ICS 03.060
CCS A 11

Q/YJSRB

永济市三禾村镇银行有限责任公司企业标准

Q/YJSRB 001—2024
代替 Q/YJSRB 001—2023

网上银行服务规范

Internet Banking Services Specification

2024－10－25 发布　　2024－10－25 实施

永济市三禾村镇银行有限责任公司　　发 布

目　次

前　言

本标准根据 GB/T 1.1-2020 给出的规则起草。

本标准由永济市三禾村镇银行有限责任公司提出并归口。

本标准起草单位：永济市三禾村镇银行有限责任公司。

本标准主要起草人：石鸽

引　言

本标准旨在提高网上银行服务的规范性，提升服务质量，防控网上银行服务风险，保护金融消费者权益。根据网上银行服务质量关于服务安全性、客户体验、创新及前瞻性、实施保障等相关要求编制了本标准。

网上银行服务规范

1 范围

本部分规定了网上银行在服务安全、客户体验、创新与前瞻性、实施保障等方面应满足的服务规范要求，主要包括通过互联网向客户提供的网上银行和通过移动通信网络向客户提供的手机银行。

本部分适用于本行网上银行系统建设、管理、运营及测评。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32315-2015 《银行业客户服务中心基本要求》

GB/T 35273-2020 《信息安全技术个人信息安全规范》

JR/T 0068-2020 《网上银行系统信息安全通用规范》

JR/T 0071-2020 《金融行业信息系统信息安全等级保护实施指引》

3 术语及定义

下列术语和定义适用于本文件。

3.1

网上银行 internet banking

商业银行等金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向客户提供的网上金融服务。

3.2

网上银行服务系统 internet banking service system

本行网上银行服务系统包括企业网上银行系统、个人网上银行系统。

企业网上银行是本行为企业客户提供的集账户管理、转账汇款、代发代付等于一体的网上金融服务平台，为企业客户提供更全面的金融服务，在充分的保证网上企业银行产品安全、方便、快捷的基础上，满足不同客户的多样化需要。

个人网上银行系统根据签约渠道氛围柜面签约版和自助签约版，其中个人网上银行自助签约版具有账户查询、本行同名转账、购买理财方式等金融交易服务。

3.3

网上银行服务对象 internet banking service object

企业网上银行的主签约账户为单位人民币活期结算账户，账户状态正常且为通存通兑。个人网上银行和个人手机银行的签约账户为凭密码支取、账户状态正常的个人人民币活期结算账户。

3.4

网上银行交易验证 internet banking transaction verification

本行为个人手机银行客户提供短信验证码、UKEY 等交易验证方式；为个人网上银行客户提供 短信验证码、UKEY 等交易验证方式；为企业网上银行客户提供 UKEY 交易验证方式。网上银行系统向客户颁发中国金融认证中心（简称：CFCA）的数字证书，客户通过企业网上银行系统、个人网上银行系统、个人手机银行系统以 UKEY 等身份认证方式办理业务时，必须采用本行向其颁发的 CFCA 证书进行数字签名认证。

3.5

网上银行交易记录 Internet banking transactions

客户在网上银行系统进行交易所产生的电子信息记录为交易记账的有效凭据，由此所产生的记账凭据作为电子信息记录处理，并在网上银行系统进行有效保存。

4 概述

网上银行服务通过与直接用户进行交互提供，交互方式可包括以下内容：

a） 基于 Web 浏览器访问网上银行

b） 基于 APP 访问网上银行

c） 基于网络社交平台上的定制功能访问网上银行

注 1：小程序和公众号是一种网络社交平台定制功能的例子；

注 2：微信和支付宝是当前流行的网络社交平台。

4.1 网上办理原则

网上办理原则包括以下内容：

a）网上银行业务实行永济三禾村镇银行总行、营业网点三级管理，遵循统一管理、分级经营、确保安 全、讲求效益的原则。

营业网点对网上银行的业务需求（包括特色业务需求），须由以书面形式提交总行，由总行统一研究和组织开发。

总行负责制定统一的客户服务协议、业务操作规程、客户指导手册及各种凭证和表格。

4.2 网银客户分类

网上银行客户是指访问本行网上银行网站，进行信息查询或办理转账结算等业务的个人、企业和事业单位。网上银行客户按客户身份性质不同，分为企业客户、个人客户。

a）个人客户是指客户携带有效身份证件及复印件到本行营业网点办理客户注册手续，与营业网点签订网上银行服务协议，从营业网点取得动态口令卡的客户。可办理网上查询、转账汇款等各种业务，个人客户交易金额单笔限为 50 万元，单日累计金额为 200 万元。

b） 企业客户是指客户携带有效证件及复印件到本行营业网点办理客户注册手续， 并与营业网点签订网上银行服务协议，从营业网点取得 USB-key 的客户。可办理网上查询、转账汇款、代发工资等各种业务，交易金额单笔不超 1000 万元、日累计最高为 5000 万元。

5 网银业务管理

5.1 总行职责

网银业务管理总行职责包括以下内容：

a）负责制定网上银行发展规划及各项管理制度。

b）负责网上银行系统和网站的运行管理及维护。

c）负责制定和修改本行统一制式性客户服务协议、业务操作规程、客户指导手册及各种凭证和表格。

d）负责网上银行产品的统一研发、测试及上线工作。

e）负责组织网上银行产品的对外统一营销宣传和对内的业务培训。

f）负责网上银行业务风险的评估、管理、防范与控制等。

g）负责辖内网上银行产品的对外营销宣传和对内的业务培训。

h）负责辖内客户网上交易的资金结算处理。

5.2 营业网点职责

网银业务管理营业网点职责包括以下内容：

a）负责引导客户正确使用网上银行产品，并做好临柜业务宣传和业务咨询等解释工作。

b）负责具体办理网上银行业务，并按业务资格、全部或部分正确行使开户网点、受理网点的责任。

c）负责拟定补充协议。

5.3 各部门职责

网银业务管理各部门职责包括以下内容：

a）科技信息部负责网上银行业务的统筹管理和网上银行业务正常运转的技术保障。

b）计划财务部、风险合规部负责协助解决网上银行业务涉及到本部门方面的问题。各相关部门紧密配合，确保网上银行业务的顺利开展。

c）客户服务中心负责业务拓展。

d）计划财务部负责业务管理、业务支持。

6 操作人员管理

操作人员是指经过法人单位授权、具有操作代码及密码、能够登录到相应网上银行管理系统进行操作的内部人员。

操作人员管理要求如下：

a） 所有操作人员使用综合业务系统中柜员号作为登录代码。

b） 网上银行管理系统操作人员根据岗位设置的不同，分为管理员和操作员。

c） 网上银行管理系统操作人员按权限划分为总行、营业网点二级操作人员。

d） 操作人员应按照岗位分离、权限制约的原则进行设置，不得进行串岗、混岗业务操作。

7 网银证书管理

7.1 基本规定

本行网上银行安全证书（以下简称证书）是指由中国移动 CA 认证中心向证书申请人发放的含有申请人特征信息、公钥等有关要素，能够确认申请人唯一身份的一组电子信息。网上银行证书分为个人客户证书和企业客户证书。 网上银行证书的存放介质主要是 UKEY。UKEY 应视同重要空白凭证保管，实行专人管理、出入库登记制度。

7.2 个人客户证书

个人客户证书业务包括证书申请、换发、补发、废止、冻结、解冻、下载。选择 UKEY 需申请证书、下载证书后方可正常使用。证书申请时自动生成下载链接,个人客户需在有效期内完成下载,过期需到柜台重新下载后方可使用。个人客户证书介质遗失、损坏时，允许其办理证书冻结。

a）证书补发。受理网点为个人客户办理证书补发，应要求客户提供本人有效身份证件及复印件和至少一个已注册的账户凭证原件，并填写业务申请表，补发后证书有效期不变。客户需下载方可使用。

b）证书换发。个人客户证书有效期为二年，逾期自动失效。客户可在到期日之前一个月内到受理网点办理证书换发手续延长有效期；证书过期也可办理换发手续，换发成功后生成新的有效期；若客户原证书介质仍可使用，客户需在办理换发时一并提供。受理网点办理个人客户证书更新，应要求客户提供本人有效身份证件及复印件和至少一个已注册账户凭证原件，并填写业务申请表。客户需下载方可使用。

c）证书冻结、解冻。受理网点办理个人客户证书冻结、解冻，应要求客户提供本人有效身份证件及复印件和至少一个已注册账户凭证原件，并填写业务申请表。

d）证书废止。更换认证方式或客户要求进行证书废止，应要求客户提供本人有效身份证件及复印件和至少一个已注册账户凭证原件，并填写业务申请表。

7.3 企业客户证书

企业客户证书实际为企业操作员证书，企业客户至少要配备两个操作员。操作员权限可分为管理、录入和授权。企业客户证书业务须由开户网点受理，业务包括证书申请、冻结、解冻、补发、换发、废止、重发两码、下载，各项业务均已建立登记簿。

a）证书申请。受理网点办理企业客户证书申请，应要求客户提供法人授权委托书（经办人为法定代表人时不用提供，下同），法定代表人、经办人、新增管理员或新增操作员的有效身份证件及复印件，填写业务申请表，并至少填写一个已注册账户的账户信息。审核通过后，受理网点进行客户证书申请处理。证书需下载到 UKEY 后方可正常使用。

b）证书冻结。受理网点办理企业客户证书冻结，应要求客户提供法人授权委托书，法定代表人、经办人的有效身份证件及复印件，填写业务申请表，并至少填写一个已注册账户的账户信息。审核通过后，受理网点进行证书冻结操作。

c）证书解冻。受理网点办理企业客户证书解冻，应要求客户提供法人授权委托书，法定代表人、经办人的有效身份证件及复印件，填写业务申请表，并至少填写一个已注册账户的账户信息。审核通过后，受理网点进行证书解冻操作。

d）证书补发。受理网点办理企业客户证书补发，应要求客户提供法人授权委托书，法定代表人、经办人的有效身份证件及复印件,填写证书补发的业务申请表,并至少填写一个已注册账户的账户信息。受理网点审核通过后，具体完成证书补发的处理，补发后证书有效期不变。

e）证书换发。受理网点办理企业客户证书换发，应要求客户提供法人授权委托书，法定代表人、经办人员的有效身份证件及复印件，填写业务申请表，并至少填写一个已注册账户的账户信息。受理网点审核通过后，具体完成证书换发的处理。

f）企业客户证书有效期为二年，逾期自动失效。客户应在到期日之前到受理网点办理证书换发手续延长证书有效期；若证书过期也可办理换发手续生成新的有效期。若客户原证书介质仍可使用，客户需在办理换发时一并提供。

g）证书废止。受理网点办理企业客户证书废止，应要求客户提供法人授权委托书，法定代表人、经办人的有效身份证件及复印件，填写业务申请表，并至少填写一个已注册账户的账户信息。受理网点审核通过后，具体完成证书废止的处理。

8 服务安全性

8.1 基本安全要求

8.1.1 安全技术

8.1.1.1 网络通信安全

网络通信应满足以下安全要求：

a）应在客户端程序与服务器之间建立安全的信息传输通道，采用的安全协议应及时更新至安全稳定版本，取消对存在重大安全隐患版本协议的支持。

b）应采用每次交易会话采取独立不同密钥的加密方式对业务数据进行机密处理，防止业务数据被窃取或者篡改。

[**来源**：JR/T 0068-2020,安全技术规范 6.2]

c）应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。

d）应保证接入网络的核心网络的带宽满足业务高峰期需要。

[**来源**：JR/T 0071.2-2020,安全通信网络 8.1.2]

e） 应对网络实施控制措施，以保证网络上信息的安全性，防止未授权访问的发生。采取的控制措施应以下措施：

1)对网络实施符合业务要求的访问控制措施；

2)采取必要的安全设备对网络的流量、病毒等进行控制；

3)密切监视网络的性能、安全与日志，及时发现隐患及问题。

8.1.1.2 服务器端安全

服务器端应满足以下安全要求：

a）跨机构联网系统服务器应与本行业务主机系统隔离，网络设备访问权限应坚持最小安全访问原则，并对网络设备进行日常监控和检查。

b）对服务器应通过人工检查方式进行病毒检查。检查的周期间隔不得长于30日。

c）服务器应建立正式的备份策略，且按照指定的备份策略进行备份。

d）在所有服务器的操作系统中，所有安装的软件及工具均应进行控制，严禁任何人私自安装非法软件，非工作需要严禁安装以下类型的工具：

1）非工作需要严禁安装网络系统管理与监控工具；

2）非工作需要严禁安装漏洞扫面、渗透测试等工具；

3）非工作需要严禁安装网络嗅探、口令破解等工具。

8.1.1.3 数据安全

数据获取、传输、存储、展示、销毁环节应满足以下要求：

a）客户端应用软件应保证内存中不应存在完整的银行卡密码和网络支付交易密码明文。

b）客户端应用软件的临时文件中不应出现支付敏感信息，临时文件包括但不限于Cookies、本地临时文件等。

c）客户端应用软件应实现身份认证过程的防截屏、录屏，如：输入手势验证码、登录口令等。

d）客户端应用软件在授权范围内，不应访问非业务必需的文件和数据。

e）应在客户端应用软件与服务器之间建立安全的信息传输通道。

f）客户端应用软件不应以任何形式存储用户的支付敏感信息与金融管业务查询口令。

g）在满足法律、管理规定的前提下，客户端应用软件应仅保存业务必需的个人金融信息，并限制数据存储量。

h）客户端应用软件应在敏感数据使用完毕后，对其立即进行清除。

i）客户端应用软件卸载完成后，文件系统中不应残留任何个人金融信息。

[**来源**：JR/T 00092-2019,数据安全 5.5]

8.1.2 安全管理

8.1.2.1 安全管理机构

安全管理机构应满足以下要求：

a）应建立与金融机构发展战略相适应的网上银行信息安全保障及风险管理组织架构，建立由董事会、高级管理层负责、相关各部门负责人及内部专家参与的网上银行信息安全领导协调机制。明确各个部门职责，对其所负责的安全保障及风险管理内容进行管理，明确各部门章程并详细定义各部门人员配置。

b）应设立网上银行信息安全保障及风险管理工作的主要负责部门，由该部门组织制定、发布相关制度、规范，协调处置网上银行信息安全管理工作中的关键事项，组织跨部门应急演练等工作，应合理设立部门内部岗位，明确人员职责，明确该部门和其他各相关部门的职责范围、工作流程和沟通协调机制。

[**来源**：JR/T 0068-2020,安全管理规范6.3]

c）应设置网上银行产品设计，系统研发、测试、集成、运行维护管理，内部审计等部门或团队。

d）应明确业务、技术、审计等各部门网上银行信息安全保障及风险管理职责。

8.1.2.2 安全策略

安全策略应包括以下内容：

a）应制定网上银行系统使用的网络设备、主机设备、安全设备的配置和使用的安全策略。

b）应建立网上银行信息安全保障以及信息安全安全风险管理框架、策略及流程。

c）应定期开展覆盖风险识别及评价、风险监测及控制、审计和评估网上银行信息安全风险管理工作。

8.1.2.3 管理制度

管理制度应满足以下要求：

a）应建立涵盖网上银行系统需求分析、设计、编码、测试等研发阶段的安全制度规范。

b）应建立涵盖网上银行运行维护以及应急处置等过程的制度规范。

c）应指定或授权专门的部门或人员负责安全管理制度的制定。

d）应对安全管理人员或操作人员执行的重要管理操作建立操作规程。

8.1.2.4 人员安全管理

人员安全管理应满足以下要求：

a）应具有员工岗位调动或离职的安全管理制度，应取回各种工作证件、钥匙等以及金融机构提供的软硬件设备，避免系统账号、设备配置信息、技术资料及相关敏感信息等泄露。

b）应建立网上银行相关的员工培训机制，制定明确的培训计划，对网上银行相关管理人员、业务操作人员、开发设计人员、运维人员、风险管理人员、审计人员等进行安全意识教育培训以及岗位技能在职专业培训。

[**来源**：JR/T 0068-2020,安全管理规范6.3]

c）应建立外来人员管理制度，禁止外来人员操作网上银行在生产环境中的系统、设备、数据，在外来人员参观访问网上银行相关的区域或内容时，应提出书面申请并由专人陪同或监督，并登记备案，必要时签署保密协议。

8.1.2.5 系统运维管理

系统运维管理应满足以下要求：

a）应具有安全策略规定允许或者拒绝便携式和移动式设备的网络接入。

b）应定期对系统进行漏洞扫描，及时修补发现的系统安全漏洞。

c）对于所有用于加密客户数据的密钥，应制订并实施全面的密钥管理流程。

8.1.3 业务运作安全

8.1.3.1 业务申请及开通

网上银行业务申请及开通应满足以下要求：

a）应充分考虑并采取有效措施防范网上银行资金类交易开通的安全风险。

b）网上银行资金类交易的开通必须由客户本人到柜台申请，申请时，应对其进行风险提示，验证客户的有效身份，并要求客户书面确认。

c）客户通过已采取电子签名验证的网上银行渠道申请资金类交易的，视同客户本人主动申请并书面确认。

[**来源**：JR/T 0068-2020,业务运营安全规范6.4]

8.1.3.2 业务安全交易机制

业务安全交易机制应包括以下内容：

a）应按照审慎原则，采取有效、可靠的身份认证手段，保证资金类交易安全。

b）应采取交易验证强度与交易额度相匹配的技术措施，提高交易的安全性。高风险业务应组合选用下列三类要素对交易进行验证：一是客户知悉的要素，例如，静态密码等；二是仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；三是客户本人生物特征要素，例如，指纹、虹膜等。应确保采用的要素相互独立，部分要素的损坏或者泄露不应导致其他要素损坏或者泄露。以下资金类交易可不受上述限制：同一客户账户之间转账并且金融机构能有效识别转入、转出方为同一客户账户的。

c）应充分考虑、深入分析交易全流程的安全隐患，通过交易确认、交易提醒、限额设定等控制机制,有效防范交易风险。

d) 应根据自身业务特点，建立完善的网上银行异常交易监控体系，识别并及时处理异常交易，交易监测范围至少包括客户签约、登录、查询、资金类交易以及与交易相关的行为特征、客户终端信息，应保证监控信息的安全性。

[**来源**：JR/T 0068-2020,业务运营安全规范6.4]

8.1.4 个人信息保护

网上银行个人信息处理应遵从以下基本原则：

a) 权责一致原则——对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

b) 目的明确原则——具有合法、正当、必要、明确的个人信息处理目的。

c) 选择同意原则——向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意。

d) 最少够用原则——除与个人信息主体另有约定外，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除个人信息。

e) 公开透明原则——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。

f) 确保安全原则——具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

g) 主体参与原则——向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法。

[**来源**：GB/T 35273-2020,个人信息安全基本原则4]

8.2 服务连续在线可信性

网上银行系统应满足以下要求：

a) 网上银行系统服务时间为7x24小时不间断运行。

b) 网上银行系统可用率≥99.99%。

c) 网上银行系统数据丢失时间(RPO)=0。

d) 网上银行系统恢复时间(RTO)≤30分钟。

e) 网上银行系统及应用可用性监控覆盖率≥99%。

8.3 增强身份认证

应支持对交易操作环境的识别，如：客户端类型、IP、设备标识、客户端系统版本等。支持增强身份认证技术，包括：USB Key数字证书、短信验证码等。

8.3.1 USB Key 数字认证

USB Key应满足以下要求:

a) 应采取有效措施防范USB Key被远程挟持，例如通过可靠的第二通信渠道要求客户确认交易信息等。

b) USB Key使用的密码算法应经过国家主管部门认定。

c) 应设计安全机制保证USB Key驱动的安全，防范被篡改或替换。

d) USB Key应能够防远程挟持，具有屏幕显示或语音提示以及按键确认等确认功能，可对交易指令完整性进行校验、对交易指令合法性进行鉴别、对关键交易数据进行输入、确认和保护。

e) USB Key应能够自动识别待签名数据的格式，识别后在屏幕上显示或语音提示交易数据，保证屏幕显示或语音提示的内容与USB Key签名的数据一致。

f）应保证PIN码和密钥的安全:

1）PIN码应具有复杂度要求。

2）采用安全的方式存储和访问PIN码、密钥等敏感信息；

3）PIN码和密钥(除公钥外)不能以任何形式输出；

4）经客户端输入进行验证的PIN码在其传输到USB Key的过程中，应加密传输，并保证在传输过程中能够防范重放攻击；

5）PIN码连续输错次数达到错误次数上限(不超过10次)，USB Key应锁定。

[**来源**：JR/T0068-2020,专用安全机制6.2.2]

8.3.2 短信验证

短信验证码应满足以下需求：

a）短信验证码发送至客户在银行系统预留的手机号码。

b）短信验证码有效期应具有时间限制（不超过5分钟），超过时间验证码实效。

c）短信验证码有效期应结合所验证交易的风险程度进行设定，对风险程度较高的交易验证应设定相对较短的短信验证码有效期。

8.4 风险控制

网上银行应满足以下风险控制要求：

a）应制定分级标准，针对不同的风险规定相应的可能性等级列表，评定风险等级，对于已发现的风险应尽快修补或制订规避措施。

b）应建立网上银行信息安全风险的持续监测机制，建立风险预警、报告、响应和处理机制，明确风险报告的内容、流程、主客体以及频率，建立符合金融机构实际状况的关键风险指标体系，实现信息安全风险监测的自动化，保证高级管理层和相关部门及时获取网上银行信息安全风险变化，验证现有控制措施的有效性。

c）应根据网上银行信息安全风险评估发现的不同等级风险，以及风险监测获取的风险变化情况，制定风险控制措施、应急处置及恢复方案以及相关的演练计划。

[**来源**：JR/T 0068-2020,安全管理规范6.31}

d）身份认证方式的风险控制措施应满足以下要求：

1)应对设备标识进行识别，对更换设备登录作风险提示；

2)应设置风险交易黑名单机制，针对黑名单用户通过网上银行进行的交易及时进行阻断；

3)应设置风险预警系统，建立风险监测模型，实时监测网上银行风险交易，及时预警；

4)针对网上银行系统及各业务环节定期开展网上银行风险检查。

9 客户体验

9.1 服务功能

9.1.1 个人账户管理

9.1.1.1 账户信息查询

网上银行应支持个人银行结算账户的账户余额查询，交易明细查询等账户信息查询功能。

9.1.1.2 账户管理

网上银行应支持网上银行可操作账户的增加、删除、账户密码修改。

9.1.2 个人结算

9.1.2.1 转账汇款

网上银行应支持转账汇款功能，根据交易的到账时间，提供实时、普通、次日三种转账汇款方式选择。

9.1.3 个人存款

9.1.3.1 通知存款

网上银行应支持通知存款功能，通知存款类型包括：七天通知存款。

9.1.3.2 定期存款

网上银行应支持定期存款功能，根据定期存款期限，提供三个月、六个月、一年、两年、三年、五年选择。

9.1.3.3 大额定期存单

网上银行应支持大额定期存单功能。

9.2 服务性能

9.2.1 易用性

9.2.1.1 易学性

网上银行应满足以下易学性要求:

a) 信息应易识别，信息可视化。
b) 应提供充分清晰的操作指引提示信息。
c) 所使用的词语应保持前后一致性。
d) 操作界面的交互形式应従命用户习惯。

9.2.1.2 差错防御性

应具备以下差错防御措施:

a) 应提供必要的控制校验，做到错误预防，设置防错交互方式。
b) 提供有效建议，及时校验，提供二次确认，操作可撤销。
c) 出错后，应具有有效的纠错机制(保存数据、有效提示等)，帮助客户解决问题等。

9.2.2 便捷性

应满足以下便捷性要求:

a) 交易功能应易于查找，交易名称能清晰表示其作用，提供交易搜索功能。
b) 交易流程应设计简洁，并具有清晰的指引信息。
c) 交易信息反馈友好，交易结果或错误信息易于理解。

9.2.3 舒适性

9.2.3.1 美观性

应遵从以下美观性原则:

a) 界面风格应协调统一，简洁和优雅的表达有效信息。

b) 应做到配色和谐，合理运用色彩含义、色彩对比。

9.2.3.2 提示文案

提示文案应做到环境贴切，与现实匹配，使用日常、自然的语言与用户进行交流。

9.2.3.3 个性化服务

应提供常用交易自定义、界面主题自定等个性化设置服务。

9.2.4 易访问性

应满足以下易访问性要求:

a) 网上银行应支持 PC 电脑终端、手机备终端的访道。

b) 应提供网上银行官方门户网站，并提供安全的程序安装途径。

c) 应提供多样的登录方式，提高登录便捷性，如手势密码登录、指纹登录等。

9.2.5 APP 闪退率

APP 闪退率（一天中发生闪退的设备数/总体活跃设备数）≤0.05%。

9.3 客户代表行为规范

我们应加强并改善金融消费者的客户体验,持续提升永济三禾村镇银行整体服务金融消费者的水平及服务竞争力，从而通过服务塑造品牌、品牌创造价值，致力为永济三禾村镇银行的品牌影响力及金融综合服务水平夯实基础。

永济三禾村镇银行通过为广大金融消费者提供简单便捷、满足其金融诉求的贴心服务，为客户创造价值、积累财富，从而为银行提供持续发展的动力。银行员工在严格执行服务规范的基础之上，面对服务规范具体条款无法全部列举的场景，应遵循 BSZ 服务原则做出适合的决定和行动：

a)值得信赖（Believable）：秉承“小而精、精而美”的服务宗旨，合规守信，切实保护广大金融消费者客户权益，成为广大百姓心目中值得信赖的贴心银行、邻家银行、百姓银行。

b)契合需求（Suitable）：以客户需求为导向，为客户提供优质便捷、满足需求的产品和服务。倡导换位思考，从客户角度考虑问题，理解其诉求；不直接否定和拒绝客户；在合理合规的框架下，全力帮助客户用最合理的方式达成需求。

c)温暖热情（Zealous）：为客户提供自然亲切、人性化的温情服务，为客户构建一个温馨、舒适的网上银行平台，让客户有更好的服务体验。

9.4 客户服务响应

客户服务响应时间应满足以下要求：

a) 电话客服平均响应时间（转接人工客服后到人工客服接通平均时间）≤15 秒。

b) 线上客服平均响应时间≤5 秒。

c) 人工客服服务时间满足 7×24 小时。

d) 电话客服接通率≥95%。

9.5 适老化服务

应在更大程度上满足老年人的支付服务需求，在硬件设施建设上设置服务老年客户的放大镜、老花镜，无障碍通道等，为老年客户办理业务提供方便，营造良好的人性化服务氛围。科学安排营业时间，在老年客户消费需求相对集中的时间段，整合柜台力量，加大弹性服务，主动做好工作，减少老年客户办理业务的等候时间。开展老年人支付服务便捷窗口建设、适老化支付服务特色银行网点建设、优化银行网点支付结算业务办理、完善银行卡支付消费场景建设、加大老年人支付结算安全守护等工作，统筹开展，力争早日达成老年人享受智能化支付服务更加普遍，传统支付服务方式更加完善，线上线下支付服务更加高效协同的工作目标，营造老年人友好型支付环境。

10 创新及前瞻性

10.1 服务创新性

10.1.1 安全服务

创新服务安全保障措施应包括：

a）应支持不同安全级别的安全认证方式灵活选择。

b）应支持客户自助定制账户安全管理设置。

c）应搭建风险预警平台，建立风险识别模型，对可疑交易进行预警。

10.1.2 线上线下一体化服务

应提供以下线上线下一体化服务：

a）应支持手机银行扫码取款、刷脸取款等全新的、无需插卡的 ATM 快捷取款方式。

b）应支持不同业务场景的线上化、自动化、电子化办理流程。

10.1.3 特色开放与互联

应支持银企互联等个性化互联服务，探索开放 API 服务，构建金融生态云服务。

10.2 技术前瞻性

10.2.1 生物识别技术

应支持人脸识别功能，人脸识别具备活体检测能力，人脸客户端采集具备人脸攻击检测能力。

10.2.2 人工智能

应持续探索利用人工智能技术，为客户提供优化建议，产品推荐，推动业务发展。

10.2.3 大数据

应持续探索以下大数据技术应用：

a）应支持使用大数据等安全防范手段，在客户身份识别、行为识别、资信等级识别、网络环境识别等方面进行安全风险综合判断。

b）应支持使用大数据对用户分层及用户画像，分层及画像应用在对客个性化服务，安全感校验及营销服务上。

c）应支持基于大数据提供线上贷款服务，如动态核算授信额度、自动审批、贷后风险预警等。

10.2.4 云计算

应持续探索以下云计算技术应用

a）应使用基础设施云提高系统硬件虚拟化程度。

b）应使用应用平台云提高系统的敏捷性、可伸缩性。

10.2.5 双活接入

网上银行服务应支持异地/同城双活接入的高可用架构，提高系统灾备能力。

10.2.6 服务创新

网上银行增设爱心捐款、客户反馈等渠道，提高客户体验感和便捷感，增强客户反馈率，提高网上银行的设施通道，为客户带来更好更便捷的金融服务。

手机银行上线老年易用版本，聚焦老年客户、服务老年群体，解决运用智能技术困难的问题。“易用版”手机银行。通过分析老年客户常用的业务功能和使用习惯，着手解决老年客户使用手机银行的困难，帮助老年客户跨越数字鸿沟，享受金融业信息化、数字化发展的成果。“易用版”手机银行界面整合了老年客户常用的账户查询、转账、存款等功能，贴心提供大字号、大图标展示，流程及交互设计更贴合老年人使用习惯，提升老年客户的使用体验。

10.2.7 明确标识贷款年化利率

永济三禾村镇银行在贷款合同中，明确体现贷款年化利率，让客户更加明了化和便利化。

10.2.8 建设乡村振兴金融平台

永济三禾村镇银行在手机银行及官网上增设“农村善融”金融服务平台，抓住数字乡村战略机遇，进一步推动农产品进城和消费扶贫工作。同时打造地域化特色信贷产品，加强村级金融服务站的建设，保证农民更加便利的享受金融服务。

11 实施保障

11.1 组织保障

应组建专门的网上银行协调决策机构、专门的组织管理部门和业务、技术后台组织架构，明确各部门职责，建立管理机制。网上银行决策协调机构与职能管理部门应保证运转顺畅，保障有力。

11.2 管理制度

应建立网上银行管理完备的制度体系，涵盖服务章程、服务协议、产品收费、安全教育和展业规定及内部操作规程。

11.3 企业标准宣传

企业标准宣传应整合网点机构、官方网站、网上银行、微信公众号等线上及线下渠道，宣传企业标准。

11.4 企业标准实施机制

企业标准应具备以下实施机制：

a)应建立企业标准学习、培训机制，制作课件、开发培训课程。

b)针对企业标准实施情况，应定期组织检查，及时发现未达标准的业务环节，制定整改计划。