ICS 03.060
CCS A 11

Q/GLB

桂林银行股份有限公司企业标准

Q/GLB 02—2022

桂林银行网上银行服务标准

Internet banking service standard of Guilin Bank

2022-9-16 发布　　2022-9-16 实施

桂林银行股份有限公司　　发布

目　　录

前　言

本标准根据GB/T 1.1-2020给出的规则起草。

本标准由桂林银行股份有限公司提出。

本标准由桂林银行股份有限公司归口。

本标准起草单位：桂林银行股份有限公司。

本标准主要起草人：王晓青、刘清萌、李伟沙、沈桂斌、黄莹、秦阳健、韦玉谷。

企业标准信息公共服务平台
公开 2022年09月22日 14点54分

桂林银行网上银行服务标准

1 范围

本标准规定了桂林银行股份有限公司向客户提供网上银行服务时，在服务安全性、客户体验、创新及前瞻性、实施保障等方面应满足的规范要求，明确了网上银行服务标准。

本标准适用于本版本发布之日桂林银行股份有限公司提供的网上银行服务。

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 35273-2017 信息安全技术 个人信息安全规范

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 37668-2019 信息技术 互联网内容无障碍可访问行技术要求与测试方法

GB/T 32315-2015 银行业客户服务中心基本要求

GB/T 35274-2017 信息安全技术大数据服务安全能力要求

GB/T 27912-2011 金融服务生物特征识别安全框架

GB/T 31488-2015 安全防范视频监控人脸识别系统技术要求

GB/T 35678-2017 公共安全人脸识别应用 图像 技术要求

JR/T 0071.2—2020 金融行业网络安全等级保护实施指引 第2部分：基本要求

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0197—2020 金融数据安全 数据安全分级指南

JR/T 0199—2020 金融科技创新安全通用规范

JR/T 0223—2021 金融数据安全 数据生命周期安全规范

JR/T 0092—2019 移动金融客户端应用软件安全管理规范

JR/T 0068-2020 网上银行系统信息安全通用规范

JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引

JR/T 0166-2020 云计算技术金融应用规范 技术架构

JR/T 0167-2020 云计算技术金融应用规范 安全技术要求

T/PCAC 0009—2021 多方安全计算金融应用评估规范

T/PCAC 0007—2020 移动金融客户端应用软件安全检测规范

T/NIFA 9—2021 移动金融客户端应用软件安全评测规范

Q/200000 AF 2001—2021 移动金融客户端应用安全规范

3 术语与定义

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其客户提供的网上金融服务。

3.2

网上银行系统 Internet banking system

网上银行系统主要由客户端、通信网络和服务器端组成。本标准所指网上银行系统，不仅包括传统方式的网上银行系统，还包括以手机、平板电脑等移动终端方式访问网上银行系统。具体分为包括企业网上银行系统、个人网上银行系统、个人手机银行系统、直销银行系统、官网系统。

3.3

数字证书 digital certificate

由中国金融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。

3.4

USB Key

一种 USB 接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，利用内置的公钥算法实现对用户身份的认证。

3.5

敏感信息 sensitive information

影响网上银行安全的密码、密钥以及交易敏感数据等信息，密码包括但不限于转账密码、查询密码、登陆密码、证书的 PIN 等，密钥包括但不限于用于确保通讯安全、报文完整性等的密钥，交易敏感数据包括但不限于有效期、CVN、CVN2、证件号码等。

3.6

隐私信息 private information

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，主要指客户使用网上银行所需要或产生的企业信息、个人信息、交易信息等，包括但不限通讯地址、通信联系方式、设备信息、账户信息、交易记录信息等。

3.7

移动终端 mobile terminal

区别于传统 PC 机方式，以手机、平板电脑、可穿戴设备等通过通信网络访问网上银行的移动设备。

3.8

生物识别 biometric recognition

又称“生物特征识别”，通过利用人体固有的生理特性、行为特征等结合高科技手段来进行个人身份的鉴定，生物识别包括但不限于指纹识别、人脸识别等。

3.9

客服代表 customer service representative (CSR)

客户服务中心前台一线工作人员，利用电话、手机、WEB 等多种信息方式并接入以人工、自动语音、WEB 等多种方式为客户提供各种咨询类服务。

3.10

用户画像 user profiling

通过收集、汇集、分析个人信息，对某特定自然人个人特征，如其职业、经济、健康、教育、个人喜好、信用、行为等方面做出分析或预测，形成其个人特征模型的过程。

4 服务安全性

4.1 基本安全要求

4.1.1 总则

网上银行的安全技术、安全管理、业务运作安全、个人信息保护等均应符合 GB/T 35273-2017、JR/T 0068-2020、JR/T 0071-2012 规范和要求。

4.1.2 安全技术

4.1.2.1 客户端安全

客户端安全应满足以下要求：

a) 客户端程序在启动和更新时应进行真实性、完整性校验，防范客户端程序被篡改或替换；
b) 客户端程序开发设计过程中应注意规避各系统组件、第三方组件、SDK 存在的安全风险，应进行选型安全测试；
c) 应采用安全的方式对客户端程序进行签名，标识客户端程序的来源和发布者，保证客户所下载的客户端程序来源于所信任的机构；
d) 客户端程序应采取代码混淆、加壳等安全机制，防止客户端程序被逆向分析，确保客户端的敏感逻辑及数据的机密性、完整性；
e) 客户端程序应提供客户输入支付敏感信息的即时防护功能，并对内存中的支付敏感信息进行保护；
f) 客户端程序应采取有效措施保证所涉及密钥的机密性和完整性；
g) 客户端程序应采取措施对密码复杂度进行校验，保证用户设置的密码达到一定的强度；
h) 客户端程序应支持通过 IPv6 连接访问网络服务，在 IPv4/IPv6 双栈支持的情况下，优先采用 IPv6 连接访问。

4.1.2.2 网络通讯安全

网络通讯安全应满足以下要求：

a) 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) 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加密处理，防止业务数据被窃取或者篡改；

c) 使用加密算法和安全协议保护网上银行服务器与其他应用服务器之间所有连接，保证传输数据的机密性和完整性。

4.1.2.3 主机安全

主机安全应满足以下要求：

a) 合理部署网络架构，在网络边界、所有互联网入口以及隔离区（DMZ）与内部网络之间部署 DDOS 防护设备、异构防火墙、负载均衡、IPS、WAF 等网络安全设备，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安全配置检查；

b) 网络设备应支持 IPv6，针对 IPv6 的防护强度应不弱于针对 IPv4 的防护强度；

c) 通过必要的安全配置、安装必要预置软件等措施实现安全加固，确保宿主机、虚拟机管理器、虚拟机安全稳定运行；

d) 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。

4.1.3 安全管理

安全管理应满足以下要求：

a) 配备独立的产品设计、系统研发、测试、集成、运行维护、管理等部门和团队；

b) 配备一定数量的专职安全管理员、系统管理员、网络管理员等，且各岗位配备多人共同管理；

c) 建立网上银行信息安全保障以及信息安全风险管理框架、策略及流程，制订针对网上银行系统设计与开发、测试与验收、运行与维护、备份与恢复、应急事件处置以及客户信息保密等的安全策略；

d) 定期开展网上银行风险识别及评价、风险监测及控制、审计和评估等信息安全风险管理；

e) 定期对网上银行的技术人员及业务人员进行安全意识教育和培训；

f) 对第三方人员进行管理，禁止第三方人员直接操作生产环境，如需操作应提交信息技术部领导审批并由专人陪同或监督，并登记备案，签署保密协议。

4.1.4 数据安全及备份恢复

数据安全及备份恢复应满足以下要求：

a) 建立重要数据的定期数据备份机制，至少每天进行一次完整的数据备份，并将备份介质存放在安全区域内；

b) 对关键数据进行同城和异地的实时备份，保证业务应用能够实现实时切换；

c) 制订灾难恢复计划并定期进行测试，确保各个恢复程序的正确性和计划整体的有效性；

d) 采用监控软件保证日志的一致性与完整性；

e) 保护审计进程，避免其遭受未预期的中断；

f) 网上银行 WEB 服务器、中间件服务器、前置服务器、数据库服务器等关键数据处理系统均应采用虚拟化集群或者容器云的方式冗余，避免单点故障和数据丢失风险。

4.1.5 业务运作安全

4.1.5.1 业务申请及开通

业务申请及开通应满足以下要求

a) 个人网上银行、手机银行开通区分大众版和专业版，大众版需要客户绑定银行卡才能开通，支持查询信息，不支持交易，专业版需要客户持有效证件信息到柜台申请，并要求书面确认；
b) 企业网上银行开通需要客户到网点柜面进行申请，并对申请材料的真实性、完整性和合规性进行审查；
c) 客户申请 USB Key 作为数字证书载体时，应持有效身份证件到柜台办理，银行将 USB Key 设备序列号与客户进行绑定；
d) 企业网上银行的初始登录密码应使用密码信封或短信发送的方式分发给客户，个人网上银行的初始登录密码为客户自行设置，首次登录需要重新设置登录密码；
e) 申请客户数字证书时，应验证公钥的有效性，证书签名请求在进入 SSL 通道前应采取安全保护措施；
f) USB Key 密码忘记或者遗失应由客户持有效证件到柜台重新办理。

4.1.5.2 交易流程

交易流程应满足以下要求：

a) 应对客户端提交的交易进行唯一性认证，应能识别并拒绝重复交易；
b) 对于资金类等高风险业务，在确保客户有效联系方式的前提下，充分提示客户相关的安全风险并提供及时通知客户资金变化的服务，实时告知客户其资金变化情况；
c) 资金类交易中，网上银行系统应具有防范数据被篡改的机制，应由客户确认资金交易关键数据（至少包含转出账号、转入账号、交易金额、交易日期和时间），并采取有效确认方式以保证待确认的信息不被篡改；
d) 根据交易的风险特征建立风险交易监控平台，对盗账户、撞库、异常登录、虚假注册、套现、洗钱等异常情况进行有效监控并对检测到的可疑交易建立报告、复核、查结机制；
e) 企业网上银行进行资金类交易时，应至少使用硬件承载的数字证书进行签名等安全认证方式；
f) 建立完善的服务器交易日志，对每笔交易均有完整的日志记录；
g) 建立完善的风险事件处理流程，在风险管理、商户协查、核实、退款、案件调查与处理等主要流程均实现标准化和规范化，加快风险处理效率。

4.1.6 个人信息保护

个人信息保护应满足以下要求：

a) 个人信息控制处理应遵循：权责一致原则、目的明确原则、选择同意原则、最少够用原则、公开透明原则、确保安全原则、主体参与原则；
b) 在信息采集上遵从合法性要求、最小化、客户授权同意的基本原则；
c) 对个人信息的保存遵从时间最小化，同时传输和存储个人敏感信息时，应采用加密等安全措施；
d) 重视支付安全、强化移动金融的安全环境，通过开展多样化的安全监测实现风险防控，注意规避各终端平台存在的安全漏洞，采用有效技术措施保证移动终端处理的敏感信息、移动终端与服务器交互的重要信息的机密性和完整性；
e) 针对客户敏感信息采取多种防护措施，包括临时文件不出现敏感信息、证件号码屏蔽、高强度加密算法等；
f) 使用安全控件输入敏感信息，对敏感信息显示加强管控，对重要信息进行加密等安全措施，减少泄露风险；
g) 在密码技术方面，采用包括国际标准的加密协议、数字证书、符合国家相关规定的国际标准、国家密码标准的算法等多项技术手段防范金融信息泄露风险；

h) 建立有效的身份认证机制：多重身份认证，双重密码+短信/语音验证码+硬件级安全策略+生物特征识别等一项或多项的组合；
i) 在柜面和网上渠道定期对客户进行提示与教育，加强客户安全防范意识。

4.2 服务连续在线可信性

服务连续在线可信性应满足以下要求：
a) 网上银行系统服务时间为7×24小时不间断运行；
b) 配备有7×24小时运维应急人员，确保系统服务连续性，同时安排各个运维专业序列组的技术人员现场值班，确保7×24小时运维现场应急响应处理；
c) 网上银行系统可用率≥99.99%；
d) 网上银行系统应做好实时数据备份，保障在系统出现问题时可及时恢复且保证数据丢失时间（RPO=0分钟）；
e) 在系统出现紧急故障时，应急人员需在30分钟内处理和恢复系统（RTO≤30分钟）；
f) 监控系统对网上银行系统实现全方位监控，网上银行系统及应用可用性监控覆盖率≥99%。

4.3 增强身份认证要求

4.3.1 增强身份认证技术

4.3.1.1 USB Key

USB Key应满足以下要求：
a) 应采取可靠的第二通信渠道等有效措施要求客户确认交易信息以防范USB Key被远程挟持；
b) 应使用指定的第三方中立测试机构安全检测通过的USB Key；
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) 对USB Key固件进行的任何改动，都必须经过归档和审计，以保证USB Key中不含隐藏的非法功能和后门；
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) USB Key使用不低于RSA2048位密钥长度算法或者国密SM2算法证书加密或签名交易数据；
g) 应保证PIN码和密钥的安全，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。

4.3.1.2 数字证书

数字证书应满足以下要求：
a) 应使用指定的第三方中立测试机构安全检测通过的数字证书；
b) 应采取可靠的第二通信渠道要求客户确认交易信息等有效措施防范数字证书被中间人攻击；
c) 应验证公钥的有效性，证书签名请求进入SSL通道前应采取安全保护措施；
d) 应有身份认证过程，例如提交授权码和参考码。

4.3.1.3 短信验证码

短信验证码应满足以下要求：
a) 短信验证码应一次有效，有效时限为60秒；
b) 控制单用户一天内验证码获取次数防止恶意重放攻击。

4.3.1.4 语音验证码

语音验证码应满足以下要求：

a) 语音验证码应一次有效，有效时限为 60 秒；

b) 控制单用户一天内验证码获取次数防止恶意重放攻击。

4.3.1.5 动态软键盘

动态软键盘应满足以下要求：

a) 软键盘上的数字应随机排列；

b) 软键盘提供切换至键盘输入状态的功能；

c) 软键盘输入后，密码应使用相同位数显示；

d) 软键盘输入后密码于屏幕显示应为*、#等隐藏显示；

e) 软键盘输入后应防止表单枚举方式的输入窃听；

f) 软键盘输入密码进行不可逆的加密处理。

4.3.2 增强身份认证机制

增强身份认证机制应满足以下要求：

a) 对交易操作环境客户端类型、IP、设备标识、客户端系统版本等识别并记录；

b) 采用双因子验证方式，交易密码+验证方式（USB Key、短信验证码、语音验证码、云证通数字证书、生物特征识别）组合认证；

c) 针对移动设备登录新设备时需要绑定设备，绑定设备时需要校验客户信息；

d) 针对电子账户开通业务需要进行人脸识别、联网核查等认证；

e) 针对敏感时间（0 点-6 点）时间段的登录采用短信验证码、语音验证码等认证；

f) 客户登录网上银行时或登录后执行账户资金操作时，若身份认证连续失败超过一定次数（不超过 5 次），应在短时间内锁定该客户网上银行登录权限，并立即通过短信或电话等方式通知客户。

4.4 风险控制能力

制定并完善我行电子银行章程、网上银行业务管理办法等相关制度文件，规范网上银行业务管理，严格按照网上银行相关管理办法进行运营管理和操作处理，并根据内控管理要求认真进行业务流程及重点控制环节的梳理，严格执行内控和风险防范措施，同时网上银行系统接入黑名单系统、反洗钱系统、反欺诈系统等防控系统，提升风险控制能力。网上银行应满足以下风险控制要求：

a) 客户办理签约业务时：

1) 进行黑名单系统检测，对黑名单客户不予办理签约业务；

2) 应按照国家监管部门规定开展反洗钱工作，认真执行反洗钱有关规定，切实履行反洗钱工作义务，对客户进行洗钱风险级别检测，对洗钱风险级别较高的客户，需经过业务主管部门审批同意后方可办理；

3) 强化客户对自身敏感信息与隐私信息的保护意识，帮助客户特别是公司客户建立网上银行业务风险管理体系。

b) 客户登录及办理交易时：

1) 身份鉴别采用生物特征识别、密码、数字证书、验证码（语音、短信）等认证方式中至少两种组合；

2) 对于网上银行涉及的敏感信息和隐私信息在通信过程中采取加密措施，在系统存储中采取保密措施；

3） 反欺诈系统实时监控，对触及反欺诈交易规则的交易及时进行增强身份认证或阻断，并通知客户进行确认；

4） 能够根据交易的不同风险等级，通过不同交互方式如短信、电话、客户端软件等对客户的可疑交易进行确认和风险提示。

c） 客户交易风险应对：

1） 根据客户的风险诉求，及时进行网上银行转账停用、全部停用或启用操作；

2） 应对客户发生的交易风险，通过操作日志、网络日志等技术手段还原交易操作记录，对访问时间、IP、设备 ID、交易信息等进行记录和备份，发生风险事件时可供检查分析；

3） 利用数据分析、用户行为建模等技术，深入解析风险事件，不断完善交易风险监控规则和机制，开展各业务环节定期风险检查。

d） 客户交易事后处理与提示：

1） 应建立高效的网上银行各种安全、风险事件（包括不限于客户欺诈、舆情事件等）事后投诉、调查和处置机制；

2） 应定期对客户进行风险意识宣传和安全教育培训，向客户宣传典型欺诈、盗刷案例，提高客户的、风险防范、防骗防盗意识。

5 客户体验

5.1 服务功能

5.1.1 网上银行系统基础功能

网上银行系统应具有以下基础功能：

a） 注册：通过个人信息进行柜面注册和自主注册，可支持本行账户或他行账户；通过企业信息进行柜面注册，支持本行账户；

b） 登录与登出：登录代表客户可以完全使用网上银行系统中一个或多个业务功能，登录可通过账号密码、生物识别、USB Key 等验证方式识别客户信息以确定客户身份，登出是在客户完成业务功能使用后退出网上银行系统；

c） 忘记密码：在客户遗忘登录密码时使用，通过验证客户预留在本行的信息和相应的验证方式，重新设置登录密码；

d） 修改密码：修改密码成功后代表客户不再使用原密码，修改后的密码将作为登录密码使用；

e） 工具下载：可提供网上银行客户端、USB Key 驱动等工具下载，辅助客户使用网上银行服务。

5.1.2 网上银行系统业务功能

网上银行系统应具有以下业务功能：

a） 账户管理：可支持账户总览、账户信息查询、交易明细查询、外汇账户查询、他行账户查询、电子对账、电子账户开户、账户绑定与解绑、账户口头挂失、无卡取款、保号换卡等；

b） 转账汇款：可提供向本行、他行账户转账、代收代付、可支持账号转账、手机号码转账、预约转账、批量转账、保存转账模板、收款人名册、联行号查询等功能；

c） 投资理财：可支持储蓄类存款产品存入、提前支取，理财类产品的购买、撤销、赎回，基金类业务和第三方存管业务，风险评估等；

d） 贷款服务：可支持各类贷款线上申请、额度测算、合同签订、放款、还款、合同注销等；

e） 信用卡服务：可支持信用卡账户管理、卡片管理、密码管理、分期管理、还款管理、交易安全、信用卡申请等；

f) 生活缴费：可支持银行代理的话费流量、水电、社保、广电、交通罚款、非税等各项缴费业务，代扣签约等；
g) 安全中心：可支持交易限额设置、账户信息维护、管理绑定设备、小额免密免签、证书更新、USB Key 密码修改、银行卡磁条交易安全锁等；
h) 客户服务：营业网点查询和预约、用户资料修改、操作日志查询等。

5.2 服务性能

5.2.1 易用性

易用性应满足以下要求：
a) 系统界面设计样式统一，布局及交互方式合理，功能菜单名称及流程统一，便于客户理解和学习使用；
b) 在数据展示方面应采取数据可视化、信息可视化，复杂的数据信息简单明了展现；
c) 应着重注意信息的展现形式，突出最主要的信息，弱化次要信息，提高信息的沟通效率，减轻用户对信息的阅读负担，提高产品的易用性；
d) 提供必要、清晰、适用的操作指引以及常见问题处理方式，操作界面应提供充分的操作说明或提示信息，让客户通过简单的提示即可自行完成操作；
e) 具备差错防御措施，进行必要的误操作控制，提供二次确认和操作撤销，交易结果或错误提示明确易于理解；
f) 营业网点应提供自助服务终端，方便客户登录、下载、开通、使用网上银行服务。

5.2.2 舒适性

舒适性应满足以下要求：
a) UI 风格设计和谐，图标和字体大小适宜易辨认，图片和视频显示清晰无变形；
b) 应符合相关设计规范，设计风格协调统一，信息表达简洁和美观；使用标准配色，符合审美要求；
c) 在产品图标文案设计中，应尽可能的避免需要用户思考才能得出的元素，使用最能让客户一目了然的表达方式；
d) 支持常用功能和界面展示个性化定制；
e) 系统在主流设备上加载速度较快，功能操作流畅不卡顿，简化流程减少操作步骤。

5.2.3 便捷性

便捷性应满足以下要求：
a) 开放式架构，所有功能外露可见，支持具体功能的搜索查找；
b) 应做到功能易找，支持客户定制页面内容及功能入口、常用功能前置、栏目分类科学、导航清晰；
c) 支持根据历史记录和最近交易记录，提供功能推荐和快捷操作等；
d) 在网上银行中应提供操作演示的功能入口，不需要注册登录就可以查看浏览网上银行的各种功能；
e) 提供手势密码、指纹登录等多样的登录方式供选择，支持各系统间的统一账户体系，方便各系统无缝切换。

5.2.4 易访问性

易访问性应满足以下要求：

a） 应支持 PC 电脑端，手机、Pad 等移动端设备访问；

b） 应支持主流操作系统、浏览器、移动终端，浏览器支持 IE、Chrome、Firefox、360、UC 等，移动端应支持苹果、安卓等主流设备；

c） 应支持 2G、3G、4G 网络和 wifi 网络的访问；

d） 应支持手机号登陆、指纹、手势密码等多种快捷登录方式，且切换便捷；

e） 应支持被主流的搜索网站或应用商店搜索到。

5.2.5 APP 闪退率

手机银行App、企业网银App闪退率(一天中发生闪退的设备数/总体活跃设备数)应满足不高于0.07%。

5.3 无障碍服务

针对老年化客群特殊需求，结合实际提供以下便捷模式：

5.3.1 关爱版

a） 应具备大字体、大图标、文字高对比度等功能特点；

b） 应实现一键操作，文本输入提示等多种无障碍功能；

c） 应采用容易阅读的字体和便于理解的词汇；

d） 应为用户提供智能搜索业务；

e） 应减少广告等注意力干扰，确保老年人等群体的注意力不会被分散；

f） 应在渠道同类或相似场景中采用一致的交互方式。

5.3.2 智能语音数字人

a） 宜支持数字人服务功能，以降低界面操作的难度；

b） 应以人工智能语音交互技术简化操作路径，支持路径引导和文字等人机交互方式，快速定位用户需要的产品和功能；

c） 应支持智能客服功能，将用户咨询、建议等内容转由智能客服进行处理。

5.3.3 尊老热线

采用系统匹配识别技术，通过进线手机号码自动识别该号码关联客户的年龄，为60岁及以上老年客户免除语音菜单，简化按键环节，优先接入人工客服。

5.4 客服代表行为规范

5.4.1 职业守则

客服代表的职业守则应满足以下要求：

a） 诚实守信：诚实不欺，恪守信用，品行端正，树立诚信理念，坚持信誉至上；

b） 遵纪守法：严格遵守各项法律法规以及规章制度，自觉抵制违法违规行为；

c） 勤业尽职：热爱岗位，精益求精、尽心尽职，以高度的热情和责任做好本职工作；

d） 专业胜任：掌握相关业务知识，精通专业技能，不断学习新知识，提高业务水平，适应工作发展的需要；

e） 严格守密：严格遵守保密法规，自觉履行保密责任，不得泄露商业秘密和侵犯客户隐私；

f） 宽容有礼：时刻保持良好的观念和心态，想客户之所想，急客户之所急，礼貌热情地为客户提供服务。

5.4.2 职场秩序

客服代表职场秩序主要包括：

a） 不得留存客户相关信息并且私自交换联系方式；
b） 不得泄露客户资料，泄露公司机密；
c） 不得告知客户接线量、接线率、每个时段在线客服人数以及行内人员情况等信息；
d） 不得提供内部电话、部门信息、公司地址给客户；
e） 不得在通话中出现“外包”“现金科”“科技部”等信息，如需帮客户问题反馈到相关部门核实，统一告知反馈后台工作人员核实；
f） 不得在微信朋友圈等社交平台发布有关公司和工作的内容（公司已出官方公告除外）；
g） 不得使用手机在办公区域内拍照发至社交软件；
h） 办公区域办公设备禁止使用 U 盘；
i） 必须使用本人账号登录系统，如有特殊情况需及时报备；
j） 不得由他人代签入系统，不得无故长时间签出系统做与工作无关的事；
k） 不可将公司内部资料拷贝上传至社交软件；
l） 不可私下使用系统帮他人查询卡片信息并且拍照；
m） 不能将网点人员私人手机号码、部门座机电话（允许对外公开的除外）等提供给客户；
n） 不得在未经允许的情况下带非本行人员进入办公区域。

5.4.3 服务意识

客服代表的服务意识应满足以下要求：

a） 应具备良好的心理素质和主动服务的观念，始终保持积极的服务态度；
b） 应主动倾听，注意力集中，不随意打断客户，保持与客户之间的良好互动；不应表现出不耐烦、推托之辞等现象；
c） 应具备较强的沟通能力和表达技巧，能有效引导客户，控制通话时间；
d） 应具有较强的服务意识和责任心，积极主动地为客户解答问题，提供相关信息或帮助。

5.4.4 服务用语

客服代表的服务用语应满足以下要求：

a） 应使用标准的开头语和结束语，正确使用服务用语，耐心的倾听客户的问题，适时回应，不出现不耐烦、插话、抢话现象；
b） 应养成良好的通话习惯，保持适当的语速和音量，吐字清晰、流畅自然；
c） 应礼貌、规范使用服务用语，提倡讲普通话，恰当使用“请、请问、您、对不起”等礼貌用语；不得使用蔑视语、质问语、否定语；当客户提出意见、不满、建议、抱怨、感谢、夸赞时，需对应使用“感谢您的宝贵建议、非常抱歉给您带来困扰、谢谢、不客气等”；
d） 不得使用服务禁言语，严禁与客户争吵、顶撞、辱骂客户、主动或借故挂断客户电话。

5.4.5 业务能力

客服代表的业务能力应满足以下要求：

a） 应准确快速判断客户问题原因，了解客户实际需求，及时解决客户问题；
b） 应熟练准确、回答完整，处理有效，正面回答，相关业务知识丰富；

c） 对于超出解答能力范围的问题，应与客户重复确认，主动记录客户问题，及时反馈至相关部门，妥善处理客户意见和投诉。

5.5 客户服务

5.5.1 客户服务范围

客户服务范围包括但不限于：

a）业务咨询；
b）业务查询；
c）业务办理；
d）投诉受理；
e）其他服务。

5.5.2 客户服务渠道

服务渠道包括：

a）电话；
b）官网；
c）微信；
d）网上银行；
e）手机银行App；
f）企业网银App。

5.5.3 客户服务方式

服务方式包括：

a）电话银行语音服务；
b）在线客服文本服务。

5.6 客户服务响应

5.6.1 服务效率指标

服务效率指标要求主要包括：

a） 电话客服平均响应时间（转接电话人工客服后到人工客服接通平均时间）≤15秒；
b）电话银行接通率≥90%，确保客户的来电服务要求能得到及时响应；
c）电话客服服务水平≥80%，确保客户在列队中的等待时间较短；
d）在线客服接通率≥95%，确保客户的进线服务需求得到及时响应。

5.6.2 运营效率指标

运营效率指标要求主要包括：

a） 客服代表平均通话时长≤190s，通过该指标来测量客服代表的工作效率；
b）示忙话后处理率≤5%，通过示忙话后处理率来测量客服代表的有效工作时间。

5.6.3 服务质量指标

服务质量指标要求主要包括：

a）电话银行人工客服服务时间为7x24小时；
b）电话银行客户满意度≥99%，通过客户满意度来了解客户真实的服务体验。

5.6.4 智能化应用指标

智能化应用指标要求主要包括：

a）语音自助分流率≥50%，通过该指标来测量自助语音渠道对人工来电的分流作用；
b）机器人文本服务分流率≥90%，通过该指标来测量在线渠道机器人对人工的分流作用；
c）机器人问题解决率≥98%，通过该指标来测量在线渠道机器人解决问题的效率。

6 创新及前瞻性

6.1 服务创新性

服务创新性应满足以下要求：

a） 应始终坚持以客户为中心，以市场为导向，贴近客户、贴近市场需求，不断提升产品的客户体验和应用成效；
b） 应以信息通信技术前沿为大背景，在互联网和移动互联网新兴技术发展趋势和大众客群需求习惯的基础上开展定网上银行业务创新，可利用云计算、大数据、生物特性识别、人工智能、区块链等技术手段，满足客户需求、优化操作流程、提升服务质量；
c） 应在符合国家法律、监管规定和本行有关规章制度的前提下依法合规开展，对涉及的风险进行全面客观的分析，并在上线前落实相关风险管控措施和报告程序。同时在上线后加强风险监控，并视情况适时追加风险缓释及控制措施；
d） 应定期制定网上银行业务创新发展规划，开展创新项目，跟踪规划实现效果，为业务发展提供前瞻性、可落地的业务规划方案；
e） 应与本行的发展战略、信贷政策和风险管理策略相匹配；
f） 应在项目上线前制定相适应的内部管理制度，明确服务流程、会计核算、后台操作、员工培训等方面，做到有章可循，有法可依；
g） 应从服务理念、服务模式、交互体验等方面寻求主动创新；
h） 应以需求为导向，面向本行客户群体和目标市场，针对不同市场和客户提供个性化服务，并不断根据市场的变化和客户的需要开发新服务和改进已有服务；
i） 应充分研究同业及网上银行发展趋势，把握好网上银行安全性与服务性能的平衡，提供良好的客户体验。

6.2 技术前瞻性

6.2.1 前沿技术应用

a） 云计算

在云计算技术应用中，应满足 JR/T 0166-2018、JR/T 0167-2018 等规范。

应持续探索以下云计算应用：

1） 应使用基础设施云提高系统硬件虚拟化程度。单点服务器出现故障可以通过虚拟化技术将分布在不同物理服务器上面的应用进行恢复或利用动态扩展功能部署新的服务器进行计算；
2） 应使用应用平台云提高系统的敏捷性、可伸缩性。云计算的兼容性非常强，不仅可以兼容

低配置机器、不同厂商的硬件产品，还能够外设获得更高性能计算。

b) 大数据

在大数据技术服务中，应严格遵守 GB/T 35274-2017、《银行业金融机构数据治理指引（银保监发【2018】22 号）》、《中国银保监会银行业金融机构监管数据标准化规范（2019 版）》等规范。

应持续探索以下大数据技术应用：

1) 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，应支持使用大数据等安全防范手段；
2) 应支持给予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；
3) 应支持使用大数据对客户分层及用户画像，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) 生物特征识别

在生物特征识别技术应用中，应严格遵循 GB/T 27912-2011 标准的规定。

应持续探索以下生物特征识别应用：

1) 应支持使用生物特征识别鉴别客户身份，具备活体检测和防御伪冒介质及篡改攻击的能力，简化服务操作流程，提升认证安全能力；
2) 可提供客户营销接待、咨询引导、个性化服务等场景应用，提升服务体验。

d) 人工智能

在人工智能技术应用中，应严格遵守 GB/T 31488-2015、GB/T 35678-2017 等规范要求。

应持续探索以下人工智能技术应用：

1) 可支持替代人工实现规范化和专业化的客户接待、业务办理、业务咨询、营销推荐等服务；
2) 可提供建立在投资组合管理模型等基础上的智能投顾、账户管理服务，根据客户的风险偏好和投资目标提供资产配置和投资建议；
3) 可提供基于风险评估模型、机器学习等打造的智能风控应用，提升风险识别防控能力和实时性。

6.2.2 高可用架构

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。 本行网上银行系统现已实现同城双活，恢复点目标（RPO）小于 30 分钟，恢复时间目标（RTO）小于 4 小时。

7 实施保障

7.1 组织保障

——应设立网上银行业务运营、信息安全保障及风险管理工作的主要相关负责部门，组织制定、发布相关制定、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。

——应设置网上银行产品设计，系统研发、测试、集成、运行维护、管理等部门或团队，明确网上银行信息安全保障及风险管理职责，执行相应的风险评估、规划实施、应急管理、监督检查、跟踪整改等工作。相关人员应详细了解网上银行相关的职责设置、信息安全保障机制等基本情况。

——全行按两个层面落实网上银行管理和运营的职责：总行部门职责、各分支机构部门职责。在总行部门职责分工的基础上，各分支机构与总行对口的部门分别落实相应管理细节。网上银行相关的管理机构包括：总行渠道管理部、总行法律合规部、总行风险管理部、总行信息技术部、总行个人金融部、总行运营管理部、各级营业网点，具体职责分工如下：

a) 总行渠道管理部负责组织企业网上银行、个人网上银行、手机银行、官网等网上银行服务的业务规划、管理、协调、考核、培训和分析；负责网上银行服务相关制度的制定、修订和完善，对制度执行情况进行监督检查；负责网上银行服务的流程制定、风险管控、营销推广、数据分析和业务升级工作；负责研究网上银行服务的发展趋势，制定发展规划，实施网上银行服务创新和落地工作；
b) 总行法律合规部负责相关规章制度及服务协议、合同等相关法律性文件的合规性审查，并负责相关法律咨询工作；
c) 总行风险管理部负责从风险管理体系角度对网上银行的业务风险状况进行独立监控；
d) 总行信息技术部负责监督网上银行系统的开发、优化升级工作，以及现场人员管理、软件开发质量及进度跟踪、上线后的日常运行维护和向其他管理部门及时反馈等工作；
e) 总行个人金融部负责组织直销银行等网上银行服务的业务规划、管理、协调、考核、培训和分析；负责相关制度的制定、修订和完善，对制度执行情况进行监督检查，以及服务的流程制定、风险管控、营销推广、数据分析和业务升级等工作；
f) 总行运营管理部负责网上银行凭证的购入、下发及回收等管理工作；负责网上银行涉及会计业务、反洗钱业务的指导工作等；处理网上银行服务中客户的咨询、投诉及业务处理等工作；
g) 各级营业网点负责执行总行的网上银行业务制度，负责受理网上银行营销、签约、注销等具体业务，落实总行网上银行工作目标、业务拓展；负责客户使用本行网上银行服务的指导工作；负责日常网上银行客户的维护与管理。

7.2 管理制度

7.2.1 产品研发、测试投产、应急响应管理

网上银行产品研发、测试投产、应急响应管理应满足以下要求：

a) 制定《桂林银行信息科技需求管理办法》、《桂林银行信息科技项目管理办法》，规范信息科技系统建设，保障本行系统建设的工作规范、质量和效率；
b) 业务需求需要项目实施组对业务需求进行分析和梳理，形成需求规格说明书，制定相应的开发计划，并通过需求评审会；
c) 项目实施组根据需求规格说明书进行系统设计，形成相应的概要设计，详细设计，数据库设计和接口设计文档，并通过系统设计评审会；
d) 开发人员需要根据相应的设计文档进行开发，同时需参照信息科技开发规范进行序开发或修订，并完成单元测试或技术测试；
e) 项目测试包括 sit、uat、准生产测试，每个阶段的测试需要遵守信息科技部的测试规范进行，同时测试完成需要出具测试报告；
f) 项目投产需要提交测试报告、测试案例、代码清单、上线申请单，进行线上审批，审批通过才能上线；
g) 项目实施过程中需要每周汇报各个阶段实施进度，遇到风险及时汇报；
h) 严格按照本行相关应急预案实施，对相关机构在应急响应中的职责范畴进行界定，全面提高对突发事件的综合管理水平和应急处置能力；
i) 定期开展应急演练，形成应急演练报告。

7.2.2 生产运营及业务管理

网上银行生产运营及业务管理应满足以下要求：

a) 制定《桂林银行电子银行章程》、《桂林银行企业网上银行业务管理办法》、《桂林银行个人网上

银行业务管理办法》、《桂林银行手机银行业务管理办法》等网上银行系统管理办法，明确各部门职责、人员分工、业务规则、交易规则、客户管理、错账处理、凭证管理、收费标准、安全管理等，规范网点柜面及业务人员业务操作流程和行为，指导网点人员开展营销和服务工作；

b) 应指定专门人员每年对网上银行涉及的管理办法、操作规程、营销指引等相关制度的制定和修订；

c) 应通过内部 OA 正式公文、邮件、通知等正式、有效的方式进行制度发布，并进行版本控制；

d) 应明确承担网上银行产品总体管理职责，牵头业务部门负责牵头统筹网上银行产品的需求分析、组织产品开发、测试、投产运行、产品评价等工作；

e) 牵头业务部门应承担负责项目的职责，协调相关业务部门、总行信息技术部进行需求确认、测试验收、投产上线。提出产品需求的相关部门应配合做好业务的测试工作，按照整体项目计划，测试验收。

7.3 企业标准宣传及实施机制

网上银行服务标准宣传及实施机制应满足以下要求：

a) 应切实加强机构内人员企业标准教育和风险提示，通过本行内部 OA 正式公文、邮件、通知等渠道发布至全行人员进行阅读和学习，并要求全行人员遵照执行；

b) 开展本服务标准全行培训体系，根据培训的目标和参加培训的人员采取相应的培训方式，确保全行人员理解并执行；

c) 建立网上银行服务标准实施监督考核机制，由相应管理部门负责监督和考核标准执行情况，可定期开展现场、非现场检查方式进行监督，通过下达任务及指标并定期通报，对执行情况进行考核，对客户使用网上银行服务的体验和满意度等通过总行集中运营中心或委托第三方机构进行跟踪和调查，发现问题及时整改落实；

d) 积极参与网上银行服务企业标准的各类评选活动，对新制定的标准及时上传至企业标准信息公共服务平台，供公众查询、借鉴和监督。