ICS 03.060
A11

Q/SJB

盛京银行股份有限公司企业标准

Q/SJB 002—2019

网上银行服务标准

Service standards for internet banking

2019－07－20 发布　　2019－07－20 实施

盛京银行股份有限公司　　发布

目　　次

前　言

本标准根据GB/T 1.1-2009给出的规则起草。

本标准由盛京银行股份有限公司零售银行部提出并归口。

本标准起草单位：盛京银行股份有限公司零售银行部。

本标准主要起草人：孙英品、刘欣。

本标准为首次发布。

网上银行服务标准

1 范围

本标准规定了网上银行服务要求，明确了网上银行服务安全技术规范、安全管理规范、业务动作安全规范、个人信息保护规范、服务连续性要求、身份认证要求和风险控制要求，提出了服务功能、服务性能、客户代表规范及客服响应等客户服务标准，确立了服务创新要求和实施保障机制。

本标准所提网上银行包括企业网上银行、个人网上银行、手机银行、电视银行、网上营业厅等。

本标准适用于网上银行业务管理及技术开发人员开展渠道管理、技术开发、服务创新、客户响应、应用推广等工作。

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。

GB/T 32315-2015 银行业客户服务中心基本要求

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/T 35678-2017 公共安全 人脸识别应用 图像技术要求

JR/T 0044-2008 银行业信息系统灾难恢复管理规范

JR/T 0068-2012 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

3 术语与定义

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其客户提供的网上金融服务。

3.2

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。

3.3

客户端程序 client application 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，包括但不限于可执行文件、控件、静态链接库、动态链接库等，不包括IE等通用浏览器。

3.4

USBKey

一种USB接口的硬件设备，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。

3.5

资金类交易 funds transaction

通过网上银行进行资金操作交易，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。

3.6

个人信息 personal 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。

3.7

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、报文完整性等的密钥，交易敏感数据包括但不局限于完整磁道信息、有效期、CVN、CVN2、证件号码等。

3.8

个人信息主体 personal data subject

个人信息所标识的自然人。

3.9

客户服务代表 customer service representative

客户服务中心前台一线工作人员。

3.10

大数据 big data

具有体量巨大、来源多样、生成极快、且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

3.11

生物特征 biometric characteristic

人体具有的生理特征或行为特征，例如人脸、指纹、虹膜和声纹等。

3.12

生物特征识别 biometric recognition

利用生物特征进行识别的过程，通常包括生物特征辨认和生物特征确认。

3.13

人脸 face

人的头顶之下、颏底线之上、左耳到右耳之间的部分。包含人脸的数字图像称为人脸图像。

3.14

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式。资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

4 网上银行服务安全

4.1 基本安全要求

网上银行安全建设应符合GB/T 35273-2017、JR/T 0068-2012、JR/T 0071-2012规定。

4.2 安全技术规范

4.2.1 客户端程序安全

客户端程序应满足如下要求：

——应对客户端处理的敏感信息、客户端与服务器交互的重要信息采取*号遮掩、加密、加壳、数字签名等安全技术措施；

——重要业务系统客户端上线前应进行严格的代码安全审计，并聘请专业第三方测试机构每年至少开展一次安全性检测；

——客户端程序在启动和更新时应进行真实性和完整性校验，防止程序被篡改或替换；

——客户端程序的临时文件中不应出现敏感信息，临时文件包括但不限于Cookies，客户端程序应禁止在身份认证结束后存储敏感信息，防止敏感信息泄露；

——应提供客户输入敏感信息的即时加密功能，例如采用密码保护控件；

——应防范恶意程序获取或篡改敏感信息，例如使用浏览器接口保护控件进行防范；

——应采用随机分布按键位置、防范键盘窃听技术、计算MAC校验码等措施；

——应保护在客户端启动时用于访问网上银行的进程，防止非法程序获取该进程的访问权限；

——应采用反屏幕录像技术，防范非法程序获取敏感信息；

——开发设计过程中应注意规避各终端平台存在的安全漏洞，例如按键输入记录、自动拷屏机制、文档显示缓存等。

4.2.2 客户端环境安全

客户端环境安全应满足如下要求：

——网上银行应采取在线杀毒服务、安全检测工具等技术措施，并在显著位置予以提醒；

——当发现客户端平台存在重大安全缺陷或安全威胁时，应在门户站点发布警示通知，并通过短信、邮件等方式警示客户。

4.2.3 网络通信安全

数据在网络传输过程中采用的通讯协议和安全认证方式，应满足如下要求：

——通讯协议

- 应采用 SSL/TLS 或其他强壮的加密算法和安全协议保护客户端与服务器之间所有连接，保证传输数据的机密性和完整性；
- SSL 协议应使用 3.0 及以上相对高版本的协议，应取消对低版本协议的支持；
- 应使用强壮的加密算法和安全协议保护网上银行支付网关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。

——安全认证

- 网上银行客户端与服务器应使用安全的协议和强壮的加密算法进行安全、可靠的双向身份认证；
- 银行端 Web 服务器应使用权威机构颁发的数字证书以标识其真实性；
- 应确保客户获取的 Web 服务器的根证书真实有效，可采用的方法包括但不限于在客户开通网上银行时分发根证书、将根证书集成在客户端控件下载包中分发等；
- 应使用获得国家主管部门认定的具有电子认证服务许可证的 CA 证书及认证服务。

4.2.4 服务器端物理安全

应在统一的物理安全体系下确保服务器端物理安全，并应满足如下要求：

——物理位置安全

- 机房场地应避免设在建筑物的高层或地下室；
- 机房场地应避免设在用水设备的下层或隔壁。

——物理访问控制

- 应在机房入口设置电子门禁，并对进出机房的人员进行登记；
- 进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围，且有我行科技人员陪同；
- 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
- 重要区域应配置电子门禁系统，控制、鉴别和记录进入人员。

——防盗窃和防破坏

- 应将设备或主要部件进行固定；
- 应对介质分类标识，存储在介质库或档案室中；
- 应利用光、电等技术设置机房防盗报警系统；
- 应对机房设置监控报警系统。

——防雷击

- 机房建筑应设置避雷装置；
- 应设置防雷保安器，防止感应雷；
- 机房应设置交流电源地线。

——防火

- 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
- 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

——防水和防潮

- 水管安装应不得穿过机房屋顶和活动地板下；
- 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

- 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

——防静电

- 主要设备应采用必要的接地防静电措施；
- 机房应采用防静电地板。

——温湿度控制

- 应设置温、湿度自动调节设施；
- 应保证机房温、湿度的变化在设备运行所允许的范围之内。

——电力供应

- 应在机房供电线路上配置稳压器和过电压防护设备；
- 应配备柴油发电机和专用 UPS，且负载在正常可用范围内；
- 应设置冗余或并行的电力电缆线路为计算机系统供电。

——电磁保护

- 电源线和通信线缆应隔离铺设，避免互相干扰；
- 应对关键设备和磁介质实施电磁屏蔽。

4.2.5 服务器端网络安全

应采取必要措施保证服务器端网络安全，并应满足如下要求：

——合理部署网上银行系统的网络架构

- 应合理划分网络区域并将网上银行网络与办公网及其他网络进行严格隔离；
- 应在网络边界、所有互联网入口以及隔离区（DMZ）与内部网络之间部署防火墙，对非业务必需的网络数据进行过滤，控制粒度为端口级；
- 应通过合理的路由控制，在柜员终端、运维区域监控终端等业务终端与网上银行服务器之间建立安全的访问路径；
- 应保证主要链路的防火墙、交换机等网络设备的处理能力具备冗余空间，满足业务高峰期需要的 1 倍以上；
- 应建立带宽管理策略，保证互联网带宽具备冗余空间，充分满足业务高峰期和业务发展需要；
- 应通过网络设备 QoS 策略、带宽管理等手段，保证网络发生拥堵时，优先保护网上银行业务流量。

——访问控制

- 应在网络结构上实现网间访问控制，应采取防火墙控制网络访问权限；
- 网络访问控制粒度应为端口级；
- 应严格限制 HTTP、FTP.TELNET 等风险较高协议的使用；
- 应限制网络最大流量数及网络并发连接数；
- 应限制只有业务需要的用户才能访问网上银行服务器，控制粒度应为单个用户；
- 应禁止开放远程拨号访问；
- 网络设备应按最小安全访问原则设置访问控制权限。

——实施网络设备管理规范和安全策略

- 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术进行身份鉴别，且口令应具有不易被冒用的特点，应有复杂度要求并定期更换；
- 应至少每 90 天修改一次用户口令；
- 口令最小长度应不低于 8 个字符；
- 口令至少包应含数字和字母；

- 应禁止提交与上次相同的新口令；
- 应对网络设备的管理员登录地址进行限制；
- 应禁止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；
- 应更改网络安全设备的初始密码和默认配置；
- 应指定专人负责防火墙、路由器和 IDS/IPS 的配置与管理，按季定期审核配置规则；
- 应实现设备特权用户的权限分离；
- 应具有登录失败处理功能，应采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
- 通过锁定用户的方式限制连续的访问企图（最多不允许超过 6 次），锁定持续时间应至少设定为 30 分钟或直至管理员为其解锁；
- 空闲超时应要求用户再次输入口令以重新激活终端；
- 应采用 SSH、SFTP 安全协议防止鉴别信息在网络传输过程中被窃听；
- 在变更防火墙、路由器和 IDS/IPS 配置规则之前，应确保更改已进行验证和审批；
- 应明确业务必需的服务和端口，不应开放多余的服务和端口；
- 应每天对网络设备运行状况进行巡检；
- 应定期检验网络设备软件版本信息，避免使用软件版本中出现安全隐患；
- 应每季度检查并锁定或撤销网络设备中多余的用户账号及调试账号；
- 应定期对网络设备的配置文件进行备份，发生变动时应及时备份，确保备份配置文件安全性。

——安全审计和日志

- 应对网络设备的运行状况、网络流量、管理员行为等信息进行日志记录，日志至少应保存 6 个月；
- 审计记录应包括但不限于事件发生的时间、相关操作人员、事件类型、事件是否成功及其他与审计相关的信息；
- 应根据记录进行安全分析，并生成审计报表；
- 应禁止除审计用户外的其他用户对审计记录进行未授权删除、修改或者覆盖；
- 应每天复审所有系统日志；
- 应部署时钟同步（NTP）服务器。

——入侵防范

- 应部署入侵检测系统/入侵防御系统（IDS/IPS），对网络异常流量进行监控，监视并记录网络攻击行为；
- 当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目标和攻击时间，在发生严重入侵事件时应提供报警或自动采取防御措施；
- 应制定合理的 IDS/IPS 的安全配置策略，并指定专人定期进行安全事件分析和安全策略配置优化。

——边界完整性检查

- 应对非授权设备私自联到生产网络的行为进行检查，并进行有效阻断；
- 应对能够访问生产网络的终端私自联到外部网络的行为进行检查，并进行有效阻断。

——恶意代码防范

- 应在网络边界部署防病毒网关，对恶意代码进行检测和清除；
- 应定期对恶意代码防护设备进行代码库升级和系统更新。

4.2.6 服务器端主机安全

确保主机安全应满足如下要求：

——身份鉴别

- 应对登录操作系统和数据库的用户进行身份鉴别，严禁匿名登录；
- 应为不同操作系统和数据库访问用户分配不同的账号并设置不同的密码，禁止共享账号；
- 应要求系统静态口令为 8 位以上，且由字母、数字、符号等混合组成；
- 应至少每 90 天更改一次密码，不允许提交与上次相同的新口令；
- 应启用登录失败处理功能，采取结束会话、限制非法登录次数和自动退出等措施，通过锁定用户的方式限制连续的访问企图（最多不允许超过 6 次），锁定持续时间至少应设定为 30 分钟或直至管理员为其解锁；
- 应采用 SSH 协议对服务器进行远程管理，防止认证信息在网络传输过程中被窃听。

——访问控制

- 应根据“业务必需”原则授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
- 应根据管理用户的角色（例如系统管理员、应用用户等）分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
- 应严格限制默认用户的访问权限，应重命名系统默认用户、修改默认用户密码、及时删除多余的或过期的用户及调试用户；
- 应严格控制操作系统重要目录及文件的访问权限。

——入侵防范

- 操作系统应遵循最小安装原则，仅安装需要的组件和应用程序；
- 应及时对主要服务器进行补丁升级；
- 应严格限制下载和使用免费软件或共享软件，应确保服务器系统安装的软件来源可靠，且在使用前进行测试。

——恶意代码防范

- 应安装国家安全部门认证的正版防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；
- 应支持防恶意代码软件的统一管理；
- 应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。

——资源控制

- 应通过设定终端接入方式、网络地址范围等条件限制终端登录，例如部署堡垒机统一管理终端接入；
- 应根据安全策略设置登录终端的操作超时锁定，超时时间应小于 15 分钟；
- 应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况，并提供资源使用异常情况下的报警功能；
- 应定期对系统的性能和容量进行规划，能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

4.2.7 应用安全

网上银行应用应满足如下要求：

——身份鉴别

- 应禁止明文显示密码，应使用相同位数的同一特殊字符（例如*和首）代替；

- 密码应有复杂度要求，密码长度应至少 6 位，应支持字母和数字共同组成；
- 在用户设置密码时，应提示不使用简单密码；
- 如有初始密码，首次登录时应强制用户修改初始密码；
- 图形认证码应由数字和字母等字符混合组成，且为随机产生，应采取图片底纹干扰、颜色变换等有效方式，防范恶意代码自动识别图片上的信息；
- 图形认证码应具有使用时间限制并仅能使用一次；
- 图形认证码应由服务器生成，客户端源文件中不应包含图形验证码文本内容；
- 应采取对整体键盘布局进行随机干扰等方式，防范密码被窃取；
- 应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；
- 应判断用户的空闲状态，当空闲超过一定时间后，自动关闭当前连接，用户再次操作时须重新登录；
- 会话过程中应维持认证状态，防止用户通过直接输入登录后的地址访问登录后的页面；
- 应禁止在客户端缓存密码、密钥等敏感信息，防范未授权用户通过浏览器后退等方式获取敏感信息；
- 退出登录或客户端程序、浏览器页面关闭后，应立即终止会话，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；
- 修改用户敏感参数（例如密码、转账限额等）时，应再次认证用户身份；
- 显示用户身份证件信息时，应屏蔽部分关键内容。

——访问控制

- 应建立安全的访问控制机制，防止越权访问他人账号的信息、在低级别的认证方式下访问高级别认证方式才能访问的功能等；
- 企业网上银行应支持用户选择使用管理员和操作员两类用户，管理员初始密码应在银行柜台设置，操作员由管理员设置，操作员权限应根据录入、复核、授权职责分离的原则设置；
- 应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
- 应建立完善的交易验证机制，每次处理的用户信息均以服务器端数据为准，并对用户请求指令的逻辑顺序进行合理控制；
- 应每季度检查并锁定或撤销应用系统和数据库中多余的、过期的用户及调试用户。

——安全审计

- 应具有保存和显示用户历史登录信息（例如时间、IP 地址、MAC 地址等）的功能，支持用户查询登录（包括成功登录和失败登录）、交易等历史操作；
- 应具有详细的交易流水查询功能，包括但不限于日期、时间、交易卡号、交易金额和资金余额等信息；
- 审计功能应覆盖所有对网上银行数据的管理操作，包括用户开通、证书发放、密码修改、冻结解冻、权限变更等操作，应对用户开通、专用安全设备更换、重要信息变更、冻结解冻等重要操作进行稽核；
- 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，并定期备份审计记录，保存时间不少于半年；
- 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
- 应合理分配交易日志的管理权限，禁止修改日志。

——软件容错

- 应提供数据有效性检验功能，严格限制输入的数据格式或长度；

- 应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用户。

——资源控制

- 应对系统的最大并发会话连接数进行限制；
- 应对单个用户的多重并发会话进行限制；
- 应对一个时间段内可能的并发会话连接数进行限制；
- 当应用系统通信双方中的一方在指定时间内未作任何响应，另一方应自动结束会话；
- 应对系统服务水平降低到预先规定的最小值进行检测和报警。

——Web 应用安全

- 应防范敏感信息泄露；
- 在网上银行系统上线前，应删除 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，并进行严格访问控制；
- 应禁止在 Web 应用程序错误提示中包含详细信息，不向用户显示调试信息；
- 应禁止在 Web 应用服务器端保存用户敏感信息；
- 应对网上银行系统 Web 服务器设置严格的目录访问权限，防止未授权访问；
- 应统一目录访问的出错提示信息；
- 应禁止目录列表浏览，防止网上银行站点重要数据被未授权下载；
- 应防范 SQL 注入攻击；
- 网上银行系统 Web 服务器应用程序应对用户提交的所有表单、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；
- 应禁止仅在客户端以脚本形式对用户的输入进行合法性判断和参数字符过滤；
- 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；
- 应防范跨站脚本攻击；
- 应防止跨站脚本注入；
- 应对 Web 页面提供的链接和内容进行控制，定期检查外部链接和引用内容的安全性；
- 应部署网页防篡改系统。

——防钓鱼

- 应具有防网络钓鱼的功能，例如显示用户预留信息、使用预留信息卡、用户自定义个性化界面等；
- 应采取防钓鱼网站控件、钓鱼网站监控工具、钓鱼网站发现服务等技术措施，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；
- 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 Referer/IP 信息的校验、设置转账白名单等；
- 应采用已有的和 IE 或其它浏览器相关联的可信网址的认证机制，保证登录的 URL 经过第三方权威机构的安全认证。

——其他要求

- 敏感信息在应用层应保持端到端加密，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；
- 网上银行系统应判断同一次登录后的重要操作使用同一台终端，例如验证 IP 地址、MAC 地址、机器码等，如发生变化，应再次对用户身份进行认证，否则服务器端自动终止会话。

4.2.8 数据安全及备份恢复

网上银行数据安全及备份恢复应满足如下要求：

——应采用加密技术对用户敏感信息、重要业务数据进行传输加密；
——应建立重要数据的定期数据备份机制，至少做到增量数据备份每天一次，完整数据备份每周一次，并应将备份介质存放在安全区域内，数据保存期限应依照国家相关规定，数据备份存放应采用多冗余方式，完全数据备份应至少保证以一个星期为周期的数据冗余；
——核心层、汇聚层的设备和重要的接入层设备均应双机热备，例如核心交换机、服务器群接入交换机、重要业务管理终端接入交换机、核心路由器、防火墙、均衡负载器、带宽管理器及其他相关重要设备；
——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双机热备或多机集群，并应设置磁盘冗余阵列以避免单一部件故障影响设备运行的风险；
——应提供冗余通信线路，应遵照与主用通讯线路不同运营商和不同物理路径的原则选择冗余通讯线路；
——应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。

4.3 安全管理规范

4.3.1 安全管理机构

网上银行系统安全管理机构岗位设置、人员配备等应满足如下要求：
——岗位设置
- 应建立与全行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，建立由董事会及高级管理层负责、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、管理规定及人员配置；
- 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及人员职责，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；
- 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，业务、技术、审计等各部门应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，相关人员应详细了解本部门网上银行相关的职责设置、信息安全保障机制等基本情况；
- 应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离。

——人员配备
- 应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；
- 专职信息安全管理人员应实行 A、B 岗制度，不可兼任其他岗位；
- 应实现关键岗位的多人共同管理。

——授权和审批
- 应根据网上银行相关部门、岗位的职责明确上下级间和各部门间的授权审批事项、审批部门和批准人等；
- 应针对网上银行业务及技术规划、架构及策略、网上银行新产品推出、网上银行重要技术路线选择、网上银行系统重要变更操作、物理访问和网上银行系统接入等事项建立审批程序，应提交管理层审批，并按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- 应记录审批过程并保存审批文档；

- 用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系，权限变更应执行相关审批流程，并有完整的变更记录；
- 应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。

——沟通和合作

- 应加强网上银行系统管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；
- 应建立与监管部门、公安机关、电信公司、同业机构、第三方机构的合作、沟通以及应急协调机制，有效处置 DDoS、网络钓鱼等网络与信息安全事件；
- 应加强与供应商、业界专家、安全公司、安全组织的合作与沟通，增强日常安全防护、突发事件处置、故障处理等方面的能力；
- 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- 应聘请信息安全专家作为常年的安全顾问，指导网上银行信息系统的信息安全建设、参与安全规划和安全评审等。

——审核和检查

- 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- 应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，应保证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；
- 应制定安全检查方案并进行安全检查，形成安全检查汇总表、安全检查报告，并将安全检查报告进行上报人民银行、银保监局等监管部门；
- 应至少每两年对网上银行开展一次审计，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及重要客户信息和交易数据的安全性、应急管理、外包管理的有效性以及其它重要信息安全保障的情况。

4.3.2 安全策略

网上银行安全策略应满足如下要求：

——应制定明确的网上银行系统总体安全保障目标，建立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；

——应结合网上银行发展战略及业务特点，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，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；

——应做好网上银行相关的新产品（业务）设计以及主要技术路线选择等关键规划的深入论证工作，关注产品及技术路线的合规性、相关业务及技术规则的一致性和延续性以及产品间、系统间的关联性、依赖性，平衡用户体验和安全性，通过增加关键控制机制等措施防范潜在重要安全隐患，避免产生潜在的信息安全风险；

——应建立网上银行信息安全风险管理策略，至少包括风险评价和定级、风险偏好、容忍度及参数制定、风险控制、成本及效益评价、控制措施有效性评价策略等，应根据网上银行发展及检查审计结果，定期修订策略；

——应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；

——在进行网上银行信息安全风险识别时，应明确保护对象，进行资产分类，识别、评估资产的重要性，综合分析其面临的内外部威胁以及可被威胁利用的脆弱性，识别并评估已有的控制措施，准确界定由此产生影响的可能性，正确识别对国家安全、金融稳定、公众利益、声誉造成影响的信息安全风险；

——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定规避措施；

——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；

——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；

——对于衍生的网上银行信息安全风险以及未按计划达到的控制目标，应重新启动信息安全风险评估流程，制定和选择新的风险控制措施，对已接受的风险，应定期进行再评估；

——应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，应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，自评估应由内独立于网上银行设计、开发、运行和管理的部门进行，外部评估应由具备评估资质的可靠专业机构进行，并与其签订保密协议或在相关服务协议中明确保密条款，避免泄漏敏感信息；

——评估依据应覆盖本标准要求项，基于评估结果，妥善选择、实施整改措施，及时将评估报告上报人民银行等监管部门；

——应按照国家及行业信息系统信息安全等级保护工作有关要求，规定所有与网上银行相关的信息资产的安全级别，并制订与其安全级别相对应的保护措施，每年开展网上银行系统信息安全测评及整改工作。

4.3.3 管理制度

网上银行相关系统应建立规范的安全管理制度，并应满足如下要求：

——应建立贯穿网上银行业务运作、网上银行系统设计、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记录手册等方面的信息安全管理制度体系；

——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；

——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；

——安全管理制度应具有统一的格式，并进行版本控制；

——应定期组织相关部门和人员对安全管理制度体系的合理性和适用性进行审计，及时针对安全管理制度的不足进行修订；

——安全管理制度应通过正式、有效的方式发布；

——安全管理制度应注明发布范围，并对收发文进行登记。

4.3.4 人员安全管理

网上银行系统相关人员安全管理应满足如下要求：

——应指定或授权专门的部门或人员负责网上银行系统相关人员录用工作；

——应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具

有的技术技能进行考核；

——应与员工签署保密协议，或在劳动合同中设置保密条款；

——应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议；

——凡因违反国家法律法规和有关规定受到过处罚或处分的人员，应不得从事与网上银行相关的信息安全管理工作；

——应对安全教育和培训的情况和结果进行记录并归档保存；

——应具有员工岗位调动或离职的安全管理制度，取回岗位调动或离职员工的各种身份证件、钥匙、徽章等以及提供的软硬件设备，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漏；

——应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开，并保证离岗员工管理及使用的系统口令须立即更换；

——应定期对各个岗位的人员进行安全技能及安全认知的考核，并对考核结果进行记录并保存；

——应对关键岗位的人员进行全面、严格的安全审查和技能考核，并对考核结果进行记录并保存；

——应建立网上银行相关的员工培训机制，对网上银行业务操作人员、开发设计人员、运维人员等进行安全意识教育、岗位技能培训和相关安全技术培训，培训内容尤为关注网上银行相关的信息安全保障框架、制度、监管要求、标准、规范，网上银行的关键技术风险、业务操作风险；

——应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；

——应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对安全教育和培训的情况和结果进行记录并归档保存；

——应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应建立存取控制机制、认证机制，列明所有用户名单及其权限，其活动应受到监控；

——针对长期或临时聘用的技术人员和承包商，尤其是从事敏感性技术相关工作的人员，应制定严格的审查程序，包括身份验证和背景调查，必要时应签署保密协议。

4.3.5 系统建设管理

网上银行系统建设管理应满足如下要求：

——安全方案设计

- 应指定和授权专门的部门对系统的安全建设进行总体规划，制定中期和远期的安全建设工作计划；
- 应对总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案的合理性和正确性进行论证和审定，经过批准后正式实施；
- 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

——产品采购和使用

- 应确保安全产品采购和使用符合国家的有关规定；
- 应确保密码产品采购和使用符合国家密码主管部门的要求；
- 应指定或授权专门的部门负责产品采购；
- 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；
- 应建立信息安全产品资产登记机制，建立信息安全类固定资产登记簿并由专人负责管理；

- 扫描、检测类安全产品的使用应经过主管领导授权，应严禁非授权人员使用，应定期查看各类信息安全产品相关日志和报表信息并定期汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告；
- 各类信息安全产品在使用中产生的日志和报表信息应备份存档至少 3 个月；
- 应及时升级维护信息安全产品，凡超过使用期限的或不能继续使用的信息安全产品，应按照固定资产报废审批程序处理。

——自行软件开发

- 应确保开发环境与实际运行环境物理分开，开发、测试不得在生产环境中进行，应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制；
- 应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，不得在程序中设置后门或恶意代码程序；
- 在应用系统上线前，应对程序代码进行代码复审，识别可能的后门程序、恶意代码和安全漏洞，例如缓冲区溢出漏洞等；
- 应严格控制对生产版本源代码的访问；
- 应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；
- 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；
- 应确保对程序资源库的修改、更新、发布进行授权和批准；
- 在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。

——外包软件开发

- 应根据开发需求检测软件质量；
- 应在软件安装之前检测软件包中可能存在的恶意代码；
- 应要求开发单位提供软件设计的相关文档和使用指南；
- 应要求开发单位提供软件源代码，并审查软件中可能存在的后门；
- 不得将信息科技管理责任外包，应合理谨慎监督外包职能的履行；
- 应实现客户资料与外包服务商其他客户资料的有效隔离，确保在中止外包协议时收回或销毁外包服务商保存的所有客户资料；
- 应按照“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；
- 应严格控制外包服务商再次对外转包，采取足够措施确保商业银行相关信息的安全；
- 应对外包服务商在服务中可能出现的重大缺失建立恰当的应急措施，包含但不限于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；
- 外包人员进行现场实施时，应事先提交计划操作内容，应指定人员在现场陪同外包人员，核对操作内容并记录，涉及敏感操作（例如输入用户口令等）应由指定人员进行操作，外包人员不得查看、复制或带离任何敏感信息；
- 应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告，应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。

——工程实施

- 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则；
- 应指定或授权专门的部门或人员负责工程实施过程的管理；
- 应制定详细的工程实施方案控制实施过程，并在模拟系统试验成功后方可实施，以确保业务系统平稳过渡，并要求工程实施单位能正式地执行安全工程过程。

——测试验收

- 应对系统测试验收的控制方法和人员行为准则进行书面规定；
- 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
- 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；
- 在测试验收前应根据设计方案或合同要求等制定测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
- 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

——系统交付

- 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- 应与外包项目建设单位签署知识产权保护协议和保密协议，不得将网上银行系统采用的关键技术措施和核心安全功能设计对外公开，应对负责系统运行维护的技术人员进行相应的技能培训；
- 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；
- 应对系统交付的控制方法和人员行为准则进行书面规定；
- 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

——安全服务商选择

- 选择安全服务提供商时，应评估其资质、经营行为、业绩、服务体系和服务品质等要素；
- 应确保安全服务商的选择符合国家的有关规定，应制定专门的部门负责安全服务提供商的资质审查；
- 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；
- 应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

4.3.6 系统运维管理

网上银行系统运维管理应满足如下要求：

——环境管理

- 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
- 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制、消防系统等设施进行维护管理；
- 应指定部门负责机房安全，指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理；
- 机房管理员应经过相关专业培训，掌握机房各类设备的操作要领；
- 应制定机房视频监控值守的制度；
- 机房所在区域应安装 24 小时视频监控录像装置，重要机房区域实行 24 小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管，保存期限不少于 3 个月，销毁录像等资料应经机构主管领导批准后实施；
- 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。

——资产管理

- 应编制并保存详细的资产清单，资产清单应包括资产的价值、所有人、管理员、使用者和安全等级等条目，并根据安全等级制定相应的安全保护措施；
- 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
- 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
- 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理；
- 应禁止在公共文件存储区存放系统相关的调试信息（代码）、设计说明、架构设计、规划蓝图等重要信息。

——介质管理

- 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；
- 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理，所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放；
- 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，应选择安全可靠的传递、交接方式，做好防信息泄露控制措施；
- 应对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；
- 技术文档应实行借阅登记制度，未经批准，任何人不得将技术文档转借、复制或对外公开；
- 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；
- 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；
- 对载有敏感信息存储介质，应报相关部门备案，并进行统一销毁，由相关部门使用专用工具进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在内部使用的情况，否则应进行信息的不可恢复性销毁；
- 应制定移动存储介质和笔记本电脑使用规范，定期核查所配发移动存储介质和笔记本电脑的在位使用情况，严禁违规使用移动存储介质和笔记本电脑；
- 应建立重要数据多重备份机制，其中至少 1 份备份介质应存放于指定的同城或异地安全区域；
- 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

——设备管理

- 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；
- 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- 应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任；
- 需要废止的设备，应由指定专门部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到其他单位，应备案并对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理，同时备案；

- 设备确需送外单位维修时，应指定专门部门彻底清除所存的工作相关信息，必要时应与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前应拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督；
- 应制定规范化的设备故障处理流程，建立详细的故障日志（包括故障发生的时间、范围、现象、处理结果和处理人员等内容）；
- 应确保信息处理设备经过审批后带离机房或办公地点；
- 应对设备进行分类和标识，建立标准化的设备配置文档；
- 新购置的设备应经过测试，测试合格后方能投入使用；
- 应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任。

——监控管理和安全管理中心

- 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户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 3 个月，应及时采取控制措施，消除监测到的安全威胁；
- 应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；
- 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，应形成分析报告，并采取必要的应对措施；
- 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理；
- 应按重要程度进行分级报警，并且重要报警应以某种方式（短信、邮件等）主动通知相关人员及时处置；
- 应制定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，并及时报告至人民银行等主管部门。

——网络安全管理

- 应建立网络安全管理制度，并对网络安全配置、日志保存时间、安全策略、系统升级、补丁更新、重要文件备份等方面作出规定；
- 应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、报警信息分析和处理工作，与负责网络设备配置更改的人员职责分离，维护记录应至少妥善保存 3 个月；
- 应建立健全网络安全运行维护档案，及时发现和解决网络异常情况；
- 应制定网络接入管理规范，任何设备接入网络前，接入方案应经过审核，审核批准后方可接入网络并分配相应的网络资源；
- 应实现设备的最小服务配置，并定期离线备份配置文件；
- 所有与外部系统的连接均应经过授权，应拒绝便携式和移动式设备的网络接入；
- 应定期检查违反网络安全策略的行为；
- 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；
- 应根据厂家提供的升级软件对网络设备进行更新，并在更新前对现有重要文件进行备份。

——系统安全管理

- 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
- 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；

- 应确保系统管理员不得兼任业务操作人员，不得对业务数据进行任何增加、删除、修改、查询等操作，确需对计算机系统数据库进行技术维护性操作的，应征得业务部门书面同意，并详细记录维护内容、人员、时间等信息；
- 应根据业务需求和系统安全分析确定系统的访问控制策略；
- 应至少每半年进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补；
- 应安装系统的最新补丁程序，在安装系统补丁前，应先在测试环境中测试通过，并对重要文件进行备份后，方可实施安装，并对系统变更进行记录；
- 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作，重要的系统变更要求至少两人在场；
- 应定期对运行日志和审计数据进行分析，以便及时发现异常行为；
- 应建立完善的系统用户权限变更申请、审批、复核流程；
- 应加强系统容量管理，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，及时提出并实施设备扩容。

——恶意代码防范管理

- 应限制在可以访问生产服务器的终端上使用 U 盘、移动硬盘等移动存储设备；
- 应禁止核心业务网、网上银行系统网与其他低安全级别网络共用病毒服务器；
- 应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序；
- 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报制度等作出明确规定；
- 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面报表和总结汇报。

——密钥管理

- 应制定与网上银行相关的密钥管理制度，并严格实施；
- 密钥和密码应加密存储；
- 采用的密码算法应经过国家主管部门认定；
- 对于所有用于加密客户数据的密钥，应制定并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、密钥更换、密钥销毁、知识分割以及双重控制密钥、防止未授权的密钥更换、更换已被知晓或可能被泄露的密钥、收回过期或失效的密钥等；
- 应在安全环境中进行关键密钥的备份工作，并设置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，过期密钥应安全归档或定期销毁；
- 密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责，密钥资料应保存在保险柜内，保险柜钥匙应由专人负责，使用密钥和销毁密钥应在监督下进行并留有使用、销毁记录。

——变更管理

- 应根据网上银行系统特点制定针对性的变更方案；
- 在网上银行系统投产、升级、改造等重大变更前，应经过科学的规划、充分的论证和严格的技术审查，应及时向人民银行、银保监局等监管部门报告有关情况，并在事后提交有关总结报告；

- 应建立变更控制的申报和审批流程，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录，保存期至少 3 个月；
- 应建立中止变更并从失败变更中恢复文件的流程，明确过程控制方法和人员职责，必要时对恢复过程进行演练并形成演练报告；
- 变更前应进行必要的风险评估，并做好应急准备，有停机风险的变更原则上放在业务低峰期进行；
- 变更前应做好系统和数据的备份，对于风险较大的变更，应在变更后对系统的运行情况进行跟踪；
- 如需要使用生产环境进行测试，应纳入变更管理，并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全；
- 当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的有效性，应尽量减少紧急变更。

——业务运行连续性

- 应制定网上银行业务连续性策略及计划；
- 应将网上银行业务连续性管理整合到组织的流程和结构中，明确指定相关部门负责业务连续性的管理；
- 应制定员工在网上银行业务连续性方面的培训计划和考核标准；
- 应定期测试并更新网上银行业务连续性计划与过程。

——备份与恢复管理

- 应明确需要定期备份的重要业务数据、系统数据等，网上银行系统应实施应用级备份，以保证灾难发生时，能尽快恢复业务运营；
- 应建立与备份、恢复相关的安全管理制度，对系统数据的备份方式、备份周期、存储介质和保存期限等方面进行规范；
- 应根据系统数据的重要性和数据对系统运行的影响，制定系统数据的备份和恢复策略，备份策略需指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输的方式等；
- 应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，所有文件和记录应妥善保存，明确规定备份数据的保存期，做好备份数据的销毁审查和登记工作，应定期导出网上银行系统业务日志文件，并加以明确标识，日志文件应至少妥善保存 3 个月；
- 应定期执行恢复程序，检查并测试备份介质的有效性，确保可以在规定的恢复程序时间内完成备份的恢复；
- 应定期对备份数据的有效性进行检查，每次抽检数据量应不低于 10%，备份数据应实行异地保存；
- 恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后妥善保管；
- 应在统一的灾难恢复策略下建立完善的网上银行系统灾难恢复体系，遵照主管部门有关要求，开展灾难恢复需求分析、策略及计划制定、灾备系统建设及演练等工作，并根据实际情况对其进行分析和改进，确保各环节的正确性以及灾难恢复体系的有效性。

——安全事件处置

- 应报告所发现的安全弱点和可疑事件，在任何情况下用户均不得尝试验证弱点；
- 应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- 应根据国家相关管理部门对信息安全事件等级划分方法和安全事件对本机构产生的影响，对本机构网上银行信息安全事件进行等级划分；

- 应建立安全事件报告和响应处理流程，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；
- 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存并及时报告本单位主管领导，其中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；
- 应结合实际情况，对造成系统中断和造成信息泄密的安全事件制定不同的处理流程和内外部报告流程；
- 重大网上银行信息安全事件应按照有关规定，在事发后 2 小时内，以书面形式报告至人民银行、银保监局等监管部门，报告要素包括事件发生时间、基本情况、影响、原因、处置措施、需监管单位协调事项，每 4 小时进行事中报告，并在事件结束后 7 个工作日内提交总结报告；
- 应定期对本机构及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有效性，及时整改发现的问题。

——应急管理

- 应在网上银行统一的应急预案框架下，制定针对不同事件的应急预案，应急预案至少包括各类事件场景下启动应急预案条件、应急处理流程、系统恢复流程、事件信息收集、分析、报告制度、事后经验总结和培训等内容；
- 应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，在任何场景下，选择处置方案应充分考虑可能消耗的时间，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，应严格按照程序做好转人工处理等应急操作；
- 应建立有效的技术保障机制，确保在安全事件处置过程中不因技术能力缺乏而导致处置中断或延长应急处置时间；
- 应建立应用系统紧急补丁（应急预案）的开发、发布流程，以备必要时提供紧急补丁或应急预案进行处理，修补重要安全漏洞；
- 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
- 应对网上银行系统相关人员进行应急预案培训，应急预案的培训应至少每年举办一次；
- 应建立应急预案演练制度，定期组织有业务部门参与应急演练，定期对双机热备系统进行切换演练，备份系统与生产系统的切换应至少每年演练一次，针对 DDoS、网络钓鱼等重要安全威胁，应定期开展有相关单位、部门参与的联合演练；
- 应建立应急预案的评估及改进机制，定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练应急预案。

4.4 业务运作安全规范

4.4.1 业务申请及开通

网上银行业务申请及开通应满足如下要求：

——网上银行资金类交易的开通应由客户本人申请，验证客户有效身份，并进行风险提示，并由客户确认，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；

——网上银行资金类交易关闭后，重新申请开通该功能，应由客户本人持有效身份证件到柜台或采取电子签名验证的网上银行渠道申请，通过网上银行渠道申请时，应通过验证发向可靠的预留

手机号码的短信验证码等方式，由客户本人对业务重新开通操作进行确认；

——企业网上银行开通应由本企业人员到柜台申请，应审查其申请材料的真实性、完整性和合规性；

——企业网上银行客户加挂账户可通过柜台或通过使用增强安全机制进行身份认证的双人复核机制后方可增加，同时应通过有效方式请求企业联系人确认，注销企业网上银行服务、重置增强安全机制密码应到柜台办理；

——通过手机终端访问网上银行的资金类交易开通应有效验证客户身份，客户应通过柜台或者通过已采取电子签名验证等安全认证手段的网上银行渠道主动申请，在柜台办理签约时，应验证客户有效身份信息、银行账户密码等信息，通过网上银行渠道申请时，应采取双因素身份认证验证客户的真实身份及银行卡交易密码，并通过验证发向可靠的预留手机号码的短信验证码等方式，请求客户本人对交易开通操作进行确认；

——客户通过网上银行渠道重置登录密码及支付密码时，应采取双因素身份认证有效验证客户的真实身份，并通过验证发向可靠的预留手机号码的短信验证码等方式，请求客户本人对密码重置操作进行确认；

——网上银行专用安全设备在暂停、终止、挂失或注销后，如需要恢复、解除挂失，应由客户本人持有效身份证件到柜台或通过客服电话办理，应核实客户信息、网银账户信息并对预留手机号码进行验证。

4.4.2 资金交易流程

网上银行资金交易过程应满足如下要求：

——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；

——在客户确认交易信息后，再次提交交易信息（例如收款方、交易金额）时，应检查客户确认的信息与最终提交交易信息之间的一致性，防止在客户确认后交易信息被非法篡改或被替换；

——资金类交易中，应对客户端提交的交易信息间的隶属关系进行严格校验，例如验证提交的账号和卡号间的隶属关系以及账号、卡号与登录用户之间的关系；

——对于资金类等高风险业务，应在确保客户有效联系方式前提下，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；

——应根据业务类别、开通渠道及身份验证方式的不同设置不同的交易限额，同时允许客户在银行设定的限额下自主设定交易限额。

4.4.3 交易过程监控

网上银行应对交易过程进行监控管理，并应满足如下要求：

——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；

——应根据审慎性原则，对于交易要素不完整、超过额度的转账支付和关注类账户的资金流动（例如疑似违规资金变动）等交易进行人工审核；

——应根据交易的风险特征建立风险交易模型，以此为基础，建立风险交易监控平台，对单个 IP 的异常登录尝试、短时间内单个账户在异地多笔交易、外部欺诈、身份冒用、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；

——应建立异常交易识别规则和风险处置机制，对监控到的风险交易进行及时分析与处置；

——风险交易监控系统应通过分析用户交易习惯和群体用户行为习惯，提高交易分析的效率和准确率；

——风险交易监控系统应通过分析欺诈行为特征创建反欺诈规则，对交易数据实时分析，根据风险高低产生预警信息，从而实现欺诈行为的侦测、识别、预警和记录；

——风险交易监控系统应能够不断更新反欺诈规则，能够实现各、主管部门和公安机关等机构间的信息共享和信息交换，完善反欺诈系统。

4.4.4 客户宣传及权益保护

应加强网上银行客户宣传及权益保护，并应满足如下要求：

——应切实加强客户培训和风险提示，向客户详细解释网上银行业务流程和安全控制措施，在网银新产品、新业务推出、相关业务操作流程变更、安全控制措施变化时，及时告知客户；

——应通过各种宣传渠道向大众提供正确的网上银行官方网址和呼叫中心号码,提示客户牢记官方网站地址和呼叫中心号码；

——应向客户印发通俗易懂的网上银行信息安全宣传手册,在网上银行官方网站首页显著位置开设信息安全培训栏目；

——应建立网上银行相关的侵犯客户权益行为的处置机制，开辟公众举报渠道，建立有效的问题机制，及时通过网站及其他可靠渠道向公众通报提示钓鱼网站、网络欺诈等重要信息；

——应建立网上银行相关的客户投诉、纠纷处理及舆情控制机制，严格按照行业、机构的相关规定和要求对外发布信息，有效维护客户权益及声誉；

——应通过多种渠道及时公告网上银行相关的服务内容、协议、资费标准等重大调整，系统重要升级或变更影响正常服务等重大事项。

4.5 个人信息保护规范

4.5.1 个人信息分类

个人信息应包含与个人相关的能够被知晓和处理且能够单独或与其他信息结合进行识别的任何信息，主要应包含以下内容：

——个人身份标识与鉴别信息，应包括静态密码、动态密码、密保问题答案、数字证书、生物特征信息等；

——个人身份信息，应包括个人姓名、性别、国籍、民族、身份证件种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等；

——个人财产信息，应包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等；

——个人账户信息，应包括银行业金融机构开立账号、银行卡有效期、卡片验证码（CVN、CVN2、CAV、CVV2、CVC、CID）、非银行支付机构的支付账户、账户开立时间、开户行、开户机构、账户余额等；

——个人信用信息，应包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息；

——个人金融交易信息，应包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人信息和客户在通过银行业金融机构或非银行支付机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人信息等；

——衍生信息，应包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息；

——个人信息还应包含在与个人建立业务关系过程中获取、保存的其他个人信息。

4.5.2 个人信息分级

应根据个人信息价值和安全风险的不同，将个人信息划分为高敏感、中敏感、低敏感、非敏感四个等级，应针对个人信息保护程度、影响程度不同，将个人信息进行特殊标注，采取必要的管理措施和技术手段，保护个人信息安全，防止未经授权检索、泄露、损毁和篡改，个人信息分级应满足如下要求：

——高敏感个人信息：应包含重要个人信息，泄露后可能致使个人资产受到严重损失；

——中敏感个人信息：应包含一般个人信息，泄露后可能致使个人资产受到损失；

——低敏感个人信息：应包含其他个人信息，泄露后可能致使个人资产受到影响；

——非敏感个人信息：应包含公开后对个人无影响的信息。

4.5.3 个人信息管理

网上银行系统对于个人信息管理应满足如下要求：

——当搜集个人信息时，应向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，并且具有合法、正当、必要、明确的个人信息处理目的；

——除与个人信息主体另有约定外，应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；

——应以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则；

——应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；

——涉及通过界面展示个人信息的（例如显示屏幕、纸面），个人信息控制者应对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险；

——应设置专职岗位负责个人信息的保护工作，工作内容应包括但不限于：

- 应制定个人信息保护制度，对个人信息处理流程进行把关，针对岗位性质分配个人信息操作权限及明确安全责任；
- 应了解个人信息保护的相关技术，在技术上审核解决方案，确保满足个人信息保护需求；
- 应明确对违反机构内部个人信息管理制度造成危害的行为的处罚规则；
- 应开展个人信息保护的宣传和培训工作，培训材料和培训频率应满足个人信息保护需求，应保证每年不少于一次；
- 应对个人信息保护工作进行监督和指导，定期对个人信息使用范围和操作方式进行检查，配合审计工作人员对工作进行定期审计。

——应对个人信息保护工作进行审计，并作为其整改或改进的材料依据；

——应制定个人信息泄露事件处理和响应机制，事件发生时应立即采取处置措施，防止信息扩散，保存有关记录，并及时向有关部门报告。

4.5.4 个人信息采集

网上银行采集个人信息时，应满足如下要求：

——个人信息采集应具遵循最小化原则，采集的个人信息不应超出网上银行业务经营活动所必要的信息范围；

——个人信息采集应遵循告知原则，应通过明示的事前约定、事中提醒等方式告知被采集方个人信息采集范围、个人信息的使用者及个人信息的使用方式；

——个人信息使用者的变动应征得客户同意；

——应采取有效技术措施使个人信息的机密性、完整性控制与全行风险偏好一致；

——应保证在任何情况下不得通过非法途径获取信息，例如不得从无个人信息采集资质的个人信息获得者购买个人信息、不得通过非法手段采集信息等。

4.5.5 个人信息存储

网上银行存储个人信息时，应满足如下要求：

——应采取必要的手段和措施，在物理上保护个人信息存储的场所和存储介质不被非法访问及人为破坏，也应在物理上控制各种可能引起数据丢失的环境因素，包括但不限于温度、湿度、电磁等因素；

——对个人信息的储存介质，应有完善的访问控制机制，在操作系统、网络、应用以及数据库层面均应采取适当的访问控制；

——应采取有效技术措施使个人信息存储时的机密性、完整性和可用性控制与全行风险偏好一致；

——个人信息存储应按照个人信息敏感等级，采取不同的加密方式：

- 对于高敏感级别个人信息，应使用不可逆密码算法加密存储，使用密码算法时方应加入盐值保证算法结果安全；
- 对于中敏感级别个人信息应采用加密存储；
- 对于低敏感级别，以及非敏感的个人信息应进行加密存储。

4.5.6 个人信息传输

进行个人信息传输时，应满足如下要求：

——对访问个人敏感信息的通道应进行限制和区分，配置严格的访问控制规则，明确个人信息传输的控制策略；

——对个人敏感信息的网络传输应符合国家与行业相关标准要求，以确保个人敏感信息传输的机密性、完整性和真实性；

——应采用时间戳、挑战与应答等保护机制防止第三方通过重放攻击获取个人敏感信息；

——对于包含高敏感级别个人信息，应在传输过程中采取应用层加密措施，以保证数据的机密性。

4.5.7 个人信息使用

网上银行使用个人信息时，应满足如下要求：

——应根据“业务需要”和“最小授权”原则，严格控制访问、展示及使用个人信息；

——个人信息访问及使用应进行权限控制；

——个人信息使用者应只能访问其开展业务所必需的个人信息，以防止未经授权擅自对个人信息进行查看、篡改或破坏；

——应严格限制对存储高敏感、中敏感等级个人信息介质的访问，包括电子介质和非电子介质；

——应对高敏感、中敏感等级信息的可疑操作进行定期审计；应以实时监控的方式对高敏感、中敏感等级信息的可疑操作进行实时控制；

——个人信息的展示规则，应包括个人信息以任何形式出现时的展示要求，例如网页页面、日志、文件记录、图像等；

——个人信息展示应遵循最小化原则、授权原则、不被批量获取原则进行保护，对用户密码、卡片验证码等高敏感级别个人信息不允许在任何场景明文展示，用户登录时，可展示用户中敏感、低敏感级别个人信息，具体如下：

- 银行卡号、身份证号码等个人信息应进行脱敏后展示，经过二次认证后可明文展示；
- 用户银行卡号应按照至多前 6 位后 4 位原则进行展示，宜按照仅显示后 4 位原则或者脱敏后展示；
- 用户身份证号应按照至多前 5 位后 3 位原则进行展示，宜按照前 1 位后 1 位原则或者脱敏后展示。

——用户未登录时，不应展示任何个人敏感信息，用户有权对其个人信息进行授权展示；

——应严格在授权范围内使用个人信息，在开发、测试等非业务环境使用时应进行脱敏处理后使用，

或在与真实生产环境同等安全防护级别下进行使用；

——对于涉及高敏感、中敏感等级信息的通讯行为、过程（例如关键交易）及使用行为应进行记录，记录内容应包括但不限于时间、源地址、用户、行为类型、对象、行为结果（是否成功）等，记录应妥善保管，以防止使用者未经授权擅自对记录进行删除、修改。

4.5.8 个人信息转移

向其他组织机构或个人转移个人信息时，应注意保护个人信息，并应满足如下要求：

——未经个人信息主体的明示同意或法律法规明确规定或未经主管部门同意，不得将个人信息转移给境外的个人信息获得者，包括位于境外的个人、境外注册的组织或机构或将主机托管在境外的组织机构；

——在转移过程前，应确保个人信息接收方能够按照本指导性技术文件的要求接收、处理、存储、使用个人信息，并明确该组织和机构的个人信息保护责任；

——在转移过程前，应向个人信息主体说明转移的目的、转移的对象、转移的具体信息；

——在转移过程中，不应违背所告知的转移目的，或超出告知的转移范围；

——在转移过程中，应保证个人信息不被个人信息获得者之外的任何第三方所获得或篡改；

——应明确转移过程中及转移完成后发生个人信息泄露事件时，转移方与接收方的责任归属；

——不得非法出售或者非法向他人提供个人信息。

4.5.9 个人信息销毁

进行个人信息销毁时，应满足如下要求：

——采集、使用、存储个人信息的机构注销时，应按主管部门相关规定对个人信息进行处理；个人信息如有需要配合司法机关协助调查的，其生命周期应按相关法律规定执行；

——存储有个人敏感信息的存储介质在被移出机构时，应对个人敏感信息进行销毁，应确保介质所用存储容器的安全性，防止存储介质被销毁前，个人敏感信息被任何人获取，具体应满足如下要求：

- 对存储高敏感级别个人信息的介质销毁时，应采用不可恢复的技术手段，例如物理粉碎、焚毁；
- 对存储中敏感级别个人信息的介质销毁时，应采用难恢复的技术手段，例如消磁、多次擦写；
- 对存储低敏感级别个人信息的介质销毁时，应采用难恢复的技术手段；
- 对存储非敏感级别个人信息的介质销毁时，可采用可恢复的技术手段。

——应做好相应的销毁操作记录，记录内容应包括但不限于销毁时间、销毁原因、销毁方式、介质类型、介质名称、执行人、监督人等。

4.6 服务连续在线可信性

网上银行系统建设应遵从JR/T 0044-2008、JR/T 0071-2012等规范，并应满足如下要求：

——网上银行系统服务应保持 7×24 小时不间断服务；

——网上银行系统运维应配备 7×24 小时运维应急人员，系统应配备 A/B/C 角色管理员，配置值班人员，确保系统服务连续性；

——网上银行系统应提供 7×24 小时的运维保障（电力保障，网络保障，物理安全等），确保系统可用率应达到 99.96%；

——网上银行系统应做好数据实时备份，确保在系统发生故障时，能够及时恢复且数据丢失时间（RPO）应小于 10 分钟；

——网上银行系统发生故障时，系统恢复时间（RTO）应小于 2 小时；
——网上银行系统可用性监控覆盖率应达到 100%，对应用服务进程、系统资源（CPU、内存、磁盘）、网络状态等实时监控。

4.7 增强身份认证要求

4.7.1 认证机制要求

网上银行身份认证机制应符合JR/T 0068-2012，并应满足如下要求：
——应针对不同场景和客户组合匹配不同的认证手段，并支持多因素认证，例如：针对交易场景和客户交易金额要求，逐渐提升安全校验机制的级别，确保客户资金安全。交易金额 5 万以内（包含），验证方式为短信验证码和取款密码；交易金额 50 万元以内（包含），验证方式为基于数字证书技术的 FIDO 认证；验证方式选用 USBKey 和取款密码验证方式，可实现在银行可控范围内的金额交易；
——应对操作环境 IP/LBS/经纬度进行识别，例如，申请开户时，通过网络环境、GPS 信息、基站信息等综合手段对开户位置进行识别，防范位置异常风险；
——应对客户使用的操作环境进行记录，对访问 IP、设备 ID 进行登记检查，应对更换设备进行短信验证码等方式验证，短时间内访问 IP 变动较大的，需再次进行身份认证；
——应对设备标识进行识别，通过设置指纹技术，采集设备信息，为每台设备分配唯一识别 ID；
——应设置访问会话时效，对会话超时无操作的应重建访问会话；
——应设置单点登录机制，对同一账户同一时间使用不同设备登录的客户进行提醒，原访问会话失效；
——应对操作设备同机多账户进行判断；
——应对频繁开销户行为进行监控；
——对客户网上银行登录密码错误次数达到规定上限的应采取相应的控制措施；
——应对用户使用同一身份或同一终端设备在短时间内开立多家银行的Ⅱ、Ⅲ类银行账户行为进行监控；
——应对集中特征风险进行监控，例如绑定账户开户行集中在少数几家银行、用户集中在同一或相似年龄段、用户集中在相近的网络地址或地理位置、用户身份证号码集中在少数几个地区、用户手机号码集中在少数几个地区、用户手机号码呈现连号或集中在同一号段等；
——客户签约网上银行所使用的手机号，应为客户签约账户（或银行卡）的预留手机号。

4.7.2 认证技术要求

网上银行系统应提供客户身份认证技术解决方案，包括USBKey、数字证书（云证通）、短信验证码等，具体要求如下：
——USBKey
- 应使用指定的第三方中立测试机构安全检测通过的 USBKey；
- 应通过可靠的第二通信渠道要求客户确认交易信息；
- USBKey 应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 USBKey 内进行；
- 参与密钥、PIN 码运算的随机数应在 USBKey 内生成；
- 密钥文件在启用期应封闭；
- 签名交易完成后，状态机成应立即复位；

- 应采取有效的措施防范 USBKey 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；
- 应设计安全机制保证 USBKey 驱动的安全，防范被篡改或替换；
- 对 USBKey 固件进行的任何改动，都应经过归档和审计，以保证 USBKey 中不含隐藏的非法功能和后门指令；
- PIN 码连续输错次数达到错误次数上限（不超过 6 次），USBKey 应锁定；
- USBKey 使用的密码算法应经过国家主管部门认定；
- USBKey 应具备抵抗旁路攻击的能力，包括但不限于抗 SPA/DPA 攻击能力、抗 SEMA/DEMA 攻击能力；
- USBKey 应能够防远程挟持，应具有屏幕显示或语音提示以及按键确认等功能，应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；
- USBKey 应能够自动识别待签名数据的格式，识别后应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 USBKey 签名的数据一致；
- 应采取加密措施防止签名数据在客户最终确认前被替换；
- 应保证未经按键确认时 USBKey 不得签名和输出，且等待一段时间后，应自动清除数据，并复位状态；
- USBKey 应能够自动识别其是否与客户端连接，应具备在规定的时间与客户端连接而未进行任何操作时的语言提示、屏幕显示提醒等功能；
- USBKey 在连接到终端设备一段时间内无任何操作，应自动关闭，须重新连接才能继续使用，以防范远程挟持。

——数字证书（云证通）

- 系统应强制使用密码保护证书私钥，防止证书私钥受到非授权访问；
- 证书导出时，客户端应对用户进行身份认证，例如验证访问密码等；
- 应保证证书私钥不可导出；
- 证书私钥备份时应提示或强制放在移动设备内。

——短信验证码

- 短信验证码应一次有效，有效时限为 60 秒，超过有效时间应立即作废；
- 应控制单用户一天内验证码获取次数，防止恶意重放攻击；
- 对于资金类交易短信验证码，应采用加密因子加密后，对交易信息进行复合验证；
- 开通手机动态密码时，应使用人工参与控制的可靠手段验证客户身份并登记手机号码，更改手机号码时，应对客户的身份进行有效验证；
- 交易关键信息应与手机动态密码一起发送给客户，并提示客户确认；
- 手机动态密码应随机产生，长度应不少于 6 位；
- 应采取有效措施防范恶意程序窃取、分析、篡改短信动态密码，保证短信动态密码的机密性和完整性，例如结合外部认证介质（如密码卡等）、采用问答方式等。

4.8 风险控制能力

金融科技的快速发展，使银行服务模式和服务场景日趋多样化，带来便捷的同时，也带来更加隐蔽、专业的欺诈风险，网上银行系统应具备如下风险控制能力：

——客户端应用软件安全

- 客户端软件中，应严格禁止在本地明文保存客户身份验证信息，操作结束后应清除缓存；
- 登录时应检查密码复杂度，防止简单密码登入；

- 输入时应采用密码控件对密码进行加密，传输时应采用专线或 https 模式，退出时应清除用户登录信息；
- 对于客户端提交生产环境前应进行加固签名保证其安全性，通过第三方安全评估确保软件自身安全。

——支付安全管理

- 应通过安全机构排查和日志分析，对支付交易中的敏感数据进行脱敏；
- 应采用国密算法对交易中的密码进行加密处理；
- 应定期开展内部审计，项目上线前应向监管机构报备。

——交易风险实时监测

- 网上银行系统应加入我行反欺诈、反洗钱等风险控制系统，对交易进行实时、高效、全面的监测来识别交易风险；
- 事前，应制定完善的风险交易处理预案，对不同风险等级的交易进行差分处理，应设置黑名单、灰名单，对灰名单内客户进行操作权限控制，对黑名单内用户拒绝使用；
- 事中，应根据反欺诈系统返回的查验结果，对交易进行正确处理，对于没有风险的交易不进行干预；应对风险事件依据风险等级进行放行、加强认证、阻断等处理；网上银行系统与行内实时风控系统的交互时间应在 40 毫秒以内，保证时效性，使客户无感；
- 事后，应根据风险事件特征进行查证、分析，按要求进行风险报送或列入灰、黑名单进行处理；
- 对客户使用网上银行系统进行Ⅱ、Ⅲ类户开户的行为，应根据监管要求，通过反欺诈系统设置相关规则，进行严格、细致管控，对可疑的Ⅱ、Ⅲ类户进行相应控制；APP 应接入设备指纹系统，对黑产设备进行精准查杀，增加黑产分子犯罪成本；
- 应保证以上要求的连续性应用并制定完善的应急预案，确保网上银行系统服务时效性、连续性。

5 客户服务

5.1 服务功能

5.1.1 基本描述

网上银行应以行内金融产品为基础，提供账户管理、转账汇款、缴费支付、存款、理财、基金、国际业务、信用卡、贷款、电子汇票等功能，同时应以客户需求为导向，在满足安全性、合规性要求的同时，不断丰富和完善服务功能，持续提升服务能力。

5.1.2 账户服务

网上银行应提供账户信息查询、账户管理等账户服务，具体应满足如下要求：

——账户信息查询：应支持个人或企业结算账户余额查询、交易明细查询等账户信息查询功能；

——账户管理：应支持可操作账户的增加、删除、账户挂失、别名设置、限额管理等功能。

5.1.3 转账汇款

网上银行应提供转账汇款、批量转账、预约转账等转账服务，具体应满足如下要求：

——转账汇款：应支持行内、行外、本人账户互转等转账汇款功能；应支持根据交易到账时间，提供实时、普通、次日三种方式选择；

——批量转账：应支持收款账户为行内账户的批量转账；

——预约转账：应支持行内指定日期、固定周期预约转账。

5.1.4 缴费支付

网上银行应提供生活缴费、无感停车、公积金、消费支付等缴费支付服务，具体应满足如下要求：

——生活缴费：应支持各项生活缴费功能，包括水费、电费、煤气费、通讯费、采暖费、交通违章罚款、学费、物业费等；

——无感停车：应支持绑定车牌、自动支付停车费；

——消费支付：应支持基于银联二维码标准的扫码支付功能。

5.1.5 存款

网上银行应提供定活互转、大额存单、通知存款、智能存款等存款服务，具体应满足如下要求：

——定活互转：应支持整存整取定期存款办理，支持定期存款销户或提前支取；

——大额存单：应支持购买大额存单产品；

——通知存款：应支持一天、七天通知存款办理；

——智能存款：应支持签约财富通系列智能存款产品。

5.1.6 理财

网上银行应提供理财产品购买、理财转让、风险评估等理财服务，具体应满足如下要求：

——理财产品：应支持理财产品查询、购买、撤销等功能；

——理财转让：应支持持有理财产品转让或购买他人转让产品；

——风险评估：应支持非首次风险评估。

5.1.7 基金

网上银行应支持代销基金产品（盛京宝）的查询、存入、提取等功能。

5.1.8 国际业务

网上银行应提供个人结售汇、汇率查询等国际业务服务，具体应满足如下要求：

——结售汇：应支持美元、欧元、港币、英镑、日元、澳元、加元、瑞士法郎、新加坡元等币种个人结售汇办理；

——汇率查询：应支持实时汇率查询。

5.1.9 信用卡

网上银行应提供信用卡申请、激活、还款、借贷、积分管理等服务，具体应满足如下要求：

——信用卡申请/激活：应支持各类信用卡在线申请、查询办卡进度、在线激活等功能；

——信用卡还款：应支持本行/他行信用卡还款；

——卡片管理：应支持信用卡账单查询、临时额度调整、自动还款设置、密码设置等卡片管理功能；

——信用卡借贷：应支持信用卡账单分期、灵活分期、分期查询等借贷功能；

——积分管理：应支持积分查询、权益兑换等积分管理功能。

5.1.10 贷款

网上银行应支持个人消费贷款额度申请、提现、还款等功能。

5.1.11 其他对公业务

网上银行应提供电子汇票、电子对账等其他对公业务，具体应满足如下要求：

——电子汇票：应支持对公账户电子汇票的发出申请、撤销申请、签收应答等功能；

——电子对账：应支持对公账户的账户余额对账、对账结果查询等功能。

5.2 服务性能

5.2.1 易访问性

网上银行服务应满足客户易访问需求，并应满足如下要求：

——应建立完善的服务体系，覆盖 PC 端、APP 等多访问渠道，提高网上银行服务易访问性；

——应提供官方门户网站、手机应用市场等 APP 下载渠道，提供安全控件、网银助手等辅助工具安装途径和指引；

——应提供多样化登录方式，例如手势密码登录、指纹登录等；

——网上银行应在安全可控的前提下，支持客户自助注册成为网上银行客户，在规定权限内使用网上银行功能。

5.2.2 易用性、舒适性和便捷性

网上银行服务应提供舒适性、易用性服务体验，并应满足如下要求：

——应加强渠道协同作用，在网上银行 PC 端、APP 及其他渠道提供一致的客户体验；

——应不断丰富网上银行的产品和服务，逐步实现网上银行的产品和服务覆盖线下业务，不断拓展金融和生活场景应用；

——应在行内统一视觉识别系统规范标准下开展网上银行系统操作界面设计，保持网上银行各渠道操作页面简洁大方、功能布局合理、交互人性化、操作简便化，为客户提供舒适、便捷的网上银行服务；

——应提供充分、清晰的操作指引提示信息，使用客户熟悉的语言，包括但不限于错误提示、交易提示、温馨提示等，避免使用系统术语，所使用的词语应保持前后一致性；

——功能交易设计应合理有效，流程及界面设计应便于操作，缩减不必要的交易流程步骤，充分考虑客户使用习惯，增强客户服务体验；

——应建立客户反馈意见响应机制，结合客户使用意见，不断优化网上银行服务；

——应提供常用交易自定义、界面主题自定义等个性化设置服务。

5.2.3 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）应在0.5%以下。

5.3 客户代表行为规范

5.3.1 基本规范

客户服务代表行为规范应遵照GB/T 32315-2015，并满足《盛京银行客户服务中心服务规范》、《盛京银行客户服务中心岗位职责手册》等制度中明确的员工工作职责、服务规范、业务流程、信息安全、风险管理、投诉管理等方面管理要求。

5.3.2 工作职责

客户服务代表应满足以下工作职责要求：

——应做好呼入、呼出业务处理工作，包括客户咨询、查询、疑难、投诉、表扬、建议等，并做好相关记录；

——应对客户的业务申请进行在线操作；
——对于无法处理的客户诉求，应发送工单至相关部门，后续跟进处理情况并回复客户；
——应根据反洗钱工作要求，负责在客户服务过程中进行客户身份的识别与确认。

5.3.3 用语规范

客户服务代表用语应符合行业规范要求，给客户带来舒适、被尊重的服务感受，不断提升服务理念，提高服务水平，并应满足如下要求：
——客户服务代表应使用标准的开场白和结束语；
——客户服务代表应语速适中，匹配客户，和蔼、有微笑感，吐字清晰、流畅自然；
——客户服务代表应在客户等待或客户等待后对客户表示歉意；
——客户服务代表应恰当的使用“请、您、谢谢、对不起、请稍等”等礼貌用语；
——客户服务代表不得使用服务禁语；
——严禁与客户争吵、顶撞、辱骂客户、主动或借故挂断客户电话等。

5.3.4 服务意识

客户服务代表在为客户服务过程中，应以客户为中心提供主动、热情、周到的服务，从专业角度提示客户相关注意事项，尽力提供超越客户期望的服务，并应满足如下要求：
——接通电话时客户服务代表应主动倾听，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；
——接通电话时客户服务代表应主动服务，思路清晰，恰当引导客户，有效控制对话节奏，在客户对某些问题比较混淆时，能使用恰当语言总结性阐述客户问题，尽快切入正题，并能注意适当控制通话时长；
——接通电话时客户服务代表应服务意识强，责任心强，积极主动为客户解答问题，主动提供额外相关信息或额外帮助。

5.3.5 能力要求

客户服务代表应不断加强业务知识学习与系统操作熟练程度，保证问题回答的准确性，为客户提供安全快捷的解决方案，并应满足如下要求：
——客户服务代表应准确快速判断客户问题原因，了解客户实际需求；
——客户服务代表应熟练准确、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；
——客户服务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（形成工单）并在必要时跟进。

5.3.6 行为要求

客户服务代表应注重客户信息安全、保护客户隐私，遵守保密规定，确保重要信息不得外泄，并应满足如下要求：
——应确保未经允许不可擅自带非部门内同事及外来人员进入办公区；
——打印、复印资料完毕后应即打即取；
——严禁在公众场合、平台、互联网未经授权发布客户信息等保密信息。

5.4 客户服务响应

5.4.1 响应时间要求

网上银行系统客户服务响应时间和服务效率应满足如下要求：

——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）应小于 15 秒；

——线上客服响应时间应小于 10 秒；

——人工客服应保持 7×24 小时不间断服务；

——电话客服接通率应高于 95%。

5.4.2 投诉处理要求

对于客户投诉事件，应及时响应、积极处理、跟进结果，并应满足如下要求：

——客户服务中心接受客户投诉时，应完整记录客户的姓名、联系方式、投诉时间、事件、诉求等要素，同时保留投诉电话录音及后续处理的相关电话录音；

——客户服务中心传递及处理投诉时应做到：

- 客户投诉由客户服务中心负责处理解决时，应负责组织对相应投诉的调查、处理工作，并在处理时限内回复客户，告知处理结果；
- 客户投诉由各单位分支机构或总行相关业务部门负责解决时，客户服务中心应以工单、电子邮件、传真、电话等方式将客户投诉及时传递到相关部门，确保对方及时收到客户投诉。

——客户服务中心应与相关业务部门保持顺畅的信息沟通，建立投诉预警预防机制，对可见的客户投诉应提前制定话术及应对方案；

——应制定客服投诉分级标准，明确不同级别投诉的受理时限，受理标准及客户满意度要求等；

——客户服务中心应定期对受理的客户投诉进行总结分析，改善服务品质，提升客户满意度。

6 创新及前瞻性

6.1 服务创新性

6.1.1 服务创新原则

网上银行服务创新工作是为适应经营发展的要求，通过引入新技术、采用新方法、开辟新市场等方式，不断提高网上银行服务能力和服务体验，并应满足如下要求：

——客户导向原则，网上银行服务创新应坚持以客户为中心、市场为导向，把不断变化的市场情况和个性化的客户需求作为开展服务创新工作的依据和方向；

——风险可控原则，网上银行服务创新应突出风险管理，加强在各项环节的风险分析和防控，强化流程管理、评估管理等工作，确保服务创新风险得到有效控制；

——依法合规原则，网上银行创新应遵守法律、法规和规章的规定，符合全行总体发展战略，不得以服务创新为名，违反规章制度或变相逃避监管；

——保护消费者原则，网上银行创新应遵守职业道德标准和专业操守，完整履行尽职义务，将保护消费者权益工作融入至产品开发准入、产品营销推介、信息披露和信息安全保护的全流程中。

6.1.2 创新要求

网上银行服务创新工作应遵照《盛京银行股份有限公司创新工作管理办法》，并应满足如下要求：

——相关部门应根据实际情况设立创新工作小组，定期或不定期开展网上银行服务创新工作；

——工作流程应至少包括需求发起、论证立项、设计开发、测试评估、审批投产、培训推广、运行评价、后续优化等阶段；

——应制定与服务创新相适应的操作规程、内部管理制度和客户风险提示，制定本业务条线的产品业务管理办法、操作流程和相关合同、协议文本等。

6.2 技术前瞻性

6.2.1 大数据

网上银行服务应与大数据技术相结合，在客户服务、产品营销、风险管理等方面提供辅助支持，应用大数据技术应满足如下要求：

——网上银行服务应充分利用大数据平台的数据挖掘成果，结合大数据平台提供的客户标签、客户画像等，为客户提供差异化服务和精准营销，提升客户体验；

——网上银行服务应选择适当场景应用大数据实时流数据处理技术，基于规则引擎、机器学习等搭建实时风控模型，当客户在网上银行进行高风险交易情境下实时预警，保障客户交易安全；在客户进行网贷申请时提供在线信用评分和额度审批等；

——在客户数据的采集和使用过程中应严格遵守法律法规，避免过度采集、滥用数据，保护客户隐私。

6.2.2 生物特征识别

生物特征识别作为新兴起的身份验证方式有着高效、便捷、不易被盗用的优势，可按照各渠道的风险大小不同来设定阈值，然后根据比对结果和事先在平台设定的阈值来进行比对，将比对的结果和分值反馈到各应用系统中。人脸识别，是基于人的脸部特征信息进行身份识别的一种生物特征识别技术，应用人脸识别技术应遵照GB/T 35678-2017，并应满足如下要求：

——人脸识别应使用摄像机或摄像头采集含有人脸的图像或视频流，并自动在图像中检测和跟踪人脸，进而对检测到的人脸进行脸部识别；

——人脸识别系统应包括四个组成部分，分别为人脸图像采集及检测、人脸图像预处理、人脸图像特征提取以及匹配与识别；

——人脸图像采集应包括静态图像、动态图像、不同的位置人脸图像、不同表情人脸图像等，当用户在采集设备的拍摄范围内时，采集设备应自动搜索并拍摄用户的人脸图像；

——人脸检测应在图像中准确标定出人脸的位置和大小，并应检测出人脸图像中的直方图特征、颜色特征、模板特征、结构特征及 Haar 特征等模式特征，作为人脸识别的预处理过程；

——人脸图像格式应为 MBP、JPEG、JPEG2000、PNG 或 BASE64 中的人一种，若图像为灰度图时，图像灰度级应为 256 级；

——人脸图像表情应中性或微笑，眼睛自然睁开，嘴唇自然闭合；

——眼镜框应不遮挡眼镜，镜片应无色无反光；

——遮挡物应不遮挡眉毛、眼镜、嘴巴、鼻子及脸部轮廓；

——两眼间距应大于 60 像素，宜大于等于 90 像素；

——姿态应面向采集设备，人脸水平转动角应在±10° 以内，倾斜角应在±10° 以内；

——亮度和对比度要适中，脸部无阴影、无过度曝光和无欠曝光；

——脸部区域应保持完整，轮廓和五官清晰，无浓妆，图像脸部区域应编辑修改性处理，几何失真应小于等于 5%,运动模糊应小于等于 0.15，高斯模糊应小于等于 0.24。

6.2.3 云计算

云计算是一种计算机资源的新型利用模式，基于云计算的IaaS、PaaS、SaaS技术架构可用于网上银行系统的应用开发和运维，云计算架构具备可弹性伸缩，高可用，高可靠等特性，对应用系统的可用性、性能和容灾等方面提供支持，具体应满足以下要求：

——云计算应具备以下特征：

- 按需自助服务，在不需或较少云服务商的人员参与下，能够根据需要获得所需计算资源，例如自主确定资源的占用时间和数量等；
- 资源池化，云服务商将资源提供给多个客户使用，根据客户的需求进行动态分配或重新分配资源；
- 快速伸缩性，能够在任何时候根据需要快速、灵活、方便的获取和释放计算资源。

——基于云计算的 IaaS、PaaS、SaaS 技术架构应满足以下要求：

- IaaS 层（基础设施即服务）应对计算资源、网络资源和存储资源进行资源管理、虚拟化和运行监控，并提供 API 接口供 PaaS 层使用，应对虚拟机全生命周期进行管理，应支持对虚拟机的创建、删除、回收、暂停、恢复、关闭、重启等操作，应支持存储容量与性能的弹性扩展；
- PaaS 层（平台即服务）应提供负载均衡、微服务中间件、分布式数据库、消息队列、发布部署、运维监控等能力，PaaS 各组件能力应具有微服务中间件的注册和发现能力，应用无需关心服务位置，应满足消息队列的可靠传输要求，不丢失消息，具备延迟队列功能；
- SaaS 层（软件即服务）应具有较低的学习曲线和低廉的初始费用；应满足所有的升级和更新无需自行下载或安装补丁；应实现无限期扩展，以满足业务不断增长需求。

6.2.4 高可用架构

为满足业务发展需要，网上银行系统应满足如下要求：

——应部署在云计算平台，应在高可用设计上采用多层次结构设计，数据库采用集群部署，保证数据库的高可用，异地数据采用实时异步复制；

——应实现异地应用级灾备，确保在系统发生故障时，异地数据中心可以快速接管业务；

——网上银行系统应用实现负载均衡模式，应用设计为无状态的容器，保证应用单个应用服务出现问题时，系统自动重启一个新的容器，达到不需要人工干预，自动判断故障和恢复业务，不影响整体系统。

7 实施保障

7.1 组织保障

7.1.1 基本原则

网上银行业务实行统一管理、分级运营原则，由总行、分行、支行根据级别和分工不同进行规范管理，严格履行工作职责，强化业务管理，积极开展业务经营活动。

总行零售银行部和公司银行部是网上银行业务的主管部门，应负责网上银行业务的统筹规划管理；信息科技部应负责技术开发和运行保障；运营管理部、计划会计管理部、合规部、风险管理部等部门应负责协助解决涉及到本部门专业相关的问题。各分行、支行应根据总行指导，在职责范围内有序推进网上银行业务经营发展。

7.1.2 总行零售银行部和公司银行部职责

总行零售银行部和公司银行部主管网上银行业务，并应承担以下职责：

——负责收集市场动态信息，进行市场调研分析；

——负责制定网上银行业务发展规划及各项管理制度；

——负责网上银行新渠道、新产品、新业务研发，对项目和业务需求进行业务可行性论证，负责需求设计、产品设计、业务测试、业务参数设定、费用标准设定，并配合验收及上线工作；

——负责制定和修改全行统一制式性合同文本和业务文档；
——负责对各分行拟申请开办的网上银行业务及各类业务需求的审批；
——负责网上银行业务的市场推广和营销规划工作；
——负责对分支行网上银行业务的督导检查；
——负责组织网上银行产品的对外统一营销宣传活动组织和对内业务培训；
——负责网上银行业务风险的评估、管理与应急演练等；
——负责网上银行业务运行指标考核；
——负责日常业务管理及监控工作，定期上报网上银行业务相关数据；
——负责管理网上银行系统的业务参数，包括系统操作员、系统机构参数、跨行转账落地限额、权限管理等；
——负责受理、搜集及处理网上银行业务相关的客户咨询、建议及投诉等；
——负责网上银行业务相关凭证管理；
——负责网上银行业务的监管报批、报备工作。

7.1.3 总行信息科技部职责

总行信息科部应负责网上银行系统的技术开发和运行保障工作，并应承担以下职责：
——负责网上银行系统的开发、上线工作；
——负责网上银行系统相关软件和硬件的配置、更新；
——负责网上银行系统的安全保障、日常运行和系统维护；
——负责对网上银行系统出现的技术性问题进行处理；
——负责网上银行系统相关数据的备份和归档工作；
——负责定期组织对网上银行系统的技术安全评估，配合做好风险评估工作，根据评估结果组织技术优化和技术整改。

7.1.4 总行运营管理部职责

总行运营管理部应在根据本部门专业职能配合网上银行业务管理，并应承担以下职责：
——负责协助网上银行业务规则制定；
——负责协助网上银行业务差错调整、对账等账务处理工作。

7.1.5 总行计划会计管理部职责

总行计划会计管理部应在根据本部门专业职能配合网上银行业务管理，并应承担以下职责：
——负责网上银行业务会计核算规则制定；
——负责网上银行收费标准审核公示。

7.1.6 总行合规部职责

总行合规部应在根据本部门专业职能配合网上银行业务管理，并应承担以下职责：
——负责根据反洗钱管理要求，依法合规履行网上银行反洗钱管理职责；
——负责对网上银行相关规章制度及服务协议、合同等文件进行合规性审查。

7.1.7 总行风险管理部职责

总行风险管理部应在根据本部门专业职能配合网上银行业务管理，并应承担以下职责：
——负责制定应急政策和管理要求；
——负责组织开展业务连续性演练。

7.1.8 分行职责

分行应在总行授权范围内开展辖内网上银行管理工作，并应做好以下工作：
——负责贯彻落实总行制定的各项规章制度；
——负责辖内机构开办网上银行业务的审批及汇总各类业务需求的申报；
——负责对辖内机构网上银行业务的督导检查；
——负责辖内网上银行产品的营销宣传和业务培训；
——负责辖内客户网上银行业务相关服务；
——负责辖内客户网上银行交易的落地处理、差错处理、交易监控；
——负责辖内网上银行业务风险的防范与控制等；
——负责辖内网上银行业务运行指标考核。

7.1.9 支行职责

支行应在总、分行指导下，严格落实各项规章制度，并应做好以下工作：
——负责引导客户正确使用网上银行产品，并做好业务宣传和业务咨询等解释工作；
——负责根据操作规程具体办理网上银行业务；
——负责机构内网上银行业务风险的防范与控制；
——完成网上银行业务各项运行指标。

7.2 管理制度

7.2.1 产品研发

网上银行产品研发应遵照《盛京银行信息科技管理体系管理总纲》、《盛京银行信息科技文件与记录管理办法》、《盛京银行信息科技内部审核与管理评审管理办法》、《盛京银行信息安全风险检查管理办法》、《盛京银行信息科技持续改进管理办法》、《盛京银行信息科技服务报告管理办法》、《盛京银行信息科技资产与配置管理办法》、《盛京银行信息科技变更发布管理办法》、《盛京银行信息科技数据安全管理实施细则》、《盛京银行信息科技外包管理办法》、《盛京银行信息科技预算与核算管理办法》、《盛京银行信息科技项目管理办法》、《盛京银行信息科技应用软件建设类项目实施细则》、《盛京银行信息科技软件开发质量管理实施细则》、《盛京银行信息科技系统与网络安全管理办法》、《盛京银行信息科技运维管理办法》、《盛京银行信息科技风险评估与处置管理办法》、《盛京银行信息科技风险管理办法》等制度规定，并应满足如下要求：

——需求管理

- 各业务部门应按照系统建设的总体性原则要求，依据条线归口管理原则，明确主要需求部门作为业务属主，统筹本条线需求管理；
- 需求部门应根据业务规划，集中编制本条线次年业务需求，包括业务需求目标、主要业务流程、业务功能等内容，并由科技部门配合完成费用概算评估后汇总形成年度需求；
- 纳入年度需求的建设项目，在正式启动前，需求部门应在充分调研的基础上，结合同业实践和本行实际，进一步完善，形成业务需求书，业务需求书至少应包括业务规则、详细业务流程、详细业务功能、用户界面设计等，达到立项条件但未列入年度需求的，应由需求部门评估业务必要性和可行性，信息科技部配合完成技术可行性和费用概算评估，制定技术解决方案，形成业务需求书。

——立项管理

- 立项管理应对拟新建系统的必要性、可行性以及系统建设预算的评估和审批；

- 应根据建设项目费用概算确定是否进行立项审批，由信息科技管理委员会负责立项必要性、可行性审批，财务部门负责项目预算审批，信息系统建设须按照文件要求逐一获得建设立项审批通过后方可进入开发建设程序。

——开发实施

- 应由信息科技部牵头且遵循项目经理负责制，按照《研发管理体系规范》和立项方案开展项目策划工作，制定项目实施计划并经过正式审批，明确项目组织架构、项目章程、项目主计划等，根据业务需求书和技术方案制定项目交付目标和验收标准；
- 项目启动后，项目组应根据业务需求书，从业务流程、应用场景、功能指标、性能指标等方面进一步分析形成软件需求规将说明书，并组织评审；
- 应根据软件需求规格说明书，进行系统设计，并组织设计评审，经相关人员签字后生效；
- 应根据设计完成编码开发工作，组织单元测试、代码走查等关键工作。

——测试投产

- 应根据行内测试管理体系要求，严格遵循准入准出规范，实施独立、客观的测试活动，每个测试阶段应引入业务、开发进行三方评审，对测试产出物进行确认，保障测的准确、有效；
- 应配置多种功能、性能、自动化、安全等专业测试工具，为测试活动提供可靠支撑；
- 应根据《盛京银行信息科技运维管理办法》要求，组织上线方案评审，系统上线方案应按照上线组织架构、业务准备、技术准备、系统应急、业务应急等内容编制，并制定详细计划；
- 项目投产时，需求部门应完成编写业务制度、操作规程、业务连续性计划及业务应急方案、业务推广计划等，信息科技部应完成生产环境准备和部署，制定《系统上线方案》以及监管报备等工作，重要信息系统投产前二十个工作日，应完成风险评估和安全评估工作；
- 应根据实际情况，选择一次性上线或分批次上线，并按需增加试运行阶段；
- 系统成功投产后，应根据系统规模大小及运行周期由项目组发起阶段验收或终验申请，由信息科技部会同需求部门组成验收小组，依据项目工作范围、目标、交付物、测试报告等内容逐一对比检查、进行验收，验收结论应分为验收合格、验收不合格，对于验收不合格的，项目组应针对不合格项组织整改直至合格后，重新发起验收申请；
- 应结合系统建设立项方案的各项指标，对系统建设完成后形成的实际指标进行客观的分析和评价，主要应包括项目目标、项目效益、项目影响等，应根据后评价结果及时对系统功能进行调整和优化。

7.2.2 业务管理

网上银行业务管理应遵守《盛京银行电子银行业务管理办法》、《盛京银行网上银行业务实施细则》、《盛京银行手机银行业务管理办法》、《盛京银行网上银行业务操作风险点指引》、《盛京银行网上银行限额管理操作规程》等，并应满足如下要求：

——开办网上银行业务应实行逐级审批制，支行开办网上银行业务应向分行提出申请，分行开办网上银行业务应向总行网上银行业务主管部门提出申请；

——为客户开通网上银行服务，应审核客户身份信息，确保本人办理，确认客户已知悉服务内容，并与客户签订相应的服务协议；

——凡办理个人金融业务的营业网点均应受理个人网上银行业务，凡办理公司金融业务的营业网点均应受理企业网上银行业务；

——网上银行操作人员应按角色、权限、岗位分为系统管理员、总行管理员、总行人事管理员、总行操作员、分行人事管理员、分行管理员、支行授权员、支行复核员、支行操作员、客服操作

员等，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，严禁共用柜员号操作业务；

——网上银行业务管理应实行自律监管与检查，应坚持“全面检查和专项检查相结合，定期检查与不定期检查相结合，自我检查与交叉检查相结合”的原则。

7.2.3 应急响应

网上银行业务应遵守《盛京银行电子银行业务突发事件应急预案》、《盛京银行电子银行业务风险应急处理办法》、《盛京银行电子银行业务连续性管理办法》等，保证业务连续性，并应满足如下要求：

——应制定信息系统突发事件预防措施、预警标准和应急策略，组织做好信息系统营运监测和维护，实施信息系统突发事件应急处置，评估总结信息系统突发事件及应急处置过程中暴露的问题并整改；

——应根据恢复时间目标（RTO）和恢复点目标（RPO），结合风险控制策略，从基础设施、网络、信息系统等不同方面，分类制定应急预案；

——应建立重要外包服务的专项应急预案，对于重要基础设施、重要设备、网络、系统集成以及其他外包服务商的技术与产品政策、服务水平、服务能力制定风险应对措施，外包服务的应急预案应能够保障银行业信息系统恢复时间目标（RTO）和恢复点目标（RPO）的要求；

——应定期对应急预案进行测试和演练，确保其有效性；

——应根据演练总结报告提出的改进措施进行整改，及时修订相应的应急预案，并组织相关部门对整改情况进行监督和检查。

7.3 企业标准宣传及实施机制

7.3.1 宣传

本标准应在全行范围开展广泛宣传，由网上银行相关部门组织发起、各分支行配合开展，并应满足如下要求：

——对于已发布的企业标准，应公示至企业标准信息公共服务平台；

——应在网上银行相关系统公告及广告版位、各营业网点海报机等投放企业标准宣传材料，包括但不限于软文、图片等，宣传企业标准工作；

——应定期对企业标准进行宣传，每半年至少一次。

7.3.2 培训

本标准培训工作应纳入全行统一培训体系范围，并应满足如下要求：

——应根据全行年度培训计划，由总行部门组织全行员工开展培训，制定培训及测验方案；

——培训方案中应包含但不限于培训主要内容、培训方式、测验方式等，对于培训后未通过测验的应开展再次培训；

——培训方式应包括但不限于现场培训、视频培训等；

——应每年至少开展一次培训。

7.3.3 实施

网上银行服务管理应严格遵照本标准执行，并应满足如下要求：

——应通过行内正式公文、行内门户网站公示等方式在全行范围普及本标准，并要求全行人员严格遵照标准实施；

——应建立实施监督机制，由总行相关部门根据职责要求确保标准实施成果，总行每年应组织至少

一次检查监督本标准执行情况，如发现未达标准的业务环节，应制定整改计划并跟进整改效果；

——应根据实际情况对本标准及时修订，并对新版本进行相应宣传和培训。