CS 03.060
A11

Q/GXGB

广西北部湾银行股份有限公司企业标准

Q/GXGB 0002—2021

广西北部湾银行网上银行服务标准

Guangxi Beibu Gulf Bank Internet Banking Service Standard

企业标准信息公共服务平台
公开 2021年11月29日 12点14分

2021－11－17 发布　　2021－11－17 实施

广西北部湾银行股份有限公司　发布

目　次

企业标准信息公共服务平台 公开 2021年11月29日 12点14分

前　言

本标准按照GB/T1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本标准代替Q/GXGB 0002—2020《广西北部湾银行网上银行服务标准》。

本标准与Q/GXGB 0002—2020相比，主要变化如下：

——增加了规范性应用文件内容（见 2）；

——增加了安全通信协议、安全套接字层/传输层安全性协议、基于安全套接字层的超文本传输协议、对称密码算法、非对称密码算法、负载均衡、恢复点目标、恢复时间目标、双活、同城双活、异地冷备、灾难恢复、本地可用性名词的定义描述（见 3.11、3.12、3.13、3.14、3.15、3.16、3.17、3.18、3.19、3.20、3.21、3.22、3.23）；

——修改了“基本安全要求”关于规范性文件的引用（见 6.1）；

——增加了服务连续在线可行性相关内容（见6.3）；

——增加了“风险监测评估与评估”下我行名单监控系统、风险决策系统内容（见6.5.6）

——增加了风险处置相关内容（见6.5.7）

——修改了APP闪退率指标内容（见7.2.4）

——增加了网银整体性能指标内容（见7.2.5）

——增加了总下载字节数指标内容（见7.2.6）

——增加了客服代表行为规范引用标准文件内容（见7.3）

——增加了贷款服务在页面标识各类贷款产品年化利率内容（见8.1）

——增加了“高可用架构”下关于本地可用性要求、同城可用性要求、异地灾备要求相关描述（见8.2.2）

本标准由广西北部湾银行股份有限公司提出。

本标准起草单位：广西北部湾银行股份有限公司。

本标准主要起草人：梁生安、韦昌宏、汪成钢。

本标准所代替标准的历次版本发布情况为：

--本标准于2020年9月首次编制。

--本次为第一次修订。

广西北部湾银行网上银行服务标准

1 适用范围

本标准明确规定了广西北部湾银行股份有限公向客户提供网上银行服务时的安全要求、功能要求、性能要求、服务质量和制度保障要求等内容。

本标准适用于广西北部湾银行所有网上银行服务。

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，仅所注日期的版本适用于本文件。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。

JR/T 0068-2020 网上银行系统信息安全通用规范
GT/T 32315-2015 银行业客户服务中心基本要求
GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
GT/T 35273-2020 信息安全技术 个人信息安全规范
GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
JR/T 0171-2020 个人金融信息保护技术规范
JR/T 0044-2008 银行业信息系统灾难恢复管理规范
JR/T 0071.1-2020 金融行业网络安全等级保护实施指引 第1部分：基础与术语
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 0071.3-2020 金融行业网络安全等级保护实施指引 第3部分：岗位能力要求和评价指引
JR/T 0071.4-2020 金融行业网络安全等级保护实施指引 第4部分：培训指引

3 定义和术语

3.1 网上银行 internet banking

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 个人网银 personal internet banking

银行面向个人用户提供的网上金融服务。

3.3 企业网银 corporate internet banking

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。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、非对称密钥、

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

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。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 智能密码钥匙 cryptographic smart token

提供密码运算、密钥管理等密码服务的终端密码设备，一般使用 USB、蓝牙、音频、SD 等接口形态。

3.8 动态口令 one-time-password(OTP), dynamic password

基于时间、事件等方式动态生成的一次性口令。

3.9 动态口令令牌 one time password token

用来生成动态口令的设备。

3.10 生物特征 biometric

人类生理上的或行为上的可测量特征，并由此可以可靠的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。

3.11 安全通信协议 security communication protocol

应用层或表示层实现，并结合了相关密码技术以保证通信数据机密性、完整性的通讯协议，如 HTTPS、SSL 等协议。

3.12 安全套接字层/传输层安全性协议 secure socket layer / transport layer security（SSL/TLS）

位于 TCP/IP 协议与各种应用层协议之间，为数据通讯提供安全支持。

3.13 基于安全套接字层的超文本传输协议 hyper text transfer protocol over secure socket layer（HTTPS）安全套接字层/传输层安全性协议 secure socket layer / transport layer security（SSL/TLS）

一种通过 SSL/TLS 实现安全传输的 HTTP 协议。

3.14 对称密码算法 symmetric cipher

一种传统密码算法，加密和解密采用相同的密钥。也称为秘密密钥算法或单密码算法。

3.15 非对称密码算法 asymmetric cipher

又称为公开密钥密码算法，它的加密和解密是相对独立的，加密和解密使用两个不同的密钥。在实现数据加密功能时，加密密钥可以公开，又叫做公开密钥，简称公钥（public key）；解密密钥必须保密，又叫做私人密钥，简称私钥（private key）。

3.16 负载均衡 workload balance

由多台服务器以对称的方式组成一个服务器集合，每台服务器都具有等价的地位，都可以单独对外提供服务而无须其他服务器的辅助。通过某种负载分担技术，将外部发送来的请求均匀地分配到对称结构中的某一台服务器上，而接受到请求的服务器独立地回应客户的请求。通过使用负载均衡器产品如F5 方式实现。

3.17 恢复点目标 recovery point objective（RPO）

灾难发生后，系统和数据必须恢复到的时间点要求。

3.18 恢复时间目标 recovery time objective（RTO）

灾难发生后，信息系统或业务功能从停顿到必须恢复的时间要求。业务补账等业务相关工作不包括在该时间范围内。对于涉及第三方的应用系统，不包括第三方的灾难恢复时间。对于灾备环境的设备配置，按照等级要求实行差异化配置，在满足对应 RTO 要求的前提下，在预定时间内达到所需的处理能力即可。

3.19 双活 dual-active

多活的一种，信息系统仅在两个物理节点部署和提供服务。

3.20 同城双活 city scope dual-active

网络本地、同城接入，应用层双活，数据层双活（含读写分离）的灾备高可用架构。

3.21 异地冷备 off-site cold backup

网络本地、异地接入，应用层主备，数据层主备的灾备高可用架构。

3.22 灾难恢复 disaster recovery

为了将信息系统从灾难造成的不可运行状态或不可接受状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受的状态而设计的活动和流程。

3.23 本地可用性 local availability

表示在没有发生重大灾难的情况下，当需要使用时应用系统可操作和可访问的程度。为提高本地可用性，应尽量减少计划或非计划的停止服务时间。

3.24 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。

3.25 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。

3.26客服代表 customer service representative

接听客户来电、处理网上互动等服务人员的总称。

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）

WAF:Web应用防火墙（Web Application Firewall）

IPv4：互联网协议第4版（Internet Protocol Version 4）

IPv6：互联网协议第6版（Internet Protocol Version 6）

HTTPS：基于安全套接字层的超文本传输协议（hyper text transfer protocol over secure socket layer）

SSL/TLS：安全套接字层/传输层安全性协议（secure socket layer/transport layer security）

MAC：消息认证码（Message Authentication Code）

SD：安全数码（Secure Digital）

SDK：软件开发工具包（Software Development Kit）

SE：安全单元（Secure Element）

TEE：可信执行环境（Trusted Execution Environment）

USB：通用串行总线（Universal Serial Bus）

5 系统描述

网上银行系统是将传统的银行业务同互联网等资源和技术进行融合，将传统的柜台通过互联网、移动通信网络、其他开放性公众网络或专用网络向客户进行延伸。网上银行系统主要包括通过PC、手机、平板电脑、智能电视、可穿戴设备等终端访问的网上银行系统，包括手机银行、微信银行等系统。网上银行系统涵盖个人网上银行系统和企业网上银行系统。

6 服务安全性

6.1 基本安全要求

广西北部湾网上银行系统的安全技术、安全管理、业务运作安全、个人信息保护根据国家和行业标准规定开展系统建设，符合以下标准相关要求：JR/T 0068-2020《网上银行系统信息安全通用规范》、JR/T 0071-2020《金融行业网络安全等级保护实施指引》、GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》、JR/T 0171-2020《个人金融信息保护技术规范》。

a)广西北部湾网上银行系统服务安全性、客户体验、创新及前瞻性、实施保障，应符合 JR/T 0068-2020 《网上银行系统信息安全通用规范》中安全规范相关要求。

b)广西北部湾网上银行系统客户端安全、通信网络安全、服务器端安全、增强身份认证要求和风险防控能力，应符合 GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T39786-2021《信息安

全技术 信息系统密码应用基本要求》、JR/T 0171-2020《个人金融信息保护技术规范》要求。

c)广西北部湾网上银行系统按照 JR/T 0071.1-2020 《金融行业网络安全等级保护实施指引》要求实施系统等级保护工作，根据系统在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，遵照 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》要求开展系统定级。

d)广西北部湾网上银行系统参照第二级安全保护能力要求进行保护，已在广西壮族自治区公安厅备案，获得信息系统等级保护二级证书。

e)广西北部湾网上银行系统能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。

6.2 安全技术规范

6.2.1 客户端安全

6.2.1.1 客户端安全情况

a)客户端程序开发设计过程中注重各系统组件、第三方组件、SDK 存在的安全风险，对开发框架和技术路线进行严格论证，必要时进行选型安全测试。

b)客户端程序具有明确的应用标识符和版本序号，设计合理的更新接口，当某一版本被证明存在重大安全隐患时，提示并强制用户更新客户端。

c)客户端程序的每次更新、升级，进行源代码检查和安全加固，以保证客户端程序不存在隐藏的非法功能和后门。

d)采用广西北部湾银行企业证书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广西北部湾银行。

e)客户端程序在启动时进行真实性、完整性校验（例如，联机动态校验等），防范客户端程序被篡改或替换。

f)客户端程序采取代码混淆、加壳和第三方安全加固等安全机制，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。

g)客户端程序保证自身的安全性，避免代码注入、缓冲区溢出、非法提权等漏洞。

h)客户端程序采取安全加固产品对进程进行保护，防止非法程序获取该进程的访问权限，扫描内存中的敏感数据或替换客户端页面等。

i)客户端程序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，采取密码控件和密码键盘实现逐字符加密、防范键盘窃听等措施。

j)客户端软件不以任何形式在本地存储用户的支付敏感信息。

k)客户端程序采取加密等有效措施保证所涉及密钥的机密性和完整性。

l)客户端程序对客户密码复杂度进行校验，保证用户设置的密码达到中及以上的密码强度。

m)客户端程序密码框禁止明文显示密码，使用特殊字符“•”代替。

n)客户端程序条码生成、展示或识读解析功能，符合《条码支付安全技术规范（试行）》（银办发〔2017〕242 号文印发）要求。

o)客户端程序定制错误信息，有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。

p)客户端程序具备用户隐私政策。

q)客户端程序在收集、使用客户信息之前，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。在采集客户个人敏感信息前应对采集的用途和必要性进行提醒。

r)客户端程序禁止访问终端中非业务必需的文件和数据。应根据最小权限原则申请系统权限（例如，申请读取通讯录、地理位置等权限），并取得用户的明示同意。

s)客户端保留最少的客户信息，并限制数据存储量和保留时间。

t)客户端程序退出时，清除非业务功能运行所必须留存的业务数据，保证客户信息的安全性。

u)采购专业第三方渠道监控服务对仿冒客户端程序进行仿冒程序监测。

6.2.1.2 客户端环境

客户端程序启动时检查客户端环境，当发现客户端环境存在重大安全缺陷或安全威胁时，对用户进行警示，如：提示用户网络处于 WIFI 环境。

6.2.2 通信网络安全

6.2.2.1 通讯协议与通信链路

a） 客户端程序与服务器之间采用加密技术建立安全的信息传输通道，保证传输数据的机密性和完整性。采用的安全协议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） 客户端通信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） 为确保数据传输的安全性，使用安全的算法组合，广西北部湾银行网上银行通讯加密支持国密加密算法。

d） 网上银行客户端和服务端之间的通讯，采用密码控件对通信数据中支付敏感信息进行加密，确保支付敏感信息不应以明文形式出现。

6.2.2.2 安全认证

a） 通过公开网络进行数据传输时，通过采用密钥、证书等密码技术手段进行认证。

b） 客户端程序对服务器端证书的合法性进行验证。

c） 整个通讯期间，经过认证的通讯线路一直保持安全连接状态。

d） 网上银行 Web 服务器使用权威机构颁发的数字证书以标识其真实性。

e） 网上银行采用国际通用的服务器根证书，确保客户获取的网上银行 Web 服务器真实有效，例如，可在客户开通网上银行时分发根证书，或将根证书集成在客户端程序安装包中分发等。

6.2.3 服务器端安全

6.2.3.1 安全通信网络

结构安全：

a） 使用前置设备实现网上银行系统主机系统的隔离，防止外部系统直接对网上银行系统主机的访问和操作。

b）网上银行系统部署网络硬件防火墙、入侵防御系统（IPS）、WEB 应用防火墙（WAF）、防毒墙等安全防护设备，实现对进出网络的数据包进行过滤区域隔离和，攻击行为拦截处置。

网上银行系统部署安全防护设备，具备自动快速封禁恶意攻击 IP 的技术。

访问控制：

a）网络访问权限按照最小安全访问原则设置访问控制权限。

b）网络和安全设备禁止使用默认密码、常见弱口令以及包含个人、机构和设备等存在一定规律信息的口令。

c）设备管理界面的访问地址设置网络访问控制策略或登录 IP 限制进行严格限定，对异常的访问请求进行记录和预警。

入侵防范：

a）制定执行合理的 IDS/IPS 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）为防范对网上银行服务器端的异常流量攻击。采取以下防护措施：

c）与电信运营商签署 DoS/DDoS 防护协议。

d）使用 DoS/DDoS 防护设备。

e）使用 IDS/IPS 设备。

f）使用负载均衡设备。

g）使用恶意流量清洗技术。

网络设备防护：

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，并指定他人定期（不超过 6 个月）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）应采取沙箱、防病毒等措施，对网络攻击进行预防、监测和处置。

h）应不定期组织针对开源系统或组件的安全测评，及时进行漏洞修复和加固处理。

i）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。

j）应定期对软硬件资产进行核查，对设备进行人工、自动化排查探测，对已弃用设备进行下线处理。

k）宜使用带外管理的方式对网络设备进行管理，以保障数据网络和管理网络的物理信道分离。

l）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。

恶意代码防范：

部署网络防毒墙设备对网络流量进行安全分析，分析可疑的网络攻击与入侵行为、僵尸网络、病毒和蠕虫的网络传播等。

6.2.3.2 安全计算环境

身份鉴别：

a）使用符合国家密码主管部门要求的加密算法对密码进行加密保护，在传输和存储过程中不允许明文密码出现。

b）网上银行系统和设备设置密码复杂度中以上。

c）通过网络隔离措施和登录 IP 限制等措施，实现对登录主机的地址进行限制，对于违规的登录尝试进行报警。

d）应防范口令暴力破解攻击，日志信息记录攻击源地址，并报警。

e）密码输入界面禁止明文显示密码，使用同一特殊字符“•”代替。

f）采取有效措施防范登录操作的重放攻击，例如，在登录交互过程提交的认证数据中增加服务器生成的随机信息成分。

g）采用密码控件实现对用户输入支付敏感信息即时加密，降低恶意软件窃取用户支付敏感信息的风险，使用软键盘方式输入密码时，采取自定义键盘等措施防范密码被窃取。

h）客户访问系统会话标识为随机并且唯一，会话过程中维持认证状态，防止客户通过直接输入登录后的地址访问登录后的页面。

i）不在客户端缓存密码、密钥等支付敏感信息，不在日志中记录支付敏感信息。

j）退出登录或客户端程序、浏览器页面关闭后，系统立即终止会话，保证无法通过后退、直接输入访问地址等方式重新进入登录后的网上银行页面。

k）退出登录时应提示客户取下（或断开）专用安全设备，例如，智能密码钥匙。

l）修改客户敏感参数（例如，密码、转账限额等）时，再次认证客户身份。

m）显示客户身份证件信息时，应屏蔽部分关键内容，例如，屏蔽身份证后六位信息等。

访问控制：

a）操作系统和数据库系统特权用户权限分离，系统管理员只具备操作系统的运维管理权限，数据库管理员只具备数据库的运维管理权限。

b）根据业务必需和最小权限原则，对主机系统的访问控制规则进行精细化配置，通过防火墙对允许访问本机的地址和端口进行限制，对异常的访问请求进行拦截和报警。

c）不应使用系统管理员账号进行业务操作。

d）企业网银支持管理员和操作员两类角色用户，管理员用户初始登录密码应在银行柜台设置，操作员用户由管理员用户设置或在柜台设置，操作员用户权限应根据录入、复核、授权职责分离的原则设置。其中企业网银专业版由管理员给操作员分配业务权限，企业网银查询版操作员用户由管理员使用 KEY 认证登录为其初始化密码并分配业务权限。

e）具备完善的交易验证机制，每次处理的客户信息均以服务器端数据为准，当服务器端检测到客户提交的信息被篡改时，及时中断交易，并对客户请求指令的逻辑顺序进行合理控制。

f）网上银行系统开放的 API 接口执行统一准入管理。

安全审计：

a）合理分配交易日志的管理权限，禁止修改日志，确保日志的机密性、完整性和可用性。

b）及时对中间件日志、应用日志、错误日志等文件进行分析，识别异常的访问行为。

入侵防范：

a）严格限制和检查外来软件和文件的使用，确保软件和文件来源可靠，且在使用前应经过严格测试。

b）采取技术手段对攻击活动进行检测和报警，主机型入侵检测、进程白名单、攻击脚本检测等。

Web 应用安全：

a）防范支付敏感信息泄露：

网上银行系统上线前，删除 Web 目录下所有测试脚本、程序。

如在生产服务器上保留部分与 Web 应用程序无关的文件，应为其创建单独的目录，使其与 Web 应用程序隔离，并对此目录进行严格的访问控制。

不在 Web 应用程序错误提示中包含详细信息，不向客户显示调试信息。

不在 Web 应用服务器端保存客户支付敏感信息。

网上银行系统 Web 服务器设置严格的目录访问权限，防止未授权访问。

统一目录访问的出错提示信息，例如，对于不存在的目录或禁止访问的目录均显示定制错误页面提示客户。

b）禁止目录列表浏览，防止网上银行站点重要数据被未授权下载。

c）防范 SQL 注入攻击：

网上银行系统 Web 服务器应用程序应对客户提交的所有表单、参数进行有效的合法性判断和非法字符过滤，防止攻击者恶意构造 SQL 语句实施注入攻击。

在网上银行服务端对客户输入字符合法性进行判断和特殊字符过滤，禁止仅在客户端执行校验。

数据库应尽量使用存储过程或参数化查询，并严格定义数据库用户的角色和权限。

d）防范跨站脚本攻击：

通过严格限制客户端可提交的数据类型、对提交数据进行有效性检查、设置响应头防护参数、对输出信息进行编码等措施防范跨站脚本注入攻击。

e）对 Web 页面提供的链接和内容进行严格控制和检查，确保外部链接和引用内容的安全性。

f）对开放的 API 接口进行安全评估与测试，保证接口的安全性和可靠性。

g）采取强制用户安装密码控件执行敏感信息加密等措施防范由于客户使用第三方浏览器（例如，手机平台浏览器）、第三方输入法带来的支付敏感信息泄露、交易数据篡改等重要信息安全风险。

h）对条码中包含的网址等信息进行校验，对非法地址和恶意请求进行拦截。

i）加强对开源及商业应用系统或组件的安全管理，进行安全评估并及时修复安全漏洞。

j）对文件的上传和下载进行访问控制，避免攻击者执行恶意文件或发起未授权访问。

k）采取部署抗拒绝服务攻击系统（DDOS）对访问应用层流量进行清洗防护，防范针对服务器端应用层的拒绝服务攻击。

图形验证码：

a）网上银行使用的验证码，为随机产生。

b）采取图片底纹干扰、颜色变换、设置非连续性及旋转图片字体、变异字体显示样式、交互式认证等有效方式，防止验证码被自动识别。

c）网上银行使用的验证码具有使用时间限制并仅能使用一次。

d）图形验证码由服务端生成，客户端源文件中不包含验证码文本。

防钓鱼：

a）网上银行具有防网络钓鱼的功能，允许客户设置预留信息，客户登录时显示客户预留信息，便于客户识别钓鱼网站。

b）采取防钓鱼网站发现措施，及时监测发现钓鱼网站，并建立钓鱼网站案件报告及快速关闭钓鱼网站的处置机制。

c）应加强防钓鱼的应用控制和风险监控措施，例如，增加客户端提交的页面来源地址信息的校验、设置转账白名单等。

数据库服务安全：

a）采用防火墙网络隔离、登录 IP 限制等技术手段控制非授权用户访问。

b）部署数据库审计系统对数据库异常连接和请求进行监控和审计，并对 SQL 注入等攻击进行监控和报警。

网上银行系统关键组件采取多点部署方式，不因单台服务器发生故障影响业务连续性。

网上银行系统（手机银行客户端）支持条码支付业务，符合监管机构《条码支付安全技术规范（试行）》要求。

网上银行系统对客户端的标识信息（IP 地址、MAC 地址等）进行记录，采用技术手段对风险进行识别，当客户 IP 地址发生变化，再次对客户身份进行认证。

应对非法攻击行为进行监控，对其终端特征（例如，终端标识、软硬件特征等）、网络特征（例如，MAC、IP、WIFI 标识等）、用户特征（例如，账户标识、手机号等）、行为特征、物理位置等信息进行识别、标记和关联分析，并与风险监控系统实现联动，及时采取封禁等防护措施。

应对恶意攻击行为进行分析，对恶意攻击事件按照网络安全相关要求及时进行上报处理。

数据保护：

a）落实中国人民银行等监管机构相关要求和国家标准，对银行卡卡号、卡片验证码、支付账户等信息进行脱敏，支持基于支付标记化技术的交易处理，采取技术手段从源头控制信息泄露和欺诈交易风险。

b）对客户办理金融业务时留存的身份信息与相关影像资料、个人财产信息、征信信息等敏感客户资料，参照国家及行业个人信息、个人金融信息相关保护要求，加强信息安全管理。

支付敏感信息在应用层保持端到端加密，即保证数据在从源点到终点的过程中始终以密文形式存在。

数据备份和恢复：

a）应提供本地数据备份与恢复功能，增量数据备份每天一次，完全数据备份每周一次，备份介质场外存放，数据保存期限依照国家相关规定。

b）应具备异地实时备份和异步备份功能，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及时切换。

c）数据备份存放方式以多冗余方式，完全数据备份至少保证以 1 个月为周期的数据冗余。

6.2.3.3 虚拟化安全

虚拟化环境加固：

a）虚拟化系统执行安全配置、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。应对虚拟机管理器进行完整性检查，确保虚拟机管理器加载的功能模块的完

整性和真实性。

b）虚拟机管理器和虚拟机更新，及时对存在重大安全隐患的系统组件等进行更新，并在更新前对软件包进行兼容性和稳定性测试。

虚拟化隔离：

a）网络划分多个安全域，不同安全级别的应用和服务运行在不同的安全域中，防止不同安全级别的应用和服务互相干扰。

b）应采用技术手段，隔离虚拟机与宿主机物理资源，保证虚拟机对宿主机物理资源的使用由虚拟机管理器完成，满足安全隔离的要求。

c）应采用技术手段对不同虚拟机进行隔离，防止虚拟机间的互相干扰。

虚拟机生命周期管理：

a）虚拟机销毁时，应彻底清除所有相关数据。

b）应按需处理业务系统在虚拟机中生成的应用数据，防止敏感数据泄露或非法恢复该虚拟机。

c）应限制对快照文件的访问，对快照文件的使用进行监测与审计，防止快照文件被非法窃取。

d）应严格保证虚拟机迁移过程中重要数据的机密性和完整性。

e）应防止虚拟机的跨安全域迁移。

6.3 服务连续在线可行性

广西北部湾银行网上银行系统服务连续在线可信性应满足以下要求：

a）系统服务时间满足公开 7×24 小时不间断运行的要求。

b）系统配备 7×24 小时运维应急人员，如有问题及时处理。

c）系统可用率达到 99.99%。

d）系统数据丢失恢复点目标（RPO）=0。

e）系统恢恢复时间目标（RTO）小于 30 分钟。

f）系统可用性监控覆盖率达 100%，监控覆盖网上银行业务探测、数据库、主机进程、端口等。

g）系统可用性监控覆盖率达 100%。

6.3.1 业务连续性与灾难恢复

业务运行连续性：

a）应制定网上银行业务连续性策略及计划。

b）应将网上银行业务连续性管理整合到组织的流程和架构中，明确指定相关部门负责业务连续性的管理。

c）机房采用双路市电输入、冗余 UPS 接入供电，同时部署大功率柴油发电机作为应急电源，信息科技运维人员日常对 UPS、柴油发电站等重要设备进行巡检，及时处置报警日志事件。

d）网上银行采用电信、联通、移动三大运营商构成冗余通信线路同时不同的物理路径部署冗余设备。

e）核心层、汇聚层的设备和重要的接入层负载均衡、交换机、路由器、防火墙等设备均为双机热备。

f）网上银行 Web 前置服务器、应用服务器、数据库服务器等关键数据处理系统均为多机集群，采

用磁盘冗余阵列存储技术，以避免单一部件故障影响设备运行的风险。

g）广西北部湾银行网上银行系统服务时间为 7×24 小时，信息技术部配备技术运维人员 7×24 小时值班监控和运维应急，保障网上银行系统连续不间断稳定运行，网上银行系统可用率≥99.99%。

h）广西北部湾银行网上银行系统接入交易监控系统和集中监控可视化系统进行系统交易和可用性监控，实现应用可用性监控覆盖率≥99%。

备份与恢复管理：

a）广西北部湾银行根据网上银行系统的业务影响性分析结果，制定数据备份策略，实施应用级备份，保证灾难发生时，能尽快恢复业务运营。

b）广西北部湾银行根据已建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录妥善保存，做好备份数据的销毁审查和登记工作。

c）广西北部湾银行定期对网上银行系统日志文件进行备份存储，日志文件应至少妥善保存 6 个月。

d）定期执行数据恢复测试程序，检查并测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

e）广西北部湾银行已建立“两地三中心”灾备架构，同城灾备中心为应用级数据灾备，可保证接管所有核心业务的运行；对于异地数据备份中心，“数据备份恢复”中有关安全技术要求。

6.3.2 安全事件与应急响应

安全事件处置：

a）发生安全事件各单位人员按照《安全事件上报制度》要求执行事件上报。对于重大信息安全事件，各单位相关人员应注意保护事件现场，采取必要的控制措施。

b）广西北部湾银行跟踪收集同业发生的网上银行信息安全事件及风险进行深入研判、分析，评估现有控制措施的脆弱性，及时整改发现的问题。

应急管理：

a）广西北部湾银行已建立业务和技术部门协调配合的网上银行信息安全事件的应急处置机制，明确优先保障业务恢复、账务正确以及数据安全，对于网络和信息安全事件导致的账务差错或异常交易的处理，严格按照程序做好转人工处理等应急操作。

b）广西北部湾银行已建立应急预案演练制度，定期组织有业务部门参与的桌面演练和生产系统实战演练，定期对系统高可用性进行切换演练，备份系统与生产系统的切换要至少每年演练一次。

6.4 增强身份认证要求

6.4.1 身份认证基本措施

a） 应采集 IP 地址、操作系统版本、设备编码等数据，用于协助交易风险判断与客户身份认证。

b） 针对同一设备在短时间内多账号登录，应采取多种验证手段，对客户身份进行加强验证。

c） 针对客户首次在新设备进行交易，且 IP、操作系统等环境信息发生明显变化时，应使用多种验证手段，对客户身份进行加强验证。

6.4.2 智能密码钥匙

本标准所涉及的智能密码钥匙包含目前网上银行系统普遍应用的 USB Key、蓝牙 Key、音频 Key 等基于硬件的 Key 产品，也包括将来可能出现的其他基于硬件的 Key 产品。

a) 广西北部湾银行使用智能密码钥匙，经国家或行业主管部门认可的第三方专业测评机构检测通过的智能密码钥匙。

b) 智能密码钥匙采用具有密钥生成和数字签名运算能力的智能卡芯片，保证敏感操作在智能密码钥匙内进行。

c) 智能密码钥匙的主文件（Master File）具有非授权拆卸密钥自毁功能，防止非授权的删除和重建。

d) 为保证私钥在生成、存储和使用等阶段的安全：

签名私钥在智能密码钥匙内部生成，不得固化密钥对和用于生成密钥对的素数。

保证私钥的唯一性。

禁止以任何形式从智能密码钥匙读取私钥或写入签名私钥。

智能密码钥匙在执行签名等敏感操作时，具备操作提示功能，包括但不限于声音、指示灯、屏幕显示等形式。

智能密码钥匙内部产生的私钥，不再需要时应及时销毁。

e) 签名交易完成后，状态机立即复位。

f) 为保证 PIN 码和密钥的安全：

PIN 码应具有复杂度要求。

采用安全的方式存储和访问 PIN 码、密钥等支付敏感信息。

PIN 码和密钥（除公钥外）不能以任何形式输出。

PIN 码连续验证失败次数达到上限（不超过 6 次）时，智能密码钥匙应主动锁定。

g) 智能密码钥匙使用的密码算法符合国家密码主管部门的要求。

h) 在外部环境发生变化时，智能密码钥匙不应泄露支付敏感信息或造成安全风险。外部环境的变化包含但不限于：

高低温。

高低电压。

强光干扰。

电磁干扰。

紫外线干扰。

静电干扰。

电压毛刺干扰。

i) 第二代以上智能密码钥匙具备防范智能密码钥匙被远程挟持功能，例如，采用具备客户主动确认功能的智能密码钥匙或通过可靠的第二通信渠道要求客户确认交易信息等。

j) 具有屏幕显示、语音提示、按键确认等提示确认功能的智能密码钥匙，应符合下列要求：

对交易指令的完整性进行校验、对交易指令的合法性进行鉴别、对关键交易数据进行输入、确认和保护，应采取有效措施防止确认环节被绕过。

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关键交易数据，屏幕显示或语音提示的内容与智能密码钥匙签名的关键数据一致。

未经按键确认等操作，智能密码钥匙不得签名和输出，在等待一段时间后，自动清除数据，并复位状态。

6.4.3 短信验证码

a）客户开通短信验证码时，柜面人员现场验证客户身份并登记手机号码。更改手机号码时，对客户的身份进行有效验证。

b）短信验证码与安全提示信息一起发送给客户，提示客户验证码使用安全。

c）短信验证码应随机产生，长度不少于 6 位。

d）短信验证码应具有时效性，最长不超过 6 分钟，超过有效时间应立即作废，防范对验证码的暴力猜解攻击。

e）短信验证码在使用完毕后立刻失效。

6.4.4 生物特征

广西北部湾银行在网上银行系统（手机银行系统）中使用生物特征技术进行身份确认或识别，遵循如下要求。

a）符合国家相关法律法规及主管部门有关管理要求，采用的生物特征解决方案通过经国家或行业主管部门认可的第三方专业测评机构检测。

b）采取适当的措施阻止已知的伪造攻击手段，降低伪造身份通过确认或识别的可能性。

c）应确定合理的生物特征数据采集、传输、处理、存储的方式，采取适当的措施避免生物特征数据或相关信息被非法泄露或非法使用。

d）采集的生物特征数据根据隐私政策要求只用于预期业务。

6.5 风险控制能力

6.5.1 沟通和合作

a）建立与相关金融监管机构、公安机关、电信公司的合作和沟通以及应急协调机制，有效处置、DDOS、网络钓鱼、假冒网站等网络安全事件。

b）持续加强与供应商、专业安全公司、安全组织的合作与沟通，不断增强日常安全防护、突发事件处置、故障处理等方面的能力。

6.5.2 审核和检查

a）制定安全审核和安全检查制度，规范安全审核和安全检查工作，按照制度要求进行安全审核和安全检查活动。至少每年开展一次网上银行全面安全检查，检查内容至少包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

b）审计部门至少每两年对信息科技开展一次审计，审计内容至少包括相关管理制度的完备性及其执行的有效性，相关操作流程的合理性与合规性，信息安全保障体系的完备性和有效性，信息安全风险管理、规划实施、信息系统运行的安全性，重要客户信息和交易数据的安全性，应急管理和外包管理的有效性以及其他重要信息安全保障的情况。

c）制定《广西北部湾银行员工违规失职行为处理办法》针对违反和拒不执行安全管理措施规定行为的处罚细则。

6.5.3 安全管理人员

a）建立外来人员管理制度，在外来人员访问网上银行相关的区域、系统、设备、信息等内容时，提出书面申请并获得批准后应由专人陪同或监督，并登记备案，必要时签署保密协议。对允许被外部人员访问的系统和网络资源建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控。

b）针对信息科技外包商人员，尤其是从事敏感性技术相关工作的人员，执行严格的审查程序，包括身份验证和背景调查，并签署保密协议。

6.5.4 安全建设管理

自行软件开发：

a）网上银行系统以自行开发为主，由总行信息技术部负责日常开发及维护工作。

b）在应用系统上线前，对程序代码进行代码复审，识别可能的后门程序、恶意代码、逻辑缺陷和安全漏洞。

c）严格控制对生产版本源代码的访问，避免代码泄露。全部或部分源代码如需交由本机构开发者之外的第三方使用或进行再次开发时，需执行严格的审批流程、明确相关责任并与第三方签署保密协议。

d）采用先进的版本管理工具对生产库源代码版本进行控制，保证当前系统始终为最新的稳定版本。

e）源代码管理系统开启访问日志对访问行为进行审计，对异常行为进行识别。

外包软件开发：

a）网上银行系统坚持“不得将信息科技管理责任外包”原则，合理谨慎监督外包职能的履行。

b）按照“必需知道”和“最小授权”原则对外包服务商相关人员授权，并签署保密协议。

c）签订合同时明确合同条款，严禁外包服务商再次对外转包，采取有效措施确保网上银行系统信息安全。

d）制定并发布《广西北部湾银行IT项目外包服务商管理应急预案》，建立恰当的应急措施以应对外包服务商在服务中可能出现的重大缺失。重点考虑外包服务商的重大资源损失，重大财务损失和重要人员的变动，以及外包协议的意外终止等情况。

e)加强驻场外包人员管理，对外包人员的背景、能力和经验进行审查。外包人员参与变更事项应事先提交计划操作内容，由广西北部湾银行人员现场陪同外包人员，核对操作内容并记录，涉及敏感操作（例如，输入用户口令等）应由广西北部湾银行人员进行操作，外包人员不得查看、复制或带离任何敏感信息。

测试验收：

a）网上银行系统上线前，清除系统中与测试有关的代码及数据。

b）网上银行系统上线前，进行严格的代码安全扫描，进行充分的功能和安全性测试。

6.5.5 安全运维管理

a）物理环境管理：

生产机房采用结构化布线系统，机柜内跳线整齐，跳线与配线架统一编号，标记清晰。

定期对生产机房基础设施进行维修保养和更新升级，加强对易损、易失效设备或部件的维护保养，及时下架更新老旧设备。

b）介质管理：

根据数据备份的需要对备份介质实行异地存储，存储地的环境要求和管理措施应与本地相同。

根据介质使用期限及时转储数据。

c）监控管理和安全管理中心：

部署网络监控系统、安全威胁感知系统对通信线路、主机、网络设备和应用软件的运行状况、网络流量、攻击行为等进行监测和报警，建立监测指标和监测模型，有效监测、预警网上银行安全事件（风险），形成记录并妥善保存，保存期限应不小于 6 个月。

及时采取控制措施，消除监测到的安全威胁。

建立网络与信息系统运行监测日报、周报、月报或季报制度，统计分析运行状况。

制定并执行《广西北部湾银行网上银行业务管理办法（修订）》、《广西北部湾银行网上银行操作规程（修订）》明确网上银行系统运行维护的服务管理规范以及相应的控制措施，包括事件处理、问题处理、变更管理等，明确岗位、职责、处理流程、升降级标准、处理时间、所需资源以及流程间的关联和衔接等，及时预警、响应和处置运行监测中发现的问题，发现重大隐患和运行事故应及时协调解决。

d）网络安全管理：

广西北部湾银行总行信息技术部指定专人对网络进行管理，配备 AB 岗专职网络管理员，负责运行日志、网络监控记录的日常维护和报警信息分析、处理工作，并与负责网络设备配置更改的人员职责分离。设备维护记录应至少妥善保存 6 个月。

网络管理员对日志记录或外发中断、日志文件损坏等异常事件进行分析。

网络管理员对网络设备严格执行最小服务配置，并定期离线备份配置文件。

网络管理员定期对网络设备系统进行漏洞扫描，及时修补发现的系统安全漏洞。

e）系统安全管理：

根据业务实际需求和系统安全分析，通过网络权限控制、系统访问控制等措施，执行严格系统访问控制策略。

系统管理人员负责对设备运行关键指标进行日常监控与分析，注意监控、分析业务高峰时段业务压力对系统的影响，合理设计、适时调整容量参数，及时提出、实施设备扩容。

f）密钥管理：

对于所有用于加密客户数据的密钥，广西北部湾银行制定《广西北部湾银行应用系统密钥管理办法》，实施全面的密钥管理流程，包括：密钥生成、密钥分发、密钥存储、密钥使用、密钥更换、密钥销毁等。

应在安全环境中进行关键密钥的备份工作，并设置遇紧急情况下密钥自动销毁功能。

各类密钥应定期更换，对已泄露或怀疑泄露的密钥应及时废除，过期密钥定期销毁。

g）变更管理：

在网上银行系统投产及系统的升级、改造等重大变更前，经过科学的规划、充分的论证和变更技术审查，严格执行审批授权制度，并在事后及时进行变更核验及评价。

6.5.6 风险监测与评估

a）广西北部湾银行已建立名单监控系统、风险决策系统、运营管控平台、反洗钱监测系统和全渠道交易监控系统等交易监控系统，实现对网上银行系统交易全监控，能够甄别并预警潜在风险的交易。

b）广西北部湾银行运营管控平台和反洗钱监测系统运用大数据分析、客户行为建模等技术，建立联动控制、准实时监控、事后监督、风险预警、定期分析、现场检查相结合的多通道风控模式，实现各类监测对象综合监控。形成“疑似电信诈骗”、“疑似非法地下钱庄”、“名单监测模型”等大数据用户异常行为分析模型，甄别并预警潜在风险交易，有效监测可疑交易，对发现可疑交易建立报告、复核并及时上报。

c）广西北部湾银行全渠道交易监控系统统通过挖掘、分析风险特征，以联机方式对网银系统交易进行在线监控，建立事前防范、事中监测及事后分析风险监控体系，实现欺诈侦测和预警功能，有效防止欺诈风险的发生。

d）广西北部湾银行聘请第三方专业安全公司每季度对网上银行系统开展远程渗透测试和漏洞扫描，从信息安全管理体系、物理安全、网络安全、系统安全、应用安全等方面进行全方位安全评估（包含渗透测试），确保第一时间发现风险隐患并及时整改。

6.5.7 风险处置

a）名单监控系统根据监管通报和行内业务数据配置诈骗名单、恐怖组织账户等黑名单，用户开户和执行转账交易时，命中规则则禁止交易。

b）反洗钱监测系统监测用户行为命中反洗钱监测模型的，经过人工核对后报送人民银行，根据人民银行要求执行相应管控。

7 客户体验

7.1 服务功能

网上银行系统应具有以下服务功能：

a）查询功能：查询本人账户列表信息、交易记录、储蓄和理财的资产。

b）账户服务:办理开通II、III类账户、账户挂失/解挂、添加/删除账户、账户充值提现等业务。

c）转账汇款：本行、跨行汇款服务，包括转账汇款、手机号转账、预约转账、交易查询、收款人维护以及转账电子回单等服务。

d）金融理财：理财签约、理财购买、产品查询、风险评估等服务。

e）储蓄：富桂存、富桂薪、多得利、大额存单、定活互转等多种储蓄服务。

f）信用卡：信用卡在线申请、信用卡激活、信用额度查询、账单查询、信用卡分期、信用卡还款、自动扣款签约、消费积分、信用卡商城等服务。

g）个人贷款：多种个人消费贷款和小微贷款服务功能，主要有北行好友贷、税信贷、普惠贷、烟商贷等功能。

h）收付款业务：基于银联二维码技术标准的快速收付款服务，付款为扫描商户或客户收款码进行快捷付款的业务，收款为生成动态收款二维码向他行快速收款的功能。

i）资金归集：有协议归集和超网转入两种资金归集业务，协议归集需要签约资金归集服务协议，仅支持部分银行的资金归集；超网转入无需签订协议，使用短信验证即可实现所有银行实时转入我行客户银行账户。

j）生活缴费：电费缴费、手机话费充值、TEC服务、交罚缴费、油卡充值、非税缴费、桂民卡充值等多种生活服务。

k）安全中心：身份证信息维护、预留信息修改、登录设置、设备管理、密码管理、云证书管理、安全锁及小额开关设置等多种安全服务。

l）其它功能：短信签约、无卡取款、现金预约、网点查询、在线客服、金融计算器等功能。

7.2 服务性能

7.2.1 易访问性

网上银行应保证客户随时可触达，包括但不限于官网有访问入口、各大应用市场均可下载、软件安装过程不复杂。

7.2.2 易操作性

网上银行在不影响功能实现的前提下，降低操作的复杂性；在确保监管要求和安全的前提下，缩减操作步骤，以方便客户使用。

7.2.3 界面舒适性

网上银行界面宜采用统一的交互、视觉规范，图像清晰，图标和字体大小适宜易辨认，有统一的操作原则,操作流程、无卡顿。

7.2.4 APP闪退率

本行APP闪退率（一天中发生闪退的设备数/总体活跃设备数）≤0.15%。

7.2.5 网银整体性能

网上银行支持1000用户同时并发，每秒完成1288.9笔交易。网银整体性能≤1.1s。

7.2.6 总下载字节数

网上银行总下载字节数约2.22MB。

7.3 客服代表行为规范

本行网上银行的客户客服代表新闻规范符合以下标准规定：GB/T 32315-2015 《银行业客户服务中心基本要求》

7.3.1 概述

客服代表的形象代表着机构的整体形象，良好的客户服务可以起到维系和发展客户的作用。

7.3.2 服务电话

客户服务中心应根据业务发展和客户需求，设立统一客户服务电话号码，为客户提供电话语音和人工服务。

7.3.3 服务渠道

客户服务中心应用信息技术扩展服务渠道，如网络渠道、手机银行客户端渠道、电子邮件渠道等，并加强服务渠道宣传。

7.3.4 服务时间

服务时间应为7×24小时，客户服务中心可根据业务情况和客户情况等进行调整。

7.3.5 职业守则

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：应以国家相关法律法规为行为准绳，严格遵守各项法律法规以及规则制度，认真学习法律知识，加强法律意识，自觉抵制违法违规行为。
c）勤业尽职：热爱自己的职业、岗位，精益求精、尽心尽职、奉公无私、兢兢业业，以高度的热情和责任心投入本职工作
d）专业胜任：掌握相关业务知识，精通专业技能，根据社会发展、市场变化，在实践中不断学习新知识，钻研新技能，通过学习提高业务水平，适应工作发展的需要。
e）严格守密：具备保密意识，保护商业秘密与客户隐私。
f）宽容有礼：保持良好的观念和心态，保持宽以待人、谦虚诚实的态度，想客户之所想，急客户之所急，礼貌热情地为客户提供服务。

7.3.6 服务意识

a）整个电话过程中始终要微笑服务，并保持良好的服务态度；
b）话音清晰、精神饱满、自然诚恳、语速适中；
c）耐心、细致、诚恳地对待客户；
d）不推诿客户；
e）禁讲服务忌语，不粗暴对待客户；
f）严禁泄露客户资料及擅自修改客户资料；
g）善于引导客户，向客户适时推介适合的业务；
h）拥有较好的业务知识，全面耐心地回答客户问题；
i）较强的解决问题的能力，能够纤细、准确及迅速地处理客户的咨询与投诉。

7.3.7 用语礼仪

a）亲切：语言要使客户听起来感到亲切，说话要轻柔，语调要低，吐字要清楚，语言要规范。

b）交谈谦逊，使客户感到易于交谈。

c）朴实：语言要大众化，力求口语化，使用语言显得朴实、自然。

d）真诚：语言内容要真实，服务态度要诚恳，通过语言反映出真诚服务的良好服务态度。

e）准确：服务语言要尽量做到用词恰当，语言清晰，表达准确。

f）简练：服务语言要简明扼要、抓住要点，突出重点使客户一听就懂。

g）文明：要使用健康、文雅、庄重的语言。

7.3.8 业务能力

a）客服代表应准确快速判断客户问题原因，了解客户实际需求；根据客户类别的业务种类，及时解决客户问题。

b）客服代表应熟练准确、回答完整，处理有效，正面回答，相关业务知识丰富，提示无遗漏并能提出适当建议，避免不必要持线。

c）客服代表应对于超出解答能力范围的问题，与客户重复确认，主动记录客户问题，及时处理客户意见，妥善处理客户投诉，并在必要时进行跟进。

7.4 客户服务响应

a）人工客户服务时间满足 7×24 小时不间断服务。

b）电话接通率≥88%。

c）平均振铃时间≤6 秒。

8 创新及前瞻性

8.1 服务创新性

a）网上银行的创新性服务，宜以信息通讯技术前沿为大背景，在互联网和移动互联网新兴技术发展趋势和大众客户群需求习惯的基础上开展。

b）服务创新的业务流程与风控规则应符合监管部门要求。

c）“以客户为中心”作为指导思想，不断丰富网上银行产品线、提升客户服务水平。

d）探索新技术，利用云计算、大数据、生物特性识别、人工智能等科技手段，满足客户需求、优化操作流程、提升服务质量。

e）深化与第三方支付机构合作，不断提升客户服务能力和水平，进一步优化客户的网上支付体验，为客户打造了更方便、快捷的网上支付服务。

f）打造安全放心的网上银行交易环境，不断加强网上银行安全管理，从银行端、互联网和客户端多维度强化安全措施，构建了网上银行的整体安全体系。

g）手机银行为客户提供办理利率贷款定价基准转换业务，并对需要进行贷款定价基准转换的客户在手机银行进行提示。

h）手机银行贷款服务在页面明确标识各类贷款产品年化利率。

i）疫情期间对电子银行落地限额进行调整，放大落地限额，确保疫情期间客户通过手机银行及网上银行的日常资金划转和抗疫救援资金的畅通划拨。

j）疫情期间联合平安集团的平安智慧城市智慧医疗，在手机银行APP和微信公众号推出了“疫情资讯”功能，帮助客户及时正确的了解疫情发展情况和最新防控知识，支持客户线上自诊问诊，增强自我防护，科学防控疫情，树立正确的疫情防控理念。

8.2 技术前瞻性

8.2.1 前沿技术应用

a） 大数据

探索大数据应用，采集客户行为信息，建立客户 360 度视图，展现千人千面效果，提升用户体验，打造智能网上银行系统。

b） 生物特征识别

生物识别技术是安全认证的重要手段，将指纹识别、人脸识别、声音识别等生物特征识别技术运用于网上银行业务场景过程中。本行生物特征识别应用须满足《GBT 27912-2011 金融服务生物特征识别安全框架》标准的规定，在保障系统安全性的前提下提升用户使用体验。

c） 云计算

在云计算的技术使用中，应满足《JR/T 0166-2018 云计算技术金融应用规范技术架构》、《JR/T 0167-2018 云计算技术金融应用规范安全技术要求》，满足高弹性、开放性、互通性、高可用性、数据安全性特征。

d） 人工智能

在满足相关业务规则和监管要求的前提下，推进人工智能技术在多场景中的落地。以智能机器人客服作为人工客服的补充，根据客户提问快速匹配，降低客户等待时间，提升客户满意度；以人工智能语音识别提供网点导航、语音交易等服务，打破传统键盘输入。

8.2.2 高可用架构

广西北部湾银行网上银行系统为多中心高可用部署，采用“同城双活”和“异地数据备份”模式提高系统灾备能力。

a） 本地可用性要求：

1） 应用服务器应实施负载均衡；

2） 集中式关系型数据库应实施集群架构技术，如 Oracle RAC，并分片部署在同城两个园区，分片数据库 1 部署在本地，分片数据库 2 部署在同城；

3） 分片数据库 2 的备份数据库应对分片数据库 2 实施冗余备份，同时对分片数据库 2 日志实施同步磁盘复制；如果每个园区有全量数据，可不实施冗余备份和同步磁盘复制；

4） 分布式数据库应实施本地半同步复制，并分片部署在同城两个园区，分片数据库 1 部署在本地，分片数据库 2 部署在同城；

5） 分布式数据库分片数据库 2 的备份数据库应对分片数据库 2 实施两个半同步复制。如果每个园区有全量数据，可只部署本地半同步备库。

b） 同城可用性要求：

1） 应用服务器应实施负载均衡，并与同城园区点构成双活；

2） 集中式关系型数据库应实施集群架构技术，如 Oracle RAC，并分片在同城两个园区部署，分片数据库 1 部署在本地，分片数据库 2 部署在同城；

3）分片数据库 1 的备份数据库应对分片数据库 1 实施冗余备份和数据库日志同步磁盘复制；如果每个园区有全量数据，可不实施冗余备份和同步磁盘复制；

4）分布式数据库应实施本地半同步复制，并分片部署在同城两个园区，分片数据库 1 部署在本地，分片数据库 2 部署在同城；

5）分片数据库 1 的备份数据库：应对分片数据库 1 实施两个半同步复制。如果每个园区有全量数据，可只部署本地半同步备库。

C）异地灾备要求：

1）在灾难发生后能够在预定时间内调配数据处理设备到灾备场地；

2）保留少量温备设备；

3）集中式关系型数据库应对主站点数据库实施异步磁盘复制；

4）分布式数据库应对主站点数据库实施异步复制，如 MySQL Replication；

5）应用服务器原则上按最小规模配置；

6）存储数据应实施定期异地磁带备份（至少每天一次）。

9 实施保障

9.1 组织保障

广西北部湾银行已建立与我行发展战略相适应的网络安全保障及风险管理组织架构，建立由高级管理层负责、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。

总行负责管理全行电子银行业务，包括:制定业务发展规划、《广西北部湾银行电子银行章程》、业务管理办法和操作规程;确定网上银行业务品牌；统一组织业务需求、系统开发、测试、验收与投产工作;负责全行性电子银行业务应用系统的运行维护；管理系统参数及相关柜员；授权各分支机构开办网上银行业务，对分支机构提交的特定业务事项进行审查；组织全行性业务培训及业务制度检查；指导全行网上银行业务工作的开展。

各一级分支机构负责管理辖内网上银行业务，包括：贯彻落实总行的各项工作目标；制定辖内业务发展计划；在权限范围内，对辖内各二级支行提交的特定业务事项进行审查、审批；组织辖内业务培训及业务制度检查；指导辖内各二级支行网上银行业务工作的开展；负责发展网上银行客户并做好客户辅导、培训等服务工作。

各二级支行负责办理具体的网上银行业务，包括：引导客户使用网上银行产品；办理网上银行业务签约、变更、注销等事项；接收、处理网上银行业务指令；收取有关费用；做好售后服务等工作。

广西北部湾银行总行风险管理部为网上银行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。

广西北部湾银行总行渠道管理部、信息技术部和审计部为网上银行产品设计、系统研发、测试、集成、运行维护、管理、内部审计等部门，业务、技术、审计等各部门已明确本部门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。

9.2 管理制度

a）广西北部湾银行已制定明确的网上银行系统总体安全保障目标、网上银行信息安全管理工作的

总体方针和策略，将网上银行信息安全保障及信息安全风险管理纳入全面风险管理体系。

b）广西北部湾银行已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，制定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。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。

c）广西北部湾银行已建立贯穿网上银行业务运营、网上银行系统需求分析、可行性分析、设计、编码、测试、集成、运行维护以及评估、应急处置等过程，并涵盖安全制度、安全规范、安全操作规程和操作手册等。

d）广西北部湾银行采取科学的分析方法开展覆盖风险识别及评价、风险监测及控制、审计和评估等过程的网上银行信息安全风险管理工作。

e）广西北部湾银行已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，建立符合广西北部湾银行实际状况的关键风险指标体系，落实信息安全风险监测，保证高级管理层和相关部门可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。

f）广西北部湾银行结合网上银行业务种类、发展规模以及信息安全新形势，关注与网上银行相关的新威胁以及隐患，调整风险控制措施以及风险评估方案。

g）每年至少开展一次对网上银行系统的信息安全风险评估及深度信息安全检测工作，评估方式不限于自评估和外部评估，自评估由总行风险管理部牵头开展，外部评估机构选择熟悉信息安全和金融行业相关标准、国家认证认可管理部门认可的专业机构，评估依据应覆盖本标准要求，并基于评估结果，妥善选择、实施整改措施。

h）在选择外部评估机构时，对其加强安全管理，签订保密协议或在相关服务协议中明确保密条款。

i）按照国家及行业网络安全等级保护工作有关要求，开展网上银行系统网络安全等级测评及整改工作。

j）主动跟踪行业主管、监管部门与信息安全行业技术组织（例如，国家互联网应急中心等）发布的安全公告、漏洞通知等信息，并及时采取安全检查、修复漏洞、调整系统配置、加强安全管理等应对手段，以保障网上银行系统不受已知安全漏洞的影响。

9.3 宣传及实施机制

a)对于已发布的企业标准，公示至企业标准信息公开服务平台。

b)全行各单位应积极开展本标准的内外部多渠道宣传，扩大受众范围，增强宣传效果。网点人员应深入了解网上银行的功能，熟悉各种操作，清晰、简单、准确的向客户介绍网上银行的功能和使用方法

c)不定期组织相关人员参加网上银行服务标准相关培训，保证相关人员具备必要的专业知识和服务能力，提高业务人员服务意识和服务水平。