

# 中国工商银行电子银行章程

## （2026年4月版）

**第一条** 为了更好地向客户提供金融服务，中国工商银行（简称“工行”）开办电子银行业务，并根据《中华人民共和国个人信息保护法》《中华人民共和国反电信网络诈骗法》《中华人民共和国反洗钱法》《电子银行业务管理办法》等有关法律、法规和监管规定，制定本章程。

**第二条** 本章程所称电子银行业务，是指工行利用面向社会公众开放的通讯通道或开放型公众网络、以及为客户建立专用网络等方式，为个人和对公客户提供的手机银行、网上银行、电话银行等金融服务。

**第三条** 工行电子银行服务向符合中华人民共和国法律规定及工行相关要求的自然人、法人或其他组织提供。

**第四条** 工行、电子银行客户及电子银行交易的其他参与方，均须遵守相关法律法规、监管规定及本章程。章程内容可通过官方网站（[www.icbc.com.cn](http://www.icbc.com.cn)）-“注册申请”-“章程协议”栏目查询。

**第五条** 客户可在工行营业网点办理电子银行业务注册，也可通过“中国工商银行”APP、“工行企业手机银行”APP、工行官方网站（[www.icbc.com.cn](http://www.icbc.com.cn)）、工行官方客户服务热线（95588）等渠道自助办理电子银行业务注册。

客户申请注册和办理电子银行业务，应按照监管规定及

工行要求提供相关资料和必要信息，并保证所提供的资料和信息真实、准确、完整、有效，工行将对客户身份、提供的资料和信息进行审查、核实。

客户所提供的资料和信息如有变更，应及时通知工行进行变更。因客户未及时更新资料和信息，导致工行无法提供电子银行服务，或提供时发生错误的，客户不得将此作为取消交易、拒绝付款的理由，并应承担相应责任。

客户所提供相关证件有效期已过期的，应及时通过上述渠道通知工行进行更新，未在合理时间内更新且未提出合理理由的，工行将暂停或终止为客户办理相关电子银行业务。

**第六条** 电子银行客户身份认证方式（以下简称认证方式）包括数字证书、动态口令、静态密码、生物特征识别、短信验证码以及其他可用于识别客户身份的方式。客户身份认证介质是实现认证方式的物理载体，如U盾、电子密码器、银行卡、身份证件等。工行根据电子银行业务类型的不同，提供一种或多种认证方式供客户选择。

**第七条** 工行根据不同的客户类别、注册状态、认证方式和申请项目，为客户提供相应的电子银行服务。在营业网点注册的客户，与自助注册客户相比，可享受更全面的电子银行服务。

工行将根据客户金融需求及风险情况，在客户注册、限额调整、申领和更换U盾等环节为客户核定电子银行渠道限额，客户应配合工行开展尽职调查。业务存续期间，为切实

保障客户资金安全，工行将对客户电子银行渠道限额实施动态调整。

第八条 工行对使用客户身份标识（包括账户账号、卡号、用户名、电话或手机号码、终端设备信息等）并按照客户在工行设定的认证方式通过身份验证的电子银行操作均视为客户本人所为，并以客户发出的指令作为办理电子银行业务的有效依据。

第九条 客户办理电子银行业务，应遵守工行有关交易规则（可通过营业网点或官方网站-“注册申请”-“章程协议”栏目查询），并根据交易提示进行正确操作。

客户办理电子支付业务，应在账户支付能力范围内进行支付，账户状态应正常，并严格遵守支付结算业务的相关法律法规和监管规定。客户知悉并认可，工行验证无误并已执行的电子支付指令，不能变更或撤销。

第十条 不具有完全民事行为能力的个人客户申请注册和变更电子银行业务，应由其监护人代为办理，监护人应遵守本章程和相关电子银行业务协议约定。

第十一条 发生以下情况，客户应及时更新或更换相应身份认证介质：

- （一）身份认证介质有效期届满。
- （二）身份认证介质遗失、信息泄露或无法正常使用。

第十二条 客户使用电子银行应注意防范风险，风险包括但不限于：

（一）电子银行登录密码、支付密码或用户名等重要信息被他人猜出、偷窥，可能导致客户账户信息泄露、资金被盗、被他人进行恶意操作等情况。

（二）U盾、电子密码器等身份认证介质被他人盗取或在未经允许的情况下被他人使用，可能造成账户资金被盗等情况。

（三）客户手机或其他电子设备被他人盗取或在未经允许情况下被他人使用，可能造成通过其接收的账户及认证等信息泄漏，并可能导致账户资金被盗等情况。客户更换手机号时，未将以原手机号开通的工银信使等业务取消，当该手机号被电信运营商发放给其他人时，可能造成客户的账户信息泄露等情况。

（四）与办理电子银行业务相关的重要资料，如身份证件、银行卡、存折、预留银行印鉴等因遗失或保管不善，被他人冒用或盗用，可能造成被他人注册电子银行，并可能因此发生账户信息泄露及资金被盗等情况。

（五）客户因设备被植入木马病毒、受骗登录假网站或非法应用程序等原因，导致电子银行登录密码、支付密码、手机号、短信验证码、身份证件信息等重要信息被他人获取，可能造成被他人恶意操作、账户信息泄露、资金被盗等情况。

（六）不法分子通过网络聊天群、直播平台、电话短信等渠道，冒充平台客服、公检法、银行机构人员等，以客户涉嫌案件、电视或电话欠费、信用卡透支、投资理财、兼职

刷单、客服退款、网络借款、网络贷款刷流水等名义，诱骗客户提供验证码等信息，或将电子银行身份认证信息或介质交给他人，或将资金转入他人控制的银行账户，造成客户资金被盗，或因客户账户被用于转移涉诈资金、洗钱等导致客户承担相应法律责任。

第十三条 客户应采取风险防范措施，安全使用电子银行。这些措施包括但不限于：

（一）避免使用与本人明显相关的信息（如姓名、生日、常用电话号码、身份证件号码等）或具有明显规律性的字符（如重复或连续的数字或字母）作为密码；办理电子银行业务的密码应不同于其他用途的密码（如银行卡/存折密码、其他网站会员密码、即时通讯工具密码、电子邮箱密码等）；电子银行登录密码、支付密码（包括静态密码、U盾密码、工银电子密码器密码等）应设置为不同内容，并做到经常更换。

（二）保护好自己的银行卡和存折密码、电子银行登录密码、电子银行支付密码等重要信息，不要告知包括银行人员在内的任何人，不要在计算机、电话、手机或其他电子设备上记录或保留。通过具有存储和显示输入号码功能的设备办理电子银行业务后，应立即清除所存储的密码和账号等信息。

客户在使用电子银行过程中暂时离开或在完成电子银行交易后，应及时退出电子银行系统。

（三）妥善保管与办理电子银行业务相关的各项重要物品或资料，如身份证件、银行卡、存折、U盾、电子密码器、预留银行印鉴、手机及其他电子设备等，不得交给他人或非授权人员保管或使用，不得出租、出借、出售、购买银行账户（包括银行卡）及其电子银行身份认证介质，不要在不信任的网站或其他场所留下卡号、存折账号、身份证号、常用电话号码等个人信息，避免被不法分子利用进行电信网络诈骗、洗钱等非法活动，导致客户承担相应的法律责任。

（四）采取有效的措施（如安装正版操作系统以及防病毒软件和网络防火墙并及时更新）保护用于办理电子银行业务的计算机或手机等终端设备的安全，防止其发生信息泄露或被他人操控。不要点击陌生链接，不要从非正规应用市场下载安装软件，不要下载安装任何涉嫌淫秽色情、赌博、毒品的违法违规的应用程序。不要在网吧等多人共用的计算机上使用网上银行；不要通过公用电话使用电话银行。更换手机号码后，应及时办理手机银行、工银信使、短信认证等电子银行业务变更。

（五）使用网上银行应通过工行官方网站 [www.icbc.com.cn](http://www.icbc.com.cn) 进行登录，使用手机银行应从工行官方网站 [www.icbc.com.cn](http://www.icbc.com.cn)、[m.icbc.com.cn](http://m.icbc.com.cn) 或设备指定的应用市场下载“中国工商银行”APP、“工行企业手机银行”APP，使用电话银行应拨打 95588 或其他在工行官方网站公布的指定电话号码。客户应避免通过其他网址、号码、链接或软件登录电

子银行。

（六）客户使用工行账户进行在线支付应仅限于与工行开展在线支付合作的特约单位，不要在来源不明的网站或商户进行在线支付，防止密码和动态口令泄露。

（七）客户在使用电子银行或接收短信验证码时，不要开启操作系统及相关软件工具的远程协助、屏幕共享等功能；进行支付时应在核对收款方、支付金额等信息无误后再确认支付；在使用完电子银行并安全退出后，还应及时取出U盾等客户证书介质并妥善保管。

（八）工行在任何情况下都不会通过短信、电话、邮件等方式主动要求客户将资金转入某一指定账户，也不会向客户索要相关密码、验证码等内容。如他人（包括银行人员）向客户索要上述内容，请不要提供。客户如收到短信或邮件，涉及引导客户打开页面链接并要求输入电子银行密码、动态口令或短信验证码，或要求客户将资金转入某一账户的，应保持警惕，仔细辨认信息真伪，如有疑问，应及时通过95588服务热线或到工行营业网点查询。

（九）客户在通过电子银行渠道进行转账汇款、线上支付时，应确认收款方身份真实、准确、合法，不向陌生账户或涉嫌赌博、诈骗等非法活动的账户转移资金。对于工行根据电子银行交易规则要求客户输入短信验证码、或通过U盾等认证方式完成交易时，客户应仔细核对短信、U盾中收款方户名、账号等信息，并按照交易提示进行正确操作，谨防

被骗。

(十) 客户应经常关注账户内资金变化，发现账户被他人操作、电子银行密码泄露或其他可疑情况时，应立即办理账户挂失、密码重置、更换身份认证介质等手续。

**第十四条** 因工行内部人员违规操作或法律规定银行负有责任的其他原因所造成的客户账户资金损失由工行承担相应责任。

因客户泄露电子银行密码或短信验证码、U盾等身份认证介质保管不善、未尽到防范风险与保密义务导致客户损失的；由于客户手机越狱、手机Root、下载安装其他软件、访问其他网站等过程中含有病毒、木马程序或其他恶意程序，威胁客户终端设备信息和数据安全而导致客户损失的；或因客户引起的其他原因导致客户损失的，工行不承担责任。

由于不可抗力等不可归因于工行的情况而导致客户损失的，工行不承担责任。

**第十五条** 客户办理电子银行须按工行对外统一公布的《中国工商银行服务价目表》支付相关费用。《中国工商银行服务价目表》可在营业网点或门户网站(www.icbc.com.cn)-常用查询-服务价目表等渠道查询。电子银行业务收费项目、收费标准如有变更，工行将按照法律法规和监管规定进行公示。

**第十六条** 当发生以下情况之一时，工行将对客户开展尽职调查，限制客户的电子银行交易权限，或暂停、终止对

客户提供相关电子银行服务，或增加客户身份认证强度，或调整客户电子银行渠道限额、笔数，或解除账户挂接关系：

（一）客户利用电子银行系统差错、故障不当得利或造成他人损失；出于恶意或其他非法目的，利用电子银行进行不正当交易。

（二）发生不法分子假借客户身份盗用电子银行或其他危及客户资金安全的事件，或存在发生这种事件的可能。

（三）客户注册后连续2年以上未使用电子银行服务，或电子银行服务所涉及的全部账户已销户，或未按《中国工商银行服务价目表》缴纳相应费用。

（四）客户存在使用虚假证件、无效证件或冒用他人证件注册电子银行等行为。

（五）客户在工行预留的身份信息不完整、不准确，且拒绝按工行的要求进行补充、更新。

（六）客户办理使用特定终端信息（如手机/电话号码、电子邮件地址、设备识别码）的电子银行业务时，所提供的终端信息错误或变更终端信息后未及时通知银行更改，造成银行无法为终端所有人正常提供相应服务。

（七）客户涉嫌从事洗钱、非法集资、网络赌博、电信诈骗等违法行为，或存在遭受电信网络诈骗等潜在风险，或拒绝配合工行开展尽职调查工作，或经尽职调查仍无法排除相关嫌疑的情况。

（八）客户涉嫌出租、出借、出售、购买银行账户（包

括银行卡)、电子银行登录用户名及密码、电子银行身份认证介质的情况。

(九) 客户经国家有关部门认定已无经营资格,或被取消、吊销、终止有关业务资格的,或被撤并、解散、宣告破产或关闭的,或所从事交易业务违反法律、法规、监管规定或国家政策,或存在经营情况恶化或突发风险事件,及其他可能导致我行较大声誉风险、业务风险等的情况。

(十) 法律法规、监管及有权机关另有规定的情况。

**第十七条** 工行将根据法律法规及监管变化情况、业务发展需要等对电子银行业务功能及相关交易规则进行升级或调整,并采取网站公告、交易提示等适当方式告知客户,客户应按照升级和调整后的业务功能或交易规则办理电子银行业务。如客户不同意有关变更,可办理电子银行注销手续,客户继续使用或未注销电子银行的,视为同意有关变更。

**第十八条** 客户使用电子银行时,如其使用的服务功能涉及到工行其他业务的,须同时遵守与该业务相关的章程、服务协议及交易规则;如使用的服务功能涉及第三方(如:医保电子凭证)的,还应同时遵守第三方的交易规则。

**第十九条** 如有问题或疑问,客户可通过工行营业网点、官方网站([www.icbc.com.cn](http://www.icbc.com.cn))或“中国工商银行”APP、“工行企业手机银行”APP在线客服咨询投诉,或拨打工行服务热线 95588。

**第二十条** 如发生争议,客户可遵照法律法规、本章程

及相关服务协议的规定与工行协商解决。

客户向工行反映电子银行状态不正常后，应配合工行进行有关调查，并对所提供情况的真实性负责。

**第二十一条** 本章程由工行制定并修改。工行如对章程进行修改，将通过营业网点或官方网站等适当方式将修改后的章程进行公告，并可通过“中国工商银行”APP等渠道向客户推送通知。公告期内，如客户对章程的修改有异议而决定不继续使用电子银行的，可办理电子银行注销手续。公告期满，客户未注销或继续使用电子银行的，视为同意接受对章程的修改。

**第二十二条** 本章程自2026年4月1日起施行，原章程同时废止。