数据被篡改。
	预期效果	通过全委托办理模式提升我行客户业务办理体验，设备适老化改造提升老年客群的业务办理体验。降低物理网点成本，延伸我行金融服务，进一步释放网点人力，助力高效运营、高效获客。在提升客户体验的同时，降本增效。
	预期规模	预计投入设备 50 台-150 台,辐射服务人数约 10 万-20 万人。
创新应用服务信息	服务渠道	线下渠道：京津冀地区部署设备的所有地点 （如：养老院、社区、园区）
	服务时间	线下渠道：9：00 至 17：00
	服务用户	天津银行京津冀地区个人客户
	服务协议书	《服务协议书-基于深度学习和智能安全终端的轻型柜面服务》（见附件 1-1）
合法合规性评估	评估机构	天津银行内控合规部
	评估时间	2024 年 9 月 26 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)、《中华人民共和国反洗钱法》、《中华人民共和国商业银行法》、《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。
	评估材料	《合法合规性评估报告-基于深度学习和智能安全终端的轻型柜面服务》（见附件 1-2）
	评估机构	天津银行信息技术部
	评估时间	2024 年 9 月 26 日
	有效期限	3 年
	评估结论	本项目严格按照《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)、《移动金融客户端应用软件安全管理规范》（JR/T 0092—

技术安全性评估		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)、《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。 后续，将在自声明前提交由外部权威专业机构出具的《金融科技创新安全通用规范》（JR/T 0199—2020）标准符合性证明材料。		
	评估材料	《技术安全性评估报告-基于深度学习和智能安全终端的轻型柜面服务》（见附件 1-3）		
	风险措施	1	风险点	物理安全风险：设备外拓使用可能存在设备被盗用风险：设备被盗或未经授权移动、屏幕操作或密码输入时被他人窥视、泄露敏感信息。
			防范措施	1、物理防盗：底座固定在桌面，安全盒固定在底座，终端无法被非法带走，安全盒具有防护 USB 口，非授权人员无法使用 USB 口； 2、屏幕与键盘防窥：屏幕使用防窥屏幕，仅客户自身可以看清屏幕内容，防止个人信息泄露。密码键盘带有防窥罩，可有效防止他人偷窥； 3、端侧智能、数据本地化：实时性能提升，减轻后端服务器网络和算力负担；数据本地化，符合数据本地化和隐私保护的要求；本地专门的硬件加速，减少数据网络传输；基于端侧算力，可实现实时异常检测； 4、重空凭证（卡）安全：使用长城销卡模块对废卡的芯片、磁条进行打孔销毁，此模块可与主机灵活搭配使用，保障原卡片中可能保留的客户隐私信息不被泄露； 5、设备 7*24 安全监控：全天候运行、多层防护、实时响应；采用冗余设计，确保系统的稳定性和可用性；运用人工智能技术进行异常行为分析和预警； 6、防拆防爆：触摸屏采取防爆设计，密码键盘采取全金属高安全设计，全机壳采取高强度金属外壳，具备防爆防拆功能，拆机自毁密钥； 7、高集成低暴露：模块隐藏式安全设计，摄像头、触摸屏幕等仅暴露人机交互触点。
		2	风险点	老年人进行业务委托书办理时，可能存在业务操作障碍、沟通障碍和理解偏差问题。
			防范措施	1、风险评估：在办理前，银行对老年人的风险承受能力、财务状况和委托需求进行全面评估，以确定合适的委托方案。 2、科技辅助：利用智能技术，采用人工智能远程客服，为老年人解答疑问，提供实时的咨询服务。

风险防控				3、多重身份验证：加强身份验证措施，如指纹识别、面部识别、短信验证码等，确保委托式办理操作是老年人本人授权。 4、限制委托权限：根据老年人的实际需求，合理设定委托办理可操作的业务范围和权限，避免过度授权。 5、加强银行员工培训：提高银行员工的职业道德和专业素养，使其能够更好地为老年人提供服务，识别潜在风险。 6、宣传教育：通过社区、老年大学等渠道，向老年人宣传全委托办理的风险和注意事项，提高他们的防范意识。
		3	风险点	网络安全风险：设备被黑客远程攻击或控制；数据传输过程中被截获或篡改；Wi-Fi 等无线连接被非法入侵。
			防范措施	1、VPN 专用传输信道：VPN 路由器通过 5G 拨号的方式连接到中心端，加密方式采用 IPSEC VPN+国密算法。轻型柜面终端采取 802.1X 认证、MAC 地址过滤、隐蔽 SSID、单点登录等多种防护策略确保能够安全链接到 VPN 路由器。 2、双向认证的传输加密：客户端与服务端的 https 通信采取双向认证，进一步提升安全性。客户端除了需要从服务器端下载服务器的公钥证书进行验证外，还需要把客户端的公钥证书上传到服务器端供服务器端进行验证，双方认证通过，才开始建立安全通信通道进行数据传输。
		4	风险点	数据安全风险：可能存在数据被窃取风险--敏感数据被非法访问或窃取；数据存储介质(如硬盘)被物理移除；数据日志被分析记录不当导致信息泄露。
			防范措施	1、硬盘访问加密：实施全面的数据加密方案，可以通过设置硬盘访问权限密码，限制硬盘存储数据的读取和下载，提升数据安全性； 2、采用安全日志记录机制：实施内存级数据处理，避免交易相关数据落盘；采用安全日志记录机制，确保日志完整性和不可篡改性。
		5	风险点	软件安全风险：即可能存在应用软件被破坏风险--未经授权的软件被安装或运行；银行应用被非法恶意删除或终结，退出到桌面导致文件系统暴露在外
			防范	1、阻止未知软件安装：采用应用保护检查应用程序来源、设置应用程序执行控制策略，检测文件损坏篡改状态，同时进行应用防护控制，设置进程防杀死，避免系统关键内核模块遭受恶意卸载，保护系统运行完整性，免受安全威胁。终端机杀毒软件也能提供端

			措施	侧全方位安全防护。 2、默认应用独占模式：全屏显示应用程序，不显示任务栏和桌面。桌面为默认应用，屏蔽所有鼠标键盘、快捷操作，仅保留启动和退出【应用】的单点登录验证，屏蔽系统通知，屏蔽系统手势。
		6	风险点	身份认证风险：可能存在身份冒用风险--身份认证被绕过，导致未授权访问；生物识别数据被复制或盗用；密码或身份信息被社会工程学手段获取。
			防范措施	1、采用指纹识别和人脸识别确认业务办理人员身份，进行业务办理人员的资质审查； 2、通过活体检测来防止非真实生物特征的攻击手段（例如照片、人脸模具）； 3、采用目标人物实时跟踪算法，确保关键业务办理过程中业务办理人员一致性。
		7	风险点	操作安全风险：即可能存在操作异常风险--异常的操作时间和地点、多次重复操作、会话超时、异常登录和登出
			防范措施	1、用户行为分析：收集并分析用户操作日志，建立用户操作模型，检测异常操作模式。实时监控用户行为，发现异常行为后，及时报警并采取相应措施，同时终端自动拍照取证，存储审计日志。 2、建立严格的权限管理机制：按照最小权限原则分配权限，基于角色的访问控制(RBAC)模型严格审计管理员操作，限制管理员权限，将管理员权限分为多个层级，并进行隔离，定期审查和调整用户权限。 3、强制实施会话超时和自动登出机制：设置会话超时时间，处于空闲状态一段时间后自动登出，登出后需重新认证才能访问集中管理和监控所有在线会话。同时对会话进行加密，防止会话劫持。建立自动化的系统开关机机制，根据预设的营业时间自动开启和关闭终端系统。
	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 向天津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（956056），选择人工服务联系客服代表。 3.门户网站 通过门户网站: http://www.bankoftianjin.com/联系我行“在线客服”。
		投诉受理与处理机制	受理部门：天津银行客服中心 受理时间：7×24 小时 受理流程:天津银行营运中心接到投诉后,形成工单流转至相关管理部门。管理部门核实情况形成意见,处理完毕后通过工单系统回复至客服中心。客服中心在规定时限内进行客户回访,听取客户反馈意见,如果客户仍不满意将重新联系相关部门进一步处理。 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
			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

		投诉受理 与处理机制	〔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）　　2024 年 9 月 26 日（盖章）

附件 1-1

基于深度学习和智能安全终端的轻型柜面服务服务协议书

本项目服务协议书包括《天津银行借记卡章程》《天津银行电子银行个人客户服务协议》《天津银行电子渠道隐私政策》。

天津银行股份有限公司

2024 年 9 月 26 日

附件 1-1-1

天津银行借记卡章程

请阅读借记卡章程

第一条 为规范天津银行借记卡的发行和使用，更好地为持卡客户提供用卡服务，依据《中华人民共和国民法典》、国务院《储蓄管理条例》、中国人民银行《银行卡业务管理办法》以及国家外汇管理局等相关法律法规和监管规定，制定本章程。

第二条 天津银行（以下简称本行）借记卡是面向个人客户（以下简称持卡人）发行的，具有存取现金、消费结算、转账支付、账户管理以及其他理财签约服务等全部或部分功能的金融支付结算工具。借记卡必须先存款后支取，不能透支。

第三条 借记卡按介质类型分为纯磁条卡（已停发）、磁条芯片复合卡（简称芯片卡）和纯芯片卡。按实现功能不同分为储蓄卡、社保卡、津卡通卡、理财通卡等。

第四条 借记卡发行对象为个人，目前发行的借记卡为标准借记卡，本行根据客户类型向持卡人提供增值服务。

本行与联名单位合作发行的借记卡称为联名（认同）借记卡，此类借记卡持卡人除可享受我行提供的服务外，

还可享受联名单位提供的附加服务。

第五条 凡符合本行办卡条件的个人均可凭本人有效身份证件向本行申领借记卡，申领时应按本行要求提供相关申请材料，确认并自愿遵守本章程。借记卡申领应符合国家实名制有关规定，开户应使用实名。原则上，个人客户开立借记卡必须本人办理，不允许代办；未成年人可由监护人代理开立借记卡（特殊卡种依具体规定办理）。

第六条 持卡人应向本行提供真实的个人资料，如个人资料发生变化，应及时到本行营业网点办理变更手续。由于持卡人未能及时向本行提供正确资料而造成的损失，由持卡人自行承担。持卡人先前提交的身份证件或身份证明文件已过有效期的，但没有在规定期限内更新且没有提出合理理由的，本行有权中止持卡人借记卡相关业务。

第七条 借记卡可同时具有借记账户、电子现金账户功能，也可具有其中一种功能。本行发行的纯磁条卡具有借记账户功能，磁条芯片复合卡兼具借记账户和电子现金功能。借记账户存款按照中国人民银行规定的相应存款利率政策及计息办法计付利息，电子现金账户资金不计息，余额不得超过人民币 1000 元。

第八条 借记卡的账户类型包括 I 类账户和 II 类账户。2016 年 11 月 30 日（含）前开立的储蓄卡、津卡通卡、理财通卡、社保卡、工会卡等账户类别均为 I 类账户。礼仪

卡和商联卡账户类别为II类账户。2016年11月30日后开立的借记卡，如持卡人未在本行开立I类账户的，可将该卡开立为I类账户；如持卡人在本行已有I类账户的，则该卡只能开立为II类账户。借记卡不能开立为III类账户。

第九条 持卡人在本行网点申领开立的借记卡原则上不得超过4张，如该客户之前已持有本行全国范围内4张（含）以上借记卡的，不得申请再开立新的借记卡，已销户的借记卡不计算在内。社会保障卡具有民生保障功能，如客户已持有4张（含）以上借记卡时，可再申请开立社会保障卡。

第十条 对于公安或司法等有权机关认定曾参与出租、出借、出售本人或他人借记卡账户等的客户（包含持卡人、申请人、代理人等），本行有权实施暂停其银行账户非柜面业务或拒绝为其新开立账户等措施，具体遵照本行个人人民币银行结算账户相关管理规范执行。

第十一条 借记卡可在本行营业网点、自助机具、POS终端、网上银行、手机银行、电话银行等渠道上使用，也可在有银联标识的境内外自助机具和银联商户POS终端等受理设备上使用。

第十二条 持卡人可持具备电子现金功能的芯片卡办理电子现金业务。芯片卡电子现金业务包括：电子现金账户的圈存、圈提、脱机消费以及查询等交易。

芯片卡电子现金交易暂不设交易密码，凡使用芯片卡电子现金进行的交易均视为持卡人本人所为。芯片卡电子现金视同现金管理，不挂失，不计息，持卡人应承担电子现金丢失、保管或使用不善等产生的责任。

第十三条 电子现金账户资金可以由芯片卡活期主账户通过柜面或自助渠道提供的圈存交易或现金充值交易转入，在销卡或正常换卡时，可通过柜面圈提交易转回活期主账户。

第十四条 持卡人必须妥善保管借记卡和个人密码。凡使用卡密码或按照本行或第三方机构约定的其他交易验证方式完成的交易，均视为持卡人本人所为并承担交易款项。依据密码和或其他验证要素等电子信息办理的借记卡各类结算交易所产生的电子信息记录均为该项交易的有效凭证。

第十五条 借记卡由持卡人本人使用，不得出租、出借和出售。持卡人应妥善保管所持卡片，因持卡人卡片保管不善、将卡片转借他人或自身使用不当而造成的损失（包括借记账户和电子现金账户），由持卡人本人承担。

借记卡持卡人委托他人代为办理业务的，须符合本行相关业务的代办规定。

第十六条 借记卡如有遗失，持卡人应及时前往本行营业网点办理口头挂失、书面挂失或拨打本行客服电话办理口

头挂失。书面挂失为正式挂失，办理时需按本行规定标准缴纳挂失手续费。口头挂失自挂失日起5日后自动解挂(社会保障卡口头挂失即视为正式挂失），口头挂失失效后，因持卡人未及时办理书面挂失而产生的损失，本行不承担任何责任。书面挂失后如需补办新卡，可凭本人有效身份证件办理补办手续，办理时需按本行规定标准缴纳工本费。

持卡人遗忘密码，应凭本人有效身份证件和借记卡向本行书面申请办理密码重置手续。

第十七条 持卡人凭借记卡密码进行交易时，对同一张借记卡同一日内在各种交易渠道连续三次借记卡密码输入错误，该借记卡即被锁定，且不会自动解锁。持卡人须持本人有效身份证件到本行任一网点申请解除密码锁定或密码挂失。

第十八条 持卡人凭借记卡在自助机具上办理业务遇到吞卡时，可按该自助机具所属银行的规定到指定网点办理领回手续。逾期未领的，自助机具所属银行有权按规定程序处理被吞卡片，持卡人应及时凭本人有效身份证件办理挂失补卡手续。

第十九条 本行根据国家相关法律、法规和规章制定借记卡服务收费项目和收费标准。收费项目和收费标准可在营业网点、网站等渠道查询。持卡人须按规定的收费项目、

收费标准和缴费方式缴纳相关费用。借记卡收费项目、收费标准如有变动，以本行最新公布为准。

第二十条 持卡人可将本人借记卡（部分特殊卡种除外）开通快捷支付、商业委托支付（自动扣款）等网络支付业务。持卡人授权发卡银行直接根据第三方支付机构、银行卡组织或商业机构的指令进行网络支付业务签约、解约、资金扣划等操作。

持卡人知悉在与第三方支付机构、银行卡组织及商业机构建立关联业务时，姓名、证件号码、借记卡卡号、手机号码等个人信息可能被其采集、保存和使用，持卡人应审慎建立关联业务，妥善保管个人信息、借记卡密码、支付交易密码（不要将借记卡密码与支付密码设置为相同的密码），及指纹、人脸等个人生物特征信息、短信验证码等其他验证信息、手机号码、开户资料，以及手机等移动设备。

因持卡人泄露相关信息、遗失移动设备或遗失账户安全认证工具等自身原因，或第三方支付机构、银行卡组织及商业机构导致的交易争议由持卡人与支付机构协商解决。

持卡人与商户、第三方支付机构等发生的任何交易纠纷均应由双方自行解决，本行不承担责任，持卡人不可以以此为由拒绝向本行支付交易款项。

第二十一条 磁条借记卡不设有效期，芯片借记卡设置有效期，有效期最长为 10 年。借记卡功能升级、卡片损坏或到期，持卡人应持本人有效身份证件和借记卡，到本行营业网点凭密码办理换卡手续。申请换卡需按本行规定标准缴纳换卡工本费。换卡后本行必须收回原卡片。

芯片借记卡有效期满后，部分功能将无法正常使用，在有效期届满前，持卡人应及时办理换卡手续，本行将积极协助持卡人办理借记卡换领卡事宜。

第二十二条 持卡人终止使用借记卡，应持本人有效身份证件和借记卡，到本行营业网点支付有关欠费（如有）后，凭密码办理销卡手续（持卡人办理未激活卡片挂失销卡的，提供本人有效身份证件办理，无需密码）。本行受理持卡人销户申请后按有关业务规定为持卡人办理销卡，销卡后本行必须收回原卡片。

第二十三条 本行依据中国人民银行规定，加强借记卡账户交易活动监测，对开户之日起 6 个月内无交易记录的借记卡账户暂停其非柜面业务，持卡人需到本行营业网点重新核实身份后，恢复其业务。

第二十四条 本行依据国家外汇管理局规定，对持卡人境外提取现金进行限额管理。持卡人在境外提取现金，每卡每日累计限额不超过等值 1 万元人民币，本人名下境内各银行所有银行卡（含附属卡）合计每个自然年度不得超过

等值10万元人民币。超过年度额度的，持卡人本年及次年将被暂停持境内银行卡在境外提取现金。

第二十五条 按照中国银联业务规则，本行发行的带有“闪付”或“QuickPass”标识的银联标准借记IC卡支持开通免密码免签名小额快速支付服务。本行对小额免密免签服务实施限额管理，单笔限额1000元，单日累计限额3000元。持卡人可根据风险偏好和实际需要在开卡时自行选择是否开通本服务，开通后可通过本行营业网点、手机银行、网上银行或客服电话渠道查询、关闭此项服务。

第二十六条 持卡人涉嫌洗钱、恐怖融资或其他违法活动，或被列入国际组织、中国或其他国家发布的制裁名单或制裁范围，或违反相关法律法规、监管规定或本章程规定，本行有权终止其用卡权利，并可授权有关单位收回其借记卡。

第二十七条 伪造、变造借记卡或冒用他人借记卡进行诈骗活动者，依法追究刑事责任。

第二十八条 根据国家法律法规规定或我国政府签署的国际协议或出于本行向持卡人提供借记卡相关服务、保障持卡人账户资金安全目的的需要，持卡人授权同意本行在依法合规的前提下，收集、存储、使用等处理持卡人办理本业务过程中提供或因使用服务而产生的与处理目的直接相关的个人信息。

本行承诺将严格遵守法律法规、监管部门规定，合法合规收集、存储、查询和使用持卡人信息，不泄露、篡改、毁损持卡人信息，通过专业技术手段采取加密储存与传输等保障持卡人个人信息安全，不出售或者非法向他人提供持卡人信息，不收集、查询、使用与所提供服务或办理业务无关的持卡人信息，不违反法律法规的规定和各方的约定收集、查询、使用持卡人信息。

本行依法对持卡人的信息承担保密义务，未经当事人同意不得向任何单位或个人披露，但法律法规、规章、金融监管机构另有规定及与持卡人另有约定的除外。

第二十九条 本行有权依照法律法规、监管规定协助国家司法机关或其他有权机关对持卡人的借记卡账户进行查询、冻结和扣划。

第三十条 因不可抗力或供电、通讯等客观原因导致持卡人借记卡暂时无法使用的，本行将视情况协助持卡人解决问题或提供必要的帮助，但不承担相关责任。

第三十一条 本章程由天津银行负责制定、修改和解释。本行有权根据国家法律和有关规定及业务发展、系统升级等需要修改本章程，并通过本行网站或营业网点等进行公告。公告满 10 个自然日后，修改后的章程即为生效。公告期内，如持卡人有异议，有权选择销卡，如持卡人继续使用借记卡及相关服务，即视为同意并接受该变更或修

订。

第三十二条 本章程未尽事宜，按照国家有关法律法规和监管规定执行。

第三十三条 如持卡人在使用借记卡过程中产生相关问题，可向本行 956056 客户服务中心或当地营业网点咨询。

第三十四条 本章程自公告期满后正式施行，原《天津银行个人借记卡章程》同时废止。

天津银行股份有限公司

附件 1-1-2

天津银行电子银行个人客户服务协议

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， **天津银行电子银行个人客户服务申请人**（以下简称“甲方”）与 **天津银行股份有限公司**（以下简称“乙方”）就天津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:

电子银行服务: 指乙方借助国际互联网、公共通讯、电话集成线路等方式为甲方提供的支付结算服务、客户理财服务及信息类服务。根据服务渠道的不同，可分为网上银行服务、手机银行服务、微信银行服务等。

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信息要素，如**客户号（用户昵称、证件号码等）、密码、电子证书、USB Key、动态口令、签约手机号码**等。

密码: 指甲方在电子银行服务中使用的各种密码，如**登录密码、交易密码、账户密码、短信验证码**等。

交易指令：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。

错误：指乙方未能执行、未能及时执行或未能正确执行甲方交易指令的情况。

第二条 电子银行服务的开通及服务内容

（一）网上银行服务的开通及服务内容

甲方通过乙方网站登记甲方个人基本信息及账户信息，并按照要求完成其他相关操作后，自助开通网上银行，成为网上银行的大众版客户。大众版客户可享受的服务包括：查询、本人账户互转等服务。甲方到乙方柜台或智能设备签约，成为网上银行的专业版客户。专业版客户可享受的服务包括：查询、转账、网上支付、缴费、证券基金业务、外汇业务、贵金属业务、信用卡、贷款业务等金融交易服务和信息服务，专业版客户还可申请开通或变更其他网上银行所提供的功能。

（二）手机银行服务的开通及服务内容

甲方通过网上银行、手机等途径登记甲方个人基本信息及账户信息，并按照要求完成其他相关操作后，自助开通手机银行，成为手机银行的大众版客户。大众版客户可享受的服务包括：账户查询、本人账户互转、信用卡查询、理财购买等服务。甲方可在乙方柜台或智能设备签约，成为手机银行的专业版客户；甲方为网上银行专业版客户的，也可通过

网上银行进行手机银行签约，成为手机银行的专业版客户。专业版客户可享受的服务包括：查询、转账、缴费、基金业务、外汇业务、信用卡、生活圈、贷款、开通微银行等服务，专业版客户还可申请开通或变更其他手机银行所提供的功能。

（三）微银行的开通及服务内容

甲方通过手机银行、天津银行微银行公众号等途径登记甲方个人基本信息及账户信息，并按照要求完成其他相关操作后，成为微银行客户。微银行客户可享受的服务包括：余额查询、理财查询、交易提醒、生活频道等服务及其他微银行提供的服务。

（四）客户享受上述电子银行服务还须具备相关电子设备、能接入相应电子银行系统的网络等前提条件。

第三条 甲方主要权利与义务

一、主要权利

（一）甲方申请开通相应电子银行服务后，有权依本协议享受乙方提供的服务。

（二）甲方有权在本协议有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，有权在乙方规定的时限内到乙方营业网点补登存折或补打交易凭证。

二、主要义务

（一）**甲方办理网上银行业务应直接登录乙方网站（网址：http://www.bankoftianjin.com），**而不要通过邮件或其他网站提供的链接登录。

（二）**甲方在享受乙方提供的电子银行服务时，应当遵守本协议以及乙方不定期通过网点、网站或电子银行等渠道公布的相关业务规则等要求，但乙方有特殊要求的除外。**

（三）甲方应保证其提供的个人资料（如手机号码、证件信息等）的真实、完整、有效，**提供的手机号码应归本人所有。**如有变更，应及时书面通知乙方并按照乙方要求办理变更手续，通过乙方电子银行服务渠道能够更改的个人资料，甲方可自行通过电子银行服务渠道变更，因甲方个人资料不真实、不正确、不完整等原因而发生的风险和责任由甲方承担。

（四）甲方不得通过电子银行渠道发送违法的、与交易无关的或破坏性的信息，不得干扰乙方电子银行系统的正常进行。

（五）甲方身份认证要素（具体内容请见本协议第一条的相关规定）是乙方在提供电子银行服务过程中识别甲方身份真实性的依据，甲方必须妥善保管，不得将身份认证要素提供给任何第三方（包括乙方工作人员） 或交于任何第三方（包括乙方工作人员）使用。**使用上述身份认证要素发出的交易指令或完成的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。**

（六）如甲方的身份认证要素（具体内容请见本协议第一条的相关规定）发生遗失、被盗、遗忘或怀疑已被他人知悉、盗用等可能导致甲方账户安全性降低的情形，甲方应立即对账户进行挂失或对相关电子银行渠道进行暂停，**在挂失或暂停生效之前发生的损失均由甲方承担**。

（七）**甲方知悉：甲方在移动运营商的手机号码销号并不会终止已开通的手机银行服务；甲方如需终止相关电子银行服务，应通过乙方任意网点或线上渠道办理。甲方手机号码销号或变更，但相关电子银行业务未及时终止或变更所产生的风险和损失由甲方承担。**

（八）甲方发出的指令经乙方执行后，甲方不得要求变更或撤销。甲方发现账户变动与本人的实际交易操作不符的，甲方应自发生该种不符后 15 日内向乙方作出书面错误通知并应说明错误发生的可能原因、有关的账号、金额等情况。对甲方发出的错误通知，乙方将及时受理并进行调查。如乙方认为错误确已发生并系乙方的原因，乙方将及时对错误加以纠正。

（九）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，防止身份认证要素（具体内容请见本协议第一条的相关规定）被盗或泄漏；甲方同时应尽到合理注意义务，在安全的环境使用相关电子银行渠道。对于自设密码，甲方应设置安全性较高的密码，避免使用简单易记的密码或

容易被他人猜到的密码。对于申请开通电子银行服务时受技术条件限制只能设置数字密码的，甲方应于开通电子银行服务后及时将其更换为安全性更高的密码。

（十）甲方应当按照乙方公布的电子银行个人客户服务收费项目及标准支付相关费用。

第四条 乙方主要权利与义务

一、主要权利

（一）为不断改进电子银行服务，提高服务的安全性、可靠性、方便性，乙方有权定期或不定期对电子银行系统进行维护、升级和改造。

（二）为保障甲方资金安全，乙方有权根据客户类别、身份认证措施、交易风险度等因素的不同设定不同的安全策略，不同安全策略对于客户身份认证措施、交易限额、操作流程等可能有不同要求，甲方应当遵守。乙方对安全策略进行调整并涉及客户权利义务变更的，应当通过网点、网站或电子银行等渠道公布或按照本协议约定予以公告。

（三）乙方有权按照所公布的电子银行个人客户服务收费项目及标准从甲方在天津银行开立的账户中扣收相关费用。已收取的费用在相关电子服务渠道终止、本协议变更或终止等情形下均不予退还。

（四）乙方有权依据国家有关规定及业务需要对服务内容、收费项目或标准和业务规则等内容进行调整，涉及收费或其

他客户权利义务变更的调整，将通过官方网站、APP、微银行等渠道正式对外公告，公告一定时期后执行并适用于本协议，不再逐一通知每位用户；如有需要，乙方将在公告前报经有关金融监管部门核准或备案；甲方有权在乙方公告期间选择是否继续使用电子银行相关服务，如果甲方不愿接受乙方公告内容的，可在乙方公告施行前向乙方申请变更或终止相关服务。如果甲方未申请变更或终止相关服务，视为甲方同意相关调整，变更后的内容对甲方产生法律约束力，若甲方不执行变更后的内容，乙方有权选择终止本服务。

（五）在乙方为甲方办理本协议项下相关事项所必需的情形下，甲方同意并授权乙方向乙方集团成员（包括乙方境内全资子公司、控股子公司）、服务机构及其他乙方认为必要的业务合作机构提供乙方获取 的甲方个人信息。乙方会向甲方告知共享或转让个人信息的目的、数据接收方的类型，并征得甲方的授权同意。涉及敏感信息的，乙方还会告知甲方敏感信息的类型、数据接收方的身份和数据安全能力，并征得甲方的明示授权同意。

（六）对于因下列原因所导致错误的发生，乙方不承担责任。

1.甲方账户余额或信用额度不足；

2.账户内资金被法定有权机构冻结或扣划；

3.甲方的行为出于欺诈等恶意目的；

4.乙方收到的交易指令不符合要求或缺乏必要的交易信息；

5.甲方未能正确依据电子银行服务的说明操作;

6.因移动运营商原因造成甲方迟收或未收到我行短信通知。

二、主要义务

（一）乙方应及时受理甲方相关电子银行服务的申请，经审查符合条件的，应及时为甲方办理相关手续、提供相应服务。

（二）对于甲方就相关业务规则的咨询，乙方应及时予以解答或向其提供查询渠道。

（三）乙方应对甲方资料进行保密，但法律法规及金融监管机构另有规定或甲方与乙方另有约定的除外。

（四）乙方根据服务项目或服务内容，对服务价格、优惠措施及其生效和终止日期、与价格相关的例外条款和限制性条款、咨询（投诉）的联系方式等信息通过乙方网点、网站等渠道以公告的方式向甲方明示。乙方亦对相关业务规则等要求通过上述渠道以公告的方式向甲方明示。 乙方公告内容构成本协议不可分割的一部分，与本协议具有同等效力。甲方应在充分知晓、理解有关公告内容后签署本协议。

（五）在乙方系统正常运行的情况下，乙方应向甲方提供甲方所申请的相应电子银行服务（部分服务须经甲方另行开通方能享受的，待甲方开通后乙方予以提供），并有义务及时准确地执行甲方的交易指令。

第五条　协议的生效、变更、中止和终止

（一）甲方通过网上银行、手机、微信公众号等自助渠道申请电子银行服务的，本协议自甲方通过自助渠道系统开通电子银行服务时生效；甲方通过乙方柜台申请电子银行服务的，本协议自乙方同意其申请并在乙方系统中设置成功后生效。

（二）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。

（三）甲方通过网上银行、手机、微信公众号等自助渠道终止电子银行服务的，本协议自甲方终止指令进入乙方系统时终止。甲方通过乙方柜台终止电子银行服务的，本协议自乙方同意其终止申请并在乙方系统中设置成功后终止。

（四）甲方不遵守本协议或存在其他侵害乙方合法权益的行为时，乙方有权终止本协议。

（五）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。

（六）本协议部分条款无效，不影响其他条款的效力。

第六条 其他约定事项

（一）乙方不介入甲方与第三方之间的交易纠纷，但可在法律法规允许的范围内协助甲方查明交易情况。

（二）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。

（三）因不可抗力（包括但不限于乙方不能预见、不能避免并不能克服的战争、暴动、严重火灾、水灾、台风、地震、政府行为、禁令、或供电、通讯、黑客攻击等客观情况）导致乙方不能按本协议履约的，根据不可抗力的影响，乙方部分或全部免除责任。

（四）甲方选择使用微银行动账通知服务的，甲方知晓微银行动账通知服务不是获取账户变动情况的唯一渠道，还可通过乙方其他电子银行和网点等服务渠道查询。

（五）如非特别指明，本协议条款均适用于网上银行客户、手机银行客户、微信银行客户。

（六）本协议未尽事宜均依据中华人民共和国法律、行政法规、人民银行及银行业监督机关的有关规章、政策规定及金融业的行业惯例办理。

（七）本合同项下的价款和价外费用均为包含增值税的含税价，但当事人另有约定的除外。

第七条 协议的适用法律及争议解决方式

（一）本协议适用中华人民共和国法律。

（二）凡因本协议引起的或与本协议有关的任何争议，应通过协商解决；协商不成的，任何一方均可向乙方住所地人民法院提起诉讼。

第八条 如何联系我行

如您对本服务协议有任何疑问、意见或建议，可以通过拨打我行 956056 客服热线或到我行各营业网点咨询反映。受理您的问题后，我们会及时、妥善处理。一般情况下，我们将在 15 个工作日内给予答复。

我行全称：天津银行股份有限公司，注册地址：中国天津市河西区友谊路 15 号，邮编 300201。

第九条 营业执照信息

名　　称：天津银行股份有限公司

类　　型：股份有限公司（上市）

成立日期：1996 年 11 月 6 日

注册地址：天津市河西区友谊路 15 号

邮政编码：300201

法定代表人：于建忠

统一社会信用代码：91120000103070298 4

金融许可证机构编码：B0108H212000001

经营范围：吸收公众存款；发放短期、中期和长期贷款；办理国内外结算；办理票据承兑与贴现；发行金融债券；代

理发行、代理兑付、承销政府债券；买卖政府债券、金融债券；从事同业拆借；从事银行卡业务；提供信用证服务及担保；代理收付款项及代理保险业务；提供保管箱服务；证券投资基金销售业务；客户交易结算资金法人存管银行业务；外汇存款、外汇贷款；外汇汇款、外币兑换；结汇、售汇；同业外汇拆借；外汇担保；外汇借款；外汇票据的承兑和贴现；资信调查、咨询、见证业务。买卖和代理买卖股票以外的外币有价证券；买卖、代理买卖外汇；经国务院银行业监督管理机构监管机构批准的其他业务。（以上范围内国家有专营专项规定的按规定办理）。

附件 1-1-3

天津银行电子渠道隐私政策

版本发布日期：2024 年 8 月 27 日

版本生效日期：2024 年 8 月 27 日

摘要

本隐私政策根据《个人信息保护法》制定，适用于使用天津银行个人电子银行的用户。天津银行股份有限公司（以下简称“我行”）深知个人信息对您的重要性，会尽力保护您的个人信息安全，并尽力采用通俗易懂的文字表述向您进行说明和告知。**如果您主动勾选，点击“同意”即视为您同意本隐私政策并授权我行按照本隐私政策规定处理您的个人信息。**

一、常用业务功能收集的个人信息种类

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（姓名、性别、国籍、职业、住址）、身份信息（证件类型、证件号码）、财产信息（银行卡信息、交易信息、订单基本信息）、通信信息（电话号码、位置）、生物识别信息（指纹、人脸图像）、手机**

号码信息，以帮助您完成电子银行注册。

2.当您使用转账汇款、手机号转账功能时，您可能需要提供**收款方的手机号码、姓名、银行卡卡号/账号、开户银行、资金用途信息**，并可能需要提供您的**姓名、手机号码、证件类型、证件号码及指纹/刷脸验证信息**，以便于验证身份及使用上述功能的支付服务。

3.当您使用“II/III 类账户”提供的实名认证服务时，我行需要您提供您的**姓名、性别、国籍、职业、地址、联系方式、证件类型、证件号码、证件有效期、银行卡号/账号、刷脸认证、证件影像信息。**如您不提供上述信息，您将无法使用该功能。

二、我行对外提供您个人信息的主要场景

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。

三、您行使权力的主要途径

1.您可以通过手机银行“我的-设置-个人信息与权限-系统权限”撤销系统权限。

2.您可以通过手机银行“我的-设置-个人信息与权限-隐私管理”撤回个人信息授权，撤销同意后将强制退出天津银行APP。

3.您可以通过手机银行“我的-设置-安全中心-注销”自助完成注销。

四、您投诉举报的主要渠道

如您对本隐私政策有任何疑问、意见建议或投诉举报，可以通过拨打我行956056客服热线或到我行各营业网点咨询反映。受理您的问题后，我们会及时、妥善处理。一般情况下，我们将在15天内完成受理并处理。如您对我们的回复不满意，特别是我们的个人信息处理行为损害了您的合法权益，您还可以通过向被告所在地人民法院提起诉讼或向中央网信办举报。

五、其他需要您关注的事项

本摘要是对本隐私政策的重点说明，为便于理解，仅向您展现可能会对您的个人权益产生影响的重点内容，但为保障您的个人权益，仍请您阅读下方隐私政策正文。

隐私政策正文：

天津银行股份有限公司（“我行”）尊重并保护所有用户的个人隐私权，深知个人信息对您的重要性，并将以高度谨慎的态度对待用户信息，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、最少够用原则、确保安全原则、主体参与原则、公开透明原则，同时，我行承诺，我们将按业界成熟的安全标准，采取相应的安全保护措施尽全力保护您的个人信息安全。

根据《常见类型移动互联网应用程序必要个人信息范围规定》天津银行 APP 属于手机银行类，基本功能服务为通过手机进行银行账户管理、信息查询、转账汇款服务，需要收集注册用户移动电话号码，用户姓名、证件类型和号码证件有效期限、证件影印件、银行卡号码、银行预留移动电话号码，转账时需提供收款人姓名、银行卡号码、开户银行信息方可使用基本功能服务。

【特别提示】请您仔细阅读本隐私政策，确保对其内容及相应法律后果已全部知晓并充分理解。对本政策中与您的权益存在重大关系的条款和个人敏感信息，我行采用粗体字进行标注以提示您注意。如您点击或勾选“同意”并确认提交，或继续使用我行的产品（或服务），即视为您同意本隐私政策,并同意我行将按照本政策来收集、使用、存储和共享您的相关信息。如您不同意政策中的任何条款，应立即停止使用相应产品服务、注销相关的用户，我行将停止收集您的相关个人信息。

本隐私协议新增内容:

1.删除飞天蓝牙、巨量引擎转化、友盟统计分析 SDK 的

描述

2.增加 APP 运动权限的描述

3.修改留存个人信息的描述

4.修改个人信息管理的路径

本隐私政策概述:

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.我行如何存储和保护您的个人信息

4.我行如何共享、转让和公开披露您的个人信息

5.您控制个人信息的权利

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

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与已识别或可识别的自然人有关的各种信息。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（指纹、人脸图像）、通信通讯联系方式、住址、账户信息、财产状况（银行卡信息、交易信息、订单基本信息）、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（指纹、人脸图像）、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）信息如何收集

为向您提供服务并确保您的电子银行服务（网上银行端、手机银行客户端、微信银行、微信小程序、网上支付）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（姓名、性别、国籍、职业、住址）、身份信息（证件类型、证件号码）、财产信息（银行卡信息、交易信息、订单基本信息）、通信信息（电话号码、位置）、生物识别信息（指纹、人脸图像）、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的服务。

您在使用个人手机银行时，已收集的个人信息可在手机银行“我的-设置-个人信息收集清单”中查看。

2.当您使用电子银行功能时，您可能在下列情况下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电子银行的其他功能或服务。

（1）如您在手机银行客户端中选择通过指纹、刷脸功能进行登录、转账、支付、身份认证（基本业务功能）、办理数字人民币，需向我行提供您的**指纹、人脸图像**信息。您可以通过手机银行客户端“安全中心”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的人脸信息将加密存储于我行信息系统中。如您不提供上述信息，我行将无法向您提供需完成指纹、人脸认证后方可使用的产品或服务。

对于手机终端自身的本地生物特征认证功能，指纹识别、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。

（2）当您使用手机银行客户端向手机号转账（移动、电信及联通手机号）、汇款短信通知、向朋友付款、缴话费涉及通讯录的功能时，**我行仅获取您从通讯录中选择的联系人姓名和手机号，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，如您拒绝提供该信息，仅会使您无法使用上述功能，将不会影响您正常使用手机银行客户端的其他功能。

（3）当您使用转账汇款、手机号转账功能（基本业务功能）时，您可能需要提供**收款方的手机号码、姓名、银行**

卡卡号/账号、开户银行、资金用途信息，并可能需要提供您的**姓名、手机号码、证件类型、证件号码及指纹/刷脸验证信息**，以便于验证身份及使用上述功能的支付服务。此外，我行还会收集您的相关**收付款交易记录**以便于您查询。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手机银行客户端的其他功能。

（4）当您使用手机银行客户端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（IMEI、MAC 地址、设备名称、Android ID、设备型号、操作系统和应用程序版本）、指纹认证、刷脸认证信息，我行还可能通过验证账号/卡密码、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。

（5）当您使用“II/III 类账户”（基本业务功能）提供的实名认证服务时，我行需要您提供您的**姓名、性别、国籍、职业、地址、联系方式、证件类型、证件号码、证件有效期、银行卡号/账号、刷脸认证、证件影像信息。**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）当您使用基于地理位置的功能（扩展业务功能）时，我行手机银行通过客户端嵌入高德地图 SDK 的方式收集

您的位置信息，包括省、市、区、经纬度、OAID、旋转矢量传感器、获取外置存储权限、IMSI，目的是为了向您提供所在位置的附近网点信息。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。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手机银行客户端的其他功能。

（7）当您通过手机银行客户端进行信息管理（基本业务功能）时，我行可能会验证您的**原登录密码、签约手机号短信验证码、生物特征。**您可以通过手机银行客户端“安全中心”解除设备绑定。

（8）当您使用金信通、微信银行动账提醒、天津银行APP 动账提醒服务（扩展业务功能）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。

（9）当您使用网上银行、手机银行客户端服务时，我行会收集您的**交易信息**，形成收款人名册，以简化您的转账操作；如您选择手机短信动态口令作为安全认证工具，我行将向您的签约手机号发送**手机短信动态口令**，用以网上银

行、手机银行客户端交易验证。

（10）为了给您更好的呈现您需要的商品或服务，我行可能会收集您使用我行产品或服务的**设备信息（包括设备名称、设备型号、操作系统和应用程序版本、语言设置、分辨率、服务提供商网络 ID（PLMN））、浏览器类型和版本**来为您提供商品信息展示的最优方式。

（11）当您操作头像修改、扫一扫、电子回单保存、生成二维码保存、协议及说明书保存（理财、保险、存单、贷款、信用卡产品）、开立电子账户、自助注册业务及静态资源文件（html、js、图片）（扩展业务功能）时，可能会用到**外置存储权限**。如您不同意外置存储权限，可能将影响部分功能、服务的使用。

3.当您使用电子银行服务时，为了维护服务的正常运行，保障您的账号安全，我行可能会收集以下基础信息，包括您的**设备型号、版本、Cookie、操作系统、手机银行客户端软件版本号、登录 IP 地址、接入网络的方式、类型和状态、网络质量数据、设备加速器（重力感应设备）、操作日志、服务日志信息（您在手机银行客户端搜索、查看的信息、服务故障信息信息）、地理位置信息、WiFi 信息、BSSID、IDFV、应用安装列表、设备硬件序列号、Android ID、UUID、进程信息、MAC 地址、获取 SSID、磁场传感器、温度传感器、光传感器、陀螺仪传感器、加速度传感器、压力传感器行为、**

外置存储权限。如您不同意我行收集上述信息，可能将无法正常使用电子银行服务或影响部分功能、服务的使用。

4.当您注册/登录微信小程序时，您可能需要提供您的手机号码、登录密码、unionid、openid；当您使用微信小程序转账功能时，您可能需要提供您的姓名、银行卡卡号/账号、开户银行、资金用途信息、手机号码、证件类型、证件号码；当您使用微信小程序网点服务时，您可能需要提供位置信息；当您使用微信小程序进行信息管理时，我行会收集您的登录密码、原登录密码。

5.为防范交易风险，我行会收集您主动发起的反馈意见、建议或举报时提供的信息，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。

6.当您首次安装运行天津银行 APP 时，弹窗提示用户同意隐私政策（含使用 sdk 权限），若您同意，则可进行后续流程，若您不同意，则弹出弹窗提示您需要同意隐私政策才能继续使用手机银行。

7.当您使用天津银行 APP 的功能或服务时，在某些特定使用场景下，我行可能会使用具有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，由第三方服务商收集您的必要信息。具体包括以下几种：

第三方SDK名称	所属公司名字	收集目的	场景描述	收集方式	个人信息收集范围	第三方隐私政策链接
通付盾设备指纹SDK	通付盾科技有限公司	向您提供手机设备指纹服务	用于指纹登录、指纹支付功能	调用系统相关接口自动采集，用户主动提供	设备的Mac地址、唯一标识码（IMEI/android ID/SIM卡IMSI信息）、应用安装列表和地理位置信息	https://cloud.tongfudun.com/#/user/serviceFingerPrint/serviceFingerPrint
银联SDK（Android HCE）	中国银联股份有限公司	向您提供银联支付的服务	用于集成银联HCE、无卡支付功能	调用系统相关接口自动采集，用户主动提供	手机终端唯一标志信息（IMEI、IMSI）、个人信息（姓名、**证件类型、证件号码、银行卡信息**）、Android ID、设备硬件序列号	http://www.unionpayintl.com/cn/privacyNotice/
云之眼身份认证SDK	云从科技	向您提供身份认证服务	用于身份活体检测、身份证上传功能	调用系统相关接口自动采集，用户主动提供	手机终端拍照、存储、个人信息(姓名、**证件类型**、**证件号码**)	https://www.cloudwalk.com/Terms
云证通SDK	中金金融认证中心有限公司	云证通电子签名服务、增强交易认证	用于资金安全交易认证、身份认证功能	调用系统相关接口自动采集，用户主动提供	手机终端唯一标志（IMEI号）、个人信息（姓名、**证件类型**、**证件号码**、**银行卡信息**）	https://www.cfca.com.cn/upload/20211117flsm.pdf
电子社保SDK	人力资源和社会保障部信息中心	向您提供电子社保卡功能	用于在客户端申请电子社保凭证	调用系统相关接口自动采集，用户主动提供	手机终端唯一标志信息（IMEI号）、个人信息（姓名、**证件类型**、**证件号码**、**银行卡信息**）、运行环境物理信息、地理位	

					置信息、Android ID、注册动态广播、获取设备传感器信息	
Mob 分享 SDK	Mob Tech 袤博科技	该 SDK 集合了新浪微博 SDK、腾讯移动开放平台 SDK 及 ShareSDK，便于您使用分享功能	用于实现一键分享功能	调用系统相关接口自动采集，用户主动提供	系统运行信息、网络状态信、设备标识信息中的一个或多个：iOS 广告标识符（IDFA）、国际移动设备识别码（IMEI）、匿名设备标识符(OAID)、国际移动用户识别码（IMSI）、SIM 卡识别码（ICCID）（仅在秒验产品中收集）、SIM 卡序列号（仅 2022 年 3 月份之前的版本收集）、Android ID(仅 2022 年 3 月份之前的版本收集）、Serial Number（仅 2022 年 3 月份之前的版本收集）、基站信息、地理位置信息、应用列表信息	https://www.mob.com/about/policy
高德地图定位 SDK	高德	向您提供基于位置服务	用于实现定位功能及基于位置服务的相关功能	调用系统相关接口自动采集，用户主动提供	手机设备信息，（包括 IMEI、IDFA、Android ID、MEID、MAC 地址、OAID、IMSI）、硬件	https://lbs.amap.com/pages/privacy/

					序列号、经纬度信息、SSID、BSSID、WIFI信息、设备传感器-旋转矢量传感器、获取应用安装列表、外置存储权限、设备传感器-压力传感器、获取IP、设备传感器-加速度传感器、获取指定包名信息、监听设备小区地理位置变更、注册动态广播、获取地理定位(监听)	
智能语音交互SDK	阿里云	向您提供语音文本识别服务	用于实现语音识别功能	调用系统相关接口自动采集，用户主动提供	手机终端语音信息	http://terms.aliyun.com/legal-agreement/terms/suit_bu1_ali_cloud/suit_bu1_ali_cloud20180228145l_77479.html?spm=a2c4g.11186623.0.0.27bd30e5QFVNfV
视频平台SDK	天津银行股份有限公司	向您提供视频平台服务	用于您在视频平台中的业务办理、身份认证	调用系统相关接口自动采集，用户主动提供	获取您的手机终端摄像头、麦克风及定位权限、个人信息（姓名、**证件类型**、**证件号码**、联系电话）	https://help.aliyun.com/document_detail/169836.html

个推 SDK	每日互动股份有限公司	为了向您提供消息推送功能，我们使用了个推 SDK,该 SDK 集成了华为推送 SDK、小米推送 SDK、魅族推送 SDK、OPPO 推送 SDK、VIVO 推送 SDK	用于推送客户端消息、公告	调用系统相关接口自动采集，用户主动提供	手机终端唯一标志信息（IMEI 号）、GET_TASK 检索应用程序、外置存储权限、获取进程信息、网络信息及位置相关信息、应用名称、包名、存储权限、设备权限、注册动态广播	https://www.getui.com/privacy
Fido-SDK	中金金融认证中心有限公司	向您提供手机设备指纹服务	用于指纹登录、指纹支付功能	调用系统相关接口自动采集，用户主动提供	手机终端唯一标志信息（IMEI 号）、个人信息（姓名、**证件类型、证件号码、指纹信息、银行卡信息**）	https://www.cfca.com.cn/upload/20211117f1sm.pdf
恒宝-蓝牙 SDK	恒宝股份有限公司	增强交易认证	用于资金安全交易认证、身份认证功能	调用系统相关接口自动采集，用户主动提供	手机终端唯一标志信息（IMEI 号）、应用列表信息、网络信息及位置相关信息、个人信息（姓名、**证件类型、证件号码、银行卡信息**）	https://ps.hbgf.net.cn/Product/PrivacyPolicy/Hengbao-PrivacyPolicy(Update20220325).pdf
移动应用安全监测 SDK	北京梆梆安全科技有限公司	安全分析	用于判断天津银行 APP 所运行的手机设备的安全性，防止恶意的用户对天津银行 APP 进行	通过申请权限采集，用户主动提供	精确位置信息、粗略位置信息、WIFI-MAC，WIFI-SSID、IP 地址、IMEI、IMSI、AndroidID、软件列表、设备 MAC 地址、硬	https://everisker.com/Privacypolicy.pdf

			网络安全攻击，保护用户的财产安全		件序列号	
移动开发平台 mPaaS	蚂蚁云创数字科技（北京）有限公司	该 SDK 集合了支付宝 SDK（帮助用户使用支付宝支付功能和支付宝登录）、小米推送（向用户提供推送）、腾讯开放平台 SDK（帮助用户登录 QQ 账户并分享信息）、微信 SDK（用于微信分享和微信登录）、UC webview SDK(提供应用内 H5 性能问题定位分析服务)、UC 啄木鸟（提供线上质量监控以及异常定位分析服务）、WebRTC（实时音视频服	为应用提供安全开发框架	调用系统相关接口自动采集，用户主动提供	不可变更/可变更唯一设备标识码（Android ID、OAID、IMEI、IMSI、MAC 地址、设备序列号、硬件序列号、传感器硬件序列号、SIM 卡序列号、ICCID）、应用列表、基本设备信息(系统设置、系统属性、设备型号、设备品牌、操作系统）、网络信息（IP 地址、网络类型、运营商信息、WiFi 状态、WiFi 参数、WiFi 列表、MAC 地址）、精确位置信息、粗略位置信息、摄像头权限、电话权限、麦克风权限、相册权限、位置权限、粘贴板权限及通讯录权限	https://render.alipay.com/p/c/180021120000000340/index.html?agreementId=AG01000579

		务）				
微信开放平台	腾讯科技（深圳）有限公司	实现将内容分享到微信	用于将内容分享到微信	调用系统相关接口自动采集，用户主动提供。	设备信息（IMEI、Android ID、MAC 地址、IMSI）、剪贴板信息。	https://privacy.qq.com/
支付宝 SDK	支付宝（中国）网络技术有限公司	实现支付宝登录	用于支付宝登录	调用系统相关接口自动采集，用户主动提供	应用安装列表、BSSID、SSID、获取进程信息、存储权限	https://opendocs.alipay.com/open/0671id
支付宝支付 SDK	支付宝（中国）网络技术有限公司	实现支付宝支付	用于支付宝支付	调用系统相关接口自动采集，用户主动提供	获取摄像头权限、GET_TASK 检索应用程序、外置存储权限、注册动态广播、获取指定包名的应用信息、获取已安装的应用、获取剪切板数据、获取 SSID、获取 BSSID WIFI、获取地理定位(监听)、获取屏幕分辨率、获取 Android ID、获取已安装的应用、获取地理定位(经纬度)	https://opendocs.alipay.com/open/54/104509
小米推送	小米科技有限责任公司	实现消息推送服务	用于推送服务	调用系统相关接口自动采集，用户主动提供	设备标识、应用包名、版本号和运行状态、设备厂商、设备型号、小米推送 SDK 版本、设备内存、操作系统版本、设备归属地、SIM 卡运营商名称、当	http://dev.mi.com/console/doc/detail?Pid=1822

					前网络类型	
阿里设备标识 SDK	蚂蚁云创数字科技（北京）有限公司	该 SDK 集合了支付宝 SDK（帮助用户使用支付宝支付功能和支付宝登录）、小米推送（向用户提供推送）、腾讯开放平台 SDK（帮助用户登录 QQ 账户并分享信息）、微信 SDK（用于微信分享和微信登录）、UC webview SDK(提供应用内 H5 性能问题定位分析服务)、UC 啄木鸟（提供线上质量监控以及异常定位分析服务）、WebRTC（实时音视频服务）	为应用提供安全开发框架	调用系统相关接口自动采集，用户主动提供	不可变更/可变更唯一设备标识码（Android ID、OAID、IMEI、IMSI、MAC 地址、设备序列号、硬件序列号、传感器硬件序列号、SIM 卡序列号、ICCID）、应用列表、基本设备信息(系统设置、系统属性、设备型号、设备品牌、操作系统)、网络信息（IP 地址、网络类型、运营商信息、存储权限、WiFi 状态、WiFi 参数、WiFi 列表、MAC 地址）、精确位置信息、粗略位置信息、摄像头权限、电话权限、麦克风权限、相册权限、位置权限、粘贴板权限及通讯录权限、外置存储权限	https://render.alipay.com/p/c/180021120000000340/index.html?agreementId=AG01000579

umeng/Utdid	友盟	该SDK集合了新浪微博SDK、腾讯移动开放平台SDK及ShareSDK，便于您使用分享功能	用于实现一键分享功能	调用系统相关接口自动采集，用户主动提供	系统运行信息、网络状态信息、设备标识信息中的一个或多个：iOS广告标识符（IDFA）、国际移动设备识别码（IMEI）、匿名设备标识符(OAID)、国际移动用户识别码（IMSI）、SIM卡识别码（ICCID）（仅在秒验产品中收集）、SIM卡序列号（仅2022年3月份之前的版本收集）、Android ID(仅2022年3月份之前的版本收集）、Serial Number（仅2022年3月份之前的版本收集）、基站信息、地理位置信息、应用列表信息、外置存储权限	https://www.umeng.com/page/policy
新浪微博SDK	新浪网络技术股份有限公司	实现分享消息	用于消息分享到微博	调用系统相关接口自动采集，用户主动提供	手机终端唯一标识信息，手机型号、系统类型、系统版本、网络类型、设备列表信息、MAC地址、运营商信息	https://www.weibo.com/signup/v5/privacy
VIVOPUSH	维沃移动	实现天津	用于消息	调用系统	设备标识信	https://de

SDK	通信有限公司	银行 APP 离线消息推送功能，推送服务	推送	相关接口自动采集，用户主动提供	息、存储权限、设备信息（设备制造商、设备型号）网络相关信息（IP 地址、网络类型）国家码申请设备权限: 网络权限、外置存储权限	v.vivo.com.cn/wap/documentCenter/doc/652#w1-12075822
华为消息推送 SDK	华为软件技术有限公司	实现天津银行 APP 离线消息推送，推送服务	用于消息推送	调用系统相关接口自动采集，用户主动提供	手机终端唯一标志信息（IMEI 号）、应用列表信息、网络信息及位置相关信息、应用名称、包名、存储权限、设备权限	https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050042177
OPPO PUSH 客户端 SDK/GpushOPPO SDK	广东欢太科技有限公司	实现天津银行 APP 离线消息推送，推送服务	用于消息推送	调用系统相关接口自动采集，用户主动提供	设备标识信息（IMEI 或 OAID、Serial、Number、IMSI、UserID、AndroidID、GoogleAdvertising ID）、获取指定包名的应用信息	https://open.oppomobile.com/wiki/doc#id=10288
啄木鸟	广州市动景计算机科技有限公司	该 SDK 集合了支付宝 SDK（帮助用户使用支付宝支付功能和支付宝登录）、小米推送（向用户提供推送）、腾讯开放	为应用提供安全开发框架	调用系统相关接口自动采集，用户主动提供	不可变更/可变更唯一设备标识码（Android ID、OAID、IMEI、IMSI、MAC 地址、设备序列号、硬件序列号、传感器硬件序列号、SIM 卡序列号、ICCID）、应用列表	http://open-uc.uc.cn/agreement/secret

		平台 SDK（帮助用户登录 QQ 账户并分享信息）、微信 SDK（用于微信分享和微信登录）、UC webview SDK(提供应用内 H5 性能问题定位分析服务)、UC 啄木鸟（提供线上质量监控以及异常定位分析服务）、WebRTC（实时音视频服务）			、基本设备信息(系统设置、系统属性、设备型号、设备品牌、操作系统)、网络信息（IP 地址、网络类型、运营商信息、WiFi 状态、WiFi 参数、WiFi 列表、MAC 地址）、精确位置信息、粗略位置信息、摄像头权限、电话权限、麦克风权限、相册权限、位置权限、粘贴板权限及通讯录权限	
魅族消息推送	魅族通讯设备有限公司	实现天津银行 APP 推送服务	用于消息推送	调用系统相关接口自动采集，用户主动提供	手机终端唯一标识信息，手机型号、系统类型、系统版本、网络类型、设备列表信息、MAC 地址、运营商信息	https://i.flyme.cn/privacy
RxJavaFX	第三方组件				获取 IP、获取 Android ID、获取进程信息（低版本）、GET_TASK 检索应用程序、外置存储权限、注册动态广播	

微信三方登录 SDK	腾讯计算机系统有限公司及关联公司	集成微信账号登录	用于快速登录	调用系统相关接口自动采集，用户主动提供	从微信获取您授权共享的账户信息(头像、昵称、地区、性别)	http://support.weixin.qq.com/cgi-bin/mmsupportacctnodeweb-bin/pages/RYiYJkLOrQwu0nb8
爱加密威胁感知 sdk	北京智游网安科技有限公司	保障天津银行 APP 运行安全&业务安全开展，避免用户受到病毒木马攻击，另外为了准确识别恶意行为，该 sdk 包含了百度安全黑产挖掘 sdk。	在天津银行 APP 运行和业务开展过程提供安全保障。	天津银行 APP 初始化 SDK,SDK 通过自身逻辑调用系统的 API 获取	设备信息(设备型号、设备标识符、设备序列号、内存使用&电量剩余、CPU 信息、IMSI、AndroidId、蓝牙 MAC 地址、WiFi-BSSID、SSID、WiFi 信号强度、设备传感器-加速度传感器、设备传感器-陀螺仪传感器、设备传感器-光传感器、设备传感器-温度传感器)，应用信息(应用安装列表、应用包名、应用版本、安装&卸载时间、证书信息)，系统信息(平台、模型、系统版本、屏幕信息、dpi)，地理位置(基站编号、位置区域码、邻近基站信息、经纬度信息)，SIM 卡/	https://www.ijiami.cn/privacypolicy/privacypolicy.html

					网络信息(运营商、移动网络代码、移动国家代码、联网方式、网络请求、IP地址)	
神策数据	神策网络科技（北京）有限公司	基础数据收集与建模，驱动业务决策分析	用于收集数据、进行用户行为分析	调用系统相关接口自动采集，用户主动提供	应用安装列表、Android ID、MAC地址、OAID、获取手机运营商信息、IMEI、设备IP	https://manual.sensorsdata.cn/sa/latest/zh_cn/tech_sdk_client_privacy_policy-22255999.html
云闪付网络支付SDK	中国银联股份有限公司	提供开通网络支付、交易处理、交易信息查询、支付相关服务	用于支付相关服务	调用系统相关接口自动采集，用户主动提供	需要获取设备信息(Android ID、INSI、IMSI)、设备传感器、网络设备信息(MAC、网络访问模式、网络运营商、wifi-ssid、wifi-bssid、sim 卡型号、SIM卡-ICCID、SIM卡-MNC、SIM卡-MCC)、位置信息(经纬度坐标)、个人网络信息(IP地址)、应用程序信息(包括应用安装列表、应用包名、应用版本号、操作系统信息(正在运行进程列表、系统版本、系统语音、系统时区、系统	https://wallet.95516.com/s/wl/WebAPP/helpAgree/page/agreement/regPrivacy.html?cntryCode=86

					包名、系统关键文件))、个人基本资料(姓名、电话号码)、个人身份信息(**证件类型、证件号码**)、个人财产信息(**银行卡信息、交易信息、订单基本信息**)、获取访问网络、位置、相册、摄像头、电话、读写存储权限、网络权限使用频率:使用频率为触发相关业务时获取	
数美风控SDK	北京数美时代科技有限公司	提供在线业务风控解决方案	用于风险控制和反欺诈，以保障账户和交易安全	调用系统相关接口自动采集	获取地理定位、设备传感器信息、获取IP、获取SSID、获取Android ID、设备硬件序列号、WIFI信息	https://www.ishumei.com/legal/cn/privacy.html
Android.support.v4	Google	为应用提供安全开发框架	用于提供安全开发框架	调用系统相关接口自动采集	外置存储权限、注册动态广播、获取屏幕分辨率、打开摄像头、获取设备传感器信息、获取指定包名的应用信息	https://developer.android.google.cn/quality/privacy-and-security
org.chromium开源框架	Google	为应用提供安全开发框架	用于提供安全开发框架	调用系统相关接口自动采集	获取IP、注册动态广播、GET_TASK检索应用程序、外置存储权限、获取设备传感器信息、	https://www.chromium.org/Home/chromium-privacy/

爱奇艺 xcrash 崩溃监控	爱奇艺	支持捕获 native 崩溃和 Java 异常	用于天津银行 APP 异常、性能分析	调用系统相关接口自动采集	注册动态广播	https://github.com/iqiyi/xCrash

第三方共享个人信息清单可在手机银行“我的-设置-第三方信息共享清单”中查看。

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，但不影响您使用电子银行的其他功能。

8.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其他功能或服务:

（1）相机权限，用于手机银行注册、识别二维码、**人脸识别**、视频平台业务办理、设置头像、II/III 账户开通、办理数字人民币用途，在人脸识别登录/转账/支付/提升认证、扫一扫、头像设置、II/III 账户开通、办理数字人民币场景中使用。拒绝授权后，上述功能将无法使用。我行将获

取的人脸数据，加密后存储于我行信息系统中。

（2）相册权限，相册权限用于头像上传、银行卡扫描功能。如您拒绝授权后，上述功能可能无法正常使用。

（3）**麦克风**，用于语音导航、智能客服、视频平台业务办理用途。拒绝授权后，上述功能将无法使用。系统后台不留存声纹数据。

（4）**手机通讯录**，在转账、缴费过程中，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，上述服务仍可正常使用，但需要手工输入手机号码。我行仅读取并记录指定电话号码和姓名，不读取客户全量通讯录。

（5）**地理位置，获取您所在地理位置，包括省、市、区、经纬度，**主要用于摇一摇、网点预约、II/III 账户开户、视频平台业务办理、主题切换、电子银行交易风控及展现城市服务。通过获取您所在地理位置，我行可为您匹配最近的营业网点，便于您办理业务；当您未主动设置过地区主题时根据您所在的地理位置可自动切换地区主题。系统后台保存您交易时的位置信息。拒绝授权后，手机银行客户端相关功能无法使用。

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

（7）设备状态，用于确定设备识别码（IMEI、Android ID、IMSI），出于登录安全考虑，我行在您登录一台新设备时，会申请设备识别码（IMEI、Android ID、IMSI），并通过安全验证手段绑定此设备，以保证账号登录的安全性。如拒绝授权后，无法完成设备绑定，影响正常登录。

（8）存储权限，用于缓存您在使用天津银行 APP 过程中产生的文本、图像、视频内容。如您拒绝授权后，上述功能可能无法正常使用。

（9）蓝牙，用于通过蓝牙将客户手机与蓝牙 USBkey 连接并交互。拒绝授权后，无法通过蓝牙连接 USBkey，无法使用 USBkey 认证手段，但不影响其他方式的认证。我行系统后台不保存客户手机蓝牙配置信息。

（10）剪切板，用于转账快捷跳转功能，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，我行手机银行将不读取剪切板内容，则您无法使用上述功能。

（11）NFC，用于银联 HEC 场景中使用。如您拒绝授权 NFC 权限，将无法使用银联 HEC 功能。

（12）日历，用于提醒用户在日历中录入的个人安排信息。

（13）面容 ID，在天津银行 APP 运行过程中会被调用，用于面容登录，如您拒绝授权后，则您无法使用上述功能。

（14）悬浮窗，用于视频客服场景中，如您拒绝授权后，

您将无法使用视频通话悬浮功能。

(15)识别身体活动权限（安卓）用于天津银行线上马拉松活动，在活动中需要记录运动过程中步数信息，来展示用户的运动成绩。

(16)运动与健康权限(IOS)用于天津银行线上马拉松活动，在活动中需要记录运动过程中步数信息，来展示用户的运动成绩。

9.生物识别信息（指纹/人脸），为了让您更安全、便捷地使用登录、转账服务，如您的设备与天津银行 APP 版本均支持指纹或面容功能，您可选择开通指纹/面容登录或指纹/面容转账功能，通过在您的设备上完成指纹/面容验证进行登录、转账。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或转账。

10.为了应用程序的正常运行以及更好的为您提供服务，天津银行 APP 在运行时会读取应用列表以及运行中进程信息，此功能的主要目的是:

(1)进行安全检测，检测当前手机运行环境是否安全。

(2)获取安卓版本、安卓型号用于设备绑定。

(3)当需要导航时获取手机上安装的地图类 APP，以便于后面唤起对应地图 APP。

(4)当使用数字人民币时在需要的时候唤起数字人民币

APP。

(5)接收推送时检测天津银行 APP 运行情况。

(6)优化天津银行 APP 运行性能。

11.当您使用天津银行 APP 时，应用的推送功能会使用自启动服务，以便用户可以及时收到消息推送。如您想关掉此功能，可能导致无法正常使用消息推送功能。您可在“我的-设置-关于我们-消息通知”关闭消息推送功能。

12.天津银行 APP 在运行过程中，会获取 WiFi 网络信息 SSID、BSSID，以便获取您的地理位置为您提供区域化的服务。另外也会使用设备序列号、mac 地址、Android_ID 进行环境安全检测、风险识别，便于为您提供风险提示。

请您知悉，若您拒绝同意隐私政策，天津银行 APP 将无法获取上述信息，您将无法正常使用天津银行 APP。

上述功能可能需要您在您的设备中向我行开启您的相机（摄像头）、**地理位置（位置信息）**、麦克风、蓝牙的访问权限，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。

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。

个人信息与权限清单可在手机银行“我的-设置-个人信息与权限”中查看。

（二）信息如何使用

1.在向您提供我行金融产品及服务时，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.为了方便您实时、便捷的了解我行当前最新系统通知、系统公告，我行可能会向您的客户端推送消息，该消息不基于个性化推荐算法，不属于个性化推送通知。同时，为保障您接收信息的自主性，您可在手机系统设置-权限管理-关闭我行客户端的消息权限，关闭消息权限将影响客户端动账通知功能，不影响其他功能。

5.您授权同意的以及法律允许的其他用途。

（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.为订立、履行个人作为一方当事人的合同所必需，或者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;

2.为履行法定职责或者法定义务所必需;

3.为应对突发公共卫生事件，或者紧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《中华人民共和国个人信息保护法》规定在合理的范围内处理个人自行公开或者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。

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。Cookie 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篮内的商品数据。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，大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。

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。

我行遵守相关法律法规要求留存您的个人信息。

1.《中华人民共和国网络安全法》第二十一条第三款要求监测、记录网络运行状态、网络安全事件的技术措施的网络日志留存不得少于六个月;

2.《电子商务法》规定商品和服务信息、交易信息保存时间自交易完成之日起不少于三年。

3.为遵守法院判决、裁定或其他法律程序的规定;

我行仅在法律法规要求的时限及实现本政策声明的目的所必须的最短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：手机号码：当您需要使用手机银行客户端服务时，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，当您注销手机银行客户端账户后，我行将删除相应的信息；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。当您注销手机银行客户端账户后，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的形式向您进行告知，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 ISO27001 认证标准的要求。

4.我行将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、推送通知的方式告知您，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。

四、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.为实现隐私政策声明的目的，或为向您提供服务之必须，我行会按照本条第 2 款的约定与附属公司、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，且我行附属公司、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。同时，我行会与其签署保密协定，要求他们按照我行的说明、本隐私政策以及其他任何相关的保密和安全措施来处理个人信息。

4.我行会对合作方获取有关信息的应用程序接口（API）、软件工具开发包（SDK）进行严格的安全检测，并与合作方约定严格的数据保护措施，令其按照我行的服务说明、本隐私权政策以及其他任何相关的保密和安全措施来处理个人信息。

5. 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。

6.根据法律法规和商业惯例，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，否则我行将要求该公司、组织重新向您征求授权同意。

7.当您与我行在发生贷款或者担保类信用业务时，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。我行依法对您的相关信息承

担保密责任，并保证要求合作机构对您的相关信息承担保密责任。

8.我行会在您明示同意或主动签约的前提下，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。

9.为了您的账户资金、交易安全，我行在提供线上开户服务时，会向跨行账户信息认证服务平台提供您的手机号、姓名、证件号码、卡号信息，用于验证实名制信息。

（二）公开披露

1.我们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，我们可能会共享、转让、公开披露用户信息无需事先征得您授权同意:

1.为订立、履行个人作为一方当事人的合同所必需，或者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;

2.为履行法定职责或者法定义务所必需;

3.为应对突发公共卫生事件，或者紧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《中华人民共和国个人信息保护法》规定在合理的范围内处理个人自行公开或者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。

五、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

您有权通过我行国际互联网网站、网上银行、手机银行客户端、微信银行访问及更正、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.您登录手机银行客户端后，可以在“我的”-“设置”-“个人信息管理”中查询修改姓名、性别、证件类型、证件号码、证件有效期、联系电话、国家/地区、职业、地址;在“安全中心”中查询、修改您的安全设置; 在“账户查

询”、“账户管理”和“电子账户”功能中管理绑定的银行卡、开通 II/III 账户、他行卡服务。

2.您登录网上银行后，可以在“客户服务”、“自助签约”中，进行预留信息设置、支付签约、短信签约、安全设置、个人信息设置。

对于修改电子渠道签约/认证手机号信息，必须通过我行柜台或自助设备办理。

（二）删除您的个人信息

在以下情形中，您可以通过本政策“如何联系我行”所述途径向我行提出删除个人信息的请求，我行将在 15 日内完成受理并处理:

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，我行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。

（三）改变您授权同意的范围或撤回您的授权

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、相机权限，随时给予或撤回您的授权同意。您可在个人手机银行“我的-设置-个人信息与权限-系统权限”功能中撤回先前做出的系统权限授权同意，在“我的-设置-个人信息与权限-隐私管理-撤销隐私政策”撤回个人信息授权。在“我的-设置-个人信息与权限-授权管理”解除第三方应用的授权。

当您自主注销我行电子银行服务（网上银行服务、手机银行客户端服务、微信银行服务、网上支付服务）的同时，将视同您撤回了对我行该电子银行服务《隐私政策》的同意，我们将不再处理相应的个人信息，但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

如您为我行电子银行注册用户，登录手机银行客户端后，可通过手机银行-设置-安全中心-注销功能，自助完成注销。您也可以到网点通过我行柜面或自助设备渠道注销您的网上银行、手机银行客户端。**网上支付服务可在交易页面**

自助注销。微信银行可通过微信银行自助注销，您可在天津银行微银行-金融频道-微信用户签约/注销交易，完成微银行注销。在“天津银行微银行”微信公众号详情页面点击“不再关注”按钮，即可取消“天津银行微银行”微信公众号的关注，请您注意，取消“天津银行微银行”微信公众号的关注不会解约微银行。

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客户端，以阻止我们获取您的个人信息。您注销电子银行账号的行为是不可逆行为，一旦您注销您的手机银行，我们将不再通过手机银行客户端收集您的个人信息，并将删除有关您手机银行的一切信息，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。

请您注意，我行电子银行注册用户仅在手机设备中删除天津银行 APP 时，我行不会注销您的手机银行用户，有关您手机银行的一切信息不会删除。您仍需注销您的手机银行方能达到以上目的。注销电子银行不会自动注销您的快捷支付授权，您可以在支付管理或者第三方主动注销授权。

（五）获取您的个人信息副本

您有权获取您的个人信息副本。如您需要获取我行收集您的个人信息副本，您可通过拨打我行 956056 客服热线。人工客服会对您进行人工信息校验，完成个人信息主体确认后，将个人信息副本通过双方协商后的方式提交给您。在符

合相关法律规定且技术可行的前提下，我行将根据您的要求向您提供您的个人信息副本，我行将在15日内完成受理并处理。

（六）个人信息转移

我们不会转让您的个人信息给任何其他第三方，除非征得您的明确同意。

随着我们业务的持续发展，我们将有可能进行合并、收购、资产转让，您的个人信息有可能因此而被转移。在发生前述变更时，我们将按照法律法规及不低于本隐私政策所载明的安全标准要求继受方保护您的个人信息，否则我们将要求继受方重新征得您的授权同意。

如果您主动提出个人信息转移的申请，可以通过在线客服、956056客服热线或到我行各营业网点联系我们，我行将在15日内完成受理并处理。

（七）个人信息跨境传输

我行在中华人民共和国境内运营中收集和产生的个人信息，存储在中国境内，以下情形除外：

（1）适用的法律有明确规定；

（2）获得您的明确授权；

（3）您通过互联网进行跨境交易的个人主动行为。

针对以上情形，我行会确保依据本隐私权政策对您的个人信息提供足够的保护。

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，我行会单独征得您的授权同意并要求接收方按照我行的说明、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。

（八）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、算法在内的非人工自动决策机制做出决定。您可以通过拨打我行956056客服热线或到我行各营业网点咨询反映，我行将会在15日内完成受理并处理。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。

（九）响应您的上述请求

为保障安全，您可能需要提供书面请求，或以其他方式自助办理相关业务，我行可能会要求您验证自己的身份，然后再处理您的请求，一般情况下，我们将在15天内完成核查和处理，请您理解。**对于您合理的请求，我行原则上不收取费用，但对于非法、违规、无正当理由、可能无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际的请求，我行可能会将予以拒绝。**

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.与个人信息控制者履行法律法规规定的义务相关的;

2.与国家安全、国防安全直接相关的;

3.与公共安全、公共卫生、重大公共利益直接相关的;

4.与刑事侦查、起诉、审判和执行判决直接相关的;

5.个人信息控制者有充分证据表明个人信息主体存在主观恶意或滥用权利的;

6.出于维护个人信息主体或其他个人的生命、财产重大合法权益但又很难得到本人授权同意的;

7.响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权

益受到严重损害的;

8.涉及商业秘密的

六、我们如何处理未成年人信息

我行的产品、网站和服务主要面向成人。如果没有父母或监护人的同意，未成年人（不满十六周岁）不得创建自己的用户账户，有关法律法规或相关监管规定另有要求的除外。

如您为不满 14 周岁的未成年人，您的个人信息都属于敏感个人信息，在使用我行服务前请您务必征得您父母或者其他监护人的明示同意。对于经父母或监护人同意而收集未成年人个人信息的情况，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未成年人所必要的情况下使用或

公开披露此信息。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个人信息，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。

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，您可查阅《天津银行儿童个人信息保护规则》或通过下文第九部分中的联系方式联系我行。

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，若发生下列重大变化情形时，我们会适时对本政策进行更新:

1.收集、存储、使用个人信息的范围、目的、规则发生变化;

2.对外提供个人信息的对象、范围、目的发生变化;

3.您访问和管理个人信息的方式发生变化;

4.数据安全能力、信息安全风险发生变化;

5.用户询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式发生变化;

6.其他可能对您的个人信息权益发生重大影响的变化。

修改后内容会通过官方网站（www.bankoftianjin.com）、推送通知、弹窗提示或其他方式来通知您，以便您及时了解本隐私政策的最新版本，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，天津银行 APP 将在登录页通过弹窗进行提示，您需要主动点击勾选再次确认同意。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。此外，您可通过“我的-设置-关于我们-隐私政策”功能查看历史版本隐私政策。

八、第三方收集和使用您的个人信息情况

当您在天津银行 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天津银行 APP 中使用第三方的相应服务，但这不影响您使用天津银行 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。

九、如何联系我行

如您对本隐私政策有任何疑问、意见建议或投诉举报，可以通过拨打我行 956056 客服热线或到我行各营业网点咨询反映。受理您的问题后，我们会及时、妥善处理。一般情况下，我行将在 15 天内完成受理并处理。

如您对我们的回复不满意，特别是我们的个人信息处理行为损害了您的合法权益，您还可以通过以下外部途径寻求解决方案:

1.向被告所在地人民法院提起民事诉讼;

2.向中央网信办举报（举报中心网址为：http://www.12377.cn，举报电话为：12377）。

个人信息控制者主体及联系方式：天津银行股份有限公司，客服电话：956056，注册地址：中国天津市河西区友谊路 15 号，邮编 300201。个人信息保护负责主体联系方式：956056。

天津银行股份有限公司

附件 1-2

基于深度学习和智能安全终端的轻型柜面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)、《中华人民共和国反洗钱法》、《中华人民共和国商业银行法》、《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。

经评估，本项目所提供金融服务符合相关法律法规要求，可依法合规开展业务应用。

天津银行内控合规部

2024 年 9 月 26 日

附件 1-3

基于深度学习和智能安全终端的轻型柜面服务技术安全性评估报告

本项目严格按照《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)、《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)、《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。

天津银行信息技术部

2024 年 9 月 26 日

附件 1-4

基于深度学习和智能安全终端的轻型柜面服务风险补偿机制

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，由天津银行股份有限公司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.当服务运行过程中产生风险并对用户合法权益造成损失时，协助用户通过仲裁、诉讼等方式取得合理补偿。

2.若因技术缺陷导致客户合法权益面临损害时，服务各方将在消费者知情授权、数据隐私、安全交易、资金保护等方面认定责任，并根据风险补偿机制积极解决，最大限度保护用户权益。

3.消费者知情权方面。服务信息披露业务贯穿开发、宣传、服务流程；在协议和服务宣传材料中，醒目位置提示客户风险，并对技术风险、数据隐私、安全交易、资金保护等重要事实，真实、准确和清晰的表述；协议和宣传材料统一

由总行制作和分发。

4.消费者投诉方面。依据“积极主动，专业高效，合规谨慎，显示处理，保证前台业务，损失最小化”为基本原则进行处理。

5.个人金融信息保护。服务按照协议收集个人相关信息，严格按照协议进行传输、加工、保存和提取；当服务出现风险，在做好客户沟通的基础上，对服务所有相关数据进行安全处理，不在其他产品或业务中进行复制、存储、使用、出售。

6.安全交易及资金保护方面。当服务出现风险时，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；同时对于超出协议范围的诉求，协助用户通过仲裁、诉讼等方式取得合理补偿。

天津银行股份有限公司

2024年9月26日

附件 1-5

基于深度学习和智能安全终端的轻型柜面服务退出机制

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、业务退出

根据与用户所签署的相关协议，由天津银行股份有限公司各渠道发布相关业务退出的公告，告知用户，在规定时间内结束相关业务，做好舆情监控。其中对采用本服务已经线上办理完成的授信类业务转传统线下流程，完成相关纸质合同签订;针对采用本服务未完成的业务，按照最后一笔业务完成全部流程，并通过相关业务人员合规确认后，在线下完成相关业务功

能。确保金融服务退出时的影响范围。

二、技术退出

1.数据处理

完成本服务相关的业务数据、交易数据等信息的数据库归档备份，将用户数据同步到相关业务系统。确保用户其他业务不受影响。

2.资源回收

回收与本服务相关的系统资源、包括服务器、数据库、基础组件等。

天津银行股份有限公司

2024 年 9 月 26 日

附件 1-6

基于深度学习和智能安全终端的轻型柜面服务应急预案

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。

具体应急预案见：附件 1-6-1《天津银行业务连续性总体应急预案》。

天津银行股份有限公司

2024 年 9 月 26 日

附件1-6-1

天津银行业务连续性总体应急预案

第一章　总则

第一条为预防或最大程度地减少突发事件导致重要业务运营中断的影响，快速恢复被中断业务，有效防范声誉风险，保障人员生命安全，提高天津银行（以下简称本行）业务连续性，依据《国家突发公共事件总体应急预案》《商业银行业务连续性监管指引》《银行业突发事件应急预案》等外部规定以及《天津银行业务连续性管理政策》《天津银行业务连续性管理办法》《天津银行重大突发事件总体应急预案》等行内规章制度，结合本行实际情况，特制定本应急预案（以下简称本预案）。

第二条本预案所称突发事件是指突然发生，对本行业务持续运营产生影响，造成或可能造成重要业务停止运营的事件。主要包括：

（一）信息技术故障：主要包括信息系统技术故障、配套设施故障、第三方技术服务中断、黑客攻击等；

（二）自然灾害：主要包括地震灾害，台风、暴雨、暴雪、寒潮、大风（沙尘暴）、冰雹等气象灾害，山体崩塌、滑坡、泥石流等地质灾害，风暴潮、海啸等海洋灾害；

（三）人为破坏：主要包括火灾、抢劫、恐怖袭击等；

（四）公共卫生：主要包括集体食物中毒、传染病等；

（五）声誉风险事件；

（六）流动性风险事件。

第三条按照其可能的影响范围、损失程度和持续时间，对各类突发事件进行分级。当突发事件同时满足多个级别的定级条件时，按最高级别确定事件等级。当突发事件随时间推移升级后，按照升级后的级别进行处理。

突发事件种类 / 突发事件等级	信息技术故障类	自然灾害类	公共卫生类	所有六类事件
特别重大突发事件（I级）	重要信息系统服务中断，或重要数据损毁、丢失、泄漏，可能造成经济秩序混乱或重大经济损失，或对公众利益、社会秩序、国家安全造成特别严重损害。	本行各机构所在地发生自然灾害事件红色、橙色预警。	本行各机构所在地发生公共卫生事件红色、橙色预警。	在业务服务时段导致两个（含）以上省（自治区、直辖市）级机构业务无法正常开展达3个小时（含）以上，或一个省（自治区、直辖市）级机构业务无法正常开展达6个小时（含）以上的事件； 业务服务时段以外，故障或事件救治未果、可能产生上述事件的事件。

重大突发事件（II级）	重要信息系统服务中断，或重要数据损毁、丢失、泄漏，可能对本行或客户利益造成严重损害。	本行各机构所在地发生自然灾害事件黄色预警。	本行各机构所在地发生公共卫生事件黄色预警。	在业务服务时段导致两个（含）以上省（自治区、直辖市）级机构业务无法正常开展达半个小时（含）以上，或一个省（自治区、直辖市）级机构业务无法正常开展达3个小时（含）以上的事件； 业务服务时段以外，故障或事件救治未果、可能产生上述事件的事件。
一般重大突发事件（III级）	重要信息系统服务中断，或重要数据损毁、丢失、泄漏，可能对本行或客户利益造成较大损害。	本行各机构所在地发生自然灾害事件蓝色预警。	本行各机构所在地发生公共卫生事件蓝色预警。	在业务服务时段导致一个省（自治区、直辖市）级机构业务无法正常开展达半个小时（含）以上的事件； 业务服务时段以外，故障或事件救治未果、可能产生上述事件的事件。

本预案适用于本行各级机构，本行附属子公司应参照此预案执行。

总行各业务连续性专项应急预案、各分支机构预案应按照上述标准，结合所针对的突发事件种类，细化突发事件分级标准，并保持总体预案、专项预案、分支机构预案中突发事件分级标准的一致性。

各分支机构应参照上述标准、根据属地监管要求、结合各机构实际，合理确定突发事件的分级标准。

第四条 本预案适用于特别重大突发事件，或超出事发地分支机构处置能力的重大突发事件的应对工作。

第五条 执行本预案的工作原则如下：

（一）居安思危，预防为主。业务连续性管理以预防为主，应急与预防相结合，通过风险评估和业务影响分析等手段，充分识别重要业务运营所需资源的脆弱性及其面临的威胁，采取有效措施尽量减少突发事件发生，最大限度地减轻突发事件的影响。

（二）统一指挥，分级负责。在总行高级管理层的统一领导和指挥下，建立健全分类管理、分级负责、总分结合的突发事件应急管理体制。

（三）快速响应，协同应对。突发事件发生后应及时报告和处置，各部门、各机构应各司其职，服从指挥；加强与政府公共应急机构、相关同业及第三方服务商的密切协作。

（四）以人为本，减少损失。突发事件应急处置始终以保护员工及客户的生命安全和健康为第一目标；快速恢复重要业务经营活动，尽量将损失降到最低；全力维护本行在公众中的信心和声誉。

第六条 本行业务连续性应急预案体系包括：

（一）业务连续性总体应急预案。总体应急预案是全行业务连续性应急预案的总纲，是总行对特别重大突发事

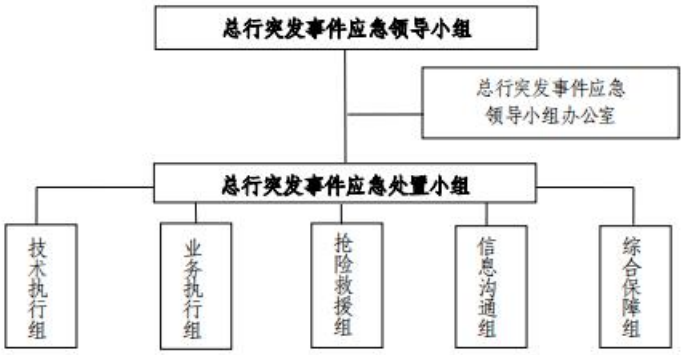
件的应急响应和处置流程，对全行业务连续性突发事件的监测预警、应急响应、应急处置与恢复、后续处置、应急保障等提出总体要求。

（二）业务连续性专项应急预案。专项应急预案主要是总行为应对某一类型或某几种类型突发事件，或者针对某项重要业务持续运营而预先制定的、覆盖应急全流程、涉及多个部门和各相关处置环节的工作方案。

（三）业务连续性分支机构应急预案。适用于分支机构辖内发生的突发事件应急处置。各分支机构按照总行预案体系和属地监管要求，结合实际，明确分支机构业务连续性应急预案体系。分支机构业务连续性应急预案应与总行应急预案、属地监管部门应急预案、属地公共服务部门应急预案衔接一致，不断提高预案的可执行性。

（四）对重大业务活动，牵头部门或主办单位应当制定应急预案。各类预案应根据实际情况不断补充、完善。第二章组织架构

第七条发生特别重大突发事件时，应急指挥、处置与恢复工作的组织架构与日常组织架构有所区别，总体应急预案启动即按照应急组织架构运行。具体应急组织架构如下：



（一）业务连续性突发事件应急领导小组（以下简称：领导小组）

组长：总行行长

副组长：总行其他高级管理层成员

具体职责包括：

1.统一领导和指挥特别重大突发事件应急处置工作；

2.决定启动、终止本预案；

3.决定特别重大突发事件的通报、对外报告和公告；

4.负责其他应急处置重要事项的决策。

必要时，领导小组在突发事件现场设立应急指挥部，领导和指挥突发事件应急处置工作。

领导小组下设办公室，领导小组办公室设在总行内控合规部。

具体职责包括：

1.按照突发事件应急领导小组要求传达应急预案启动及应急响应指令。

2.对突发事件处置信息进行收集汇总和报告。

3.推进应急响应及处置等预案落实工作。4.完成领导小组交办的其他工作。

（二）突发事件应急处置小组

组长：按突发事件性质由总行相应分管行领导担任

成员：总行办公室/消费者权益保护办公室、董事会办公室、监事会办公室、公司业务部、机构业务部、交易银行部、小微普惠金融部/科创金融部、投资银行部、零售金融部、零售信贷部、E银行部、金融市场部、资产管理部、风险管理部、授信管理部、法律事务部、内控合规部、资产负债管理部、财务会计部、运营管理部、国际业务部、人力资源部、信息技术部、行政事务部、安全保卫部、营运中心等部门负责人及相关分支机构负责人。

具体职责包括：负责对突发事件处置进行指挥、组织、协调与督促。

根据突发事件处置需要，突发事件应急处置小组下设相关专业组，包括技术执行组、业务执行组、抢险救援组、信息沟通组、综合保障组等，接受突发事件应急处置小组的指挥，并向突发事件应急领导小组进行报告。各专业组由总行相关部门或分支机构人员组成，组成人员在应急处置工作中接受所在专业组组长以及副组长的领导。

突发事件应急处置小组办事机构按突发事件性质由总行各相关条线部门担任。

（三）技术执行组

由总行、分支机构信息科技相关人员组成，成员包括总行信息技术部负责人、信息技术部各团队负责人、相关分支机构技术骨干及其他相关应急处置人员。其中，组长由总行信息技术部负责人或其授权的部门负责人担任。

技术执行组具体负责突发事件中相关的技术应急处置工作，在目标时间范围内恢复重要信息系统的运行。

（四）业务执行组

由总行、分支机构运营管理部、E银行部等相关人员组成，成员包括上述总行部门负责人、部门各团队负责人、相关分支机构运营管理部负责人及相关具体应急处置人员。其中，组长由总行运营管理部负责人或其授权的部门负责人担任，副组长分别由总行E银行部负责人担任。发生流动性风险事件时，由总行资产负债管理部相关人员参加业务执行组，资产负债管理部负责人任业务组副组长。

业务执行组具体负责突发事件发生时重要业务的应急处置及后续业务处理，在目标时间范围内恢复对外服务。

（五）抢险救援组

该组仅在发生自然灾害、人为破坏或公共卫生类事件时设置。发生自然灾害类和公共卫生类突发事件时，由行政事务部负责人任组长，人力资源部、财务会计部负责人为副组长，各部门相关团队负责人为成员。发生人为破坏类突发事

件时，由安全保卫部负责人任组长，人力资源部、财务会计部负责人为副组长，各部门相关团队负责人为成员。

抢险救援组具体负责自然灾害、人为破坏或公共卫生事件发生时，采取有效措施确保员工生命安全，同时对重要办公场所进行保护，为重要业务恢复运营提供人力、场地保障。

（六）信息沟通组

由总行办公室/消费者权益保护办公室、董事会办公室、监事会办公室、人力资源部等部门及相关分支机构综合管理部人员组成，成员包括总行办公室/消费者权益保护办公室、董事会办公室、监事会办公室、人力资源部等部门负责人、上述部门相关团队负责人、相关分支机构综合管理部负责人及相关具体应急处置人员。其中，组长由总行办公室主任担任。

信息沟通组具体负责在突发事件应急处置过程中及处置结束后，做好舆情监测及牵头组织负面舆情处置工作，做好与员工、客户、股东、董事、监事、监管机构、媒体等利益相关者的信息沟通工作。

（七）综合保障组

由总行办公室/消费者权益保护办公室、法律事务部、行政事务部、安全保卫部、财务会计部、人力资源部、内控合规部以及相关分支机构综合管理部门人员组成，成员包括

上述部门负责人、相关团队负责人以及相关具体应急保障人员。其中，由总行行政事务部负责人担任组长，安全保卫部负责人担任副组长。

综合保障组具体负责营运中断事件应急处置过程中所需人力、物力和财力等资源的保障，做好指挥中心布置、秩序维护、安全保障、交通运输与食宿、法律咨询、保险理赔和人员安抚等相关工作，综合保障组人员的具体分工按照上述部门的日常职责进行。

（八）分支机构突发事件应急组织

各分支机构应参照总行突发事件应急组织架构，结合各自实际，明确应急处置组织架构，确保分工明确、有效运转。必要时，总行派出工作组指导分支机构突发事件应急处置工作。

第三章　监测与预警

第八条 监测预警机制建设

总行办公室/消费者权益保护办公室、资产负债管理部、运营管理部、信息技术部、行政事务部、安全保卫部等相关部门及各分支机构要针对各种可能发生的突发事件，建立并完善监测预警机制，开展风险分析，做到早发现、早报告、早处置。总行信息技术部要加强运维监控平台建设与维护，设定风险预警指标，实时监控全行生产设备及应用系统运行使用情况，及时发现异常情况，及时预警。

第九条 预警信息内容

预警信息包括突发事件的类别、预警级别（与突发事件级别相对应）、起始时间、可能影响范围、警示事项、应采取的措施和发布单位等。

第十条 预警信息发布、调整和解除

预警信息的发布、调整和解除可通过邮件、广播、警报器等方式进行，预警信息的发布、调整和解除应得到本行主管行领导的同意，依照程序启动并事先告知总行内控合规部及相关职能部门。

预警信息的具体发布、调整和解除程序应在专项应急预案中明确。

第四章　应急响应

第十一条 事件报告

（一）基本原则：及时性、准确性、规范性。

（二）主要报告内容

1.事件所涉及的机构名称、地点、时间。

2.事件的发生原因、性质、涉及业务及系统、涉及人数、危害程度、影响范围。

3.建议（初判）事件等级。

4.事态发展趋势、可能造成的损失、已采取及拟采取的应对措施。

5.其他与本事件有关的内容。

（三）报告程序与时限要求

1.总行条线管理部门业务连续性工作责任人、分支机构业务连续性管理牵头部门工作责任人应在获悉突发事件发生后立即电话报告所属总行条线管理部门和领导小组办公室，营业时间内发生的应同时在1小时之内向领导小组办公室上报《业务连续性突发事件报告》（非工作时间送达总行行政值班室）。每30分钟报告1次突发事件处置情况，直至应急结束，或按应急领导小组要求的频度持续报告。

2.事发单位或部门应按照相关专项预案的规定流程和内容要求，进行突发事件报告。

3.对外报送应按照本行重大突发事件报告相关制度执行。

对于上级领导同志在重大突发事件报告上有批示意见，应迅速传达，抓好落实，并按照上级单位的要求及时报告贯彻落实情况。

第十二条 先期处置

突发事件发生后，事发地分支机构或总行条线管理部门在进行信息报告的同时，根据职责和权限启动相关应急预案，及时、有效地进行处置。

总行各部门、相关分支机构要上下协同、密切配合、积极主动，共同做好现场救助、客户安抚、系统故障排除、业务恢复等工作，有效避免事态扩大。

第十三条 损害评估

特别重大突发事件发生后，总行相关条线管理部门应根据掌握的事件信息，对突发事件进行损害评估，初步判定突发事件等级，报突发事件应急领导小组。

第十四条 预案启动

突发事件应急领导小组对突发事件等级进行综合判断，考虑事件性质、影响范围及程度，决定应急预案启动；由应急领导小组组长宣布本行进入紧急状态并启动本预案。

第五章　应急处置与恢复

第十五条 决策与指挥

本预案启动后，应急处置小组组织各专业组，在相关专项应急预案、各分支机构应急预案的基础上，汇总分析突发事件具体情况及掌握的信息，提出初步处置建议。

突发事件应急领导小组进行分析研判，在已有各类预案基础上，结合实际情况和各专业组的初步处置建议进行决策。

突发事件应急处置小组根据领导小组的决策，负责指挥、组织、协调和督促做好各项应急处置工作。

总行信息技术部、行政事务部指定人员按照事先确定的标准以及综合保障组组长的要求，确保指挥中心电话、视频设备、电脑、打印机、网络、文具、白板、投影机等应急处置环境就绪。

第十六条 应急处置与恢复

各专业组根据应急领导小组的决策，按照相关专项预案进行具体应急处置工作，有效保护员工、客户生命安全，恢复信息系统、场地及对外服务。

自然灾害、人为破坏、公共卫生类突发事件发生时，抢险救援组、综合保障组应主动与政府公共应急部门联系，按规定接受其应急指挥，共同做好员工、场地的应急救援工作，为尽快恢复对外服务获得必要的后勤保障。

经突发事件应急领导小组决策，需将信息系统进行切换到灾备中心运行、需迁移至备份场所或临时场所开展业务的，技术组和业务组应做好对灾备系统、备份场所或临时场所的测试、检查工作，按照相关预案制定方案并有序实施。综合保障组应全力做好必要的后勤保障工作。

分支机构发生特别重大突发事件，总行突发事件应急领导小组确定处置策略并派出工作组，现场指挥分支机构进行应急处置。

第十七条 舆情处置

信息沟通组中总行办公室/消费者权益保护办公室、分支机构综合管理部人员密切关注媒体对突发事件以及事件处理的有关报道和社会舆论，按照相关预案牵头组织做好负面舆情应急处置工作。任何单位或个人未经许可不得对外进行宣传解释和发布相关信息。

第十八条 应急结束

出现异常或发生中断的信息系统在数据中心本地恢复或切换到灾备中心（同城和异地），或政府公共应急部门解除灾害预警，业务运营基本恢复正常，由突发事件应急领导小组组长宣布应急结束。

第六章　后续处置

第十九条 事后报告

处置工作完成后，突发事件应急处置小组应组织相关部门对整个事件的发生过程、原因、处置措施以及教训等进行总结，并以《业务连续性突发事件平息报告》送交突发事件应急领导小组。领导小组办公室根据领导小组组长指示，按照监管机构和上级单位规定的报送要求向监管机构及上级单位报告。

第二十条 事后监测

突发事件应急处置工作结束后，总行信息技术部、运营管理部、E银行部等相关部门以及各分支机构应密切关注信息系统运行和业务开展情况，防止突发事件出现反复。

行政事务部、安全保卫部应做好自然灾害、公共卫生、人为破坏事件的后续监测工作，防止次生、衍生灾害发生。

在自然灾害、人为破坏等突发事件发生后，人力资源部应组织做好必要的员工心理干预工作，有效降低重大事件对员工心理健康的影响。

第二十一条 数据补录与验证

应急结束后，突发事件涉及到的总行、分支机构各条线管理部门应按照专项应急预案及应急操作手册对业务数据进行必要的数据补录、验证。

第二十二条 重建与回退

如突发事件导致办公场所、营业机构发生损毁，本行重要业务可能需在备份场所或临时场所开展。在应急处置结束后，应制定办公场所、营业机构及信息系统的修复、重建计划，组织实施系统重建与业务回退工作。

第七章　应急保障

第二十三条 人力资源保障

总行各部门、各分支机构在完善应急预案的基础上，明确应急处置人员的具体职责，将各项应急处置措施落实到人，严格落实AB角色制，最大限度保证各类突发事件发生时A角与B角至少有一人到岗可用。加强应急处置人员的业务培训和应急演练，确保B角与A角具备同等的应急处置能力。

第二十四条 财力保障

财务会计部保证所需突发事件应急准备和处置所需备付能力，简化财务手续，明确应急状态下资金的借用及报销流程。在应急处置工作结束后，对应急处置资金使用情况进行评估。

第二十五条 物资保障

信息技术部做好生产系统备件的储备工作，与第三方供应商建立紧急供货协议，确保应急状态下信息系统设备可靠供应。运营管理部要建立运营条线专项应急预案并按照预案严格执行。行政事务部要做好必要的员工生活物资储备，并及时予以补充和更新。

第二十六条 基本生活保障

行政事务部做好应急处置人员的基本生活保障，并与所在地宾馆、超市、饭店、医院签署必要的合作协议。相关部门按照各自职责做好与当地公共应急部门的沟通，并接受其指导。

第二十七条 交通运输保障

行政事务部保证紧急情况下应急交通工具的优先安排、优先调度，做好与公安交通管理部门、铁路部门以及航空公司的沟通工作。

第二十八条 通讯保障

1.突发事件应急领导小组办公室应掌握突发事件应急领导小组成员、应急处置小组组长、各专业组（副）组长、

骨干人员的有效联系方式（不少于2个）以及电子邮箱；应急处置小组成员应掌握组内成员的联系方式和相关第三方应急联系方式，应急人员应确保其通讯畅通（通讯方式发生变化后，第一时间通知总行内控合规部、信息技术部、运营管理部、办公室/消费者权益保护办公室、行政事务部、安全保卫部）。

2.各分支机构保持与属地政府、监管部门的通讯联系畅通。

3.信息技术部加强行内网络以及通讯系统的建设与维护，确保应急状态下通信畅通。

4.所有通讯及信息共享应符合国家及行内有关保密规定。

第二十九条 安全保障

安全保卫部加强对数据中心、办公大楼、营业网点、重要物资和设备的安全保护，确保应急处置工作有序开展及员工、客户的人身安全。

第八章　演练与持续改进

第三十条 为满足监管要求，并验证应急预案的完整性、可操作性和有效性，验证业务连续性资源的可用性，提高运营中断事件的综合处置能力，本行应当至少每三年对全部重要业务开展一次业务连续性演练。

第三十一条 演练组织架构

本行业务连续性演练组织架构由演练决策层、演练指挥层、演练执行层和演练保障层组成。

（一）演练决策层由本行高级管理层人员组成，负责审批业务连续性演练各专项预案及批准启动业务连续性演练等;

（二）演练指挥层由总行内控合规部、执行部门、保障部门负责人以及各分支机构行长组成，负责业务连续性演练应急指挥和组织协调，督导各业务连续性专项预案演练实施;

（三）演练执行层由业务连续性各执行部门及分支机构人员组成，具体负责各类业务连续性专项预案演练的执行工作;

（四）演练保障层由本行业务连续性管理保障部门以及分支机构相关人员组成，负责各类业务连续性演练所需人力、物力和财力等资源的保障，负责各类对外报告、宣告、通报和沟通与协调，以及对外媒体公关、秩序维护、安全保障、法律咨询和人员安抚等相关工作。

第三十二条 演练职责分工

（一）业务连续性总体应急预案或涉及多个专项应急预案的演练由总行内控合规部负责牵头组织，总行各部门、各分支机构按各自职责制定演练方案、做好演练前各项

准备工作并积极参加演练；各执行、保障部门具体分工如下：

1.信息技术部：负责制定演练中信息系统切换的技术方案和回退方案，并按方案严格执行。

2.演练涉及业务条线管理部门：负责制定演练中信息系统切换后的业务验证方案和测试数据，确保切换后业务能够正常运转，拟包含演练影响的业务种类、业务中断时间、业务恢复时间等要素的客户短信告知内容，并按方案严格执行。

3.办公室/消费者权益保护办公室：负责制定演练前的舆情应急预案；负责在演练之前在本行官网发布由演练部门提供的客户提示。

4.行政事务部：负责制定演练中供应电力、场地、办公设备等的工作方案，并按方案严格执行。

5.安全保卫部：负责制定演练办公场地安全保卫工作方案，并按方案严格执行。

（二）各类专项应急预案的演练由该预案牵头制定部门负责牵头组织，各相关部门、分支机构按照预案要求及实际演练需要积极参加，总行内控合规部予以必要的指导；

（三）分支机构业务连续性应急预案的演练分工由各机构自行安排。

第三十三条 演练计划

（一）信息系统灾备演练。每年年初由总行内控合规部协同信息技术部根据目前本行业务系统现状，会同各相关业务部门制定当年业务连续性各种类型演练的演练计划，注明演练类型、时间，并由总行内控合规部审核与备案。原则上，应严格按照计划实施演练；如有特殊情况，应报备总行内控合规部并说明原因。

（二）业务连续性总体预案、专项预案、分支机构预案演练。每年年初由上述各预案制定部门、机构制定当年业务连续性各预案演练计划，注明演练类型、时间，并报送总行内控合规部审核与备案。原则上，应严格按照计划实施演练；如有特殊情况，应报备总行内控合规部并说明原因。

第三十四条 演练准备

演练前应制定演练方案，明确演练目标、演练形式、涉及的层次及范围，设定演练场景，确定演练流程、演练内容，做好演练保障准备，对演练的风险进行评估，有效防范演练风险；对存在较大风险的演练，应事先报备监管部门。涉及到全行的重要业务业务连续性实战演练，应将汇总涉及到的各条线演练方案提交业务连续性管理委员会审议，并同时由信息技术部、业务条线管理部门负责人和演练决策层审批通过后才能执行演练。

第三十五条 演练执行

演练过程中应严格按照各演练方案执行，加强演练过程控制，对演练过程进行完整记录，做好演练安全保障工作。

第三十六条 演练报告与评估改进

演练结束后及时进行评估、总结，按要求将演练评估报告、总结报告报送总行内控合规部；对演练中发现的问题应采取有效措施予以改进；演练资料归档保存。对全行性业务连续性演练，应在演练结束后45个工作日内向监管机构提交演练总结报告。

第九章　附则

第三十七条 对造成突发事件发生以及迟报、谎报、瞒报、漏报信息或其他违规违纪行为，按照本行问责管理有关规定予以处理。对突发事件应急处置过程中做出突出贡献的部门、人员按照有关规定予以表彰和奖励。

第三十八条 本预案未尽事宜，按照《天津银行重大突发事件总体应急预案》执行。

第三十九条 本预案由总行风险控制委员会负责解释。

天津银行股份有限公司