ICS 35.240.40
A11

Q/GXNX

广 西 农 村 信 用 社 企 业 标 准

Q/GXNX 002-2020

网上银行服务企业标准

GUANGXI RURAL CREDIT UNION

Service Specification of Internet Banking

2020 - 09 - 30 发布　　2020 - 10 - 30 实施

广 西 壮 族 自 治 区 农 村 信 用 社 联 合 社 发 布

目　　次

前　言

本标准按照GB/T 1.1 2009给出的规则起草。

本标准由广西壮族自治区农村信用社联合社提出。

本标准由广西壮族自治区农村信用社联合社电子银行部归口。

本标准起草单位：广西壮族自治区农村信用社联合社。

本标准主要起草人：韦晓刚、郑胜前、马华、高干、彭雯、沈超、战韦达、劳谦。

本标准为首次制定。

广西农村信用社网上银行服务企业标准

1 范围

本标准包含了服务安全、客户体验、创新及前瞻、机制保障四大模块内容，明确网上银行服务标准。
本标准适用于广西农村信用社（农村商业银行、农村合作银行）网上银行服务相关工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。
[1] GB/T 35273—2017 信息安全技术个人信息安全规范
[2] JR/T 0068—2020 网上银行系统信息安全通用规范
[3] JR/T 0071 金融行业网络安全等级保护实施指引
[4] JR/T 0171-2020 个人金融信息保护技术规范
[5] GBT27912-2011金融服务生物特征识别安全框架
[6] GB/T32315-2015银行业客户服务中心基本要求
[7] GM/Z 0001-2013 密码术语
[8] GB/T 22239-2019 8.1.1信息安全技术网络安全等级保护基本要求
[9]《银行业金融机构数据治理指引》
[10]《银行业金融机构监管数据标准化规范》
[11]《电子银行业务管理办法》

3 术语与定义

下列术语和定义适用于本文件。
为了便于使用，以下重复列出了GM/Z 0001-2013 中的一些术语和定义。

3.1

网上银行 internet banking
商业银行等银行业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

个人网银 personal internet banking
商业银行等银行业金融机构面向个人用户提供的网上金融服务。

3.3

企业网银 corporate internet banking
商业银行等银行业金融机构面向企事业单位和其他组织提供的网上金融服务。

3.4

支付敏感信息 payment sensitive information

影响网上银行安全的密码、密钥以及交易敏感数据等。

注：密码包括但不限于转账密码、查询密码、登录密码、证书的 PIN 等，密钥包括但不限于用于确保通讯安全、报文完整性等的对称密钥、私钥等，交易敏感数据包括但不限于完整磁道信息、有效期、CVN、CVN2 等。

3.5

移动终端 mobile terminal

区别于 PC 机方式，以手机、平板电脑、可穿戴设备等访问网上银行的移动设备。

3.6

客户端程序 client program

为网上银行客户提供人机交互功能的程序，以及提供必需功能的组件。

注：包括但不限于可执行文件、控件、静态链接库、动态链接库等。本标准中客户端程序包括运行于移动终端上的应用软件，不包括 IE 等通用浏览器。

3.7

数字证书 digital certificate

也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.8

SSL协议 secoure socket layer protocol

一种传输层安全协议，用于构建客户端和服务端之间的安全通道。

3.9

生物特征 biometric

人类生理上的或行为上的可测量特征，并由此可以可靠地区分某个人不同于其他人，以便识别登记者的身份，或者确认其所声称的已登记的身份。

3.10

资金类交易 funds transaction

通过网上银行进行的资金操作交易。

注：例如，转账、订单支付、缴费等。本人名下的投资理财、托管账户以及本人签订委托代扣协议的委托代扣等风险可控的资金变动不属于此范畴。

3.11

信息及业务变更类交易 information and business changing transaction

通过网上银行变更客户相关信息或开通、取消业务的交易。

注：例如，客户修改基本信息、调整交易额度、授权委托交易、修改交易订单、开通（签订）新业务、取消某项业务、电子合同签署、电子保单等。

3.12

客服代表

通过多种渠道（电话、互联网等）为客户提供服务的一线人员。

3.13

农信银中心

农信银资金清算中心有限责任公司（以下简称农信银）是为全国农村中心金融机构提供资金清算服务的全国性专业特许清算组织。

4 缩略语

下列缩略语适用于本文件。

DoS/DDoS：拒绝服务/分布式拒绝服务（Denial of Service/Distributed Denial of Service）

IDS/IPS：入侵检测系统/入侵防御系统（Intrusion Detection System/Intrusion Prevention System）

SDK：软件开发工具包（Software Development Kit）

DNS：域名系统（Domain Name System）

VPN：虚拟专用网络（Virtual Private Network）

RPO：恢复点目标(Recovery Point Object)，指业务系统所能容忍的数据丢失量。

RTO：恢复时间目标（Recovery Time Objective, RTO），网络或应用停止工作的最高可承受时间。

5 服务安全性

5.1 基本安全规范

5.1.1 等级保护要求

应满足 JR/T 0068—2020 网上银行系统信息安全通用规范中的要求。

5.1.2 客户端安全要求

a) 客户端程序在上线前应该完成代码安全性测试。
b) 应有累计登录错误次数控制。客户首次登录时，系统应提示客户修改登录密码。应设置密码复杂度校验规则对用户设置的密码复杂度进行校验。在客户端程序应实现超时自动退出。
c) 应有权限控制机制的安全措施。
d) 应采用预留信息，私密问题设置安全机制帮助客户有效识别正确的客户端。
e) 客户端在收集、使用客户信息之前，应明示收集、使用信息的目的、方式和范围，公开其收集、使用规则，并取得客户的明示同意。
f) 客户端应用软件向移动终端操作系统申请权限，应遵循最小权限原则。
g) 涉及资金变动交易，应采取交易验证强度与交易额度相匹配的技术措施，提高交易安全性。
h) 用户敏感信息（账户余额、卡号、身份证号、手机号、输入密码等）应默认脱敏显示。

5.1.3 通讯网络安全

5.1.3.1 安全基础

a) 应符合 GB/T 22239-2019 8.1.1 安全物理环境、GB/T 22239-2019 8.1.2 安全通信环境、安全区域边界中的相关要求。
b) 网上银行的互联网出口应部署 DDOS 防御、清洗的设备或者服务。
c) 应部署防火墙设备、网络入侵检测/防御系统（IDS/IPS）、WAF（web 应用防火墙）。
d) 应进行网络区域隔离，防止来自外部的黑客攻击，并隐藏内部服务器的真实地址。

5.1.3.2 结构安全

a) 应使用前置设备实现跨机构联网系统与入网金融机构业务主机系统的隔离,防止外部系统直接对入网金融机构业务主机的访问和操作。
b) 应对进出网络的数据包进行过滤，识别可疑的数据包并进行处置。
c) 应定期对无线访问点进行排查,应在连接无线访问点的网络和其他网络之间采取隔离等有效的防护措施，避免访问者渗透到其他网络。
d) 具备互联网访问入口的测试环境，网络安全防护要求应同生产环境保持一致。

5.1.3.3 通讯协议

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加密处理,防止业务数据被窃取或者篡改。
c) 根据数据传输的安全要求，应使用安全的算法组合。
d) 应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。

5.1.3.4 访问控制

a) 网络设备应按最小安全访问原则设置访问控制权限。
b) 应定期对网络设备、安全设备、堡垒机、VPN 等设备的密码进行排查，避免使用默认密码、常见弱口令以及包含个人、机构和设备等信息的口令，避免使用存在一定规律的口令。
c) 应对设备的密码进行严格管控，强制定期更新密码。
d) 应对设备管理界面的访问地址进行严格限定，对异常的访问请求进行记录和预警。
e) 应在与分支机构、合作单位等网络边界设置基于协议及应用内容的访问控制措施。

5.1.3.5 入侵防范

a) 应使用 IDS/IPS 设备,制定合理的安全策略配置,并指定专人定期进行安全事件分析和安全策略配置优化。
b) 应防范对网上银行服务器端的异常流量攻击:安全设备开启 DoS/DDoS 防护功能, 使用负载均衡和恶意流量清洗设备。

5.1.3.6 网路安全管理

a) 将关键网络设备存放在安全区域,应使用相应的安全防护设备和准入控制手段以及有明确标志的安全隔离带进行保护。
b) 不应将管理终端主机直接接入核心交换机、汇聚层交换机、服务器群交换机、网间互联边界接入交换机和其他专用交换机。

c) 应更改设备的初始密码和默认设置，并定期采用技术手段进行检测等方式以识别不安全的配置。
d) 指定专人负责防火墙和路由器的配置与管理，并定期审核配置规则。
e) 在变更防火墙、路由器和 IDS/IPS 配置规则之前，确保变更已进行验证和审批。
f) 应对网络设备运行状况进行日常监控和检查，发现异常应及时报警和处理。
g) 应不定期组织安全测评，及时进行漏洞修复和加固处理。
h) 应对 VPN、堡垒机的操作行为进行监控和审计，对异常的账户创建、设备访问等行为进行监控和预警。
i) 应定期对软硬件资产进行核查，对已弃用设备进行下线处理。

5.1.4 与外部通讯安全

5.1.4.1 线路安全

a) 专线接入：
   1) 专线传输交易信息时，对报文进行加密；对传输信道加密；对报文进行完整性验证；对报文进行防抵赖认证。
   2) 在租用专线时，备份线路和主线选用不同的运营商。
b) 互联网接入：
   1) 使用安全传输通道进行通讯，传输数据时进行认证。
   2) 传输会话依据安全策略要求定时重新协商会话密钥。
   3) 采用白名单、数字证书等技术手段，防止 DNS 欺骗、流量劫持等攻击。

5.1.4.2 数据安全

a) 对外部机构发送的报文进行校验，保证数据报文的完整性。采用签名运算时，签名数据应包含报文中的关键信息。使用符合国家密码主管部门认可的密码算法。
b) 对与外部机构交互的报文进行传输加密，保证信息传输安全。
c) 对支付敏感信息的采集、展示、传输、存储、使用等环节制定保护策略。
d) 应使用安全加密算法加密或者签名交易数据。

5.1.5 安全管理规范

a) 应设立专门的安全管理机构，并制定网上银行相关的安全管理办法。
b) 应明确安全管理机构和其他各相关机构的职责范围、工作流程和沟通协调机制；
c) 应为网上银行系统建立整体安全评估机制，并重点关注新系统上线和系统功能变更的安全评估；
d) 应为网上银行系统建立定期的源代码安全审计、安全渗透测试和漏洞检查机制；
e) 应为网上银行系统建立安全风险分析及处置机制；
f) 应为网上银行系统建立安全应急管理机制，具备安全事件的应急处理能力；
g) 应定期对网上银行系统相关的技术及业务人员进行安全意识教育及培训。

5.1.6 业务运营安全规范

5.1.6.1 操作人员管理

操作人员需经过法人单位授权，权限划分应职责清晰、按照岗位分离、权限制约，严禁他人代操作，不得串岗、混岗操作。

5.1.6.2 用户管理

网上银行用户根据身份性质和交易认证方式的不同，分为不同的用户类型。

5.1.6.3 证书管理

a) 网上银行证书分为企业客户证书和个人客户证书。
b) 证书存放介质 USBKey 或 V 盾作为重要空白凭证管理，实行专人管理。
c) 数字证书在发放时，客户、证书、USBKey 或 V 盾三者需相互对应。

5.1.6.4 安全业务管理

网上银行系统各级操作人员必须按照规定履行各自职责，严格遵守相关规定办理各项业务。指定一定数量的管理员对网上银行系统进行监控，发现可疑信息或客户对交易有疑义的，要及时进行核查和处理。建立网上银行业务的自律监管与检查制度。

5.1.7 个人信息保护

满足GB/T 35273-2017所规定基本要求。

5.2 服务连续的在线可信性

服务连续在线可信性应满足以下要求：
a) 网上银行系统支持 7×24 小时不间断运行。
b) 配备 7×24 小时运维值班人员，保障系统平稳运行。
c) 网上银行系统年可用率≥99.99%。
d) 应用的灾难恢复所需时间目标（RTO）≤4 小时。
e) 应用的灾难恢复时间点目标（RPO）≤30 分钟。
f) 网上银行系统的可用性监控覆盖率≥99%。

5.3 身份认证

5.3.1 身份认证技术

a) 对于不同限额的转账，使用不同的身份认证技术，如进行大额交易时使用 USBkey 或 V 盾来加强身份认证。对短信验证码设置有限时限，防止恶意重发。
b) 对客户端系统版本，设备标识，客户端类型进行识别并记录。采用对因子验证的方式，组合认证。
c) 应设计合理的安全机制保证 U-Key 的驱动安全以及 V 盾的硬件数字证书的安全,防止被篡改或替换。使用的 U-Key 或 V 盾应通过有资质的检测机构安全检测。

5.3.2 增强身份认证

a) 对客户端系统版本，设备唯一标识，客户端类型进行识别并记录。
b) 采用多因子验证的方式，组合认证；
c) 在进行自助开户时加入人脸识别、联网核查等技术认证。
d) 若客户在操作网上银行时身份认证连续失败超过一定数量,应锁定客户当日网上银行的登录权限，并立即通过短信或电话等方式通知客户。

5.4 风险控制能力

a) 应建立事前预防、事中监控、事后处置的风险控制体系。
b) 事前预防包括按照监管规则审核业务的合规性，保证业务规则符合监管要求，建立相应的业务制度、操作规程，根据客户交易场景、交易金额组合不同的安全认证手段。
c) 事中监控应具备客户交易监控，发现可疑交易，可采取核实、阻断等手段，建立黑名单机制，可禁止高风险、可疑客户使用网上银行。
d) 事后处置可快速对确认风险事件的客户交易，采取紧急处理、加黑名单等措施，及时进行风险处置。

6 客户体验

6.1 网上银行服务功能

6.1.1 客户登录

网上银行提供多种登录方式与核验要素，支持密码等登录方式，采用身份证号或者指纹识别作为登录凭证，支持密码找回和密码修改。

6.1.2 转账汇款

网上银行提供转账汇款服务，包括行内转账、跨行转账、实时转账、手机号转账、常用联系人、提供电子回单等功能。

6.1.3 缴费

网上银行提供缴费服务，包括充值缴费、生活缴费、交通罚款、校企一卡通充值等功能。

6.1.4 储蓄服务

网上银行提供储蓄服务，包括定活互转、通知存款、桂盛宝等功能。

6.1.5 社保服务

网上银行提供社保缴费（税务收缴、人社代缴）、社保卡激活等功能。

6.1.6 利农商城

网上银行提供利农商城的服务，包括助农扶贫、电器城、特色广西等功能。

6.1.7 保险

网上银行提供保险服务，包括保险购买、缴纳保费等功能。

6.1.8 外汇业务

网上银行提供外汇业务的服务，包括结售汇、境外汇款等功能。

6.1.9 账户查询

网上银行提供账户查询、添加账户、交易明细、转账明细查询等功能

6.1.10 信用卡

网上银行提供信用卡的服务，包括我的信用卡、信用卡申请、申请进度等功能。

6.1.11 理财业务

网上银行提供理财产品服务，包括查询在售情况、购买、持有查询等功能。

6.1.12 线上开户

网上银行提供线上开通二三类户的功能。

6.2 网上银行服务性能

6.2.1 易用性

a) 网上银行服务应流程简洁，各流程界面信息应根据重要程序进行主次层级展示。
b) 网上银行服务应根据客户类别智能呈现页面信息，兼顾新用户的学习和老用户的效率。
c) 网上银行服务应通过智能或技术手段减轻用户的操作成本，如拍照识别收款账号。

6.2.2 舒适性

a) 网上银行服务常用功能应突出、显眼，方便客户操作，在不同环境适配良好，展示没有偏差。
b) 网上银行服务应支持用户根据使用习惯调整主界面，如主界面菜单、模块、主题色彩等。
c) 网上银行服务应使用协调、统一的网格，简洁和优雅地表达产品定位及理念，如色彩搭配协调、图标网格统一、控件交互一致等。
d) 网上银行服务的提示信息应使用一致性的文风、句式。

6.2.3 便捷性

a) 网上银行服务应提供清晰可见的操作引导，如开户流程前，清晰提示用户准备的相关证件信息。
b) 网上银行服务注册过程应操作便捷，提示当前步骤，支持用户回退。
c) 网上银行服务应提供及时反馈，告知用户信息填写是否有效。

6.2.4 易访问性

a) 网上银行服务应在门户网站对其功能及服务进行介绍，且提供帮助信息，对客户常见问题进行相关指引。
b) 网上银行服务所需应用和插件易安装、易登录。
c) 网上银行服务应在明显位置提供在线客服功能。

6.2.5 APP 闪退率

a) 完整功能测试，保证无功能性闪退。
b) 多机型兼容性测试，避免机型兼容性闪退。
c) APP 健壮性测试，避免运行环境造成 APP 闪退。
d) APP 灰度发布策略，避免大面积闪退。
e) 提供闪退报告渠道及快速修复手段，减少大面积闪退。

6.3 客服代表行为规范

客服代表服务，应满足GB/T32315-2015标准的规定。

6.3.1 语言礼仪

a) 标准发音：做到发音标准，语句清晰。

b) 称呼恰当，亲切得体：称呼客户要使用恰当的尊称。
c) 语言文雅，用语规范：使用规范的文明用语，语气腔调温和礼貌。
d) 语速适当：与客户沟通时，要流畅自然。

6.3.2 服务态度

a) 热诚待客：积极投入工作，态度和蔼、礼貌热情、有微笑感、主动服务。
b) 用心聆听：与客户交谈时要认真耐心，要积极主动的为客户解答问题。
c) 有问必答：回答客户的询问要尽可能做到主动、耐心、具体、清楚。
d) 虚心克制：虚心听取客户意见，对合理要求尽量满足。

6.3.3 服务标准

a) 接听电话：电话响时要尽快接听，通话结束时应感谢客户的来电。
b) 外呼电话：呼出电话时应先自报身份，礼貌确认对方身份，结束通话前，应对客户表示感谢。

6.3.4 服务效率

a) 快捷准确：按照操作流程完整办理每笔业务，工作效率高，保证业务无差错。
b) 有效指引：接通电话时应思路清晰，恰当引导客户，有效控制对话节奏。

6.4 客户服务响应

6.4.1 服务职责

a) 客服代表执行 7×24 小时工作制，受理客户咨询、投诉、建议、业务办理、交易需求等。
b) 客服代表需定期收集、整理、统计客户反馈的各类信息。
c) 客服代表需严格遵守系统操作规程及业务规章制度，以保证工作有序开展。
d) 客服代表需严格执行各项职业道德规范、服务规范和标准，正确使用规范用语，用心服务。
e) 客服代表需爱护话务设备，发现故障及时向上级汇报，确保通信畅通无阻。
f) 客服代表需努力学习各项业务知识，积极参加各种培训，不断提升自身业务水平。

6.4.2 服务指标

a) 接通率
计算方法：（人工接听电话总数÷转入人工服务电话总数）×100%
指标要求：不低于 85%。
b) 客户满意率。
计算方法：（满意的电话数÷总参评电话数）×100%
指标要求：不低于 95%。
c) 服务指标要求会随着中国银行业协会客户服务委员会管辖的多家客服中心服务指标平均值，和客服中心运营情况进行相应的改动。

7 创新及前瞻

7.1 服务创新

a) 支持不同安全级别的安全认证方式，对账户交易进行监控，实时阻断高危交易，加强对高风险交易的安全防控。

b) 手机银行提供客户在线办理贷款利率（LPR）定价基准转换。
c) 提供智能客服系统，支持机器人在线自动回复问题，对机器人无法回复的问题，引导客户转接人工客服应答。
d) 针对疫情推行健康疫情咨询、广西健康码（申领）。

7.2 技术前瞻性

7.2.1 人脸识别技术

持续探索应用人脸识别等生物识别技术，不断增强网上银行服务能力。
a) 人脸识别技术运用于移动信贷、手机银行、自助设备、安全保卫、VIP 客户精准营销上等场景中，增强业务风险防范能力，拓展线上业务范围。

7.2.2 分布式

根据市场分布式技术发展成熟情况，稳妥、逐步探索使用分布式技术来扩展网上银行系统处理能力、与稳定性，保证在各种因素导致某一节点服务不可用时，其它节点服务仍可以持续对外提供服务。

7.2.3 云计算

探索使用云计算技术提高系统资源的虚拟化程度，提高系统兼容不同厂家硬件、服务机器的能力。增强在业务高峰期，快整扩容应对大流量，高并发的金融交易场景；充分发挥云计算平台资源能快速灵活伸缩优点，避免资源过度配置。

7.2.4 大数据

充分利用大数据技术数据存储量大、处理速度快的优点，探索将大数据技术应用于网贷风险评估、产品推荐、风险防控、反欺诈等各类服务场景中，提升对用户的精准刻画能力，增强网上银行欺诈防控能力。

7.2.5 人工智能

应持续探索以下人工智能技术应用：
b) 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；
c) 可提供建立在投资组合管理模型等基础上的智能投顾、账户理财服务，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；
d) 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。

8 机制保障

8.1 组织保障

8.1.1 组织架构

网上银行服务的组织架构保障包括但不限于：
a) 广西壮族自治区农村信用社联合社（以下简称区联社）建立网上银行服务管理体系，持续不断完善网上银行服务的组织管理部门和业务、技术后台组织架构。

b) 区联社电子银行部制定业务发展策略和发展规划；制定业务运行和管理的规章制度；业务指南及风险控制措施；统筹业务的营销宣传管理；完善产品功能，并组织提出新功能需求。
c) 区联社计算机网络中心，根据电子银行部对网上银行服务提出业务功能需求，组织开展系统研发、科技管理、系统运维等相关技术工作。
d) 信贷管理部、公司机构金融部、个金融部、三农小微金融部等业务条线部门负责各自领域的产品线上化管理。
e) 各县级农合机构作为经营主体，定期按照监管部门及区联社相关规定组织风险自查，并及时汇报自查情况；建立职责清晰的管理机制，对从业人员进行法律法规、业务知识、操作技能等方面的培训与考核。

8.1.2 人才队伍

网上银行服务的人才队伍保障包括但不限于：
a) 应具备完善的网上银行业务、技术人才体系。
b) 网上银行系统规划、研发、运维、管理、后台客服人员结构合理分布，能够促进和保障网上银行业务发展。
c) 应定期组织全省农合机构开展网上银行业务、技术人员准入、培训和考核，提升员工专业综合素质与业务能力。
d) 人员年龄和专业知识人员结构分布合理，满足网上银行业务发展需要。

8.2 管理制度

8.2.1 产品研发

网上银行服务系统功能产品研发过程包括但不限于：
a) 制定完备的过程管理计划，指导和管理信息系统功能开发。对各阶段的目标、主要工作内容、文档要求、使用的方法和工具等作出相应的技术规定和管理约定。
b) 建立完善的、科学的项目变更控制流程，并严格按照流程进行变更控制。
c) 应搭建信息系统开发、测试、准生产、系统上生产前所需的基础环境。
d) 从项目管理、需求管理、产品设计与实现、产品功能测试、技术评审、质量保证、配置管理、度量分析等过程，对投产项目实施过程进行监控和控制，确保质量和过程能达成既定目标。

8.2.2 测试投产

网上银行服务系统功能测试投产过程包括但不限于：
a) 应建立完善系统功能投产流程，保证信息系统顺利上线及相关作业的有效执行，提高投产的准确性、可靠性以及试运行期间的可控管理。
b) 网上银行系统功能上线或变更，应协调安全管理部门对待投产系统进行安全审查、渗透检测等安全评估工作，并出具相应安全评估报告。
c) 信息系统正式投产前，应经过准生产环境进行投产过程测试，并记录好操作日志。
d) 应制定好全面的版本管理，确保投产安全和平稳。

8.2.3 生产运营

a) 制定机房安全管理制度；机房采用结构化布线系统；定期对机房设施进行维修保养。
b) 建立数据级和应用级灾备，确保在发生灾难时能够快速恢复数据，同时主数据中心发生故障的情况下，能够在灾备中心接管应用，有效减少系统停机时间。

c) 建立灾备系统演练制度，每年定期进行生产系统灾备切换演练，以验证灾备系统的有效性。提升网上银行无间断服务能力。

8.2.4 应急响应

网上银行系统的应急响应包括客户、系统两个层面，确保对突发事件、问题的快速响应和妥善处置，尽可能减少损失和降低对客户的影响。

a) 客户应急沟通：编制网上银行产品的相关业务连续性方案，其中包括在各应急场景下与客户沟通的话术等预案。
b) 系统应急响应：依据广西农村信用社信息系统突发事件应急处置工作指引，应对各项紧急事件、问题，对于网上银行系统制定具体系统应急预案，日常定期组织应急演练，包括对同城异地的灾备系统的切换演练。

8.3 企业标准及宣传实施机制

a) 广西农村信用社整合官方网站，网上银行，微信公众号等线上线下渠道，开展多种形式的企业标准宣传普及。
b) 应建立企业标准学习培训机制，包括制作课件，开发培训课件。
c) 应建立畅通的咨询渠道，及时解答客户疑问。
d) 应针对企业标准实施情况定期组织检查，及时发现未符合标准的业务环节，并及时整改。