ICS 35.240.40
A 11
备案号：

JR

中华人民共和国金融行业标准

JR/T 0117-2014

征信机构信息安全规范

Specification for information security of credit information service agency

2014-11-17 发布　　2014-11-17 实施

中国人民银行　发布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行征信管理局、中国金融电子化公司。

本标准主要起草人：王煜、陈波、张永福、李斌、李家先、王俊山、王晓燕、马国照、谢业华、常可、陈广辉。

征信机构信息安全规范

1 范围

标准规定了不同安全保护等级征信系统的安全要求，包括安全管理、安全技术和业务运作三个方面。

标准适用于征信机构信息系统的建设、运行和维护，也可作为各单位开展安全检查和内部审计的安全性依据。接入征信机构信息系统的信息提供者、信息使用者也可参照与本机构有关的条款执行，标准还可作为专业检测机构开展检测、认证的依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。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 22239-2008 信息安全技术 信息系统安全等级保护基本要求

ISO/IEC 27001:2013 信息技术 安全技术 信息安全管理体系

3 术语和定义

下列术语和定义适用于本文件。

3.1

征信业务 credit information service

对企业、事业单位等组织的信用信息和个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。

3.2

征信机构 credit information service agency

依法设立的，主要经营征信业务的机构。

3.3

征信系统 credit information system

征信机构与信息提供者协议约定，或者通过互联网、政府信息公开等渠道，对分散在社会各领域的企业和个人信用信息，进行采集、整理、保存和加工而形成的信用信息数据库及相关系统。

3.4

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。

3.5

敏感信息 sensitive information

影响征信系统安全的密码、密钥以及业务敏感数据等信息，密码包括但不限于查询密码、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，业务敏感数据包括但不限于信息主体的身份信息、婚姻状况以及银行账户信息等涉及个人隐私的数据。

3.6

客户端程序 client program

征信机构开发的、通过浏览器访问征信系统并为征信系统客户提供人机交互功能或实现征信系统其他功能（如数据采集）的程序，并提供必需功能的组件，包括但不限于：可执行文件、控件、浏览器插件、静态链接库、动态链接库等（不包括IE等通用浏览器）；或信息提供者、信息使用者以独立开发的软件接入征信系统的客户端程序。

3.7

安全规范测评 test and evaluation of security specifications

按照本规范要求对征信机构进行安全测评的活动。

4 符号和缩略语

以下缩略语和符号表示适用于本文件：

B/S	浏览器/服务器（Browser/Server）
CA	数字证书签发和管理机构（Certification Authority）
C/S	客户机/服务器（Client/Server）
IPSEC	IP安全协议（IP Security Protocol）
SSL	安全套接字层（Secure Sockets Layer）
TLS	传输层安全（Transport Layer Security）
WTLS	无线传输层安全（Wireless Transport Layer Security）

5 征信系统概述

5.1 系统标识

在系统标识中应标明以下内容：

名称：XXXX征信系统/信用信息系统/信用信息平台（全称或简称）。

5.2 系统定义

征信系统是指征信机构与信息提供者协议约定，或者通过互联网、政府信息公开等渠道，对分散在社会各领域的企业和个人信用信息，进行采集、整理、保存和加工而形成的信用信息数据库及相关系统。征信机构通过对征信系统中的企业和个人信用信息进行处理、加工，形成信用报告等征信产品，提供给社会经济活动中有合法需求的信息使用者。

不同征信机构的征信系统规模、架构以及接入方式并不完全相同，部分机构直接面向互联网，以B/S架构建立；部分机构通过与信息提供者相连，以C/S或B/S架构建立。本标准力求对各类征信系统的安全

需求进行归纳，提出统一的规范要求。如无特殊说明，则规范要求对C/S架构、B/S架构都适用，针对只适用于C/S架构或B/S架构的情况，将会单独说明。

5.3 系统描述

征信系统主要由客户端、通信网络和服务器端组成。征信系统包括个人征信系统和企业征信系统，本规范条款如无特殊说明，则同时适用于个人征信系统和企业征信系统。

5.3.1 客户端

客户端是指安装有征信系统人机交互客户端程序的PC终端、笔记本、移动终端等，也包括安装有实现征信系统部分功能的客户端程序的PC终端、笔记本、移动终端等，如数据采集客户端，将来可能还包括其他形式的终端产品。

5.3.2 通信网络

通信网络指的是由客户端、服务器及相关网络基础设施组建的网络连接。征信系统通过互联网或网络专线等方式与信息提供者、信息使用者相连，征信系统安全设计应在综合考虑建设成本、网络便利性等因素的同时，采取必要的技术防护措施，有效应对网络通讯安全威胁。

5.3.3 服务器端

服务器端是指用于提供征信系统核心业务处理和应用服务的服务器设备及安装的相关软件程序。征信机构应充分利用有效的物理安全技术、网络安全技术、主机安全技术、应用安全技术及数据安全与备份恢复技术等，在外部威胁和受保护的资源间建立多道严密的安全防线。

6 总体要求

本标准从安全管理、安全技术和业务运作三个方面提出征信系统的安全要求。安全管理从安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面提出要求，安全技术从客户端、通信网络、服务器端等方面提出要求，业务运作从系统接入、系统注销、用户管理、信息采集和处理、信息加工、信息保存、信息查询、异议处理、信息跨境流动、研究分析、安全检查与评估等方面提出要求。

征信机构应按照法律法规、国家信息安全主管部门和国务院征信业监督管理部门规定对征信系统进行定级，并根据定级情况达到相应的安全要求。个人征信系统应符合国家信息安全保护等级二级或二级以上标准，企业征信系统由征信机构根据实际情况自行确定安全保护等级。征信系统不同的安全保护等级所应达到的安全要求如下表所示：

表1 征信系统安全保护等级要求

序号	征信系统安全保护等级	管理和技术要求	业务操作要求
1	征信系统安全保护等级为四级	达到GB/T 22239-2008中相应的安全要求	符合本规范的业务操作要求
2	征信系统安全保护等级为三级	同时满足本规范的基本要求和增强要求	符合本规范的业务操作要求

3	征信系统安全保护等级为二级	达到本规范的基本要求	符合本规范的业务操作要求
4	征信系统安全保护等级为一级	达到GB/T 22239-2008中相应的安全要求	符合本规范的业务操作要求

征信机构要提升征信系统自主可控能力，大力推广使用安全可控产品，自行完成征信系统的规范设计、建设开发、运维应急、安全保障等。

7 安全管理

7.1 安全管理制度

征信机构应根据征信系统的建设、运行和管理情况，建立和完善信息安全管理制度，并定期进行评审和修订。

7.1.1 内部管理制度

基本要求：

a） 应制定信息安全工作的总体方针和安全策略，说明本机构安全工作的总体原则、目标、范围和安全框架等。

b） 应建立征信系统建设和运维管理制度，对机房管理、资产安全、设备管理、网络安全和系统安全等方面做出明确规定。

c） 应建立征信系统安全审批流程，系统投入运行、网络系统接入等重大事项由信息安全管理负责人审批，并签字确认。

d） 应对安全管理人员及操作人员执行的重要操作建立操作规程，并进行定期培训。

e） 应建立日常故障处理流程，重要岗位应建立双人负责制。

f） 应建立软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。

g） 应建立数据管理制度，对数据的存储、访问、使用、展示、备份与恢复、传输及样本数据处理等进行规范。

h） 应建立外包服务管理、外部人员访问等方面的管理制度，对外部人员在本机构内的活动进行规范化管理。

i） 应建立安全事件及重大事项报告制度，重大信息安全事故应及时向中国人民银行及其派出机构报告。

j） 应建立突发事件应急预案制度，有效避免事故造成的危害。

k） 应建立信息安全检查制度，定期或根据需要（如可能存在安全隐患时）不定期开展安全自查工作，主动接受和配合中国人民银行及其派出机构的安全检查。

增强要求：

a） 应建立征信系统建设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。

b） 应建立密码使用、变更管理及数据备份与恢复等方面的管理制度，对系统运行维护过程中重要环节的审批与操作等做出明确规定。

c） 应按照ISO/IEC 27001:2013的相关要求建立完善的信息安全管理体系。

7.1.2 安全审计制度

基本要求：

a） 应建立信息安全内部审计制度，定期对可能带来信息安全风险的因素进行审计和评估，个人征信机构每年至少1次，企业征信机构每两年至少1次。
b） 应对安全管理制度的制定和执行情况进行审计，审计内容包括是否按照法律法规和中国人民银行的相关规定建立信息安全管理制度，安全管理制度的执行情况，是否定期对制度进行评审和修订。
c） 应对网络安全、主机安全、应用安全和数据安全等技术安全进行审计，审计内容包括安全配置、设备运行状况、网络流量、重要用户行为、系统异常事件以及重要系统命令的使用等。
d） 应对业务操作进行审计，审计内容包括系统接入和注销、用户管理、信息采集和处理、信息加工、信息保存、异议处理、信息跨境流动等。
e） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；应保护系统中的审计记录，避免受到未预期的删除、修改或覆盖等，保存期至少半年；纸质版审计记录保存期应不少于三年。

增强要求：

a） 应定期委托外部专业审计机构，有重点、有计划的开展信息科技总体风险审计、征信系统专项审计。
b） 在内部审计和外部审计中发现的重大安全隐患应及时向中国人民银行及其派出机构报告。

7.2 安全管理机构

征信机构应成立由高级管理人员及相关部门负责人组成的信息安全领导小组，并指定专门的部门负责信息安全管理工作。

7.2.1 岗位设置

基本要求：

a） 应设立安全主管、信息安全管理员岗位，明确安全主管和信息安全管理员的岗位职责。
b） 应设立系统管理员、网络管理员、数据库管理员等岗位，并定义各个工作岗位的职责。
c） 除科技部门外，其他部门应设置部门计算机安全员。

增强要求：

a） 应通过制度明确安全管理机构各个部门和岗位的职责、分工和技能要求。
b） 应建立数据安全管理组织，明确数据安全管理责任人、数据资产管理人，明确数据安全管理的责任，确保有效落实和推进数据安全的相关工作。

7.2.2 人员配备

基本要求：

a） 应配备安全主管、信息安全管理员、系统管理员、网络管理员、数据库管理员等。
b） 安全主管不能兼任信息安全管理员、网络管理员、系统管理员、数据库管理员等。
c） 信息安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。

增强要求：

a） 关键事务岗位，如信息安全管理员、数据库管理员等，应配备至少两人，且互为A、B角共同管理。

7.2.3 授权和审批

基本要求：

a） 应根据各个部门和岗位的职责明确授权审批部门及批准人。
b） 应针对系统投入运行、网络系统接入、系统变更、重要操作和重要资源的访问等关键活动建立审批流程，由责任人审批后方可进行，对重要活动应建立逐级审批制度。
c） 应记录审批过程并保存审批文档。

增强要求：

a） 应每年审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

7.2.4 沟通和合作

基本要求：

a） 应加强各部门、各岗位之间以及信息安全职能部门内部的合作与沟通。
b） 应加强与同业机构、通讯服务商及监管部门的合作与沟通。

增强要求：

a） 信息安全管理部门应定期召开各职能部门、各岗位人员参加的协调会议，共同协作处理信息安全问题。
b） 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。

7.3 人员安全管理

征信机构应加强人员安全管理，明确不同岗位的职责，规范人员录用、离岗、考核和培训等工作。

7.3.1 安全主管

基本要求：

a） 应选派具有较高计算机水平、业务能力和法律素养的人员担任安全主管。
b） 安全主管可由信息安全管理部门的相关领导担任，也可指定专人担任，主要履行以下职责:
- 组织落实监管部门信息安全相关管理规定和本机构信息安全保障工作。
- 将征信机构信息安全领导小组讨论形成的安全决策，分解为安全任务部署落实。
- 对信息化建设项目中的安全建设方案、安全技术方案或其他安全方案进行审批。
- 对征信机构内部其他信息安全相关管理事项进行审批。

c） 安全主管调离岗位时，应办理交接手续，并履行其调离后的保密义务。

增强要求：

a） 安全主管应加强信息安全知识的学习和技能的掌握，及时关注国内外信息安全动态，为加强和改进本机构的信息安全管理工作提供合理化建议。

7.3.2 信息安全管理员

基本要求：

a） 应选派具有较高计算机水平、业务能力和法律素养的人员担任信息安全管理员。
b） 信息安全管理员每年至少进行一次信息安全方面的技术和业务培训。
c） 信息安全管理员应履行以下职责：
- 在安全主管的指导下，具体落实各项安全管理工作，并协调各部门计算机安全员开展工作。
- 在安全主管的指导下，组织相关人员审核本机构信息化建设项目中的安全方案，组织实施信息安全项目建设，维护、管理信息安全专用设施。
- 在计算机系统应用开发、技术方案设计和实施、集成等工作中提出安全技术方案并组织实施。

- 负责本机构计算机系统部署上线前的安全自测试方案的审核。
- 定期检查网络和征信系统的安全运行状况，组织检查运行操作、备份、机房环境与文档等安全管理情况，发现问题，及时通报和预警，并提出整改意见，统计分析和协调处置信息安全事件。
- 定期组织信息安全宣传教育活动，与相关部门配合开展信息安全检查、评估与培训工作。

d） 信息安全管理员调离原岗位时，应办理交接手续，并履行其调离后的保密义务。

增强要求：

a） 信息安全管理员应加强信息安全知识的学习和技能的掌握，及时关注国内外信息安全动态，为贯彻落实本机构的信息安全策略和方案提出合理化建议。

7.3.3 部门计算机安全员

基本要求：

a） 各部门的计算机安全员应由较熟悉计算机知识的人员担任，并报信息安全管理部门备案，如有变更应及时通报信息安全管理部门。

b） 部门计算机安全员应积极配合信息安全管理员的工作，各部门应优先选派部门计算机安全员参加信息安全技术培训。

c） 部门计算机安全员应履行以下职责：

- 负责配合信息安全管理部门完成本部门计算机病毒防治、补丁升级、非法外联防范、系统故障应急处置、移动存储介质管控等工作。
- 全面负责本部门的信息安全管理工作。负责提出本部门信息安全保障需求，及时与信息安全管理部门沟通本部门信息安全情况。做好信息安全通报工作，发现情况及时向信息安全管理部门报告。
- 负责本部门相关文档资料的安全管理，以及本部门国际互联网、征信系统网络的使用和接入安全管理，组织开展本部门信息安全自查，协助信息安全管理部门完成本机构的信息安全检查工作。

d） 部门计算机安全员调离原岗位时，办理交接手续，并履行其调离后的保密义务。

增强要求：

a） 部门计算机安全员每年应至少参加一次信息安全培训，积极配合信息安全管理员做好本部门的信息安全管理和风险防范知识宣传落实工作。

7.3.4 技术支持人员

基本要求：

a） 内部技术支持人员（本机构正式员工，负责或参与征信机构机房环境、网络、计算机系统等建设、运行、维护的人员，如系统管理员、网络管理员、数据库管理员等）在落实征信系统建设和日常运行维护工作过程中，履行以下职责：

- 严格遵守本机构各项安全保密规定和征信系统安全管理相关制度。
- 严格权限访问，未经业务部门书面授权和本部门领导批准，不得擅自修改征信系统应用设置或修改系统生成的任何业务数据。
- 检测和监控机房、网络、安全设备、计算机系统的安全运行状况，定期进行风险评估、应急演练，发现安全隐患或故障及时报告安全主管、信息安全管理员，并及时响应和处置。

b） 外部技术支持人员（非本机构人员）应严格履行服务外包合同（协议）中的各项安全承诺，在提供技术服务期间，严格遵守征信机构相关安全规定与操作规程。

增强要求：

a） 外部技术支持人员未经业务部门书面授权和所在部门领导批准，不得擅自接触、查看或修改征信系统的应用设置或相关业务数据等；确需接触、查看或修改时，须取得业务部门书面授权和所在部门领导批准，并且在内部技术人员现场陪同下，方可进行。

7.3.5 业务操作人员

基本要求：

a） 业务操作人员（指征信机构内部直接使用征信系统进行业务处理的业务部门工作人员，包括业务管理员和一般业务操作人员）应履行以下职责：

- 严格按照征信机构相关业务操作规程操作、使用征信系统及相关数据，严禁各种违规操作。
- 严格按照征信机构信息安全管理相关规定操作、使用征信系统的业务数据，防止征信信息外泄。
- 妥善保管好征信系统的用户账号和密码，并按要求定期更换密码，禁止将账户和密码提供给他人使用。
- 发现征信系统出现异常，及时向部门计算机安全员报告。
- 定期清理业务操作终端业务数据，不得在业务操作终端上安装与业务处理无关的计算机软件和硬件，不得擅自修改征信系统的运行环境参数。

b） 业务操作按照“权限分设、相互制约”原则，严格进行操作角色划分和授权管理；技术支持人员不得兼任业务操作人员。

增强要求：

a） 业务操作人员应实现A、B角管理。

7.3.6 一般计算机用户

基本要求：

a） 一般计算机用户（指征信机构内部使用接入征信系统网络的计算机及外设的所有人员）应履行以下职责：

- 及时安装计算机病毒防治软件和客户端防护软件，按规定使用移动存储介质，自觉接受部门计算机安全员的指导与管理。
- 不得安装与工作无关的计算机软件和硬件，不得将征信系统相关计算机擅自接入未经授权的网络。

b） 未经信息安全管理部门批准和检测的计算机及外设不得接入征信系统网络。

增强要求：

a） 一般计算机用户不得私自改变计算机用途。

b） 一般计算机用户应统一安装、统一升级及更新计算机病毒防治软件。

7.4 系统建设管理

7.4.1 系统定级

基本要求：

a） 应明确信息系统的边界和安全保护等级。

b） 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由。

增强要求：

a） 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定。

7.4.2 安全方案设计

基本要求：

a） 应根据征信系统的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。

b） 应以书面形式描述对征信系统的安全保护要求、策略和措施等内容，形成系统的安全方案。

c） 应对安全方案进行细化，形成能指导征信系统安全建设、安全产品采购和使用的详细设计方案。

d） 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过征信机构相关领导批准后，正式组织实施。

增强要求：

a） 应指定和授权专门的部门对征信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。

b） 应统一考虑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，并形成配套文件。

c） 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过征信机构相关领导批准后，正式组织实施。

d） 应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。

7.4.3 安全产品采购和使用

基本要求：

a） 应确保安全产品采购和使用符合国家的有关规定。

b） 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。

c） 应指定或授权专门的部门负责安全产品的采购。

增强要求：

a） 应预先对安全产品进行选型测试，确定产品的候选范围。

7.4.4 自行软件开发

基本要求：

a） 应确保开发测试环境与实际运行环境物理分开。

b） 应确保开发人员和测试人员分离，只能使用自制测试数据或已脱密的生产数据进行测试，测试数据和测试结果应受到控制。

c） 应确保开发人员不兼任系统管理员或业务操作人员。

d） 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。

增强要求：

a） 应制定代码编写安全规范，要求开发人员参照规范编写代码。

b） 应确保对程序资源库的修改、更新、发布进行授权和批准。

7.4.5 外包软件开发

基本要求：

a） 应根据开发要求检测软件质量。
b） 应确保开发单位提供软件设计的相关文档和使用指南。
c） 应在软件安装之前检测软件包中可能存在的恶意代码。
d） 应要求开发单位提供软件源代码，并对软件源代码进行“后门”检测。

增强要求：

a） 应具有第三方检测机构的安全检测报告。
b） 应与外包单位签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开。

7.4.6 工程实施

基本要求：

a） 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。
b） 应制定详细的工程实施方案，控制工程实施过程。

增强要求：

a） 应按照工程实施管理制度的相关要求对工程实施全过程进行管理。

7.4.7 测试验收

基本要求：

a） 征信系统测试验收应包含安全性测试相关内容。
b） 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。
c） 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。

增强要求：

a） 应对征信系统测试验收的控制方法和人员行为准则进行书面规定。
b） 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。

7.4.8 系统交付

基本要求：

a） 应制定征信系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。
b） 应对负责征信系统运行维护的技术人员进行相应的技能培训。
c） 应确保提供征信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。

增强要求：

a） 应对征信系统交付的控制方法和人员行为准则进行书面规定。
b） 应指定或授权专门的部门负责征信系统交付的管理工作，并按照管理规定的要求完成征信系统交付工作。

7.4.9 系统备案

基本要求：

a） 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用。
b） 应将系统等级及相关材料报中国人民银行及其派出机构备案。

7.4.10 安全规范测评

基本要求：

a） 征信系统上线运行前，必须进行安全规范测评，运行过程中，应至少每两年对系统进行一次安全规范测评，发现不符合相应标准要求的要及时整改。

b） 个人征信机构应选择具有国家信息安全等级保护测评资质的机构进行安全规范测评，测评报告应在报告出具后20日内上报中国人民银行及其派出机构。

c） 企业征信机构可以选择具有国家信息安全等级保护测评资质的机构进行安全规范测评，也可以自行测评，测评报告报中国人民银行及其派出机构。

增强要求：

a） 应在征信系统发生重大变更时及时对系统进行安全规范测评，发现不符合本规范要求的要及时整改。

b） 在征信系统运行过程中，应至少每年对系统进行一次安全规范测评，发现不符合本规范要求的要及时整改。

c） 应指定或授权专门的部门或人员负责安全规范测评的管理。

7.4.11 外包及安全服务商管理

基本要求：

a） 应与选定的外包及安全服务商签订与安全相关的协议，明确约定相关责任。

b） 应确保选定的外包及安全服务商提供技术支持和服务承诺，必要情况下，应与其签订服务合同。

c） 应确保外包服务受托方的系统访问权限受到约束，涉及敏感操作（如输入用户口令等）应由委托方人员进行操作。

d） 外包服务的受托方进行现场技术支持服务时，应事先提交计划操作内容。委托方应在现场陪同外包服务人员，核对操作内容并准确记录实际操作内容。外包服务的受托方人员不得查看、复制或带离任何敏感信息。

e） 外包服务的受托方应履行服务外包合同（协议）中的各项安全承诺，在提供技术服务期间，应遵守委托方相关安全规定与操作规程。

增强要求：

a） 应制定外包服务应急计划，有效应对外包服务变更。

7.5 系统运维管理

7.5.1 环境管理

基本要求：

a） 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理。

b） 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理。

c） 应按照机房安全管理制度的相关要求，对机房物理访问，物品带进、带出机房和机房环境安全等方面进行管理。

d） 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙、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质文件等。

增强要求：

a） 应指定专人每日对环境设备设施进行巡检，并进行记录。

7.5.2 资产管理

基本要求：

a） 应编制与征信系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

b） 应按照资产安全管理制度的相关要求，明确征信系统资产管理的责任人员或责任部门，并对资产管理和使用的行为进行管理。

增强要求：

a） 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。

b） 应对信息分类与标识方法做出规定，并对信息的使用、传输和存储等进行规范化管理。

7.5.3 介质管理

基本要求：

a） 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。

b） 应对介质归档和查询等过程进行记录，并根据介质存档的目录清单定期盘点。

c） 应对需要送出维修或销毁的介质，首先清除其中的敏感数据或送有相关保密管理责任的部门实施销毁，防止信息泄漏。

d） 非征信机构内部存储介质，未经审核授权不得使用。

增强要求：

a） 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，对介质归档和查询等进行登记记录，并根据介质存档的目录清单定期盘点。

b） 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。

c） 对载有敏感信息存储介质的销毁，应由科技部门进行信息消除、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征信机构内部使用的情况，否则应进行信息的不可恢复性销毁。

d） 应根据数据备份的需要对介质实行异地存储，存储地的环境要求和管理方法应与本地相同。

7.5.4 设备管理

基本要求：

a） 应对征信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。

b） 应按照设备安全管理制度的相关要求，对征信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申报和审批，并进行规范化管理。

c） 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，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。

d） 非征信机构内部设备未经审核授权不得接入内部征信系统。

e） 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。

增强要求：

a） 应严格按照设备安全管理制度的相关要求，对配套设施、软硬件维护等方面进行有效管理，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。

7.5.5 监控管理

基本要求：

a） 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，形成记录并妥善保存。

b） 应组织相关人员每月对监测和报警记录进行分析，发现可疑行为，形成分析报告，并采取必要的应对措施。

增强要求：

a） 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。

7.5.6 网络安全管理

基本要求：

a） 应指定人员对网络进行管理，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。

b） 应严格按照网络安全管理制度的相关要求，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面进行有效管理。

c） 应根据厂家提供的软件升级版本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，同时应做好应急恢复准备。

d） 应每年定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时修补。

e） 应对网络设备的配置文件进行定期备份。

f） 应保证所有与外部系统的连接均得到授权和批准。

增强要求：

a） 应依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。

b） 应监控和检查违反网络安全策略的行为。

7.5.7 系统安全管理

基本要求：

a） 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。

b） 应每年定期对系统进行安全漏洞扫描，对发现的系统安全漏洞及时进行修补。

c） 应安装系统的最新安全补丁程序，在安装系统补丁前，应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。

d） 应通过系统安全管理制度，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做出规定。

e） 应依据操作手册对征信系统进行维护，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。

f） 应至少每月对运行日志和审计数据进行分析，以便及时发现异常行为。

增强要求：

a） 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。

b） 应定期对征信系统进行信息安全风险评估，针对发现的风险，制定相应的风险处置措施，并付诸实施。

c） 应及时关注中国国家信息安全漏洞库（http://www.cnnvd.org.cn/）中发布的漏洞情况，及时排除系统隐患。

7.5.8 恶意代码防范管理

基本要求：

a） 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

b） 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。

c） 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等做出明确规定。

增强要求：

a） 应至少每月一次检查征信系统内各种产品的恶意代码库的升级情况并进行记录，对防病毒产品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汇总报告。

7.5.9 密码管理

基本要求:

a） 应至少每半年修改一次密码，包括网络设备用户密码、操作系统用户密码、数据库用户密码和应用程序用户密码等。密码设置规则应符合以下安全强度的要求：

- 不包含全部或部分用户名（任意连续 3 个字符）。
- 长度至少为 8 个字符。
- 至少包含英文大写字母、小写字母、数字和特殊字符这 4 种类型字符中的 3 种字符。

b） 网络设备、操作系统、数据库和应用程序的超级管理员用户密码要纸质密封交专人保管，而其他普通用户密码可根据本机构实际情况采取必要的安全手段妥善保管。

增强要求：

a） 使用密钥的征信机构应对密钥进行严格管理，包括以下要求：

- 所有密钥资源必须登记造册、严格保管，不得以任何形式非法复制、修改或外泄。在条件许可的情况下，应对其进行定期验证，以确保其可用性和完整性。
- 与密钥资源相关的人员离岗或转岗时应做好交接，密钥资源的管理、保管、制作和使用都应遵循多重控制、角色分离的原则。
- 密钥资源的领用应严格审批，制作、加载、更换、验证维护和销毁必须按照相关管理规定执行。灾备和生产环节的密钥资源移交应经各相关部门审批，并指定专人办理移交手续。

7.5.10 变更管理

基本要求：

a） 征信系统发生变更前，应经过审批，在做好征信数据的备份和恢复工作基础上，方可实施变更，并在实施后向相关人员通告。

b） 应针对征信系统中的重要变更，制定相应的变更方案。

增强要求：

a） 应按照变更管理制度中的相关要求，建立起基于申报和审批的变更控制程序，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。

b） 应按照变更管理制度中的相关要求，对中止变更并从失败变更中恢复的过程进行管理，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。

7.5.11 备份与恢复管理

基本要求：

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等。

b） 应规定备份信息的备份方式、备份频度、存储介质、保存期等。

c） 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略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方法。

增强要求：

a） 应按照数据备份和恢复的制度要求，对备份过程进行记录，备份介质和记录文件应妥善保存。

b） 应每季度执行恢复程序，检查和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。

7.5.12 安全事件处置

基本要求：

a） 应报告所发现的安全弱点和可疑事件，且任何情况下用户均不应尝试验证弱点。

b） 应通过安全事件报告和处置管理制度来明确安全事件类型，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。

c） 应根据安全事件对征信系统产生的影响，采用国家相关管理部门对计算机安全事件等级划分方法，对征信系统计算机安全事件进行等级划分。

d） 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监控事态发展，采取措施避免安全事件发生。

增强要求：

a） 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。

b） 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。

c） 对造成征信系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

7.5.13 应急管理

基本要求：

a） 应在统一的应急预案框架下制定不同安全事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。

b） 应对征信系统相关的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。

增强要求：

a） 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。

b） 应定期对应急预案进行演练和评估，根据不同的应急恢复内容，确定演练的周期，应至少每年演练一次，并及时组织开展预案评估工作。

c） 应定期审查和更新应急预案。

8 安全技术

8.1 客户端安全

8.1.1 客户端程序

基本要求：

a） 征信机构及与之相连的信息提供者、信息使用者应采取有效技术措施，保证客户端所处理的信息、客户端与服务器交互信息的机密性和完整性；征信机构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） 应对征信系统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。

c） 征信系统客户端程序应通过采用密码保护控件等方式，提供客户输入敏感信息的即时加密功能，防范恶意程序获取或篡改敏感信息。

d） 征信系统客户端程序应对用户输入的信息进行数据有效性校验以防止SQL注入、跨站脚本攻击等漏洞。

e） 征信系统客户端程序应提供图形验证码等防止口令暴力破解的手段，同时确保这些保护手段不易被破解、绕过。

f） 征信系统客户端程序出现错误时应提示用户错误代码，并使用文字说明等方式引导用户解决问题。

g） 征信系统客户端程序应保证不在本地的任何地方如硬盘等保存敏感信息，内存中的信息使用后应及时清除。

增强要求：

a） 征信机构应建立定期对客户端程序进行安全检测的机制，或要求接入征信系统的信息提供者、信息使用者定期对客户端程序进行安全检测。

b） 应保护在客户端启动的用于访问征信系统的进程，防止非法程序获取该进程的访问权限。

c） 征信系统客户端程序应采用有效技术措施，防范非法程序获取敏感信息，例如，反屏幕录像技术。

d） 征信系统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。

e） 征信系统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。

f） 征信系统客户端程序应采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

g） 征信系统客户端程序应能检测和防止多个应用实例同时运行。

h） B/S模式客户端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。

8.1.2 客户端环境安全

基本要求：

a） 征信机构应采取有效措施提升本机构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；同时应要求接入征信系统的信息提供者、信息使用者采取有效措施提升本机构客户端环境安全级别。

b） 当征信机构发现其客户端环境存在重大安全缺陷或安全威胁时，应当在门户站点发布警示通知，并通过短信、邮件等方式警示用户。

8.2 通信网络安全

本条内容指信息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。

8.2.1 通讯协议

基本要求：

a） 面向互联网的征信系统，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，保证信息传输的机密性和完整性，例如，使用SSL/TLS、IPSEC和WTLS等协议。

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征信系统与其他应用服务器之间所有连接，保证信息传输的机密性和完整性。

8.2.2 安全认证

基本要求：

a） 征信系统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、可靠的身份认证。

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。

增强要求：

a） 面向互联网的征信系统Web服务器应使用获得工信部《电子认证服务许可证》的电子认证服务机构颁发的CA证书及认证服务。

b） 应确保客户获取的面向互联网的征信系统Web服务器的根证书为合法电子认证服务机构所颁发，且真实有效，可采用的方法包括但不限于：在客户注册征信系统时分发根证书，或将根证书集成在客户端控件下载包中分发等。

c） 对于提供批量信息服务的重要客户端，应采用双向身份认证。双向身份认证指不仅服务器对客户端身份进行认证，客户端也应认证服务器的身份。

8.3 服务器端安全

8.3.1 物理安全

基本要求：

a） 物理位置的选择

- 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。

b） 物理访问控制

- 机房出入口应安排专人值守，控制、鉴别和记录进入的人。
- 需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。

c） 防盗窃和防破坏

- 应将主要设备放置在机房内。
- 应将设备或主要部件进行固定，并设置明显的不易除去的标记。
- 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。
- 应对介质分类标识，存储在介质库或档案室中。
- 主机房应安装必要的防盗报警设施和监控报警系统。

d） 防雷击

- 机房建筑应设置避雷装置。
- 机房应设置交流电源地线。

e） 防火

- 机房应设置灭火设备和火灾自动报警系统。

f） 防水和防潮
- 水管安装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。

g） 防静电
- 关键设备应采用必要的接地防静电措施。

h） 温湿度控制
- 机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

i） 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。
- 应提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求。

j） 电磁防护
- 电源线和通信线缆应隔离铺设，避免互相干扰。

增强要求：

a） 物理位置的选择
- 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

b） 物理访问控制
- 应对机房划分区域管理，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、鉴别和记录进入的人员。

c） 防盗窃和防破坏
- 应利用光、电等技术设置机房防盗报警系统。

d） 防雷击
- 应设置防雷保安器，防止感应雷。

e） 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。

f） 防水和防潮
- 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。

g） 防静电
- 机房应采用高架防静电地板。

h） 电力供应
- 应设置冗余或并行的电力电缆线路为计算机系统供电。
- 应建立备用供电系统。

i） 电磁防护
- 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

8.3.2 网络安全

基本要求：

a） 结构安全
- 应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。

- 应保证接入网络和核心网络的带宽满足业务高峰期需要。
- 应绘制与当前运行情况相符的网络拓扑结构图。
- 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

b） 访问控制

- 应在网络边界部署访问控制设备，启用访问控制功能。
- 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，控制粒度为网段级。
- 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。
- 应限制具有拨号访问权限的用户数量。

c） 安全审计

- 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。
- 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

d） 边界完整性检查

- 应能够对内部网络中出现的内部用户未经准许私自联接到外部网络的行为进行检查。

e） 入侵防范

- 应在网络边界处监视以下攻击行为：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。

f） 网络设备防护

- 应对登录网络设备的用户进行身份鉴别。
- 应对网络设备的管理员登录地址进行限制。
- 网络设备用户的标识应唯一。
- 身份鉴别信息应具有不易被冒用的特点，口令应符合“6.5.9 密码管理”的相关要求，有效期最长为六个月。
- 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。
- 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。

增强要求：

a） 结构安全

- 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径。
- 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。
- 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

b） 访问控制

- 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。
- 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制。
- 应在会话处于非活跃状态一定时间或会话结束后终止访问连接。
- 应限制网络最大流量及网络连接数。
- 重要网段应采取技术手段防止地址欺骗。

- 应对实施查询的客户端网络地址等信息进行识别与记录。

c） 安全审计
- 应能够根据记录数据进行分析，并生成审计报表。
- 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

d） 边界完整性检查
- 应能够对非授权设备私自联到内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。
- 应能够对内部网络用户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。

e） 入侵防范
- 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

f） 恶意代码防范
- 应在网络边界处对恶意代码进行检测和清除。
- 应维护恶意代码库的升级和检测系统的更新。

g） 网络设备防护
- 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来进行身份鉴别。
- 应实现设备特权用户的权限分离。

8.3.3 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系统的用户进行身份标识和鉴别。
- 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应符合“6.5.9 密码管理”的相关要求，有效期最长为六个月。
- 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。
- 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。
- 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

b） 访问控制
- 应启用访问控制功能，依据安全策略控制用户对资源的访问。
- 应根据管理用户的角色分配权限，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。
- 应实行操作系统和数据库系统特权用户的权限分离。
- 应限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。
- 应及时删除或禁用多余的、过期的账户，避免共享账户、过期账户的使用。

c） 安全审计
- 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户。
- 审计内容应包括用户权限、重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全操作。
- 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。
- 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

d） 入侵防范

- 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，并通过设置升级服务器等方式保持系统补丁及时得到更新。

e） 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。
- 应根据安全策略设置登录终端的操作超时锁定。
- 应限制单个用户对系统资源的最大或最小使用限度。
- 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。

增强要求：

a） 身份鉴别

- 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。

b） 安全审计

- 应能够根据记录数据进行分析，并生成审计报表。
- 应保护审计进程，避免发生未预期的中断。

c） 入侵防范

- 应能够检测到对重要服务器进行入侵的行为，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。

d） 资源控制

- 系统的服务水平降低到预先规定的最小值时，应能够进行检测和报警。

8.3.4 应用安全

基本要求：

a） 身份鉴别

- 应提供专用的登录控制模块对登录用户进行身份标识和鉴别。
- 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。
- 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。
- 用户身份鉴别信息应符合“6.5.9 密码管理”的相关规定，有效期最长为六个月。

b） 访问控制

- 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。
- 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。
- 应由授权主体配置访问控制策略，并严格限制默认账户的访问权限。
- 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。

c） 安全审计

- 应提供覆盖到每个用户的安全审计功能，对用户权限及应用系统重要安全事件进行审计；
- 应保证无法删除、修改或覆盖审计记录。
- 审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等。

d） 通信完整性

- 应采用校验码技术保证通信过程中数据的完整性。

e） 通信保密性

- 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。

- 应对通信过程中的敏感信息字段进行加密。

f） 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。
- 在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施。

g） 资源控制

- 当应用系统通信双方中的一方在一段时间内未作任何响应时，另一方应能够自动结束会话。
- 应能够对应用系统的最大并发会话连接数进行限制。
- 应能够对单个账户的多重并发会话进行限制。

增强要求：

a） 身份鉴别

- 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

b） 访问控制

- 应具有对重要信息资源设置敏感标记的功能。
- 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。

c） 安全审计

- 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。
- 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

d） 剩余信息保护

- 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。
- 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） 通信完整性

- 应采用密码技术保证通信过程中数据的完整性。

f） 通信保密性

- 应对通信过程中的整个报文或会话过程进行加密。

g） 抗抵赖

- 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能。
- 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

h） 软件容错

- 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。

i） 资源控制

- 应能够对一个时间段内可能的并发会话连接数进行限制。
- 应能够对一个访问账户或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。

8.3.5 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

- 征信系统应采用加密或其他有效措施实现系统管理数据和鉴别信息传输保密性。
- 征信系统应采用加密或其他保护措施实现系统管理数据和鉴别信息存储保密性。

c） 备份和恢复

- 应提供本地数据备份与恢复功能，增量数据备份至少每天一次，完全数据备份至少每周一次，备份介质场外存放。
- 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

增强要求：

a） 数据保密性

- 征信系统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。
- 征信系统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。

b） 备份和恢复

- 数据备份应实现实时本地备份。
- 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。
- 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。
- 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

9 业务运作

9.1 系统接入

系统接入应满足以下要求：

a） 系统接入是指征信机构与信息提供者、信息使用者协议约定，通过接口规范接收信息提供者提供的征信业务数据，或者向信息使用者提供查询服务。通过非接口规范方式接收征信业务数据，或提供查询服务的征信机构，不适用本条规定。

b） 征信机构应当建立外部机构接入征信系统的管理办法，明确信息提供者、信息使用者的接入条件、提交的申请材料、申请和审核程序等。

c） 征信机构应当对外部机构申请接入征信系统的必要性、业务系统及业务现状、安全管理水平、网络条件等是否符合前款规定进行综合评估，确认符合条件的方可接入征信系统。

d） 征信机构应当在测试环境下对信息提供者、信息使用者的接口规范程序、网络条件等进行测试，测试通过后方可接入征信系统生产环境。

9.2 系统注销

系统注销应满足以下要求：

a） 征信机构应当建立外部机构从征信系统注销的管理办法，明确信息提供者、信息使用者从征信

系统注销的流程、提交的材料、时限要求、已提供信息的后续处理以及征信机构主动注销操作等事项。

b） 征信机构应当按照规定流程对信息提供者、信息使用者的注销申请进行审核，确认申请机构不存在未结清业务数据、异议信息等遗留问题，审核通过后再进行注销操作。

c） 停止经营活动且营业执照等已注销，但是不主动申请从征信系统注销的机构，征信机构经核实后可发起主动注销操作。

9.3 用户管理

用户管理包括内部用户管理和外部用户管理，具体要求如下：

a） 内部用户管理

- 征信机构应当建立征信系统内部用户管理制度，明确各类内部用户的申请、创建、变更、终止及用户操作等相关要求，关键岗位不得互相兼任。

b） 外部用户管理

- 征信机构应当要求通过接口方式接入征信系统的外部机构（信息提供者、信息使用者）制定用户管理制度，明确管理员用户、数据查询用户、数据报送用户、异议处理用户等的职责和权限，建立各类用户的操作规程。
- 征信机构应当规范管理通过非接口方式访问征信系统的外部用户，合理配置其访问权限，采取必要措施防范外部用户操作风险。

c） 征信机构应当建立征信系统监控制度，对内部用户和外部用户的异常操作行为进行监控，必要时采取措施暂停违规用户权限，保障征信系统安全运行。

d） 征信机构应当定期对内外部用户的设置、用户权限、用户操作及用户管理制度的执行情况等进行检查。

9.4 信息采集和处理

信息采集和处理包括接口规范方式和非接口规范方式两种，具体要求如下：

9.4.1 接口规范方式

a） 征信机构应当制定合适的信息采集流程和处理策略，明确信息采集的范围、内容、方式和频次、报文接收与反馈、意外事件处理及相关岗位职责等，合理控制报文加载顺序、进度，确保征信信息及时加载入库。

b） 征信机构接收信息提供者按照征信系统接口规范生成的征信业务数据报文，记录报文登记信息，自动进行解密和加载处理，业务操作人员应及时跟踪报文的接收和处理情况。

c） 征信系统对征信业务数据报文进行处理时，加载成功的信息，按照征信系统接口规范生成反馈报文，反馈给信息提供者。

d） 征信系统对征信业务数据报文进行处理时，加载异常的信息，征信系统应将错误信息反馈给信息提供者，由其进行重报。征信机构业务操作人员应及时联系信息提供者相关人员，进行跟踪处理。

9.4.2 非接口规范方式

a） 征信机构应当制定通过手工录入、介质导入等非接口方式采集信息的具体流程，明确信息采集范围、内容、方式和频次、信息审核、错误数据修改及相关岗位职责等。

b） 征信机构应当对信息来源和内容进行审核，审核通过后再发起手工录入、介质导入等操作。

c） 征信系统应当对手工录入、介质导入的征信业务数据进行合法性校验，无法正常录入征信系统的信息，由业务操作人员通过专门数据修改流程进行核查处理。

9.5 信息加工

信息加工应满足以下要求：

a） 征信机构对采集的信息进行整理，形成信用报告等基础征信产品，应当遵循客观性原则，不得擅自更改原始数据。

b） 征信机构对采集的信息进行加工，形成信用评分、信用评级及其他增值类征信产品，不得擅自更改原始数据；同时，征信机构还应对信息加工所采用的方法和模型作出说明，便于信息使用者、信息主体理解和接受。

9.6 信息保存

信息保存应满足以下要求：

a） 征信系统应在一定时期内保存对外交互过程中产生的信息文件，如信息提供者的原始报文文件、反馈文件、信息查询文件等；同时应保存交互时间、交互对方系统信息、交互是否成功等日志信息，以便事后可追查；对征信系统的交互信息文件和日志文件进行严格的权限控制和操作审计，防止个人信息泄露。

b） 征信系统采集的个人不良信息应当按照法律法规规定的期限进行保存；超过保存期限的个人不良信息，应当从征信系统中删除，或者进行去标识化处理，移入非生产数据库保存。

c） 征信机构应当采取有效措施，确保个人不良信息去标识化处理后，个人身份不被直接或间接识别。

9.7 信息查询

信息查询包括单笔查询和批量查询两种方式，具体要求如下：

a） 单笔信息查询

- 征信系统应当对查询用户输入的查询条件设置一定的校验规则，并在用户查询时进行有效性检查。
- 征信系统应当记录查询用户所属机构、查询用户、查询时间、查询原因、被查询对象等信息。

b） 批量信息查询

- 查询机构应当按照规定的格式填写批量查询请求文件，请求文件的内容至少应包括查询用户所属机构、查询用户、查询时间、查询原因、查询内容、被查询对象、查询请求记录数等，征信系统应当对上述内容予以记载。
- 征信机构应当通过专线、加密通道或专用存储设备等安全、可靠的方式将批量查询结果文件反馈给查询机构。

c） 信息使用者发生异常查询的，征信机构可以采取暂停查询权限等紧急措施，并及时核查异常查询产生的原因。

9.8 异议处理

异议处理应满足以下要求：

a） 征信机构应当建立异议处理制度，对异议申请与受理、内外部核查、异议信息更正等事项作出明确规定。

b） 异议处理人员查询信息主体信用报告，应当严格按照异议处理制度及流程执行，并进行登记，不得将信用报告用于异议处理以外的用途。

c） 征信机构应当对异议信息核查情况予以记载。核查无误的，不得更改相关信息；核查有误的，按照规定予以更正，或者通知信息提供者提供更新后的信息；核查后仍不能确认的，应允许信息主体提出“个人声明”，并在征信系统中记载。

9.9 信息跨境流动

信息跨境流动应满足以下要求：

a） 征信机构在中国境内开展征信业务及相关活动，其生产数据库、备份数据库应设在中国境内。

b） 征信机构对采集的信息进行整理、保存和加工等活动，应当在中国境内进行，不得通过网络或携带存储介质出境等方式，将采集的信息传输至境外。

c） 征信机构向境外组织和个人提供信息，应当遵守法律法规和中国人民银行的有关规定。

9.10 研究分析

研究分析应满足以下要求：

a） 征信机构基于理论研究、模型设计、产品开发等目的使用个人信息的，应当以汇总统计数据或者不能识别个人身份的方式进行。

b） 征信机构的研究成果只能在个人身份不被识别的情况下予以披露、发表或者传播。

9.11 安全检查与评估

安全检查与评估应满足以下要求：

a） 征信机构应当定期检查征信系统的安全建设和运行情况，可通过自评估或委托评估方式对征信系统进行安全评估，分析、发现并解决征信系统在管理制度、技术措施和业务操作等方面存在的问题，保障征信系统安全运行和信用信息合规使用。

b） 征信机构应建立信息泄漏应急处置制度，发生或者有可能发生重大信息泄露事件时，应当立即采取必要措施，避免损害扩大，并向中国人民银行及其派出机构报告。