ICS 03.060
CCS A 11

Q/HRCB

江苏海安农村商业银行股份有限公司企业标准

Q/HRCB 001—2023
代替 Q/HRCB 003—2022

网上银行信息系统安全通用规范

general specification of information security for internet banking system

2023－04－04 发布　　2023－04－04 实施

江苏海安农村商业银行股份有限公司
发 布

目　　次

前　　言 I
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 符号和缩略语 2
5 网上银行系统概述 3
5.1 系统标识 3
5.2 系统定义 3
5.3 系统描述 3
5.4 安全性描述 4
6 安全规范 4
6.1 安全技术规范 4
6.2 安全管理规范 17
6.3 业务运作安全规范 28

前　言

本文件旨在有效增强我行网上银行系统安全防范能力，促进网上银行规范、健康发展。

本文件根据GB/T 1.1-2020给出的规则起草。

本文件由江苏海安农村商业银行股份有限公司提出并归口。

本文件起草单位： 江苏海安农村商业银行股份有限公司。

本文件主要起草人：吴智星、朱骞、刘飞。

本文件的历次发布情况为：

——2021年首次发布。

——2022年第一次修订。

——本次为第二次修订。

网上银行系统信息安全通用规范

1 范围

本文件包含了网上银行系统的描述、安全技术规范、安全管理规范、业务运作安全规范。

本文件适用于网上银行系统建设、运营及测评。

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 25069 信息安全技术 术语

3 术语和定义

GB/T 25069确立的以及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网上金融业务的服务。

3.2

互联网 Internet

因特网或其他类似形式的通用性公共计算机通信网络。

3.3

敏感信息 sensitive information

主要指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。

3.4

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，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。

3.5

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。

3.6

USB Key固件 USB Key firmware

影响USB Key安全的内置在USB Key内的程序代码。

3.7

移动终端 mobile terminal

本文件中特指区别于传统PC机方式，以手机、平板电脑等通过通信网络访问网上银行的移动设备。

3.8

强效加密 strong encryption

一个通用术语，表示极难被破译的加密算法。加密的强壮性取决于所使用的加密密钥。密钥的有效长度应不低于可比较的强度建议所要求的最低密钥长度。

3.9

资金类交易 funds transaction

指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。

3.10

信息及业务变更类交易 information & 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，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。

3.11

企业网银 corporate banking

指商业银行等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。

4 符号和缩略语

以下缩略语和符号表示适用于本文件：

CA　　数字证书签发和管理机构（Certification Authority）

Cookies　　为辨别客户身份而储存在客户本地终端上的数据

COS　　卡片操作系统（Card Operating System）

C/S　　客户机/服务器 (Client/Server)

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）

IPSEC　　IP安全协议（Internet Protocol Security）

OTP　　一次性密码 （One Time Password）

PKI　　公钥基础设施（Public Key Infrastructure）

SSL 安全套接字层（Secure Socket Layer）
SPA/DPA 简单能量分析/差分能量分析 (Simple Power Analysis/ Differential Power Analysis)
SEMA/DEMA 简单电磁分析/差分电磁分析 （Simple Electromagnetism Analysis/ Differential Electromagnetism Analysis）
TLS 传输层安全（Transport Layer Security）
WTLS 无线传输层安全（Wireless Transport Layer Security）
VPN 虚拟专用网络（Virtual Private Network）
IMEI 国际移动设备身份码（International Mobile Equipment Identity）
IMSI 国际移动用户识别码（International Mobile Subscriber Indentification Number）

5 网上银行系统概述

5.1 系统标识

在系统标识中应标明以下内容：
－名称：XX 银行网上银行系统
－所属银行

5.2 系统定义

网上银行系统是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各种金融服务的信息系统。网上银行系统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，是商业银行等金融机构在网络经济的环境下，开拓新业务、方便客户操作、改善服务质量、推动生产关系变革等的重要举措，提高了商业银行等金融机构的社会效益和经济效益。

5.3 系统描述

网上银行系统主要由客户端、通信网络和服务器端组成。本文件所指网上银行系统，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。网上银行系统包括个人网银和企业网银。本文件条款中如无特别指明“企业网银”，则同时适用于个人网银和企业网银。

5.3.1 客户端（含专用安全设备）

网上银行系统客户端主要包括客户端交易终端和客户端程序。客户端交易终端不具备或不完全具备专用金融交易设备的可信通讯能力、可信输出能力、可信输入能力、可信存储能力和可信计算能力，因此，需要专用安全设备，并通过接受、减轻、规避及转移的策略来应对交易风险。目前，客户端交易终端主要包括PC客户端和手机、平板电脑等移动终端客户端，将来可能包括其他形式的终端产品。专用安全设备用于保护数字证书、动态口令和静态密码等，应按照其在交易中具备的可信通讯能力、可信输出能力、可信输入能力、可信存储能力和可信计算能力五种能力的组合对其进行分类分析，并制订与之适应的交易安全风险防范策略。客户端程序是指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。

5.3.2 通信网络

网上银行借助互联网、移动通信网络等技术向客户提供金融服务，其最大特点是开放性，开放性带来的优点是交易成本的降低和交易便利性的提高，缺点是交易易受到安全威胁及通讯稳定性降低。因此，网上银行业务设计应充分利用开放网络低成本和便利的特点，有效应对开放网络通讯安全威胁，同时采取手段提高交易稳定性和成功率。

5.3.3 服务器端

网上银行系统服务器端用于提供网上银行应用服务和核心业务处理，应充分利用各种先进的物理安全技术、网络安全技术、主机安全技术、访问控制技术、密码技术、安全审计技术、系统漏洞检测技术和黑客防范技术，在攻击者和受保护的资源间建立多道严密的安全防线。

5.4 安全性描述

网上银行系统是一个涉及相关业务流程、不同的应用系统、客户对象、数据敏感程度等的复杂信息系统。网上银行系统信息安全保障以保障国家安全、金融稳定及公众利益为目标，遵循“纵深防御”战略，在人员通过技术实施操作的各个层面，采取控制措施保障交易全过程安全性，保障交易双方的双向可信、交易信息的安全性及交易授权的不可抵赖性。网上银行系统信息安全保障是一个涵盖风险管理、策略制定、规划实施、监督检查、改进完善的动态运作过程，需要网上银行高级管理层的高度重视以及业务、技术、风险管理、审计等相关部门协调配合，共同构建、实施全面性、系统性的保障体系。

在网上银行系统的描述中，应根据应用系统、客户对象、数据敏感程度等划分安全域。安全域是一个逻辑的划分，它是遵守相同的安全策略的用户和系统的集合。通过对安全域的描述和界定，可更好地对网上银行系统信息安全保障进行描述。具体而言，网上银行系统主要包括：客户端、网上银行访问子网、网上银行业务系统、中间隔离设备和安全认证设备等。

6 安全规范

本文件分为安全技术规范、安全管理规范和业务运作安全规范三个部分，安全技术规范从客户端安全、专用安全设备安全、网络通信安全和网上银行服务器端安全几个方面提出要求；安全管理规范从安全管理机构、安全策略、管理制度、人员安全管理、系统建设管理、系统运维管理几个方面提出要求；业务运作安全规范从业务申请及开通、业务安全交易机制、客户教育及权益保护几个方面提出要求。另外，考虑到业务相关性，本文件还包含与网上银行相关的网上支付部分安全要求。下面将分别对其进行阐述。

6.1 安全技术规范

6.1.1 客户端安全

6.1.1.1 客户端程序

基本要求：

a) 金融机构应采取有效技术措施保证客户端处理的敏感信息、客户端与服务器交互的重要信息的机密性和完整性；应保证所提供的客户端程序的真实性和完整性，以及敏感程序逻辑的机密性。
b) 客户端程序上线前应进行严格的代码安全测试，如果客户端程序是外包给第三方机构开发的，金融机构应要求开发商进行代码安全测试。金融机构应建立定期对客户端程序进行安全检测的机制。
c) 客户端程序应通过指定的第三方中立测试机构的安全检测，每年至少开展一次。

d) 应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。
e) 客户端程序在启动和更新时应进行真实性和完整性校验，防范客户端程序被篡改或替换。
f) 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，防止敏感信息的泄露。
g) 客户端程序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。

下面的条款只针对PC客户端：

h) 客户端程序应具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对客户端程序的调试、分析和篡改。
i) 客户端程序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。
j) 客户端程序应防范键盘窃听敏感信息，例如防范采用挂钩 Windows 键盘消息等方式进行键盘窃听，并应具有对通过挂钩窃听键盘信息进行预警的功能。

下面的条款只针对移动终端客户端：

k) 客户端程序应提供敏感信息机密性、完整性保护功能，例如采取随机布放按键位置、防范键盘窃听技术、计算 MAC 校验码等措施。

增强要求：

下面的条款只针对PC客户端：

a) 客户端程序应保护在客户端启动的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。
b) 客户端程序应采用反屏幕录像技术，防范非法程序获取敏感信息。

下面的条款只针对移动终端客户端：

c) 客户端程序应采取代码混淆等技术手段，防范攻击者对客户端程序的调试、分析和篡改。
d) 客户端程序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。

6.1.1.2 客户端环境安全

基本要求：

a) 应采取有效措施提升客户端环境安全级别，例如，在线杀毒服务、安全检测工具等，并在显著位置予以提醒。
b) 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。

6.1.2 专用安全设备安全

6.1.2.1 USB Key

基本要求：

a) 金融机构应使用指定的第三方中立测试机构安全检测通过的 USB Key。
b) 应采取有效措施防范 USB Key 被远程挟持，例如通过可靠的第二通信渠道要求客户确认交易信息等。
c) 应在安全环境下完成 USB Key 的个人化过程。
d) USB Key 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 USB Key 内进行。

e) USB Key 的主文件（Master File）应受到 COS 安全机制保护，保证客户无法对其进行删除和重建。

f) 应保证私钥在生成、存储和使用等阶段的安全：
- 私钥应在 USB Key 内部生成，不得固化密钥对和用于生成密钥对的素数。
- 应保证私钥的唯一性。
- 禁止以任何形式从 USB Key 读取或写入私钥。
- 私钥文件应与普通文件类型不同，应与密钥文件类型相同或类似。
- USB Key 每次执行签名等敏感操作前均应经过客户身份鉴别。
- USB Key 在执行签名等敏感操作时，应具备操作提示功能，包括但不限于声音、指示灯、屏幕显示等形式。

g) 参与密钥、PIN 码运算的随机数应在 USB Key 内生成，其随机性指标应符合国际通用标准的要求。

h) 密钥文件在启用期应封闭。

i) 签名交易完成后，状态机应立即复位。

j) 应保证 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、密钥等敏感信息。
- PIN 码和密钥（除公钥外）不能以任何形式输出。
- 经客户端输入进行验证的 PIN 码在其传输到 USB Key 的过程中，应加密传输，并保证在传输过程中能够防范重放攻击。
- 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。
- 同一型号 USB Key 在不同银行的网上银行系统中应用时，应使用不同的根密钥，且主控密钥、维护密钥、传输密钥等对称算法密钥应使用根密钥进行分散。

k) USB Key 使用的密码算法应经过国家主管部门认定。

l) 应设计安全机制保证 USB Key 驱动的安全，防范被篡改或替换。

m) 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指令。

n) USB Key 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

o) 在外部环境发生变化时，USB Key 不应泄露敏感信息或影响安全功能。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

增强要求：

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

b) 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。
c) 应采取有效措施防止签名数据在客户最终确认前被替换。
d) 未经按键确认，USB Key 不得签名和输出，在等待一段时间后，可自动清除数据，并复位状态。
e) USB Key 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、屏幕显示提醒等的功能。
f) USB Key 在连接到终端设备一段时间内无任何操作，应自动关闭，必须重新连接才能继续使用，以防范远程挟持。

6.1.2.2 文件证书

此部分要求仅针对C/S模式客户端。
基本要求：
a) 应严格控制申请、颁发和更新流程。避免对个人网上银行客户的同一业务颁发多个有效证书。
b) 用于签名的公私钥对应在客户端生成，禁止由服务器生成。私钥只允许在客户端使用和保存。
c) 应保证私钥的唯一性。
d) 应强制使用密码保护私钥，防止私钥受到未授权的访问。
e) 应支持私钥不可导出选项。
f) 私钥导出时，客户端应对客户进行身份认证，例如验证访问密码等。
g) 私钥备份时，应提示或强制放在移动设备内，备份的私钥应加密保存。
增强要求：
a) 在备份或恢复私钥成功后，金融机构应通过可靠的第二通信渠道向客户发送提示消息。
b) 文件证书应与计算机主机信息绑定，防范证书被非法复制到其他机器上使用。
c) 应采用验证码对关键操作（例如签名）进行保护，防范穷举攻击。

6.1.2.3 OTP 令牌

基本要求：
a) 金融机构应使用指定的第三方中立测试机构安全检测通过的 OTP 令牌设备及后台支持系统。
b) 应采取有效措施防范 OTP 令牌被中间人攻击，例如通过可靠的第二通信渠道要求客户确认交易信息等。
c) 应采取有效措施保证种子密钥在整个生命周期的安全。
d) 口令生成算法应经过国家主管部门认定。
e) 动态口令的长度不应少于 6 位。
f) 应防范通过物理攻击的手段获取设备内的敏感信息，物理攻击的手段包括但不限于开盖、搭线、复制等。
g) OTP 令牌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
h) 在外部环境发生变化时，OTP 令牌不应泄露敏感信息或影响安全功能。外部环境的变化包含但不限于：
   - 高低温
   - 强光干扰
   - 电磁干扰
   - 紫外线干扰

- 静电干扰

i) 对于基于时间机制的 OTP 令牌，为了时间同步，应在服务器端设置认证 OTP 密码的时间窗口，认证服务器可以接受的 OTP 密码时间窗口越小，口令被误用的风险越小，应设置此时间窗口最大不超过口令的理论生存期前后 60 秒（理论生存期是指如果令牌和服务器时间严格一致，令牌上出现口令的时间范围），结合应用实践，设置尽可能小的理论生存期，以防范中间人攻击。

j) 采用基于挑战应答的 OTP 令牌进行资金类交易时，挑战值应包含用户可识别的交易信息，例如转入账号、交易金额等，以防范中间人攻击。

k) 如使用 OTP 令牌，登录和交易过程中口令应各不相同，且使用后立即失效。

增强要求：

a) OTP 令牌设备应使用 PIN 码保护等措施，确保只有授权客户才可以使用。

b) PIN 码和种子应存储在 OTP 令牌设备的安全区域内或使用其他措施对其进行保护。

c) PIN 码连续输入错误次数达到错误次数上限（不超过 6 次），OTP 令牌应锁定。

6.1.2.4 动态密码卡

基本要求：

a) 动态密码卡应与客户唯一绑定。

b) 应使用涂层覆盖等方法保护口令。

c) 服务器端应随机产生口令位置坐标。

d) 动态口令的长度不应少于 6 位。

e) 应设定动态密码卡使用有效期，超过有效期应作废。

f) 动态密码卡应具备有效使用次数。

6.1.2.5 其他专用安全设备

本部分规定的是已使用的其他专用安全设备，如出现新的专用安全设备，可参照6.1.2节的要求，保证专用安全设备自身安全机制的可靠性以及其所保护信息的安全性。

手机短信动态密码：

基本要求：

a) 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。

b) 交易的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。

c) 手机动态密码应随机产生，长度不应少于 6 位。

d) 应设定手机动态密码的有效时间，最长不超过 6 分钟，超过有效时间应立即作废。

e) 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。

指纹识别：

基本要求：

a) 如果通过指纹鉴别客户身份，应防止指纹数据被记录和重放。

b) 禁止在远程身份鉴别中采用指纹识别。近距离身份鉴别（例如使用专用安全设备对使用者的身份鉴别）可采用指纹识别。

移动终端硬件加密模块：

本部分条款参照6.1.2.1的要求执行。

6.1.3 网络通信安全

本部分内容指数据在网络传输过程中采用的通讯协议和安全认证方式，不包括网络基础设施方面的内容。

6.1.3.1 通讯协议

基本要求：

a) 应使用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，例如，使用 SSL/ TLS、IPSEC 和 WTLS 协议。

b) 如果使用 SSL 协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持。

增强要求：

a) 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。

6.1.3.2 安全认证

基本要求：

a) 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。双向身份认证是指不仅客户端对服务器身份进行认证，服务器也应认证客户端身份。

b) 整个通讯期间，经过认证的通讯线路应一直保持安全连接状态。

c) 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。

d) 应确保客户获取的金融机构 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，或将根证书集成在客户端控件下载包中分发等。

增强要求：

a) 金融机构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。

6.1.4 服务器端安全

6.1.4.1 物理安全

应在金融机构统一的物理安全体系下，遵照国家及行业有关要求，加强网上银行系统物理安全防护，对物理安全的基本要求见附录C。

6.1.4.2 网络安全

基本要求：

a) 合理部署网上银行系统的网络架构

- 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隔离。
- 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。
- 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。
- 维护与当前运行情况相符的网络拓扑图，并区分可信区域与不可信区域。
- 采用 IP 伪装技术隐藏内部 IP，防止内部网络被非法访问。
- 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。
- 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。

- 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。

b) 访问控制

- 在网络结构上实现网间的访问控制，采取技术手段控制网络访问权限。
- 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。
- 限制 HTTP、FTP、TELNET 等风险较高的协议的使用。如果使用这些协议，应采取补偿的安全控制措施并实现对协议命令级的控制。
- 应在会话处于非活跃一定时间或会话结束后终止网络连接。
- 应限制网络最大流量数及网络并发连接数。
- 在不影响双机切换等情况下，应对重要主机的 IP 地址与 MAC 地址进行绑定，例如，Web 服务器、中间件服务器、前置服务器、数据库服务器等主机。
- 应限制只有业务需要的用户才能访问网上银行服务器，控制粒度为单个用户。
- 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。

c) 网络设备的管理规范和安全策略

- 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。
- 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。
- 应对登录网络设备的用户进行身份鉴别。身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换：
  - 至少每 90 天修改一次用户口令
  - 口令最小长度不低于 8 个字符
  - 使用包含数字和字母的口令
  - 不允许提交与上次相同的新口令
- 网络设备用户的标识应唯一。
- 应对网络设备的管理员登录地址进行限制。
- 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设置。
- 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，可采取结束会话、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）
  - 锁定持续时间至少设定为 30 分钟或直至管理员为其解锁
  - 如果一个会话空闲的时间超过 15 分钟，要求用户再次输入口令以重新激活终端
- 当对网络设备进行远程管理时，应采取必要措施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，确保更改已进行验证和审批。
- 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检查。
- 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，确保备份配置文件的安全性。

d) 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。
- 应对审计记录进行保护，避免被未授权删除、修改或者覆盖：
  - ♦ 只允许具有工作需要的人员查看
  - ♦ 及时备份到集中的日志服务器上或难以更改的介质上
  - ♦ 使用文件完整性监视和变更检测软件保护日志，确保已有的日志被改变时产生报警
  - ♦ 每天复审所有系统的日志
- 采取措施保障关键网络设备时间同步，例如，设置网络时间协议（NTP）服务器。

e) 入侵防范
- 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，监视并记录以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。
- 当检测到攻击行为时，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。
- 制订合理的 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。
- 应防范对网上银行服务器端的 DoS/DDoS 攻击。可参考的加固措施包括但不限于：
  - ♦ 与电信运营商签署 DoS/DDoS 防护协议
  - ♦ 防火墙只开启业务必需的端口并开启 DoS/DDoS 防护功能
  - ♦ 使用 DoS/DDoS 防护设备
  - ♦ 使用 IDS/IPS 设备
  - ♦ 使用负载均衡设备

f) 边界完整性检查
- 应能够对非授权设备私自联到生产网络的行为进行检查，准确定出位置，并对其进行有效阻断。
- 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，准确定出位置，并对其进行有效阻断。

g) 恶意代码防范
- 在网络边界部署入侵检测/防护系统、防病毒网关等防病毒设备，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。

网络防护架构参考图分别参见附录A和附录B。

6.1.4.3 主机安全

基本要求：

a) 身份鉴别
- 应对登录操作系统和数据库的用户进行身份标识和鉴别，严禁匿名登录。

- 为不同的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初始密码，禁止共享账号和密码。
- 应要求系统的静态口令在 8 位以上，由字母、数字、符号等混合组成。
- 首次登录系统时应强制修改密码，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。
- 在收到用户重置密码的请求后，应先对用户身份进行核实再进行后续操作。
- 应启用登录失败处理功能，可采取结束会话、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）
  - 锁定持续时间至少设定为 30 分钟或直至管理员为其解锁
- 应确保对密码进行强效加密保护，不允许明文密码出现。
- 对服务器进行远程管理时，如果数据通过不可信网络传输，应采取加密通信方式，防止认证信息在网络传输过程中被窃听。
- 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，并且身份鉴别信息至少有一种是不可伪造的，例如以密钥证书、动态口令卡、生物特征等作为身份鉴别信息。
- 系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。

b) 访问控制

- 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、安全管理员、安全审计员等）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。
- 应实现操作系统和数据库系统特权用户的权限分离。
- 严格限制默认用户的访问权限，重命名系统默认用户，修改默认用户密码，及时删除多余的、过期的用户及调试用户。
- 严格控制操作系统重要目录及文件的访问权限。

c) 安全审计

- 审计范围应覆盖到服务器和管理终端上的每个操作系统用户和数据库用户。
- 审计内容应包括重要用户行为、系统资源的异常使用和重要信息系统命令的使用、账号的创建分配与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件。
- 审计记录包括时间、类型、访问者标识、访问对象标识和事件结果，保存时间不少于半年。
- 应根据记录数据进行安全分析，生成审计报表，并及时备份到集中的日志服务器上或难以更改的介质上。
- 应保护审计进程，避免受到未预期的中断。
- 应保护审计记录，避免遭受未授权的删除、修改或覆盖：
  - 只允许具有工作需要的人员查看
  - 使用文件完整性监视和变更检测软件保护日志，确保已有的日志被改变时产生报警
  - 每天复审所有系统的日志

d) 入侵防范

- 应能够检测到对重要服务器进行入侵的行为，包括但不限于主机运行监视、特定进程监控、入侵行为监测和完整性检测等，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

- 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施或在检测到完整性即将受到破坏时进行事前阻断。
- 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，禁用所有不必要和不安全的服务和协议，移除所有不必要的功能。
- 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。

e) 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，对于依附于病毒库进行恶意代码查杀的软件应及时更新防恶意代码软件版本和恶意代码库，对于非依赖于病毒库进行恶意代码防御的软件，例如主动防御类软件，应保证软件所采用的特征库有效性与实时性，对于某些不能安装相应软件的系统可以采取其他安全防护措施来保证系统不被恶意代码攻击。
- 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。
- 应支持防恶意代码工具的统一管理。
- 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。

f) 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。
- 应限制单个用户对系统资源的最大或最小使用限度。
- 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。
- 所有的服务器应全部专用化，不使用服务器进行收取邮件、浏览互联网等客户端操作。

增强要求：

a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

c) 应对重要信息资源设置敏感标记。

d) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

6.1.4.4 应用安全

基本要求：

a) 身份鉴别

- 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#）代替。
- 密码应有复杂度的要求，包括：
  - ♦ 长度至少 6 位，支持字母和数字共同组成
  - ♦ 在客户设置密码时，应提示客户不使用简单密码
  - ♦ 如有初始密码，首次登录时应强制客户修改初始密码
- 应具有防范暴力破解静态密码的保护措施，例如在登录和交易时使用图形认证码，图形认证码应满足：

- ♦ 由数字和字母等字符混合组成
- ♦ 随机产生
- ♦ 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、变异字体显示样式等有效方式，防范恶意代码自动识别图片上的信息
- ♦ 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

- 使用软键盘方式输入密码时，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。
- 应保证密码的加密密钥的安全。
- 应采取有效措施防范登录操作的重放攻击，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。
- 应可判断客户的空闲状态，当空闲超过一定时间后，自动关闭当前连接，客户再次操作时必须重新登录。
- 会话标识应随机并且唯一，会话过程中应维持认证状态，防止客户通过直接输入登录后的地址访问登录后的页面。
- 禁止在客户端缓存密码、密钥等敏感信息，例如，在包含上述信息的页面设置禁止缓存参数，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。
- 退出登录时应提示客户取下专用安全设备，例如 USB Key。
- 修改客户敏感参数（例如，密码、转账限额等）时，应再次认证客户身份。
- 显示客户身份证件信息时，应屏蔽部分关键内容。
- 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。

b) 访问控制

- 应建立安全的访问控制机制，防止用户访问无权访问的功能或资源，例如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。
- 企业网上银行可支持客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，每次处理的客户信息均以服务器端数据为准，并对客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及数据库中多余的、过期的用户及调试用户。

c) 安全审计

- 应具有保存和显示客户历史登录信息（例如，时间、IP 地址、MAC 地址等）的功能，支持客户查询登录（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。
- 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。

d) 软件容错

- 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。
- 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。
- 应能够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。

e) 资源控制

- 应能够对系统的最大并发会话连接数进行限制。
- 应能够对单个用户的多重并发会话进行限制。
- 应能够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，另一方应能够自动结束会话。
- 应能够对一个访问账户或者一个请求进程占用的资源分配最大限额和最小限额。
- 应能够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。
- 应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

f) Web 应用安全

- 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。
  - 如果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。
  - 禁止在 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。
  - 禁止在 Web 应用服务器端保存客户敏感信息。
  - 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。
  - 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以“目录不存在”提示客户。
  - 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。
- 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。
  - 禁止仅在客户端以脚本形式对客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。
- 防范跨站脚本攻击
  - 应通过严格限制客户端可提交的数据类型以及对提交的数据进行有效性检查等有效措施防止跨站脚本注入。
- 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。
- 应采取网站页面防篡改措施，例如部署网页防篡改系统等。
- 应采取有效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）带来的敏感信息泄露、交易数据篡改等重要信息安全风险。

g) 防钓鱼

- 应具有防网络钓鱼的功能，例如，显示客户预留信息、使用预留信息卡、客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。
- 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。

h) 域名解析服务

- 域名解析系统应不间断运行，在排除不可抗因素的情况下，按月统计，权威服务器和递归服务器业务可用性均应大于 99.99% 。
- 递归服务器自身不应同时兼备权威服务器功能，同时不提供除了域名服务之外的其他服务；对权威域名服务系统，应保持主服务器对辅服务器（组）的记录信息进行更新，保证数据同步。
- 应采用内外网隔离或加密等保护措施避免远程访问和域名数据在公共互联网的明文传输。
- 应建立对关键数据和重要信息进行备份和恢复的管理和控制机制。关键数据包括但不限于域名系统架构、域名解析软件及配置、域名区文件、域名解析日志、域名系统监控数据。
- 如采用委托第三方运营的域名解析系统，应要求其提供与自建域名解析系统相同的安全防护要求。

增强要求：

a) 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。

b) 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，应再次对客户身份进行认证，否则服务器端自动终止会话。

c) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

d) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

e) 应具有对重要信息资源设置敏感标记的功能。

f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

6.1.4.5 数据安全及备份恢复

基本要求：

a) 数据完整性

- 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。
- 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

b) 数据保密性

- 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性。
- 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

c） 备份和恢复

- 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，并将备份介质存放在安全区域内，数据保存期限依照国家相关规定。
- 数据备份存放方式应采用多冗余方式，完全数据备份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，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。

6.2 安全管理规范

6.2.1 安全管理机构

基本要求：

a） 岗位设置

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

b） 人员配备

- 金融机构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。
- 应配备专职信息安全管理人员，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。

c） 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，必须提交高层管理层审批，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。

d) 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。
- 应建立与相关金融机构、公安机关、电信公司的合作、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、专业的安全公司、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。

e) 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，并将安全检查报告上报人民银行等金融机构主管部门。
- 内部审计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。

6.2.2 安全策略

基本要求：

a) 应制订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金融机构全面风险管理体系。

b) 应结合金融机构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。应制订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) 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，平衡客户体验和安全性，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。

d) 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、容忍度及参数制订、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。
e) 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。
f) 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、金融机构声誉造成影响的信息安全风险。
g) 应制定分级标准，针对不同的风险规定相应的可能性等级列表，评定风险等级，对于已发现的风险应尽快修补或制订规避措施。
h) 应建立网上银行信息安全风险的持续监测机制，建立风险预警、报告、响应和处理机制，明确风险报告的内容、流程、主客体以及频率，建立符合金融机构实际状况的关键风险指标体系，实现信息安全风险监测的自动化，保证高级管理层和相关部门及时获取网上银行信息安全风险变化，验证现有控制措施的有效性。
i) 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。
j) 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，定期进行再评估。
k) 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，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，自评估应由金融机构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，评估依据应覆盖本文件要求项，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金融机构主管部门。
l) 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，开展网上银行系统信息安全测评及整改工作。
m) 在选择外部评估时，应对其加强安全管理，签订保密协议或在相关服务协议中明确保密条款，避免泄漏敏感信息。
n) 金融机构如提供跨境网上银行服务，应充分考虑境内外法律法规、监管要求等的差异性，在深入评估相关风险的基础上，妥善选择相应的安全控制措施。

增强要求：

a) 应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。

6.2.3 管理制度

基本要求：

a) 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。
b) 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。
c) 应指定或授权专门的部门或人员负责安全管理制度的制订。
d) 安全管理制度应具有统一的格式，并进行版本控制。

e） 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。
f） 安全管理制度应通过正式、有效的方式发布。
g） 安全管理制度应注明发布范围，并对收发文进行登记。

6.2.4 人员安全管理

基本要求：
a） 应指定或授权专门的部门或人员负责人员录用。
b） 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。
c） 应与员工签署保密协议，或在劳动合同中设置保密条款。
d） 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。
e） 凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不得从事与网上银行相关的信息安全管理工作。
f） 应对安全教育和培训的情况和结果进行记录并归档保存。
g） 应具有员工岗位调动或离职的安全管理制度，应取回各种身份证件、钥匙、徽章等以及金融机构提供的软硬件设备，避免系统账号、设备配置信息、技术资料及相关敏感信息等泄漏。
h） 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，并保证离岗人员管理及使用的系统口令必须立即更换。
i） 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。
j） 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。
k） 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。
l） 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。
m） 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。
n） 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。
o） 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，必要时签署保密协议。

6.2.5 系统建设管理

基本要求：
a） 安全方案设计
- 指定和授权专门的部门对系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划。
- 制定安全保障体系的总体安全策略、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，组织相关部门和有关安全技术专家对其合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

- 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。

b) 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的采购。
- 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必须经过主管领导授权，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属于重要技术资料，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，要按照固定资产报废审批程序处理。

c) 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。

d) 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。
- 实现金融机构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。尹
- 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。
- 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。
- 建立恰当的应急措施，应对外包服务商在服务中可能出现的重大缺失。尤其需要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。若需要外包人员进入进行现场实施时，应事先提交计划操作内容，金融机构人员应在现场陪

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）应由金融机构人员进行操作，外包人员不得查看、复制或带离任何敏感信息。

- 应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。
- 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。

e） 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。

f） 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订测试验收方案，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。

g） 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。
- 外包项目建设单位应与金融机构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。

h） 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。金融机构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。

6.2.6 系统运维管理

基本要求：

a） 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。

b) 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，并根据安全等级制订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。

c) 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。
- 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，应报金融机构相关部门备案，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金融机构内部使用的情况，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金融机构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。

d) 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必须请生产设备的科研单位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。
- 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必须经过审批才能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。

e) 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，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，并且重要报警要能以某种方式（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金融机构主管部门。

f) 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（兼）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。

- 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。
- 应制定远程访问控制规范，确因工作需要进行远程访问的，应提请金融机构开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。
- 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应经过授权。
- 应根据安全策略允许或者拒绝便携式和移动式设备的网络接入。
- 应定期检查违反规定拨号上网或其他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版本软件对网络设备进行更新，并在更新前对现有的重要文件进行备份。

g) 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。
- 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，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装，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，重要的系统设置要求至少两人在场。
- 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。
- 应加强对系统容量管理，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、实施设备扩容。

h) 恶意代码防范管理

- 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。
- 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。
- 金融机构全系统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，并形成书面的报表和总结汇报。

i) 密钥管理

- 应制订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。
- 金融机构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，金融机构应制订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。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。

j) 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及系统的升级、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，应及时向人民银行等金融机构主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文件化程序，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，保存时间至少 3 个月。
- 应建立中止变更并从失败变更中恢复的文件化程序，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建立演练报告。
- 变更前要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。
- 变更前做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪。
- 如果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。

k) 业务运行连续性

- 应制订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。
- 应制订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。

l) 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，制订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，确保可以在恢复程序规定的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，每次抽检数据量不低于 10%。备份数据要实行异地保存。
- 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与数据备份介质一并妥善保管。
- 应在金融机构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，遵照金融机构主管部门有关要求，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。

m) 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应尝试验证弱点。
- 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。
- 应制定安全事件报告和响应处理程序，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。
- 应结合金融机构自身情况，对造成系统中断和造成信息泄密的安全事件应制定不同的处理程序和内外部报告程序。
- 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等金融机构主管部门，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，报告内容包括，事件基本情况（起始时间、发生地点、发现方式、现象、持续时间、处置措施及恢复过程等）；事件影响（影响地域及内外部机构的个数、名称，影响系统的名称、功能、硬件、软件、部署图、冗余情况等，影响的业务，影响的数据，其他影响）；事件损失评估（资金损失，数据损失，其他损失）；事件根源分析（技术方面，管理方面）；事件责任认定；事件处置经验与教训（事件处置经验，事件处置教训）；改进措施。重大网上银行信息安全事件是指符合以下条件之一的事件：导致机构两个（含以上）省（自治区、直辖市）网上银行业务无法正常开展达 30 分钟及以上，或一个省（自治区、直辖市）网上银行业务无法正常开展达 2 个小时及以上的事件；数据丢失或被窃取、篡改、假冒对国家安全、社会秩序、公众利益和金融机构造成重大影响的事件；其他对国家安全、社会秩序、公众利益和金融机构造成重大影响的事件。
- 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脆弱性，及时整改发现的问题。

n) 应急管理

- 应在网上银行统一的应急预案框架下，制订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的条件、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，选择处置方案必须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会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（应急方案）的开发、发布流程，以备必要时提供紧急补丁或应急方案进行处理，以修补重要安全漏洞。
- 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的桌面演练和生产系统实战演练，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要至少每年演练一次。针对DDoS、网络钓鱼等重要安全威胁，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。

6.3 业务运作安全规范

6.3.1 业务申请及开通

基本要求：

a) 金融机构应充分考虑并采取有效措施防范网上银行资金类交易开通的安全风险。网上银行资金类交易的开通必须由客户本人到柜台申请，申请时，金融机构应对其进行风险提示，验证客户的有效身份，并要求客户书面确认。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。以下资金类交易可不受上述限制：开通同一客户账户之间转账并且金融机构能有效识别转入、转出方为同一客户账户的,客户预先通过柜台签约对转入账户进行绑定同时指定交易电话的。

b) 网上银行资金类业务关闭后，重新申请开通该功能，必须要求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。采取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，请求客户本人对业务重新开通操作进行确认。

c) 企业网上银行开通必须由本企业人员到柜台申请，金融机构应审查其申请材料的真实性、完整性和合规性。

d) 企业网上银行客户加挂账户可通过柜台或通过需使用专用安全设备工具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、重置专用安全设备工具密码必须到柜台办理。

e) 通过手机终端访问网上银行的资金类交易开通必须有效验证客户身份，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。应建立手机号和银行账户的关联关系，例如手机号与客户身份证绑定、手机号与客户银行账户信息绑定等，采用移动终端硬件加密模块的，应建立硬件加密模块与客户身份证或银行账户信息的关联关系。通过网上银行渠道申请时，金融机

构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。

f) 如果网上银行登录密码以密码信封方式发送给客户或者初始登录密码由金融机构设置，金融机构应强制客户首次登录时修改初始密码。

g) 客户重置登录密码及支付密码时，必须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申请。通过网上银行渠道申请时，金融机构必须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。

h) 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。

i) 下载客户数字证书时，应有身份认证的过程。通过提交授权码和参考码等方式保证客户数字证书只能被下载一次，身份认证信息应设置有效期，超出有效期而未下载证书，应重新办理。

j) 客户申请 USB Key 作为数字证书载体或申请其他安全设备时，应持有效身份证件到柜台办理，金融机构应采取将安全设备序列号与客户信息进行绑定等措施，并在客户下载证书时将其作为客户身份认证因素之一，以防止证书被冒下。如果安全设备丢失，应持有效证件到柜台重新办理，原有安全设备和客户绑定关系解除。

k) 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、解除挂失需客户本人持有效身份证件到柜台或通过金融机构客服电话办理，金融机构应核实客户信息、网银账户信息并对预留手机号码进行验证。

6.3.2 业务安全交易机制

6.3.2.1 身份认证

基本要求：

a) 金融机构应按照审慎原则，采取有效、可靠的身份认证手段，保证资金类交易安全。

b) 网上银行资金类交易、重要信息及业务变更类等高风险业务应使用双因素身份认证。双因素身份认证由以下两种身份认证方式组成：一是客户知晓、注册的客户名称及密码。二是客户持有、特有并用于实现身份认证的信息，包括但不限于物理介质或电子设备等。以下资金类交易可不受上述限制：同一客户账户之间转账并且金融机构能有效识别转入、转出方为同一客户账户的。

c) 禁止仅使用文件证书或使用文件证书加静态密码的方式进行资金类交易。

d) 使用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。

e) 应采取有效措施引导客户设置与银行卡交易密码不同的网上银行登录、交易密码，使用不相同的登录密码及交易密码。

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 10 次），应在短时间内锁定该客户网上银行登录权限或交易账户使用权限，并立即通过短信或电话等可靠的方式通知客户。

g) 金融机构用于发送网上银行交易提示短信、动态验证码等信息的客户预留手机号码变更时应符合下列要求之一：客户持有效身份证件到柜台办理；客户通过网上银行渠道变更预留手机号码，金融机构必须采取双因素身份认证验证用户的真实身份及银行卡交易密码，并通过验证发向原预留手机号码的短信验证码等可靠的方式，请求客户本人对预留手机号码变更操作进行确认。

如果通过网上银行系统开展网上支付业务，还应满足如下条款：

h) 网上银行系统接受商户或非金融支付机构的系统建立连接请求时，应通过验证其服务器数字证书、预留 IP 地址比对等方式认证其系统的身份。应对网上银行系统和商户或第三方系统之间发送和接收的信息采用数字证书机制进行签名及验签，保证交易数据的完整性和不可抵赖性。

6.3.2.2 交易流程

基本要求：

a) 金融机构应充分考虑、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。

b) 资金类交易中，应具有防范客户端数据被篡改的机制，应由客户确认资金类交易关键数据（至少包含转入账号和交易金额），并采取有效确认方式以保证待确认的信息不被篡改，例如，通过发送包含确认信息的短信验证码、在 USB Key 内完成确认等。

c) 资金类交易中，如果客户端对交易数据签名，签名数据除流水号、交易金额、转入账号、交易日期和时间等要素外，还应包含由服务器生成的随机数据。对于从网上银行客户端提交的交易数据，服务器应验证签名的有效性并安全存储签名。

d) 通过移动终端提交交易请求时，金融机构应采取有效措施鉴别客户身份，保证敏感信息和交易数据的机密性、完整性，并设置与安全防护能力相适应的交易限额以控制交易风险。通过移动终端客户端程序提交交易请求时，应上送终端相关信息，例如，IMEI、IMSI 等。后台服务器应对编号信息和登记信息进行一致性验证。如果对交易数据签名，签名数据应包含此类信息。

e) 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替换。

f) 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。

g) 金融机构可根据自身情况界定高风险业务及其风险控制规则，对于资金类交易等触发风险控制规则的情况，应使用可靠的第二通信渠道请求客户反馈确认交易信息。

h) 对于资金类等高风险业务，金融机构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。

i) 应采取适当的安全措施确保客户对所做重要信息及业务变更类交易的抗抵赖。

j) 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。

如果通过网上银行系统开展网上支付业务，还应满足如下条款：

k) 金融机构在与商户及非金融支付机构合作时，应采取有效措施保证交易指令的安全性，并要求商户和非金融支付机构提供必要的订单信息，以用于客户交易确认，保障支付交易安全。

l) 支付网关应对交易订单的唯一性进行检查，防止订单重复支付。

m) 通过可靠的数字签名等机制保证订单信息的真实性、完整性，验证订单的有效性并存储订单，防止交易篡改、伪造订单等。

n) 金融机构应与商户、非金融支付机构配合，在资金拨付前，校验、确认支付相关信息，以防范木马篡改或替换订单导致持卡人资金损失的风险，可采取的措施包括但不限于以下内容：

- 支付网关向客户发送确认信息，其中包含在商户网站生成的订单号，并提醒客户到商户网站确认此订单号对应的详细信息和所选购商品的一致性。
- 商户或非金融支付机构向客户确认订单信息的真实性和完整性，支付网关验证订单信息和支付用户信息的关联性，确保订单提交人与支付用户的一致性（代付情况除外）。例如，在生成订单时，商户或非金融支付机构应要求客户提交其银行账户绑定的手机号码，并将此手机号码作为订单信息的字段，商户或非金融支付机构向此手机号码发送确认消息（包

含但不限于商户名称、商品类别、交易金额、收货人标识、订单提交人的客户标识等），并将手机号码及订单关键信息（例如订单编号、订单金额）提交到支付网关，支付网关在进行划款支付时验证手机号码和客户银行账户的绑定关系。

- 金融机构提供可显示交易信息及计算校验码的第三方插件供商户调用，此插件对客户的关键订单信息（包含但不限于商户名称、商品类别、交易金额、收货人标识、订单提交人的客户标识等）计算校验码，并将此校验码作为唯一标识上送到支付网关，支付网关在和客户的确认消息中包含此校验码，并提醒客户到商户网站手工计算校验码并进行比对。
- 支付网关向客户发送确认信息，其中包含关键订单信息，客户据此确认订单的真实性和完整性，订单信息包含但不限于：非金融支付机构名称、商户名称、商品类别、交易金额、收货人标识、订单提交人的客户标识。

o) 订单信息中应包含商品类别信息，能够标识商品的实体状态（实物或虚拟）。对虚拟类商品：

- 应要求商户提供收货人地址或收货人标识，在支付界面上提供收货人地址或收货人标识供客户确认。
- 设置支付限额，超过支付限额，拒绝交易。
- 通过可靠的第二渠道向客户确认支付请求信息。

p) 应设置网上支付类交易风险监控规则（例如交易限额和交易频率），对于触发风险监控规则的交易，应通过可靠的第二通信渠道发送确认消息，客户确认信息包含应至少包含关键订单信息或者订单标识信息（例如订单编号、订单校验码）、交易金额以及收款方名称。

q) 支付网关在确认支付前，应向客户提示支付风险。

r) 支付网关应准确完整记录交易的支付请求信息，例如，商户编号、商户名称、非金融支付机构名称、商户订单号、交易金额、交易日期及时间等。

s) 支付网关应准确完整记录交易的支付结果信息，例如，支付时间、交易金额、支付方式、付款方、收款方、支付状态等。

t) 应禁止在支付网关应用系统的日志中保存敏感账户信息。

u) 应要求支付网关连接的商户和非金融支付机构采用可靠的密钥保护机制，例如采用专门的硬件加密设备，用来保存认证密钥。

v) 应根据“业务必需”原则与商户、非金融支付机构及其他金融机构共享信息，金融机构未经客户直接授权，不得与其他机构共享客户的敏感信息，不得保存其他机构客户的敏感信息。

w) 如果商户和非金融支付机构系统参与敏感信息的处理，应禁止存储客户的敏感信息；对因业务需要存储的交易数据，应采取严格的访问控制措施。

6.3.2.3 交易监控

基本要求：

a) 金融机构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。

b) 应制定网上银行异常交易监测和处理的流程和制度。

c) 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。

d) 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。

e) 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。

增强要求：

a) 金融机构的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。

b) 金融机构的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。

c) 金融机构的风险交易监控系统应能够不断更新反欺诈规则，能够实现各金融机构、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。

6.3.3 客户教育及权益保护

基本要求：

a) 金融机构应切实加强客户教育和风险提示，向客户详细解释本机构网上银行业务流程和安全控制措施，在网银新产品（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。

b) 金融机构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，提示客户牢记金融机构官方网站地址和呼叫中心号码。

c) 金融机构应向客户印发通俗、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教育栏目。

d) 金融机构应向客户明确提示网上银行相关的安全风险和注意事项，并根据网上银行安全形势的变化，及时更新相关事项，包括但不限于提示客户不在非自主可控的终端上登录网上银行，维护良好的客户端环境，及时更新操作系统及浏览器补丁，安装并更新客户端防病毒软件，避免设置与客户端常用软件相同的网上银行登录及交易密码，避免将本人网上银行登录及交易等敏感信息告知他人，避免将本人的网上银行专用安全设备转借他人使用，在网上银行操作完成后立即退出相关界面并及时拔下与终端相连的专用安全设备，不安装或运行来历不明的客户端软件和程序，不打开陌生人发送的电子邮件及其附件或网站链接，谨防虚假网上银行链接，注意对网上银行的敏感信息进行保护等内容。

e) 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，及时通过金融机构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。

f) 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金融机构声誉。

g) 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。