

长沙银行股份有限公司企业网络银行个人信息保护政策

尊敬的企业用户：我行对《长沙银行股份有限公司企业网络银行个人信息保护政策》进行了更新，此版本个人隐私政策的更新内容主要为：根据实际业务情况调整插件表。

版本发布日期：2024 年 7 月 12 日

版本生效日期：2024 年 7 月 12 日

长沙银行股份有限公司（以下简称“我行”）深知个人信息对贵司法人代表、实际控制人及代表贵司办理企业网络银行业务的自然人（简称“您”）的重要性，我行将按照法律法规的规定，尽全力保护您的个人信息安全。我行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、最小必要原则、确保安全原则、主体参与原则、公开透明原则、诚信原则、信息质量原则等。同时，我行承诺，将依法采取相应的安全保护措施来保护您的个人信息。

第一部分 定义

1. 个人信息：个人信息是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，不

包括匿名化处理后的信息。包括但不限于客户姓名、性别、国籍、职业、住所地或工作单位地址、联系方式等。

2. 敏感个人信息：敏感个人信息是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，包括身份证件号码、个人生物识别信息、金融账户、财产信息、交易信息、征信信息、行踪轨迹、宗教信仰、特定身份、医疗健康、不满 14 周岁未成年人的个人信息等。敏感个人信息在本政策中会做加粗提示。

3. 企业网络银行：包括企业网上银行（企业网银）、企业 e 钱庄（手机银行）、对公服务大厅（企业微信小程序）等线上渠道。

第二部分 隐私保护政策

本《企业网络银行个人信息保护政策》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. 我行如何存储和保护您的个人信息
3. 我行如何对外提供、转让、公开披露您的个人信息
4. 我行如何处理未成年人信息
5. 我行如何使用 Cookie 和同类技术
6. 您控制个人信息的权利
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

（一）信息如何收集

为了更好地向您提供服务并确保您在服务过程中的个人信息安全，我行将遵循合理、相关、必要原则，且以您同意为前提收集信息，不会收集法律法规禁止收集的信息。因向您提供的产品和服务种类众多，我行将根据具体产品/服务范围 and 不同功能，收集和使用您的个人信息。您理解并同意，基于不断完善产品和服务的目的，我行将不时推出优化功能，可能增加或变更收集、使用个人信息的范围、目的和方式。对此，我们将通过更新本政策，并以弹窗或站内信的方式向您明确告知，并为您提供同意与否的选项，我行会按照业务功能所需的最小频率收集您的个人信息。您有权拒绝同意本政策的更新，但您同时知悉并理解，一旦您拒绝我们收集、处理您的个人信息属于开展业务或提供服务所必要的情形时，我们将可能无法为您开展更新后的业务或提供更新后的服务，但您原有正常办理的业务或接受的服务不受影响。我行会收集您在使用我行服务过程中主动输入或因使用服务而产生或需向第三方收集的信息：

1. 当您开通企业网络银行服务时，依据法律法规及监管要求，我行会收集您的身份信息（包括证件类型/证件号码/证件有效期/姓名）、手机号码、单位信息（单位名称/单位类型/法定代表人或单位负责人姓名、身份证件类型、身份证件号码、身份证件有效期/注册资本/联系方式/开户银行/银行

账号/成立日期/地址），除上述信息外，在您通过企业微信小程序自助注册时，我行还会收集您的**微信公开信息（昵称、头像、所在地区）、企业名称**，以帮助您完成企业微信小程序业务的开通。上述信息主要用于验证您的身份真实性以及与企业的相关情况，我行还可能通过联网核查的方式对有关信息进行核验。如果您拒绝提供这些信息，您可能无法开通企业网络银行或无法正常使用我行的服务。

2. 当您使用企业网络银行在线开户服务时，我行需要收集您的**单位名称、证照（营业执照、登记证书、批文）等信息、证照影像以及单位法定代表人或负责人、业务经办人等相关人员的真实姓名、身份证件类型、身份证件号码、身份证件有效期、身份证件影像、手机号码、联系方式、地址（个人信息）**，我行收集这些信息进行身份核验，才能为您提供线上开户服务。您在使用在线开户意愿核实功能时，我行将会收集您的**现场人像信息**，通过合法的机构对身份信息的真实性进行核验，并对人像进行验证。如您拒绝提供上述信息，您将无法使用我行企业网络银行的在线开户功能。

3. 当您登录我行企业网络银行时，我行会收集您的**身份证号、手机号、密码、短信验证码/Ukey设备信息、网络 IP 及设备 MAC 地址、IMEI、AndroidID 信息、传感器列表**，如您拒绝提供上述信息，您将无法登录我行企业网络银行。

4. 为了让您更安全、快速地使用企业网络银行业务，在需要短信验证码的环节，可能需要读取**验**

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，我行企业网络银行将不读取短信内容，需要您手动输入验证码。

5. 我行企业网络银行为您提供了**指纹登录、面容登录**功能（基于 FaceID，仅支持 ios 手机部分机型）。为了让您更安全、便捷地使用登录服务，如果您的设备与企业 e 钱庄 App 版本均支持**指纹/面容**功能，您可选择**开通指纹/面容登录**功能。您需在您的设备上录入您的**指纹信息/面容信息**，在您进行**指纹登录/面容登录**时，您需在您的设备上完成**指纹/面容验证**。我行仅接收验证结果，并不收集您的**指纹信息/面容信息**。如您不想使用**指纹验证/面容登录**，仍可通过其他方式进行登录。

6. 当您使用企业网络银行**转账汇款**功能时，您需要提供**收款方的姓名/单位名称、银行账号信息、开户行信息**（若为使用**数字人民币对公钱包转账及批量转账**时，需要提供**收款方名称、数字钱包名称、钱包 ID 及手机号**），以便于使用上述功能的支付服务。此外，我行还会收集您的**相关转账交易记录**以便于您查询；为了简化您的转账操作，将会根据上述交易信息，形成收款人名册；如您拒绝提供上述信息，仅会使您无法使用该功能，但不影响您正常使用企业网络银行的其他功能。

7. 当您使用企业网络银行申请开立**数字人民币对公钱包**时，我行将根据法律法规、监管要求及相关数字人民币运营机构的要求，收集您的**身份信息**（包括**证件类型/证件号码/证件有效期/姓名**）、

手机号码、单位信息（单位名称/单位类型/法定代表人/单位负责人姓名、身份证件类型、身份证件号码、身份证件有效期/注册资本/联系方式/开户银行/银行账号/成立日期/地址/员工人数/上一年度营业收入），上述信息主要用于验证您的身份真实性以及与企业的相关情况、以及是否符合开立数字人民币对公钱包的相关要求。我行还可能通过联网核查的方式对有关信息进行有效性核验。如果您拒绝提供这些信息，您将无法开通数字人民币对公钱包或无法正常使用我行的数字人民币对公钱包服务。

8. 当您使用企业网络银行提供的操作员管理功能时，您需提供**操作员的姓名、身份证号码及手机号**（个人信息），我行还可能通过合法的联网核查通道对上述身份信息进行核验。如您拒绝提供上述信息，仅会使您无法使用该功能，但不影响您正常使用企业网络银行的其他功能。

9. 当您使用企业网络银行的单位证件线上更新功能时，我行需收集您的**单位证照（营业执照、登记证书、批文等）名称、影像及证件号码、证件有效期，法定代表人（或负责人）身份证件影像、证件号码、身份证件有效期、手机号（个人信息）**，用于完成单位信息核验和更新。如您拒绝提供上述信息，仅会使您无法使用该功能，但不影响您正常使用企业网络银行的其他功能。

10. 当您通过企业网络银行申请出口快贷、快乐 e 贷系列等贷款产品时，我行需要收集您的**单位**

名称、证照以及单位的法定代表人（负责人）的真实姓名、身份证号码、手机号码、银行卡账号信息（个人信息），我行收集上述信息为您提供快乐e贷系列等贷款产品申请服务。如您拒绝提供上述信息，仅会使您无法使用该服务，但不影响您正常使用企业网络银行的其他服务。

11. 当您使用企业网络银行的员工批量开卡功能时，我行会收集**代理人、领卡人的姓名、身份证件信息、手机号码**。同时可能会收集开户员工的**个人基本资料、国籍、身份信息、手机号码、通讯地址、单位信息、学历信息、税收居民身份信息**。如您拒绝提供上述信息，仅会使您无法使用该服务，但不影响您正常使用企业网络银行的其他服务。

12. 当您使用企业网络银行的单位结算卡产品时，我行需要收集您的**单位名称、证照以及持卡人的姓名、手机号码、银行卡账号信息**。如您拒绝提供上述信息，仅会使您无法使用该服务，但不影响您正常使用企业网络银行的其他服务。

13. 当您使用企业网络银行的对账单申请服务时，我行需要收集您的**邮箱信息**。如您拒绝提供上述信息，仅会使您无法使用该服务，但不影响您正常使用企业网络银行的其他服务。

14. 当您使用企业网络银行的微信消息通知服务时，我行需要收集您的**微信授权信息**。如您拒绝提供上述信息，仅会使您无法使用该服务，但不影响您正常使用企业网络银行的其他服务。

15. 当您使用企业网络银行的国际业务汇出汇款功能时，您需要提供收款方的**姓名/单位名称、银行账号信息、开户行信息、业务经办人或业务联系人姓名及联系电话**，以便于使用上述支付服务。此外，我行还会收集您的相关**转账交易记录**以便于您查询；为了简化您的转账操作，您可自主选择是否根据上述交易信息，形成收款人名册；如您拒绝提供上述信息，仅会使您无法使用该功能，但不影响您正常使用企业网络银行的其他功能。

16. 当您使用企业网络银行国际业务汇入汇款功能时，您需要提供业务经办人或业务**联系人姓名及联系电话**，我行将收集**付款方的姓名/单位名称、银行账号信息、开户行信息**，以便于使用上述收款服务。此外，我行还会收集您的相关**收款交易记录**以便于您查询；如您拒绝提供上述信息，仅会使您无法使用该功能，但不影响您正常使用企业网络银行的其他功能。

17. 当您使用企业网络银行国际业务结汇时，您需要提供业务经办人或业务**联系人姓名及联系电话**，以便于使用上述结汇服务。此外，我行还会收集您的相关**结汇交易记录**以便于您查询；如您拒绝提供上述信息，仅会使您无法使用该功能，但不影响您正常使用企业网络银行的其他功能。

18. 当您使用企业网络银行银联账户实名认证及关联支付验证服务时，我行会收集您的**姓名、证件类型、证件号码、手机号码、银行卡卡号/账号信息**，向我行的合作机构发送上述信息用于核实所

输银行卡是否为用户本人银行卡，并可能需要提供刷脸认证信息，我行还会通过验证账号/密码方式对有关信息进行有效性核验。如您拒绝提供使用该功能所必要的个人信息，仅会使您无法使用该服务，但不影响您使用其他功能。

19. 当您使用企业网络银行服务时，在涉及监管要求、业务风控要求需进一步加强身份验证时，我行将会开启人脸识别身份验证，需采集您的**个人影像及身份证证件人像、姓名、身份证号码相关个人信息**，通过合法机构对信息的一致性和有效性进行验证。

20. 当您使用企业网络银行的以下服务时，我行通过嵌入的第三方插件（含 SDK）收集您的个人信息。如收集您的**地理位置信息**，用于提供网点导航服务；获取您的**摄像头、相册权限**，用于预约开户、证件更新功能中的资料上传；获取您的**麦克风权限**，用于远程客服语音沟通与智能客服的语音输入等服务；获取**网络通讯服务**权限，用于消息推送服务。上述信息仅保存在长沙银行系统中，不会提供给第三方。如您拒绝提供上述信息，仅会使您无法使用对应的服务，但不影响您正常使用企业网络银行的其他服务。我行所使用第三方插件（含 SDK）详细列表见附件。

21. 当您使用企业网络银行服务时，为了保障服务的正常运行及保护您的账号安全，我行需收集以下基础信息，包括您的**设备型号、操作系统、唯一设备标识符、企业 e 钱庄软件版本号、浏览器版**

本、ip 地址、MAC 地址、IMEI、AndroidID、网上银行 ukey 设备类型、ukey 编号、ukey 有效期、ukey 状态、登录名、登录时间、登录地区、登录次数信息、微信号、微信公开信息（昵称、头像、所在地区）、微信版本号、微信 openid 信息、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（如您的操作行为信息、服务故障信息等）。

22. 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，我行会收集您使用企业网络银行业务的行为信息（浏览信息、屏幕信息、访问时间、功能点击情况、广告点击情况、页面点击频次、页面停留时间、交易信息、地址、定位信息、启动次数、登录次数），用于统计、分析，并会根据用户行为向您提供更优质的服务或产品。上述采集的数据，我行将通过技术手段对您的信息数据进行去标识化处理，该等去标识化的信息将无法识别信息主体，我行有权在不经您同意的情况下直接使用，有权对用户数据库进行分析并予以商业化的利用。

23. 当您使用我行企业网络银行服务时，为保障您正常使用我行的服务，维护我行服务的正常运行，改进及优化我行的服务体验以及保障您的账号安全，我行可能需要您授予我行使用您的如下系统权限：

摄像头（相机）权限：您可开启摄像头进行个人头像上传、意见反馈、身份校验（身份证识别及人脸

识别)、扫描二维码、身份证信息维护、拍照并上传图片资料操作以及使用视频审核服务;

相册权限: 当您使用对公开户、快乐 e 贷-企业快贷、快乐 e 贷-政采贷、出口快贷、身份认证等需要提交证明材料的功能时,您可从本地相册中选择图片上传;

生物特征识别(人脸/指纹)权限: 您可授权调取您使用的设备的指纹验证或面容 ID 功能,帮助我行完成个人身份识别、登录、验证、确权、交易指令操作。当您进行指纹验证或面容验证时,我行仅收集验证结果,并不收集您的生物特征信息;

麦克风权限: 您可选择麦克风设备来进行特定场景的语音输入与沟通;

地理位置权限: 您可开启定位服务,以便在网点查询功能中获得更好的客户体验;

消息推送权限: 您可授权 APP 消息推送(通知)功能,该功能将推送转账交易、复核授权、账户变动、活动推广、官方公告的实时消息。开启/关闭消息推送功能方式如下(注意:因手机系统不同,方式各有差异以下方式仅供参考):

企业 e 钱庄 APP: 安全中心->系统授权管理->开启或关闭“允许通知”;

ios(苹果系统): 设置->通知->APP 列表中选择“企业 e 钱庄”->开启或关闭“允许通知”;

Android(安卓系统): 设置->通知中心(通知管理)->APP 列表中选择“企业 e 钱庄”->开启或关闭“允许通知”;

网络通讯权限：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。

存储权限：用于通过手机银行下载批量开卡名单、结构性存款协议、政采贷合同、企业管理协议；用于通过手机银行保存转账制单复核结果页、电子回单照片；用于访问和上传在线开户所需证件照片、企业快贷借款用户资料照片、证件更新所用的证件照片、申请房 e 贷的银行卡照片、反馈问题的上传照片。拒绝授权后，将无法通过手机银行下载批量开卡的名单、结构性存款协议、政采贷合同、企业管理协议，也无法通过手机银行保存转账制单复核结果页、电子回单照片；无法上传在线开户所需证件照片、企业快贷借款用户资料照片、证件更新所用的证件照片、申请房 e 贷的银行卡照片、反馈问题的上传照片，也无法通过手机银行使用 OCR 图片文字自动识别功能，但可以手动输入银行信息或身份信息。

设备信息权限：用于手机银行获取设备指纹面容信息来使用设备指纹面容支付功能，用于获取设备号、UUID、物理地址、设备唯一值、移动设备国际身份证等信息来使用云盾功能。拒绝授权后，手机银行将无法使用设备指纹面容支付功能和云盾功能。

蓝牙权限：用于手机银行的 mPaaS 框架提供蓝牙通信服务。拒绝授权不影响手机银行功能使用。

短信读取权限：手机银行用于读取接收的指定短信

来自动填充短信验证码。拒绝授权后将不影响短信验证码验证，但需要手动输入短信验证码。

NFC 权限：用于手机银行的 mPaaS 框架提供近距离无线通信服务。拒绝授权不影响手机银行功能使用。

日志权限：用于手机银行的 mPaaS 框架获取日志来分析手机银行 APP 的缺陷，用于神策用户行为分析平台获取日志来分析用户行为。拒绝授权不影响手机银行功能使用。

手机通讯录权限：用于在企业管家通过手机通讯录快速选取通讯录电话号码，无需您手动输入。拒绝授权后，上述功能仍可以使用，但需要手工输入手机号码。

拨打电话权限：用于拨打客服电话反馈问题和查询交易限额、拨打客户经理电话查询商机管理进度和查询转账进度。

上述功能需要您在您的移动设备中向我行开启您的摄像头（相机）、相册、网络通讯、生物特征识别（人脸/指纹）、麦克风、地理（定位）、消息推送功能的访问权限，以实现这些功能所涉及的信息收集和使用。

您确认并同意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；您也可以遵循您所使用设备的操作系统指示变更或者取消这些授权，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，但这不会对您使用企业网络银行其他服务产生影响。

（二）信息如何使用

1. 在向您提供经您授权同意使用的我行金融产品和服务，我行也会使用这些信息来维护和改进前述业务功能。

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，除非您对我行有特别授权，我行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。同时，我行在向您提供金融服务期间，您授权我行通过留存手机号码以短信、电话等方式向您进行满意度回访。

4. 为向您本人提供高效、便捷、个性化的服务，我行可能会使用您的个人信息进行自动化决策，我行保证决策的透明度和结果公平、公正，不会对您个人在交易价格等交易条件上实行不合理的差别待遇。

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. 与刑事侦查、起诉、审判和判决执行司法或行政执法直接相关的；

4. 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；

5. 所收集的个人信息是您自行向社会公众公开的，但您明确拒绝或我行收集、使用该信息侵害您重大利益的除外；

6. 从合法公开披露的信息中收集个人信息的，包括合法的新闻报道、政府信息公开等渠道，但您明确拒绝或我行收集、使用该信息侵害您重大利益的除外；

7. 根据与您签订和履行相关协议或其他书面文件所必需的；

8. 用于维护所提供的产品及/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；

9. 为公共利益实施新闻报道、舆论监督等行为所必需的；

10. 法律法规及监管要求规定的其他情形。

（四）单独授权

☐为享受综合性金融服务，提升服务体验，本人同意并授权贵行通过电话、短信、微信、APP消息及网页消息等形式向我推送贵行其他金融产品和服务的相关资讯。

如授权后您不想接收此类信息，可通过电话我行客服进行取消，或通过微信、短信、消息推送设

置等方式进行退订或关闭。您还可以在企业 e 钱庄 APP-设置-个性化推荐管理中，关闭个性化推荐功能。

二、我行如何存储和保护您的个人信息

（一）信息如何存储

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。确需向境外提供的，我行将在具备法定条件下，向您告知境外接收方的名称或姓名、联系方式、处理目的、处理方式、个人信息的种类以及您向境外接收方行使权利的方式和程序等事项，并在获得您的单独同意后，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；超出必要期限后，我们将对您的个人信息进行删除或匿名化处理，但法律法规另有规定的除外。例如：

手机号码：当您需要使用企业 e 钱庄服务时，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，当您注销企业 e 钱庄账户后，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。当您选择恢复默认头像后，我行将删除您设置的头像信息。

生物识别信息：当您使用生物识别信息服务时，我行需要保存您的人脸、声纹等信息，以保证您正常使用该服务，当您不再使用生物识别信息服务后，我行将删除相应信息。

（二）信息如何保护

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，保护您的或您提供的个人信息。例如：

（1）我行设立了网络安全和个人信息保护机构，专门负责网络安全和个人信息保护事务；

（2）我行会使用【SM2/SM4/RSA】加密技术确保数据的保密性；

（3）我行会使用受信赖的保护机制防止数据遭到恶意攻击；

（4）我行会部署访问控制机制，确保只有授权人员能够访问个人信息；

（5）我行会把您的或您提供的个人信息同步存储至我们的备份数据库；我行在存储时采取了不可逆的加密存储或隔离存储，在信息展示和下载时采取了脱敏处理，传输时采取了专线传输、加密传输、密钥和数据介质隔离传输技术措施，以确保您的个人信息安全；

（6）我行采用代码安全检查、数据访问日志

分析技术进行个人信息安全审计；

(7) 我行与所有可能接触个人信息的员工签订了保密协议，对关键岗位人员进行背景审查，并建立了严格的访问权限控制、权限审批流程和监控、审计机制；

2. 当我行的产品或服务发生停止运营的情况时，我行将以公告、推送通知、站内信等形式通知您，并在合理期限内删除您的个人信息或进行匿名化处理，法律法规另有规定的除外。

3. 我行会采取一切合理可行的措施，确保未收集无关的个人信息。

4. 请您理解，由于管理水平及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。

5. 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。

6. 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行的任何信息的安全性。如果我行的物理、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，我行将承担相应的法律责任。

三、我行如何对外提供、转让、公开披露您的个人信息

（一）对外提供

1. 为了提升信息处理效率、降低信息处理成本、提高信息处理准确性，我行可能会委托有能力的关联公司或其他专业机构（以下简称“受托人”）代表我行来处理信息。我行将与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。要求受托人不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，要求受托人将个人信息返还我行或者予以删除，不得保留。要求受托人不得转委托他人处理个人信息。

2. 如果为了向您提供服务而需要将您的信息提供至其他信息处理者，我行会按照法律法规及国家标准的要求，以页面提示、交互流程、确认协议、具体场景下的文案确认、弹窗提示的形式（我行将根据实际情况选择一种或多种方式）向您告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得您的同意或确认第三方已经征得您的同意。我们将要求信息接收方在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。如果接收方变更原先的处理目的、处理方式的，我行将依照本法规定重新取得个人同意。

3. 委托他人处理您的信息或向他人提供您的个人信息，我行将评估该第三方收集信息的合法性、正当性、必要性，对个人权益的影响及安全风险、所采取的保护措施是否合法、有效并与风险程度相适应。我行将要求第三方对您的信息采取保护措施并且严格遵守相关法律法规与监管要求。

（二）转让

1. 我行不会向其他任何公司、组织和个人转让您的个人信息，但以下情形除外：

（1）事先获得您的明确同意的；

（2）根据法律法规规定，或者政府主管部门、司法机关的强制要求必须对外转让的。

2. 根据法律法规和商业惯例，在合并、收购、资产或业务转让、破产清算或类似的交易时，如涉及到个人信息转让，我行会向您告知接收方的名称或者姓名和联系方式，并要求新的持有您个人信息的公司、组织和个人继续受本政策的约束，否则我们将要求该等公司、组织或个人重新取得您的授权同意。

（三）公开披露

1. 我行不会公开披露您的或您提供的个人信息，但以下情形除外：

（1）事先获得您的明确同意的；

（2）根据法律法规规定，或者政府主管部门、司法机关的强制要求必须公开披露的。

2. 我行如确需公开披露您的个人信息的，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，并事先征得您的同意。

（四）征求授权同意的例外

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、国防安全直接有关的；
2. 与公共安全、公共卫生、重大公共利益直接有关的；
3. 与刑事侦查、起诉、审判和判决执行司法或行政执法直接有关的；
4. 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；
5. 所收集的个人信息是您自行向社会公众公开的，但您明确拒绝或我行收集、使用该信息侵害您重大利益的除外；
6. 从合法公开披露的信息中收集个人信息的，包括合法的新闻报道、政府信息公开等渠道，但您明确拒绝或我行收集、使用该信息侵害您重大利益的除外；

四、我行如何处理未成年人信息

1、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。如您提供的信息归属为未成年人，请未成年人的监护人仔细阅读本指引，并在征得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。

2、如果您是 14 周岁以下的未成年人，请特别注意，您的个人信息都属于敏感信息。对于经监护人同意而收集您的信息的情况，我们只会在受到法律允许、监护人明确同意或者保护您的权益所必要的情况下使用或公开披露此信息。如您的监护人不同意您按照本政策使用我们的服务或向我们提供信息，请您立即终止使用我们的服务并及时通知我们，以便我们采取相应的措施。

3、如您为未成年人的监护人，当您对您所监护的未成年人的信息处理存在疑问时，请通过本文中的联系方式联系我们。

五、我行如何使用 Cookie 和同类技术

（一）Cookie

为了确保网站正常运转，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数据。我们不会将 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。您可以清除移动设备上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。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

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。

六、您控制个人信息的权利

根据国家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、更正及更新个人信息

您有权访问个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，我行在企业网络银行为您提供了相应的操作设置，可以参考下面的指引进行操作。

1. 企业网上银行渠道：

（1）登录信息查询：企业网银登录后首页->查询当前企业网银用户本次登录时间，上次登录时间、登录 IP；

（2）操作员管理：企业网银登录->系统设置->操作员管理，可对操作员的企业网银登录密码及操作员企业 e 钱庄交易密码进行重置；修改操作员的登录名、姓名、证件类型、证件号码、手机号信息；

（3）单位信息更新：企业网银登录->系统设置->证件更新->更新单位证照及法定代表人的证件有效期；

（4）企业网络银行的云盾设置：企业网银登录->系统设置->云盾设置->单位管理员给操作员下发云盾；

（5）修改交易密码：企业网银登录->客户服

务->修改交易密码;

(6) 修改登录密码: 企业网银登录->客户服务->修改登录密码。

2. 企业 e 钱庄渠道:

(1) 登录方式设置: 企业 e 钱庄->我的->安全中心, 开启或关闭指纹识别、手势密码的登录方式;

(2) 证件更新: 企业 e 钱庄->我的->通用->证件更新, 更新企业证照及法定代表人的证件有效期;

(3) 修改交易密码: 企业 e 钱庄->我的->安全中心->修改交易密码, 修改账号交易密码;

(4) 云盾服务管理: 企业 e 钱庄->我的->安全中心->云盾服务管理, 解绑、更换设备或对转账额度进行修改;

(5) 操作员管理: 我的->操作员, 可查询本单位的管理员、操作员账号信息和权限列表; 修改操作员的登录名、姓名、证件类型、证件号码、手机号信息进行修改。

如果您无法通过上述方式访问这些个人信息, 您可以拨打客服电话 (0731-96511) 或通过在线客服与我行联系, 我行将在 15 个工作日内完成核查和处理。对于您在使用我行的产品或服务过程中产生的其他个人信息, 只要我行不需要过多投入, 我行会向您提供。如果您想行使数据访问权, 请拨打客服电话 (0731-96511) 或通过在线客服与我行联

系。

当您发现我行处理的关于您的个人信息有错误时，您有权通过我行柜面、企业 e 钱庄 App、企业网银等渠道访问及更正、更新您的个人信息，法律法规、监管政策另有规定的除外。您有责任及时更新您的个人信息。在您修改个人信息之前，我行会验证您的身份。如果您无法通过上述方式更正这些个人信息，请拨打客服电话(0731-96511)或通过在线客服与我行联系，我行将在 15 个工作日内完成核查和处理。

（二）删除个人信息

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了法律法规；
2. 如果我行收集、使用您的个人信息，却未征得您的同意（依法无需征得同意的情况除外）；
3. 如果我行处理个人信息的行为违反了与您的约定；
4. 如果您不再使用我行的产品或服务，或您注销了账号；
5. 如果我行不再为您提供产品或服务。

我行收到您的删除请求后，会根据您及相关法律法规的要求在 15 个工作日内完成核查和处理并向您反馈结果。若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。

如法律、行政法规规定的保存期限未届满，或者删除您的信息从技术上难以实现的，我行将停止除存储和采取必要的安全保护措施之外的处理。

（三）改变授权同意的范围

每个业务功能需要一些基本的个人信息才能得以完成。对于为提升产品或服务体验而额外收集、使用的个人信息（如位置、手机通讯录等），您可以根据手机的不同品牌和型号，在手机系统设置中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，随时给予或撤回您的授权同意：

您可通过手机银行企业e钱庄的操作路径“我的->关于我们->个人信息保护政策->撤销同意协议”，撤回对我行《企业网络银行个人信息保护政策》的授权。

请您注意，您自主注销我行企业网络银行服务（网络银行服务、手机银行服务、短信金融服务、微信银行服务等）的同时，将视同您撤回了对我行该《企业网络银行个人信息保护政策》的同意，例如您注销我行手机银行服务，视同您撤回了对我行手机银行《企业网络银行个人信息保护政策》的同意。当您撤回同意后，我行将不再处理相应的个人信息。但您撤回同意的决定，不会影响此前基于您的授权而开展的个人信息处理。

（四）注销账户

您可在工作日前往营业网点注销企业网络银行服务，我行会在 15 个工作日内完成核查和处理。我行将停止为您提供产品或服务，并依据您的要求，删除您的个人信息，法律法规另有规定的除外。

（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，您有权要求我行作出解释，我行也将提供适当的救济方式。

（六）举报和投诉

如果您发现您的个人信息可能被泄露，或者我的工作人员或合作伙伴在处理您的个人信息时有任何违法违规行为，您可以通过拨打客服热线或者发送电子邮件的方式向我们进行举报和投诉，我行会在 15 个工作日内完成核查和处理。

（七）响应您的上述请求

为了确保上述请求的提出系由您本人操作，保障您的个人信息安全，我行会对您的身份进行验证（必要时可能需要您提供书面请求），在身份验证通过后，会在 15 个工作日内完成对您的请求的核查和处理。对于您合理的请求，我们原则上不收取费用，但对于多次重复、超出合理限度的请求，我们将视情况收取一定的成本费用。对于那些无端重复、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（例如，涉及备份磁带上存放

的信息) 的请求, 我们可能会予以拒绝。

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. 与我们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、司法调查、审判和执行判决等直接相关的;
5. 有充分证据表明您存在主观恶意或滥用权利的;
6. 出于维护您或者其他个人的生命、财产等重大合法权益但又很难得到本人同意的;
7. 响应您的请求将导致您或者其他个人、组织的合法权益收到严重损害的;
8. 涉及商业秘密的。

七、本政策如何更新

根据国家法律法规变化及产品服务的更新变化, 我行将对本政策及相关规则进行修改, 修改后的内容会通过我行网站、网上银行、微信客户端等渠道发布公告, 企业 e 钱庄推送通知或者弹窗等方式 (我行将根据实际情况选择一种或多种方式) 公布并再次征求您的授权同意。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, 我行

将执行更新内容。更新后的隐私政策访问路径为：企业 e 钱庄 App-我的-关于我们-个人信息保护政策。

八、如何联系我行

如果您对本政策有任何疑问、意见或建议，可以通过拨打我行 96511 客服热线、登录我行官方网站（www.bankofchangsha.com）或到我行各营业网点咨询或反映。受理您的问题后，我行会在 15 个工作日内完成核查和处理。如果您对我们的回复不满意，特别是认为我们的个人信息处理行为损害了您的合法权益，您还可以向人民银行、支付清算协会、网信、公安及工商等监管部门进行投诉或举报。

个人信息控制主体全称：长沙银行股份有限公司

个人信息控制主体联系电话：0731-96511

个人信息控制主体联系地址：中国湖南省长沙市岳麓区滨江路 53 号

附件：长沙银行企业网络银行第三方插件（含 SDK）使用列表

为了向您提供更便捷、更安全的金融服务体验，在特定场景中，我行将调用第三方机构提供的应用服务工具。以下内容包含了您在使用企业网络银行业务中可能会触及的插件（含 SDK）产品，供您查询了解，具体如下：

1. 活体检测控件（云从 SDK）

机构名称：广州云从信息科技有限公司

获取信息：访问摄像头，获取人像识别信息
使用目的：在对公开户时，使用活体检测控件，
进行身份核验

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.cloudwalk.com/Terms/legal>

2. OCR 控件

机构名称：阿里巴巴网络技术有限公司

获取信息：读取上传的证照信息

使用目的：用于识别用户提供的营业执照、身
份证信息，用于身份验证模块

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

3. 百度地图定位 SDK

机构名称：北京百度网讯科技有限公司

获取信息：位置信息、设备唯一标识
(AndroidID)、sd 卡存储

使用目的：支持用户在网点查询功能中使用位
置信息、识别和存储设备标识

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://lbsyun.baidu.com/index.php?title=openprivacy>

4. 安全加固

机构名称：北京梆梆安全科技有限公司

获取信息：手机设备信息

使用目的：用于保护移动应用不被恶意篡改及破坏

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.bangcle.com/>

5. 云证通

机构名称：中金金融认证中心有限公司

获取信息：无

使用目的：使用数字证书进行移动端签名

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.cfca.com.cn/20180329/100002470.html>

6. 指纹控件 IFAA

机构名称：阿里巴巴网络技术有限公司

获取信息：指纹信息

使用目的：实现指纹快捷登录

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

7. 密码控件

机构名称：北京微通新成网络科技有限公司

获取信息：无

使用目的：对密码信息进行加密处理，防止密码被截取，确保密码输入的安全性

信息是否向第三方提供：否

隐私政策链接或官网地址：

<http://www.microdone.cn>

8. 签名控件

机构名称：中金金融认证中心有限公司

获取信息：无

使用目的：调用 U 盾数字证书对交易请求进行数字签名

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.cfca.com.cn/upload/20211117f1sm.pdf>

9. UC 浏览器内核

机构名称：阿里巴巴网络技术有限公司

获取信息：剪切板信息

使用目的：支持 H5 页面的展示及交互、用于访问剪切板（如账户总览、复制卡号等便捷客户操作）

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

10. 设备指纹（xindunSDK）

机构名称：北京芯盾时代科技有限公司

获取信息：终端标识信息（设备名称、设备型号、设备系统信息、设备序列号、mac、imei、imsi、root 状态、AndroidID）、传感器信息、位置信息、电话状态

使用目的：用于企业网络银行使用中的反欺诈识别功能、终端威胁感知和用户分析。

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.trusfort.com/private.html>

11. 威胁感知（trusfortSDK）

机构名称：北京芯盾时代科技有限公司

获取信息：终端标识信息（设备名称、设备型号、设备系统信息、mac、imei、imsi、root 状态、AndroidID）、位置信息、已安装的应用、电话状态、传感器列表

使用目的：检测设备运行环境安全性，防范恶意用户对 APP 进行网络安全攻击，进行风险分析，保护用户的信息和资金安全。例如：识别位置欺诈、风险进程、应用破解及调试、虚假设备、病毒库或虚假应用扫描等

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.trusfort.com/private.html>

12. 语音识别

机构名称：科大讯飞股份有限公司

获取信息：麦克风权限

使用目的：用于企业 e 钱庄企业智能乐乐客服机器人进行语音识别转化文字

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.xfyun.cn/doc/policy/privacy.html>

13. 神策分析 SDK

机构名称：神策网络科技（北京）有限公司
获取信息：设备信息（包括 Android ID、IDFA、IDFV、OAID、UUID 等）、唯一应用程序编号、浏览信息、屏幕信息、访问时间、功能点击情况、广告点击情况、页面点击频次、页面停留时间、位置信息、启动次数、登录次数
使用目的：基础数据收集与建模，驱动业务决策分析，收集使用企业网络银行的行为信息，用于统计、分析，强化风险控制，并向用户提供更优质的服务或产品
信息是否向第三方提供：否
隐私政策链接或官网地址：
https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_privacy_policy22255999.html

14. 视频客服

机构名称：网易云信
获取信息：摄相关权限、麦克风权限
使用目的：用于企业 e 钱庄在线开户客服认证审核。
信息是否向第三方提供：否
隐私政策链接或官网地址：
<https://netease.im/clauses?serviceType=>

15. 企业管家 (sinosunSDK)

机构名称：深圳兆日科技股份有限公司

获取信息：定位权限、摄相关权限、麦克风权限、存储权限（sd 卡存储）、蓝牙权限、手机终端唯一标识、手机自启动信息

使用目的：企业管家打卡，聊天使用定位权限，聊天发送图片和文件，使用存储权限（sd 卡存储），聊天拍照使用摄像头权限，聊天使用麦克风权限，密码器使用蓝牙权限，监听手机自启动完成广播

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.sinosun.com/>

16. 微信小程序 API

机构名称：深圳市腾讯计算机系统有限公司

获取信息：位置信息、微信昵称、微信头像、微信登录手机号码、微信 OpenId

使用目的：用于用户使用企业微信小程序时进行定位、分享、拍摄照片和视频、跳转呼啦快贷微信小程序

信息是否向第三方提供：否

隐私政策链接或官网地址：

https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy

17. UC 浏览器

机构名称：阿里巴巴网络技术有限公司

获取信息：APP 性能日志(设备型号、系统信息、设备名称、系统时间、设备厂商、ip、用户手机号)

使用目的：支持 H5 页面的展示、上传 APP 性能日志

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

18. 消息推送

机构名称：阿里巴巴网络技术有限公司

获取信息：deviceID、IMSI 号

使用目的：用于企业 e 钱庄消息推送

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

19. 移动分析

机构名称：阿里巴巴网络技术有限公司

获取信息：获取企业 e 钱庄运行日志，崩溃日志，数据日志，埋点日志、存储诊断日志

使用目的：上传 app 运行日志，用作系统分析，数据分析，性能分析

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

20. 阿里 UTDID 控件（UtdidSDK）

机构名称：阿里巴巴网络技术有限公司

获取信息：手机设备信息（手机终端唯一标志信息、IMEI、IMSI）、sd 卡存储

使用目的：用于设备标识以及存储设备标识

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

21. 阿里 mPaaS 框架控件（支付宝 SDK）

机构名称：阿里巴巴网络技术有限公司

获取信息：APP 性能日志（ip、位置信息、设备名称型号、设备系统信息、用户手机号、网络状态）、安卓系统消息、sd 卡存储

使用目的：统计 APP 性能、推送消息、请求接口、存储设备标识和移动分析日志

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

22. 阿里 mPaaS 框架无线控件

机构名称：阿里巴巴网络技术有限公司

获取信息：无

使用目的：无

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://www.aliyun.com/>

23. 华为消息推送 SDK

机构名称：华为软件技术有限公司

获取信息：唯一设备识别码（MAC、IMEI、IMSI、AndroidID）、手机型号、系统类型、系统版本、网络类型等

使用目的：华为消息推送

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://developer.huawei.com/consumer/cn/doc/HMSCore-Library/android-sdk-downl>

oad-0000001050986071

24. 小米开放平台消息推送 SDK

机构名称：小米科技有限责任公司

获取信息：唯一设备识别码（MAC、IMEI、IMSI、AndroidID）、手机型号、系统类型、系统版本、网络类型等

使用目的：小米开放平台消息推送，提升小米手机用户推送消息到达率

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://dev.mi.com/platform/push>

25. 微信 Open SDK

机构名称：深圳市腾讯计算机系统有限公司

获取信息：唯一设备识别码（MAC、IMEI、IMSI、AndroidID）、微信昵称、微信头像、微信登录手机号码、微信 OpenId

使用目的：用于分享、拉起小程序、跳转呼啦快贷微信小程序

信息是否向第三方提供：否

隐私政策链接或官网地址：

<https://sz.open.weixin.qq.com/>

