ICS 03.060
A 11

JR

# 中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0071.2—2020
代替 JR/T 0071—2012

# 金融行业网络安全等级保护实施指引
# 第2部分：基本要求

Implementation guidelines for classified protection of cybersecurity of financial industry—Part 2：Basic requirements

2020-11-11 发布　　2020-11-11 实施

中国人民银行　　发布

# 目　　次

前言 III
引言 V
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 6
5 网络安全等级保护概述 6
5.1 等级保护对象 6
5.2 不同级别的安全保护能力 7
5.3 安全通用要求和安全扩展要求 7
5.4 金融行业增强性安全要求 7
6 网络安全保障框架 8
6.1 概述 8
6.2 技术体系 9
6.3 管理体系 10
7 第二级安全要求 11
7.1 安全通用要求 11
7.2 云计算安全扩展要求 22
7.3 移动互联安全扩展要求 24
7.4 物联网安全扩展要求 25
8 第三级安全要求 27
8.1 安全通用要求 27
8.2 云计算安全扩展要求 45
8.3 移动互联安全扩展要求 48
8.4 物联网安全扩展要求 50
9 第四级安全要求 53
9.1 安全通用要求 53
9.2 云计算安全扩展要求 72
9.3 移动互联安全扩展要求 76
9.4 物联网安全扩展要求 78
附录 A （规范性附录） 关于金融行业安全通用要求、安全扩展要求和增强性安全要求的选择和使用81
附录 B （规范性附录） 关于等级保护对象整体安全保护能力的要求 86
附录 C （规范性附录） 等级保护安全框架和关键技术使用要求 87

附录D （资料性附录） 云计算应用场景说明.....89
附录E （资料性附录） 移动互联应用场景说明.....91
附录F （资料性附录） 物联网应用场景说明.....93
附录G （资料性附录） 大数据应用场景说明.....94
附录H （资料性附录） 敏感数据和个人金融信息类别.....99
参考文献.....101

# 前　言

JR/T 0071《金融行业网络安全等级保护实施指引》分为六部分构成：

——第1部分：基础和术语；

——第2部分：基本要求；

——第3部分：岗位能力要求和评价指引；

——第4部分：培训指引；

——第5部分：审计要求；

——第6部分：审计指引。

本部分为JR/T 0071的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0071—2012《金融行业信息系统信息安全等级保护实施指引》，与JR/T 0071—2012相比，主要技术变化如下：

——增加了“网络安全等级保护概述”（见第5章）；

——修改了“网络安全保障框架”（见第6章，2012年版第5章）；

——修改了“第二级安全要求”的“安全通用要求”中“安全物理环境”“安全通信网络”“安全区域边界”“安全计算环境”“安全管理中心”“安全管理制度”“安全管理机构”“安全管理人员”“安全建设管理”“安全运维管理”相关要求项（见7.1，2012年版6.1）；

——增加了“第二级安全要求”中“云计算安全扩展要求”“移动互联安全扩展要求”“物联网安全扩展要求”（见第7章）；

——修改了“第三级安全要求”的“安全通用要求”中“安全物理环境”“安全通信网络”“安全区域边界”“安全计算环境”“安全管理中心”“安全管理制度”“安全管理机构”“安全管理人员”“安全建设管理”“安全运维管理”相关要求项（见8.1，2012年版6.2）；

——增加了“第三级安全要求”中“云计算安全扩展要求”“移动互联安全扩展要求”“物联网安全扩展要求”（见第8章）；

——修改了“第四级安全要求”的“安全通用要求”中“安全物理环境”“安全通信网络”“安全区域边界”“安全计算环境”“安全管理中心”“安全管理制度”“安全管理机构”“安全管理人员”“安全建设管理”“安全运维管理”相关要求项（见9.1，2012年版6.3）；

——增加了“第四级安全要求”中“云计算安全扩展要求”“移动互联安全扩展要求”“物联网安全扩展要求”（见第9章）；

——删除了“等级保护实施措施”（2012年版附录A）；

——修改了“金融行业安全要求的选择和使用说明”（见附录A，2012年版附录B）；

——增加了“关于等级保护对象整体安全保护能力的要求”（见附录B）；

——增加了“等级保护安全框架和关键技术使用要求”（见附录C）；

——增加了“云计算应用场景说明、不同云服务模式下安全管理责任主体”（见附录D）；

——增加了“移动互联应用场景说明”（见附录E）；

——增加了“物联网应用场景说明”（见附录F）；

——增加了“大数据应用场景说明”（见附录G）；

——增加了“敏感数据和个人金融信息类别”（见附录H）。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC 180）归口。

本部分起草单位：中国人民银行科技司、中国银行保险监督管理委员会统计信息与风险监测部、中国金融电子化公司、北京中金国盛认证有限公司、银行卡检测中心、中国平安保险（集团）股份有限公司、北京天融信网络安全技术有限公司、华为技术有限公司、中国人民银行营业管理部、中国人民银行广州分行、中国人民银行数字货币研究所、中国人民银行金融信息中心、国泰君安证券有限公司、中国人寿保险股份有限公司、中国人民财产保险股份有限公司、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、交通银行股份有限公司、蚂蚁科技集团股份有限公司、中国金融认证中心、亚信安全科技有限公司。

本部分主要起草人：李伟、陈立吾、沈筱彦、车珍、曲维民、昝新、夏磊、方怡、张海燕、唐辉、李凡、王海涛、张璐、邓昊、潘丽扬、侯漫丽、孙国栋、刘文娟、赵方萌、乔媛、崔莹、陈雪峰、马成龙、杜巍、李瑞锋、刘书元、渠韶光、高强裔、李博文、李金华、金朝、任勇强、赵江、于惊涛、胡珊、谢虹、杨剑、李建彬、于国强、肖松、白阳、张宇、赵华、薛金川、陈喜鹏、穆长春、狄刚、吕毅、何军、袁慧萍、陈凯辉、郭松青、李锐、肖鹏哲、赵旭、张耀峰、黄春芳、杨晨、王衍锋、高红英、陈雪秀、韩涛、叶宁、俞国栋、姜志辉、李松涛、隆峰、许定航、陆霖、郭涛。

本部分所代替标准的历次版本发布情况为：

——JR/T 0071—2012。

# 引　言

网络安全等级保护是国家网络安全保障工作的一项基本制度，金融行业重要系统关系到国计民生，是国家网络安全重点保护对象，因此需要一系列适合金融行业的等级保护标准体系作为支撑，以规范和指导金融行业等级保护工作的实施。随着云计算、移动互联、物联网、大数据等新技术的广泛应用，金融机构正根据自身发展的需要，持续推进 IT 架构的转型。为适应新技术、新应用和新架构情况下金融行业网络安全等级保护工作的开展，现对 JR/T 0071 进行修订。修订后的 JR/T 0071 依据国家网络安全等级保护相关要求，为金融行业的网络安全建设提供方法论、具体的建设措施及技术指导，完善金融行业网络安全等级保护体系，更好适应新技术在金融行业的应用。

# 金融行业网络安全等级保护实施指引
# 第2部分：基本要求

## 1 范围

本部分规范了金融行业网络安全保障框架和不同安全等级对应的安全要求。

本部分适用于指导金融机构、测评机构和金融行业网络安全等级保护的主管部门实施网络安全等级保护工作。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。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—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32400—2015 信息技术 云计算 概览与词汇

GM/T 0054—2018 信息系统密码应用基本要求

JR/T 0171—2020 个人金融信息保护技术规范

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**网络安全 cybersecurity**

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/T 22239—2019，定义3.1]

3.2

**定级系统 classified system**

已确定安全保护等级的系统。

注1：定级系统分为第一级、第二级、第三级、第四级和第五级系统。

注2：改写GB/T 25070—2019，定义3.2。

3.3

**安全保护能力** security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

[GB/T 22239—2019，定义3.2]

3.4

**定级系统安全保护环境** security environment of classified system

由安全计算环境、安全区域边界、安全通信网络和（或）安全管理中心构成的对定级系统进行安全保护的环境。

[GB/T 25070—2019，定义3.3]

3.5

**安全计算环境** security computing environment

对定级系统的信息进行存储、处理及实施安全策略的相关部件。

[GB/T 25070—2019，定义3.4]

3.6

**安全区域边界** security area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

[GB/T 25070—2019，定义3.5]

3.7

**安全通信网络** security communication network

对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。

[GB/T 25070—2019，定义3.6]

3.8

**安全管理中心** security management center

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台或区域。

[GB/T 25070—2019，定义3.7]

3.9

**跨定级系统安全管理中心** security management center for cross classified system

对相同或不同等级的定级系统之间互联的安全策略及安全互联部件上的安全机制实施统一管理的平台或区域。

[GB/T 25070—2019，定义3.8]

3.10

**定级系统互联** classified system interconnection

通过安全互联部件和跨定级系统安全管理中心实现的相同或不同等级的定级系统安全保护环境之间的安全连接。

[GB/T 25070—2019，定义3.9]

3.11

**云计算 cloud computing**

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

注：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。

[GB/T 31167—2014，定义3.1]

3.12

**云服务 cloud service**

通过云计算已定义的接口提供的一种或多种能力。

[GB/T 32400—2015，定义 3.2.8]

3.13

**云服务商 cloud service provider**

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络交付云计算的资源。

[GB/T 31167—2014，定义 3.3]

3.14

**云服务客户 cloud service customer**

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31168—2014，定义 3.4]

3.15

**云计算平台/系统 cloud computing platform/system**

云服务商提供的云计算基础设施及其上的服务软件的集合。

[GB/T 22239—2019，定义 3.6]

3.16

**团体云 community cloud**

由一组特定的云服务客户使用和共享，且资源被云服务商或使用者控制的一种云部署和云服务模式。

3.17

**基础设施即服务 infrastructure as a service；IaaS**

云服务商向云服务客户提供可动态申请或释放的计算资源、存储资源、网络资源等基础设施的服务模式。

3.18

**平台即服务 platform as a service；PaaS**

云服务商向云服务客户提供应用软件所需的支撑平台，供云服务客户在此基础上开发和提供相关应用的服务模式。

3.19

**软件即服务 software as a service；SaaS**

云服务商向云服务客户提供运行在云基础设施之上的应用软件的服务模式。

3.20

**虚拟机 virtual machine**

通过各种虚拟化技术，为用户提供的与原有物理服务器相同的操作系统和应用程序运行环境的统称。

注：虚拟机通常使用物理服务器的资源，在用户看来其与物理服务器的使用方式完全相同。

3.21

**资源池 resource pool**

按照一定规则可从中获取、释放、或回收资源的物理资源或虚拟资源的集合。

注：资源包括物理机、虚拟机、物理存储资源、虚拟存储资源、物理网络资源和虚拟网络资源等。

3.22

**宿主机 host machine**

运行虚拟机监视器的物理服务器。

[GB/T 22239—2019，定义 3.8]

3.23

**敏感数据 sensitive data**

一旦泄露可能会对用户或金融机构造成损失的数据。

3.24

**个人金融信息 personal financial information**

金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

注：个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

[JR/T 0171—2020，定义 3.2]

3.25

**个人金融信息主体 personal financial information subject**

个人金融信息所标识的自然人。

[JR/T 0171—2020，定义 3.4]

3.26

**移动互联 mobile communication**

采用无线通信技术将移动终端接入有线网络的过程。

[GB/T 22239—2019，定义 3.9]

3.27

**移动终端 mobile device**

在移动业务中使用的终端设备，包括智能手机、平板电脑、个人电脑等通用终端和专用终端设备。

[GB/T 22239—2019，定义 3.10]

3.28

**无线接入设备 wireless access device**

采用无线通信技术将移动终端接入有线网络的通信设备。

[GB/T 22239—2019，定义 3.11]

3.29

**无线接入网关 wireless access gateway**

部署在无线网络与有线网络之间，对有线网络进行安全防护的设备。

[GB/T 22239—2019，定义 3.12]

3.30

**移动应用软件 mobile application**

针对移动终端开发的应用软件。

[GB/T 22239—2019，定义 3.13]

3.31

**移动终端管理系统 mobile device management system**

用于进行移动终端设备管理、应用管理和内容管理的专用软件，包括客户端软件和服务端软件。

[GB/T 22239—2019，定义 3.14]

3.32

**物联网 internet of things；IOT**

将感知节点设备（含 RFID）通过互联网等网络连接起来构成的一个应用系统，其融合信息系统和物理世界实体，是虚拟世界与现实世界的结合。

注：改写 GB/T 22239—2019，定义 3.15。

3.33

**网关节点设备 gateway node**

将感知节点设备所采集的数据传输到数据处理中心的关键出口，连接传统信息网络（有线网、移动网等）和传感网的设备。

注：简单的感知层网关只是对感知数据的转发（因电力充足），而智能的感知层网关可以包括对数据进行适当处理、数据融合等业务。

3.34

**感知节点设备 sensor node**

物联网系统的最终端设备或器件，能够通过有线、无线方式发起或终结通信，采集物理信息和/或接受控制的实体设备。

注：感知节点设备也叫感知终端设备（end sensor）、终端感知节点设备（end sensor node）。

3.35

**感知网关节点设备 sensor layer gateway**

将感知节点所采集的数据进行汇总、适当处理或数据融合，并进行转发的装置。

[GB/T 22239—2019，定义 3.17]

3.36

**动态口令 one-time-password（OTP）；dynamic password**

基于时间、事件等方式动态生成的一次性口令。

[GM/T 0054—2018，定义 3.1]

3.37

**大数据 big data**

具有数量巨大、种类多样、流动速度快、特征多变等特性，并且难以用传统数据体系结构和数据处理技术进行有效组织、存储、计算、分析和管理的数据集。

3.38

**大数据平台 big data platform**

采用分布式存储和计算技术，提供大数据的访问和处理，支持大数据应用安全高效运行的软硬件集合。

注：大数据平台通常包括监视大数据的存储、输入/输出、操作控制等大数据服务软硬件基础设施。

3.39

**接口服务 interface service**

依托应用程序编程接口技术实现内部与外部互联的服务模式。

## 4 缩略语

下列缩略语适用于本文件。

AP：无线访问接入点（Wireless Access Point）

API：应用程序编程接口（Application Programming Interface）

CPU：中央处理单元（Central Processing Unit）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）

DoS：拒绝服务（Denial of Service）

IP：互联网协议（Internet Protocol）

IT：信息技术（Information Technology）

RFID：射频识别（Radio Frequency Identification）

SSID：服务集标识（Service Set Identifier）

SQL：结构化查询语言（Structured Query Language）

TCB：可信计算基（Trusted Computing Base）

VPN：虚拟专用网络（Virtual Private Network）

WEP：有线等效加密（Wired Equivalent Privacy）

WPS：WiFi保护设置（WiFi Protected Setup）

XSS：跨站脚本攻击（Cross-Site Scripting）

## 5 网络安全等级保护概述

### 5.1 等级保护对象

等级保护对象是指网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相

关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网和采用移动互联技术的系统等。等级保护对象根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为五个安全保护等级。

等级保护对象的安全保护等级确定方法见 GB/T 22240—2020。

## 5.2 不同级别的安全保护能力

不同级别的等级保护对象应具备的基本安全保护能力如下：

第一级安全保护能力：应能够防护免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能。

第二级安全保护能力：应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。

第四级安全保护能力：应能够在统一安全策略下防护免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。

第五级安全保护能力：在此不做说明。

## 5.3 安全通用要求和安全扩展要求

由于业务目标的不同、使用技术的不同、应用场景的不同等因素，不同的等级保护对象会以不同的形态出现，表现形式可能称之为基础信息网络、信息系统（包含采用移动互联等技术的系统）、云计算平台/系统、大数据平台/系统、物联网系统等。形态不同的等级保护对象面临的威胁有所不同，安全保护需求也会有所差异。为了便于实现对不同级别的和不同形态的等级保护对象的共性化和个性化保护，等级保护要求分为安全通用要求和安全扩展要求。

安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，应根据安全保护等级实现相应级别的安全通用要求；安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景选择性实现安全扩展要求。安全通用要求和安全扩展要求共同构成了对等级保护对象的安全要求。安全要求的选择见附录 A，整体安全保护能力的要求见附录 B 和附录 C。

本部分针对云计算、移动互联、物联网、大数据系统提出了安全扩展要求。云计算应用场景参见附录 D，移动互联应用场景参见附录 E，物联网应用场景参见附录 F，大数据应用场景参见附录 G。对于采用其他特殊技术或处于特殊应用场景的等级保护对象，应在安全风险评估的基础上，针对安全风险采取特殊的安全措施作为补充。

## 5.4 金融行业增强性安全要求

本部分新增“金融行业增强性安全要求（F 类）”，金融行业增强性安全要求在结合金融行业相关规定的基础上对等级保护要求进行补充和完善，F2 表示二级增强性安全要求，F3 表示三级增强性

安全要求，F4 表示四级增强性安全要求。

## 6 网络安全保障框架

### 6.1 概述

以国家等级保护要求为原则，以金融行业特点为基础，形成了兼顾技术与管理的金融行业网络安全保障总体框架，如图 1 所示。金融行业网络安全保障总体框架包含两项要求和两个体系，遵循技管交互、综合保障的原则。

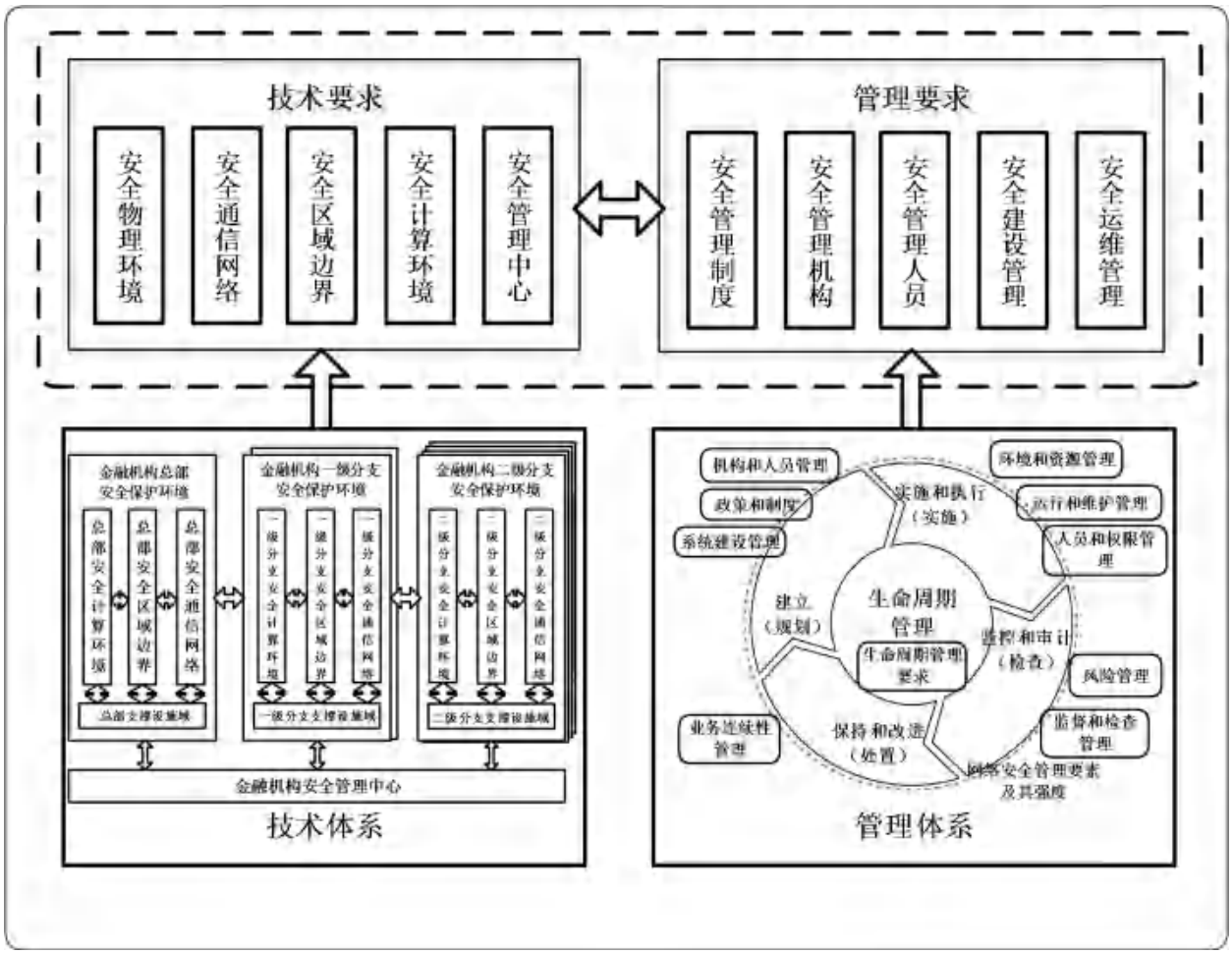



**图 1 网络安全保障总体框架图**

两项要求指由技术要求和管理要求综合形成的保障要求，技术要求涉及安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五方面要求；管理要求涉及安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五方面要求。

两个体系指由技术体系和管理体系综合形成的保障体系。技术体系以“一个中心，三重防护”为核心理念，划分安全计算环境、安全区域边界、安全通信网络与安全管理中心，并且结合金融行业的系统与业务现状，进行分区分域保护；管理体系遵从生命周期法则，从建立、实施和执行、监控和审计、保持和改进四个过程进行科学化的管理，通过循环改进的思路形成“生命环”的管理方法。

技管交互指技术要求与管理要求的交融以及技术体系与管理体系的互补，从安全保障要求和安全保障方法两方面体现技术与管理并重的基本思想。

综合保障指该框架通过对保障要求和保障方法的综合考虑，通过技术与管理的有效结合，在遵循国家等级保护要求的前提下，满足金融行业的业务特殊性要求。

## 6.2 技术体系

金融行业网络安全等级保护基本要求结合GB/T 25070—2019中的安全域模型，将“安全域纵深防护”“多层次立体防御”和“网络安全等级保护”等安全防护思想相结合，建立金融行业网络安全保障技术体系模型。依据金融行业的组织结构、网络架构将每个机构作为一个整体保护对象，设计金融机构网络安全保障框架，如图2所示，总部和各个分支机构都是独立的安全域，每个安全域又细分安全计算环境域、安全区域边界、安全通信网络和安全支撑设施域，各金融机构根据本机构结构情况参考执行。

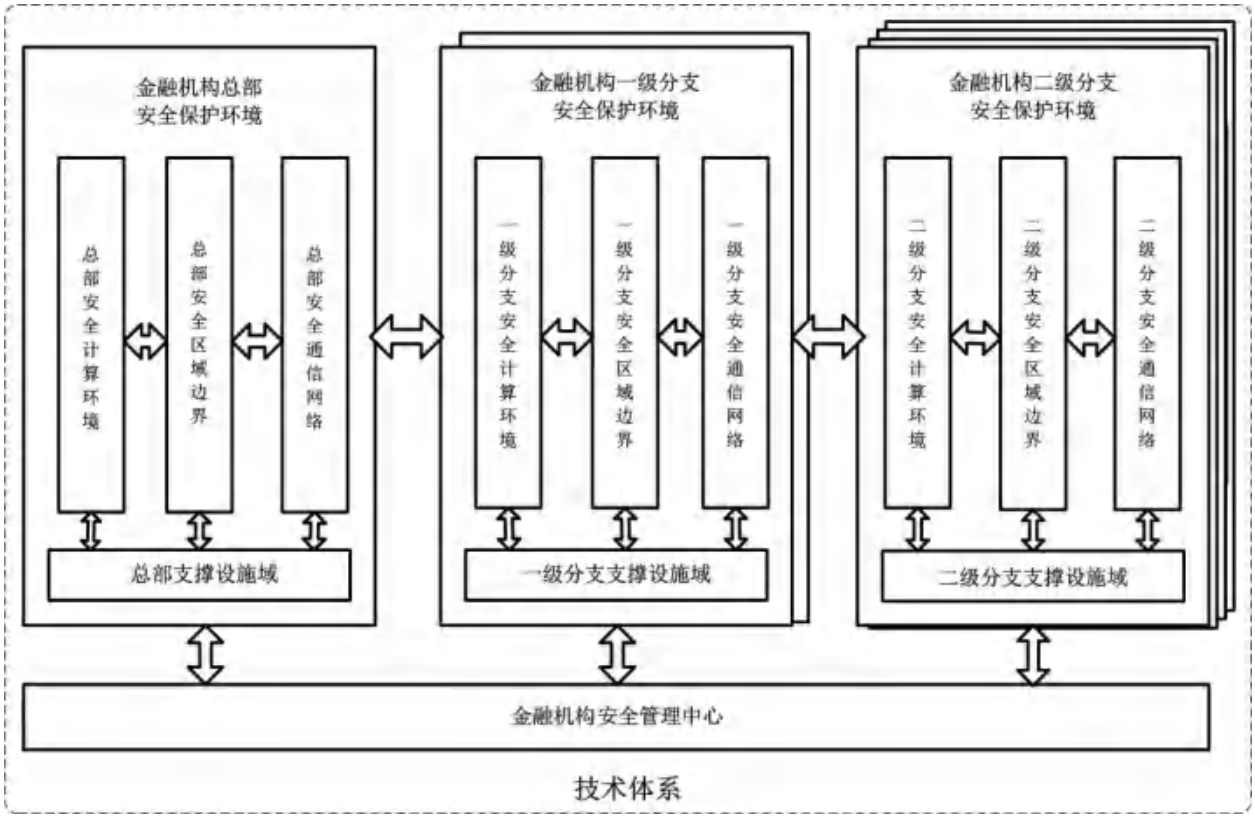



图 2 金融机构网络安全保障总体技术架构图

通过划分安全域的方法，将金融行业等级保护对象按照业务流程及特点、重要程度和不同层面划分为不同的安全域，各个安全域内部又可以划分为不同的安全子域，并针对每个安全域或安全子域来标识其中的关键资产，分析所存在的安全隐患和面临的安全风险，然后给出相应的保护措施，从而建立纵深防御体系，实现深度防护的目标。

安全计算环境包含保障终端安全、服务器操作系统安全、网络设备安全、数据库安全、上层应用系统安全以及应用业务处理全过程的安全等。通过在操作系统核心层设置以访问控制为主体的系统安全机制，形成严密的安全保护环境，从而有效防止非授权用户访问和授权用户越权访问，为定级对象的正常运行、免遭恶意破坏提供支撑和保障。

安全区域边界指通过对进入和流出应用环境的信息流进行安全检查和访问控制，确保不会有违背系统安全策略的信息流经过边界。不同定级对象之间存在业务互联和数据互联，但是不同定级对象间存在安全级别、安全风险不同的情况，安全区域边界必须确保不同等级对象之间的可信互联，必须基于较高级别对象或安全域的安全防护要求设置可信互联安全策略，通过对不同等级对象之间的可信互联进行严

格约束，保证不会出现因高级别对象与低级别对象之间的防护差异而导致的安全漏洞。

安全通信网络通过合理规划网络区域、分配网络资源以及设计安全的网络架构，保证网络的可用性，实现不同网络区域之间的安全隔离。通过对通信双方进行可信鉴别验证，建立安全通道，并实施数据传输保护，确保数据在传输过程中不会被窃听、篡改和破坏。

安全支撑设施对计算环境、区域边界和通信网络实施统一的安全策略管理，确保系统配置完整可信，用户操作权限严格划分和审计全程追踪，从功能上可细分为系统管理、安全管理、审计管理以及物理支撑设施管理等，各管理员职责和权利明确，相互制约。

### 6.3 管理体系

要建成完善的安全管理体系，首先根据金融机构信息化建设进程的实际需求，逐步建立起安全管理组织架构和各项安全管理制度，配备相应的安全管理人员。其次通过对制度的执行，提高网络安全保障能力，后续根据执行结果检查各项制度存在的问题并对制度进行改进。从而形成建立、实施和执行、监控和审计、保持和改进的循环过程，形成完善的管理体系。如图3所示。

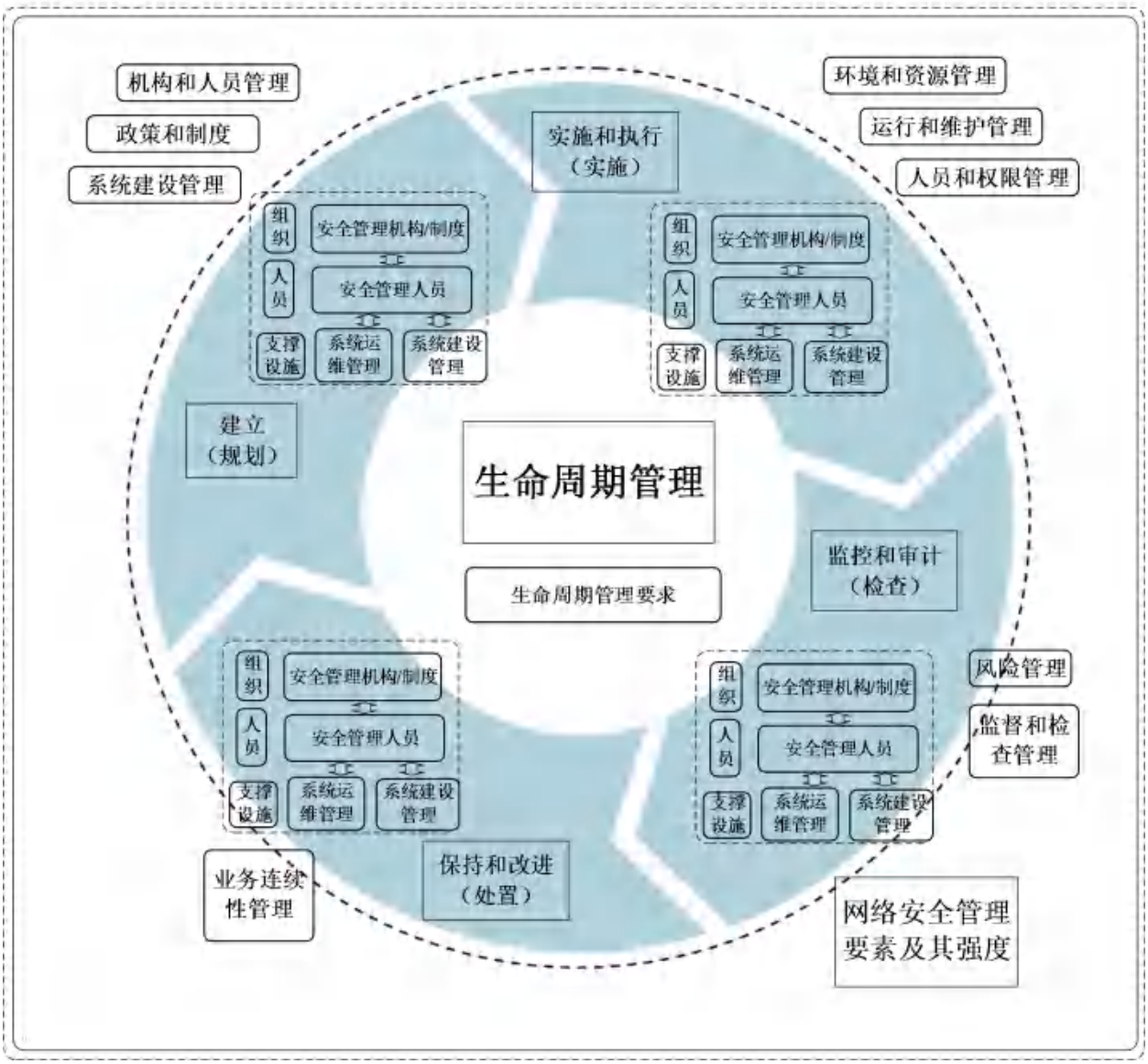



图 3 网络安全管理体系框架图

安全管理内容涵盖组织、人员、支撑设施三大类。其中，组织涉及机构与制度管理；人员涉及人员管理；支撑设施涉及系统建设和系统运维管理。

# 7 第二级安全要求

## 7.1 安全通用要求

### 7.1.1 安全物理环境

#### 7.1.1.1 物理位置选择

本项要求包括：

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内。

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

#### 7.1.1.2 物理访问控制

本项要求包括：

a) 机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

b) **可对机房划分区域进行管理，并根据各区域特点提出相应的访问控制要求。（F2）**

#### 7.1.1.3 防盗窃和防破坏

本项要求包括：

a) 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识。

b) 应将通信线缆铺设在隐蔽安全处。

c) **应建立机房视频监控系统和动环监控系统，对机房风冷水电设备、消防设施、门禁系统等重要设施实行全面监控，视频监控记录和门禁系统出入记录至少保存3个月。（F2）**

#### 7.1.1.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

#### 7.1.1.5 防火

本项要求包括：

a) 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。

b) 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。

c) **机房内部通道设置、装修装饰材料、设备线缆等应满足消防要求，并对机房进行消防验收。（F2）**

#### 7.1.1.6 防水和防潮

本项要求包括：

a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

b) 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。

#### 7.1.1.7 防静电

应采用防静电地板或地面并采用必要的接地防静电措施。

#### 7.1.1.8 温湿度控制

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。

#### 7.1.1.9 电力供应

本项要求包括：

a) 应在机房供电线路上配置稳压器和过电压防护设备。
b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
c) **机房重要区域、重要设备应提供UPS供电。（F2）**

#### 7.1.1.10 电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

### 7.1.2 安全通信网络

#### 7.1.2.1 网络架构

本项要求包括：

a) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

#### 7.1.2.2 通信传输

应采用校验技术保证通信过程中数据的完整性。

#### 7.1.2.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

### 7.1.3 安全区域边界

#### 7.1.3.1 边界防护

应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

#### 7.1.3.2 访问控制

本项要求包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。
d) 应能根据会话状态信息为进出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。（F2）**

#### 7.1.3.3 入侵防范

应在关键网络节点处监视网络攻击行为。

#### 7.1.3.4 恶意代码和垃圾邮件防范

本项要求包括：

a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

b) **应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。（F2）**

#### 7.1.3.5 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b) 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。

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

#### 7.1.3.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

### 7.1.4 安全计算环境

#### 7.1.4.1 身份鉴别

本项要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，**静态口令应在8位以上，由字母、数字、符号等混合组成**并定期更换。**（F2）**

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

#### 7.1.4.2 访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限。

b) 应重命名或删除默认账户，修改默认账户或**预设账户**的默认口令。**（F2）**

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。

e) **应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一功能专用权限等。（F2）**

#### 7.1.4.3 安全审计

本项要求包括：

a) 应提供安全审计功能，审计应覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b) 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。

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，**审计记录保存时间应不少于6个月。（F2）**

d) **审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正确性。（F2）**

#### 7.1.4.4 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序。
b) 应关闭不需要的系统服务、默认共享和高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。
d) 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内容符合系统设定要求。
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
f) **应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。（F2）**
g) **所有安全计算环境设备应全部专用化，不得进行与业务不相关的操作。（F2）**
h) **应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F2）**

#### 7.1.4.5 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期**统一**进行升级和更新防恶意代码库。**（F2）**

#### 7.1.4.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

#### 7.1.4.7 数据完整性

应采用校验技术保证重要数据在传输和**存储**过程中的完整性。**（F2）**

#### 7.1.4.8 数据保密性

**应采用加密或其他保护措施保证鉴别信息在传输和存储过程中的保密性。（F2）**

#### 7.1.4.9 数据备份恢复

本项要求包括：
a) 应提供重要数据的本地数据备份与恢复功能。
b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。

#### 7.1.4.10 剩余信息保护

应保证**操作系统、数据库系统和应用系统用户**鉴别信息所在的存储空间被释放或重新分配前得到完全清除，**无论这些信息是存放在硬盘上还是内存中。（F2）**

#### 7.1.4.11 个人信息保护

本项要求包括：
a) **金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。（F2）**
b) 应仅采集和保存业务必需的用户个人**金融**信息。**（F2）**
c) **应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限，**应禁止未授权访问和非法使用用户个人**金融**信息。**（F2）**
d) **金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。(F2)**

e) **金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F2）**

f) **应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F2）**

g) **开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F2）**

### 7.1.5 安全管理中心

#### 7.1.5.1 系统管理

本项要求包括：

a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

c) **应每月对设备的配置文件进行备份，发生变动时应及时备份。（F2）**

d) **应定期对设备运行状况进行监测。（F2）**

e) **应定期检验设备的软件版本信息，并留存记录。（F2）**

f) **应提供数据备份与恢复功能，增量数据备份至少每天一次。（F2）**

#### 7.1.5.2 审计管理

本项要求包括：

a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。

b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

### 7.1.6 安全管理制度

#### 7.1.6.1 安全策略

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

#### 7.1.6.2 管理制度

本项要求包括：

a) 应对安全管理活动中的主要管理内容建立安全管理制度。

b) 应对安全管理人员或操作人员执行的日常管理操作建立操作规程。

#### 7.1.6.3 制定和发布

本项要求包括：

a) **金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应制定适用辖内的安全管理制度。（F2）**

b) 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。
c) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。

#### 7.1.6.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

### 7.1.7 安全管理机构

#### 7.1.7.1 岗位设置

本项要求包括：

a) **网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。（F2）**
b) **除网络安全管理部门外，其他部门均应指定至少一名网络安全员，协助网络安全管理部门开展本部门的网络安全管理工作。（F2）**
c) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。
d) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

#### 7.1.7.2 人员配备

本项要求包括：

a) 应配备一定数量的系统管理员、审计管理员和安全管理员等。
b) **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。（F2）**

#### 7.1.7.3 授权和审批

应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等，**对系统投入运行、系统变更、网络系统接入和重要资源（如敏感数据等资源）的访问等关键活动应执行审批过程。（F2）**

注：敏感数据具体分类见附录H中敏感数据和个人金融信息类别中的敏感数据类别内容。

#### 7.1.7.4 沟通和合作

本项要求包括：

a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。
b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。
c) 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。

#### 7.1.7.5 审核和检查

应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

### 7.1.8 安全管理人员

#### 7.1.8.1 人员录用

本项要求包括：

a) 应指定或授权专门的部门或人员负责人员录用。
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。

c) **应对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。（F2）**

d) **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，不应从事网络安全管理工作。（F2）**

#### 7.1.8.2 人员离岗

应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

#### 7.1.8.3 安全意识教育和培训

本项要求包括：

a) **应制定安全教育和培训计划。（F2）**

b) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

c) **每年应至少对网络安全管理人员进行一次网络安全培训。（F2）**

#### 7.1.8.4 外部人员访问管理

本项要求包括：

a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。

b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。

c) 外部人员离场后应及时清除其所有的访问权限。

d) **获得系统访问授权的外部人员应签署保密协议，不得进行非授权的增加、删除、修改、查询数据等操作，不得复制和泄露金融机构的任何信息。（F2）**

### 7.1.9 安全建设管理

#### 7.1.9.1 定级和备案

本项要求包括：

a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。

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

c) 应保证定级结果经过相关部门的批准。

d) 应将备案材料报主管部门和相应公安机关备案。

#### 7.1.9.2 安全方案设计

本项要求包括：

a) 应根据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) 应根据保护对象的安全保护等级进行安全方案设计。

c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

#### 7.1.9.3 产品采购和使用

本项要求包括：

a) 应确保网络安全产品采购和使用符合国家的有关规定。

b) 应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。

c) **各机构购置扫描、检测类网络安全产品应报本机构科技主管部门批准、备案。（F2）**

d) **扫描、检测类网络安全产品应仅限于本机构网络安全管理人员或经主管领导授权的技术人员使用。（F2）**
e) **应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取应急措施并按规定程序报告。（F2）**
f) **应定期对各类网络安全产品产生的日志和报表进行备份存档。（F2）**
g) **应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。（F2）**

#### 7.1.9.4 自行软件开发

本项要求包括：

a) **应将开发环境、测试环境、实际运行环境相互分离，敏感数据经过脱敏后才可在开发或测试中使用。（F2）**
b) **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。（F2）**
c) 应在软件开发过程中**对代码规范、代码质量、代码安全性进行审查**，在软件安装前对可能存在的恶意代码进行检测。**（F2）**

#### 7.1.9.5 外包软件开发

本项要求包括：

a) 应在软件交付前检测其中可能存在的恶意代码。
b) 应保证开发单位提供软件设计文档和使用指南。
c) **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。（F2）**
d) **应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F2）**
e) **应定期对外包服务活动和外包服务商的服务能力进行审核和评估。（F2）**

#### 7.1.9.6 工程实施

本项要求包括：

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) 应制定安全工程实施方案控制工程实施过程。

#### 7.1.9.7 测试验收

本项要求包括：

a) 应制定测试验收方案，并依据测试验收方案实施测试验收，**在测试验收过程中应详细记录测试验收结果，**形成测试验收报告。**（F2）**
b) 应进行上线前的安全性测试，并出具安全测试报告。
c) **对于在生产系统上进行的测试工作，应先进行风险分析和告知，同时制定详细的系统测试方案、数据备份与系统恢复措施、应急处置措施后，经主管领导审批后开展测试工作，以确保生产系统的安全。（F2）**

#### 7.1.9.8 系统交付

本项要求包括：

a) 应制定交付清单，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) 应对负责运行维护的技术人员进行相应的技能培训。

c） 应提供建设过程文档和运行维护文档。

**d） 外部建设单位应与金融机构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。（F2）**

#### 7.1.9.9 等级测评

本项要求包括：

a） 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。

b） 应在发生重大变更或级别发生变化时进行等级测评。

c） 应确保测评机构的选择符合国家有关规定。

#### 7.1.9.10 服务供应商选择

本项要求包括：

a） **应评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。（F2）**

b） 应确保服务供应商的选择符合国家的有关规定。

c） 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。

### 7.1.10 安全运维管理

#### 7.1.10.1 环境管理

本项要求包括：

a） 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。

b） 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等方面。

c） **机房布线应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F2）**

d） **进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。（F2）**

e） **机房管理员应经过相关培训，掌握机房各类设备的操作要领。（F2）**

f） **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F2）**

g） **机房出入口和内部应安装7*24小时录像监控设施，录像至少保存3个月。（F2）**

h） **机房应设置弱电井或桥架，并留有可扩展空间。（F2）**

i） 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。

#### 7.1.10.2 资产管理

应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

#### 7.1.10.3 介质管理

本项要求包括：

a） 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。

b） 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，并对介质的归档和查询等进行登记记录。

c） **所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F2）**

d） **对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应进行电子化审批流转登记管理。（F2）**

e) **对载有敏感信息存储介质的销毁，应报有关部门备案，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。（F2）**
f) **应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F2）**
g) **应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F2）**

#### 7.1.10.4 设备维护管理

本项要求包括：

a) 应对各种设备（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) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
c) **新购置的设备应经过验收，验收合格后方能投入使用。（F2）**
d) **应制定设备管理规范，落实设备使用者的安全保护责任。（F2）**
e) **需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复性销毁处理；信息消除处理仅限于废止设备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。（F2）**
f) **设备确需送外单位维修时，应彻底清除所存的工作相关信息，并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。（F2）**
g) **应制定规范化的故障处理流程，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）。（F2）**

#### 7.1.10.5 漏洞和风险管理

应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

#### 7.1.10.6 网络和系统安全管理

本项要求包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。
b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。
c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。
d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。
e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
f) **应对网络环境运行状态进行巡检，保留记录，并由操作人员和复核人员确认。（F2）**
g) **金融行业网间互联安全应实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F2）**
h) **应制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）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。（F2）**
i) **各机构应以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。（F2）**

j) **网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经科技主管部门授权，任何外部机构与人员不得检测或扫描机构内部网络。（F2）**

k) **系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对计算机系统数据库进行技术维护性操作的，应征得业务部门审批，并详细记录维护信息过程。（F2）**

l) **每年应至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补。（F2）**

#### 7.1.10.7 恶意代码防范管理

本项要求包括：

a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。

b) 应对恶意代码防范要求作出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

c) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。

d) **客户端应统一安装病毒防治软件，设置用户口令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。（F2）**

#### 7.1.10.8 配置管理

应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

#### 7.1.10.9 密码管理

本项要求包括：

a) 应遵循密码相关的国家标准和行业标准。

b) 应使用国家密码管理主管部门认证核准的密码技术和产品。

c) **应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工。（F2）**

d) **系统管理员、数据库管理员、网络管理员、业务操作人员均应设置口令密码，并定期更换，口令密码的强度应满足不同安全性要求。（F2）**

e) **应支持各类环境中密码设备使用、管理权限分离。（F2）**

#### 7.1.10.10 变更管理

本项要求包括：

a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

b) **变更前应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。（F2）**

#### 7.1.10.11 备份与恢复管理

本项要求包括：

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和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

d) **恢复及使用备份数据时需要提供相关口令密码的，应妥善保管口令密码密封与数据备份介质。（F2）**

e) **应建立灾难恢复计划，定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。（F2）**

#### 7.1.10.12 安全事件处置

本项要求包括：

a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件。

b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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等。

c) 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。

#### 7.1.10.13 应急预案管理

本项要求包括：

a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。

b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

c) **突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F2）**

d) **突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。（F2）**

e) **应定期对原有的应急预案重新评估，修订完善。（F2）**

#### 7.1.10.14 外包运维管理

本项要求包括：

a) 应确保外包运维服务商的选择符合国家的有关规定。

b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

c) **应要求外包运维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。（F2）**

d) **应制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F2）**

### 7.2 云计算安全扩展要求

#### 7.2.1 安全物理环境

##### 7.2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

#### 7.2.2 安全通信网络

##### 7.2.2.1 网络架构

本项要求包括：

a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统。

b) 应实现不同云服务客户虚拟网络之间的隔离。

c) 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。

#### 7.2.3 安全区域边界

##### 7.2.3.1 访问控制

本项要求包括：

a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

##### 7.2.3.2 入侵防范

本项要求包括：

a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。

##### 7.2.3.3 安全审计

本项要求包括：

a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。
b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

#### 7.2.4 安全计算环境

##### 7.2.4.1 访问控制

本项要求包括：

a) 应保证当虚拟机迁移时，访问控制策略随其迁移。
b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。

##### 7.2.4.2 镜像和快照保护

本项要求包括：

a) 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。
b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。

##### 7.2.4.3 数据完整性和保密性

本项要求包括：

a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。
b) 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限。
c) 应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

##### 7.2.4.4 数据备份恢复

本项要求包括：

a) 云服务客户应在本地保存其业务数据的备份。
b) 应提供查询云服务客户数据及备份存储位置的能力。

##### 7.2.4.5 剩余信息保护

本项要求包括：

a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除。
b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

#### 7.2.5 安全建设管理

##### 7.2.5.1 云服务商选择

本项要求包括：
a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。
b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标。
c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。

##### 7.2.5.2 供应链管理

本项要求包括：
a) 应确保供应商的选择符合国家有关规定。
b) 应将供应链安全事件信息或威胁信息及时传达到云服务客户。

#### 7.2.6 安全运维管理

##### 7.2.6.1 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

### 7.3 移动互联安全扩展要求

#### 7.3.1 安全物理环境

##### 7.3.1.1 无线接入点的物理位置

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

#### 7.3.2 安全通信网络

##### 7.3.2.1 通信传输

**应在移动终端与服务器之间建立安全的信息传输通道，并进行双向认证，例如使用有效安全版本的TLS或IPSec等协议。（F2）**

#### 7.3.3 安全区域边界

##### 7.3.3.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

##### 7.3.3.2 访问控制

无线接入设备应开启接入认证功能，并且禁止使用WEP方式进行认证，如使用口令，长度不小于8位字符。

#### 7.3.3.3 入侵防范

本项要求包括：

a) 应能够检测到非授权无线接入设备和非授权移动终端的接入行为。
b) 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。
c) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。
d) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。
e) 应禁止多个 AP 使用同一个认证密钥。

### 7.3.4 安全计算环境

#### 7.3.4.1 移动终端管控

本项要求包括：

a) **应保证移动终端安装、注册并运行终端管理客户端软件。（F2）**
b) **移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。（F2）**

#### 7.3.4.2 移动应用管控

本项要求包括：

a) 应具有选择应用软件安装、运行的功能。
b) 应只允许可靠证书签名的应用软件安装和运行。

#### 7.3.4.3 访问控制

**客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。（F2）**

#### 7.3.4.4 入侵防范

**客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。（F2）**

### 7.3.5 安全建设管理

#### 7.3.5.1 移动应用软件采购

本项要求包括：

a) 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。
b) 应保证移动终端安装、运行的应用软件由可靠的开发者开发。

#### 7.3.5.2 移动应用软件开发

本项要求包括：

a) 应对移动业务应用软件开发者进行资格审查。
b) 应保证开发移动业务应用软件的签名证书合法性。

## 7.4 物联网安全扩展要求

### 7.4.1 安全物理环境

#### 7.4.1.1 感知节点设备物理防护

本项要求包括：

a) 感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动等，**使用环境与外壳防护等级（IP 代码）范围一致。（F2）**

b) 感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。

c) **感知节点设备的部署应遵循封闭性原则，降低设备被非法拆除、非法篡改的风险。（F2）**

#### 7.4.1.2 感知网关节点设备物理安全要求

本项要求包括：

a) **关键感知网关节点设备应具有持久稳定的电力供应措施。（F2）**

b) **应保证关键感知网关节点设备所在物理环境具有良好的信号收发能力（如避免信道遭遇屏蔽）。（F2）**

c) **关键感知网关节点设备应具有定位装置。（F2）**

### 7.4.2 安全区域边界

#### 7.4.2.1 接入控制

本项要求包括：

a) 应保证只有授权的感知节点可以接入。

b) **每个感知节点和感知网关节点应具备传感网络中唯一标识，且该标识不应被非授权访问所篡改。（F2）**

c) **具有指令接收功能的感知节点设备，应保证只有授权过的系统、终端可以对感知节点下发指令。（F2）**

d) **由第三方平台提供感知节点、感知网关节点中转接入时，第三方平台的安全保护等级应不低于接入的物联网系统的安全保护等级。（F2）**

#### 7.4.2.2 入侵防范

本项要求包括：

a) 应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为。

b) 应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

### 7.4.3 安全计算环境

#### 7.4.3.1 感知节点设备安全

本项要求包括：

a) **应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。（F2）**

b) **应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力。（F2）**

c) **应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。（F2）**

#### 7.4.3.2 网关节点设备安全

本项要求包括：

a) **应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力。（F2）**

b) **应具备过滤非法节点和伪造节点所发送的数据的能力。（F2）**

### 7.4.4 安全运维管理

#### 7.4.4.1 感知节点管理

本项要求包括：

a) 应指定人员**或使用自动化巡检手段**，定期**检查**感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。**（F2）**

b) 应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。

c) **应在经过充分测试评估后，在不影响关键感知节点、感知网关节点安全稳定运行的情况下进行补丁、固件更新等工作。（F2）**

d) **关键感知节点、感知网关节点应通过安全传输通道进行固件与补丁更新，在检测到异常时应能将结果上报至安全管理中心。（F2）**

e) **应对感知节点状态进行监测，发现异常时应进行处理。（F2）**

## 8 第三级安全要求

### 8.1 安全通用要求

#### 8.1.1 安全物理环境

#### 8.1.1.1 物理位置选择

本项要求包括：

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内。

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

c) **机房应避开火灾危险程度高的区域，周围100米内不得有加油站、燃气站等危险建筑。（F3）**

#### 8.1.1.2 物理访问控制

本项要求包括：

a) 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

b) **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。（F3）**

#### 8.1.1.3 防盗窃和防破坏

本项要求包括：

a) 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识。

b) 应将通信线缆铺设在隐蔽安全处。

c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统，**非7*24小时人员值守和巡查的机房，主要出入口应安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。（F3）**

d) **应建立机房视频监控系统和动环监控系统，并对监控内容进行记录，对机房风冷水电设备、消防设施、门禁系统等重要设施实行连续24小时全面监控，视频监控记录和门禁系统出入记录至少保存3个月。（F3）**

#### 8.1.1.4 防雷击

本项要求包括：

a) 应将各类机柜、设施和设备等通过接地系统安全接地。

b) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

c) **机房应通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。（F3）**

#### 8.1.1.5 防火

本项要求包括：

a) 机房应设置火灾自动消防系统，能够**通过在机房内、基本工作房间内、活动地板下、吊顶里及易燃物附近部位设置烟感、温感等多种方式进行**自动检测火情、自动报警，并自动灭火。**（F3）**

b) 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。

c) 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

d) **机房应备有一定数量的对电子设备影响小的手持式灭火器，消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发。（F3）**

e) **机房内部通道设置、装修装饰材料、设备线缆等应满足消防要求，并对机房进行消防验收，纸张、磁带和胶卷等易燃物品要放置于防火柜内。（F3）**

f) **主机房宜采用管网式洁净气体灭火系统，也可采用高压细水雾灭火系统，应同时设置两种火灾探测器，且消防报警系统应与空调系统、新风系统、门禁系统、灭火系统联动，凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。（F3）**

g) **应定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练。（F3）**

h) **机房应设置消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用，在机房通道上应设置显著的消防标志。（F3）**

#### 8.1.1.6 防水和防潮

本项要求包括：

a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

b) 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。

c) **为便于地下积水的转移，漏水隐患区域地面周围应设排水沟或地漏等排水设施，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。（F3）**

d) 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。

e) **应对温湿度调节设备安装漏水报警装置，并设置防水堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。（F3）**

#### 8.1.1.7 防静电

本项要求包括：

a) 应采用防静电地板或地面并采用必要的接地防静电措施。

b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

c) **主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。（F3）**

#### 8.1.1.8 温湿度控制

本项要求包括：

a) 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。

b) **机房应采用专用温湿度调节设备，并应满足机房监控系统的要求。（F3）**

c) **温湿度调节设备的工作能力应满足机房负载要求，并应保有一定的余量。（F3）**

#### 8.1.1.9 电力供应

本项要求包括：

a) 应在机房供电线路上配置稳压器和过电压防护设备。
b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
c) 应设置冗余或并行的电力电缆线路为计算机系统供电。
d) **应提供应急供电设施，以备供电系统临时停电时启用，并确保应急供电设施能在UPS供电时间内到位，每年需进行应急供电设施的带负载模拟演练，并定期对备用电力供应设备及应急供电设施进行检修和维护，确保其能正常使用。（F3）**
e) **UPS供电系统的冗余方式应采用N+1、N+2、2N、2(N+1) 等方式，未建立备用发电机应急供电系统的单位，UPS后备时间至少1小时，已建立备用发电机应急供电系统的单位，UPS后备时间应满足至少15分钟以上。（F3）**
f) **机房内要求采用机房专用插座，市电、UPS电源插座分开，满足负荷使用要求。（F3）**
g) **计算机系统应选用铜芯电缆，避免铜、铝混用，若不能避免时，应采用铜铝过渡头连接。（F3）**
h) **机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。（F3）**
I) **机房重要区域、重要设备应提供UPS单独供电。（F3）**

#### 8.1.1.10 电磁防护

本项要求包括：

a) 电源线和通信线缆应隔离铺设，避免互相干扰。
b) 应对关键设备实施电磁屏蔽。

### 8.1.2 安全通信网络

#### 8.1.2.1 网络架构

本项要求包括：

a) 应保证网络设备的业务处理能力满足业务高峰期需要，**如：业务处理能力能满足业务高峰期需要的 50%以上。（F3）**
b) 应保证网络各个部分的带宽满足业务高峰期需要。
c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性，**双线路设计时，宜由不同的电信运营商提供。（F3）**

#### 8.1.2.2 通信传输

本项要求包括：

a) 应采用校验技术或密码技术保证通信过程中数据的完整性，**并按照国家密码管理部门与行业有关要求使用密码算法。（F3）**
b) 应采用密码技术保证通信过程中数据的保密性，**并按照国家密码管理部门与行业有关要求使用密码算法。（F3）**

#### 8.1.2.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

#### 8.1.3 安全区域边界

##### 8.1.3.1 边界防护

本项要求包括：

a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制。
c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制。
d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

##### 8.1.3.2 访问控制

本项要求包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。
d) 应能根据会话状态信息为进出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。（F3）**
e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
f) **应对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。（F3）**
g) **应定期检查并锁定或撤销网络设备中不必要的用户账号。（F3）**

##### 8.1.3.3 入侵防范

本项要求包括：

a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。
c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。
d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
e) **应采取技术手段对高级持续威胁进行监测、发现。（F3）**
f) **应建立诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析。（F3）**

##### 8.1.3.4 恶意代码和垃圾邮件防范

本项要求包括：

a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

##### 8.1.3.5 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b) **应记录无线网络接入行为，形成日志进行留存，保存时间不少于6个月。（F3）**
c) 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) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，**审计记录保存时间不少于6个月。（F3）**
e) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
f) **所有的审计手段需要具备统一的时间戳，保持审计的时间标记一致。（F3）**

#### 8.1.3.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

### 8.1.4 安全计算环境

#### 8.1.4.1 身份鉴别

本项要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，**应实现身份鉴别信息防窃取和防重用。静态口令应在8位以上，由字母、数字、符号等混合组成并每半年更换口令，不允许新设定的口令与前次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定期更换。（F3）**
b) 应具有登录失败处理功能，应配置并启用结束会话、**限制登录间隔**、限制非法登录次数和当登录连接超时自动退出等相关措施。**（F3）**
c) 当进行远程管理时，**应对管理终端进行身份标识和鉴别，采用密码技术**防止鉴别信息在网络传输过程中被窃听。**（F3）**
d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

#### 8.1.4.2 访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限。
b) 应重命名或删除默认账户，修改默认账户或**预设账户**的默认口令。**（F3）**
c) **应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。（F3）**
d) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。
e) 应授予管理用户所需的最小权限，实现管理用户的权限分离。
f) **应严格限制默认账户或预设账户的权限，如默认账户或预设账户的权限应为空权限或某单一功能专用权限等。（F3）**
g) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。
h) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。
i) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

#### 8.1.4.3 安全审计

本项要求包括：

a) 应启用安全审计功能，审计应覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
b) 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。

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，**审计记录保存时间应不少于6个月。（F3）**

d) 应对审计进程进行保护，防止未经授权的中断。

e) **对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息。（F3）**

f) **审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正确性。（F3）**

#### 8.1.4.4 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序。

b) 应关闭不需要的系统服务、默认共享和高危端口。

c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

d) 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内容符合系统设定要求。

e) 应能**通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时**发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。**（F3）**

f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

g) **所有安全计算环境设备应全部专用化，生产设备不得进行与业务不相关的操作。（F3）**

h) **应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F3）**

#### 8.1.4.5 恶意代码防范

本项要求包括：

a) 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，将其有效阻断**并定期统一进行升级和更新防恶意代码库。（F3）**

b) **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。（F3）**

#### 8.1.4.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

#### 8.1.4.7 数据完整性

本项要求包括：

a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

#### 8.1.4.8 数据保密性

本项要求包括：

a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于**系统**鉴别数据、重要业务数据**和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护其存储过程中的保密性。（F3）**

8.1.4.9 数据备份恢复

本项要求包括：

a) 应提供重要数据的本地数据备份与恢复功能，**采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指标（如RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放，数据保存期限依照国家相关规定。（F3）**

b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。

d) **对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。（F3）**

e) **为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试结果。（F3）**

f) **数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星期为周期的数据冗余。（F3）**

g) **异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资源（相关软硬件以及数据等资源）已完全满足但设备 CPU 还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU 也在运行状态。（F3）**

8.1.4.10 剩余信息保护

本项要求包括：

a) 应保证**操作系统、数据库系统和应用系统用户**鉴别信息所在的存储空间被释放或重新分配前得到完全清除，**无论这些信息是存放在硬盘上还是内存中。（F3）**

b) 应保证**操作系统、数据库系统和应用系统用户**存有敏感数据的存储空间被释放或重新分配前得到完全清除，**无论这些信息是存放在硬盘上还是内存中。（F3）**

8.1.4.11 个人信息保护

本项要求包括：

a) **金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。（F3）**

b) 应仅采集和保存业务必需的用户个人**金融**信息。**（F3）**

c) **应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限，**应禁止未授权访问和非法使用用户个人**金融**信息。**（F3）**

d) **金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F3）**

e) **金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F3）**

f) **应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F3）**

g) **开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F3）**

#### 8.1.5 安全管理中心

##### 8.1.5.1 系统管理

本项要求包括：

a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

c) **应每月对设备的配置文件进行备份，发生变动时应及时备份。（F3）**

d) **应使用自动化技术手段对设备运行状况进行实时监测，运维人员应每天定期查看并记录系统运行状况。（F3）**

e) **应每季度检验网络设备软件版本信息，并通过有效测试验证后进行相应的升级，同时留存测试验证相关记录。（F3）**

##### 8.1.5.2 审计管理

本项要求包括：

a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。

b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

c) **应严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审计用户的权限分离，避免非授权的删除、修改或覆盖。（F3）**

##### 8.1.5.3 安全管理

本项要求包括：

a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。

b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

##### 8.1.5.4 集中管控

本项要求包括：

a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。

b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。

c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。

d) 应对分散在各个设备上的**安全事件**、审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。**（F3）**

e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

f) 应能对网络中发生的各类安全事件进行识别、报警、分析、**响应和处置。（F3）**

g) **应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。（F3）**

#### 8.1.6 安全管理制度

##### 8.1.6.1 安全策略

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等，**并编制形成网络安全方针制度文件。（F3）**

##### 8.1.6.2 管理制度

本项要求包括：

a) 应对安全管理活动中各类管理内容建立安全管理制度。

b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。

c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

##### 8.1.6.3 制定和发布

本项要求包括：

a) **金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应负责制定适用辖内的安全管理制度。（F3）**

b) 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。

c) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。

##### 8.1.6.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

#### 8.1.7 安全管理机构

##### 8.1.7.1 岗位设置

本项要求包括：

a) **网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。（F3）**

b) **应设立由本机构领导、业务与技术相关部门主要负责人组成的**网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权，**负责协调本机构及辖内网络安全管理工作，决策本机构及辖内网络安全重大事宜。（F3）**

c) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。

d) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

e) **应设立专门的网络安全审计岗位，负责网络安全审计制度和流程的实施，制订和执行网络安全审计计划，对网络安全整个生命周期和重大事件等进行审计。（F3）**

f) **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，信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。（F3）**

g) **除网络安全管理部门外，其他部门均应指定至少一名网络安全员，协助网络安全管理部门开展本部门的网络安全管理工作。（F3）**

##### 8.1.7.2 人员配备

本项要求包括：

a) 应配备一定数量的系统管理员、审计管理员和安全管理员等。

b) 应配备专职安全管理员，**实行A、B岗制度，**不可兼任。**（F3）**

#### 8.1.7.3 授权和审批

本项要求包括：

a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。

b) 应针对**系统投入运行、重要资源（如敏感数据等资源）的访问、**系统变更、重要操作、物理访问和系统接入等事项建立审批程序，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。**（F3）**

c) 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。

d) **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。（F3）**

e) **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。（F3）**

#### 8.1.7.4 沟通和合作

本项要求包括：

a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。

b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。

c) 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。

#### 8.1.7.5 审核和检查

本项要求包括：

a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

b) 应定期进行全面安全检查，检查内容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。

c) **应建立对门户网站内容发布的审核、管理和监控机制。（F3）**

d) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，对安全检查结果进行通报并报上一级机构科技部门备案。（F3）**

e) **应制定违反和拒不执行安全管理措施规定的处罚细则。（F3）**

### 8.1.8 安全管理人员

#### 8.1.8.1 人员录用

本项要求包括：

a) 应指定或授权专门的部门或人员负责人员录用。

b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。

c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

d) **应对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。（F3）**

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，不应从事网络安全管理工作。（F3）**

#### 8.1.8.2 人员离岗

本项要求包括：

a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

#### 8.1.8.3 人员考核

本项要求包括：

a) **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。（F3）**

b) **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。（F3）**

c) **应对考核结果进行记录并保存。（F3）**

#### 8.1.8.4 安全意识教育和培训

本项要求包括：

a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

b) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。

c) **每年应至少对网络安全管理人员进行一次网络安全培训。（F3）**

#### 8.1.8.5 外部人员访问管理

本项要求包括：

a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。

b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。

c) **应对允许被外部人员访问的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。（F3）**

d) 外部人员离场后应及时清除其所有的访问权限。

e) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权的**增加、删除、修改、查询数据等**操作，不得复制和泄露**金融机构的任何信息。（F3）**

### 8.1.9 安全建设管理

#### 8.1.9.1 定级和备案

本项要求包括：

a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。

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

c) 应保证定级结果经过相关部门的批准。

d) 应将备案材料报主管部门和相应公安机关备案。

#### 8.1.9.2 安全方案设计

本项要求包括：

a) 应根据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) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。
c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

#### 8.1.9.3 产品采购和使用

本项要求包括：

a) 应确保网络安全产品采购和使用符合国家的有关规定。
b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
c) **各机构购置扫描、检测类网络安全产品应报本机构科技主管部门批准、备案。（F3）**
d) 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。
e) **扫描、检测类网络安全产品仅限于本机构网络安全管理人员或经主管领导授权的技术人员使用。（F3）**
f) **应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取控制措施并按规定程序报告。（F3）**
g) **应定期对各类网络安全产品产生的日志和报表进行备份存档，至少保存6个月。（F3）**
h) **应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。（F3）**

#### 8.1.9.4 自行软件开发

本项要求包括：

a) **应将开发环境、测试环境、实际运行环境相互分离，敏感数据经过脱敏后才可在开发或测试中使用。（F3）**
b) **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。（F3）**
c) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。
d) 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。
e) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制。
f) 应保证在软件开发过程中对**代码规范、代码质量、代码安全性进行审查**，在软件安装前对可能存在的恶意代码进行检测。**（F3）**
g) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。
h) 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
i) **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。（F3）**

#### 8.1.9.5 外包软件开发

本项要求包括：

a) 应在软件交付前检测其中可能存在的恶意代码。
b) 应保证开发单位提供软件设计文档和使用指南。
c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
d) **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。（F3）**
e) **应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F3）**

f) **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。（F3）**

8.1.9.6 工程实施

本项要求包括：

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) 应制定安全工程实施方案控制工程实施过程。

c) 应通过第三方工程监理控制项目的实施过程。

d) **应制定灾难备份系统集成与测试计划并组织实施，通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求。（F3）**

e) **系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。（F3）**

8.1.9.7 测试验收

本项要求包括：

a) **应根据设计方案或合同要求等**制订测试验收方案，并依据测试验收方案实施测试验收，**在测试验收过程中应详细记录测试验收结果，**形成测试验收报告。**（F3）**

b) 应**由项目承担单位（部门）或公正的第三方制订安全测试方案，**进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容，**并将测试报告报科技部门审查。（F3）**

c) **新建应用系统投入生产运行前，原则上应进行不少于1个月的模拟运行和不少于3个月的试运行。（F3）**

d) **对于在生产系统上进行的测试工作，应先进行风险分析和告知，同时制定详细的系统测试方案、数据备份与系统恢复措施、应急处置措施后，经系统用户和主管领导审批同意后，才能开展测试工作，以确保生产系统的安全。（F3）**

8.1.9.8 系统交付

本项要求包括：

a) 应制定交付清单，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) 应对负责运行维护的技术人员进行相应的技能培训。

c) 应提供建设过程文档和运行维护文档。

d) **外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将采用的关键安全技术措施和核心安全功能设计对外公开。（F3）**

8.1.9.9 等级测评

本项要求包括：

a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。

b) 应在发生重大变更或级别发生变化时进行等级测评。

c) **应选择公安部认可的全国等级保护测评机构推荐目录中的测评单位进行等级测评，并与测评单位签订安全保密协议。（F3）**

8.1.9.10 服务供应商选择

本项要求包括：

a) **应评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。（F3）**

b) 应确保服务供应商的选择符合国家的有关规定。
c) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
d) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

#### 8.1.10 安全运维管理

##### 8.1.10.1 环境管理

本项要求包括：

a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理，**填写机房值班记录、巡视记录。（F3）**
b) 应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作出规定。
c) **机房布线应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F3）**
d) **机房管理员应经过相关培训，掌握机房各类设备的操作要领。（F3）**
e) **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F3）**
f) **进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。（F3）**
g) **应设置弱电井，并留有足够的可扩展空间。（F3）**
h) **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单位主管领导批准后实施。（F3）**
i) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。

##### 8.1.10.2 资产管理

本项要求包括：

a) 应编制并保存与保护对象相关的资产清单，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。
c) 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。

##### 8.1.10.3 介质管理

本项要求包括：

a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。
b) 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，做好防信息泄漏控制措施，**并对介质的归档和查询等进行登记记录。**（F3）**
c) **所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F3）**
d) **对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应进行电子化审批流转登记管理。（F3）**
e) **对载有敏感信息存储介质的销毁，应报有关部门备案，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。（F3）**
f) **应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F3）**
g) **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科技部门指定的同城或异地安全区域。（F3）**

h) **应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。（F3）**

i) **应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F3）**

#### 8.1.10.4 设备维护管理

本项要求包括：

a) 应对各种设备（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、维修和服务的审批、维修过程的监督控制等。

c) **设备确需送外单位维修时，应彻底清除所存的工作相关信息，并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。（F3）**

d) **应制定规范化的故障处理流程，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）。（F3）**

e) **新购置的设备应经过验收，验收合格后方能投入使用。（F3）**

f) **应制定设备管理规范，根据设备使用年限，及时进行更换升级，落实设备使用者的安全保护责任。（F3）**

g) 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。

h) **需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复性销毁处理，同时备案；信息消除处理仅限于废止设备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。（F3）**

#### 8.1.10.5 漏洞和风险管理

本项要求包括：

a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

#### 8.1.10.6 网络和系统安全管理

本项要求包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。

b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。

c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。

d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。

e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容，**重要运维操作要求至少两人在场，保留记录，并由操作和复核人员进行确认，维护记录和确认记录应至少妥善保存6个月。（F3）**

f) **应制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，经过审批后才可开通，操作过程中应保留不可篡改的审计日志，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。（F3）**

g) **各机构应以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。（F3）**

h) **网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不应对外公开，未经科技主管部门授权，任何外部机构与人员不应检测或扫描机构内部网络。（F3）**

i) **金融行业网间互联安全应实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F3）**

j) **所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。（F3）**

k) **系统管理员不应兼任业务操作人员，系统管理员不应对业务数据进行任何增加、删除、修改等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门审批，并详细记录维护内容、人员、时间等信息。（F3）**

l) **每半年应至少进行一次漏洞扫描，对发现的安全漏洞及时进行修补，扫描结果应及时上报。（F3）**

m) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。

n) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。

o) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

p) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。

q) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

#### 8.1.10.7 恶意代码防范管理

本项要求包括：

a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。

b) 应定期验证防范恶意代码攻击的技术措施的有效性。

c) **客户端应统一安装病毒防治软件，设置用户口令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。（F3）**

#### 8.1.10.8 配置管理

本项要求包括：

a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

#### 8.1.10.9 密码管理

本项要求包括：

a) 应遵循密码相关的国家标准和行业标准。

b) 应使用国家密码管理主管部门认证核准的密码技术和产品。

c) **应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理。（F3）**

d) **系统管理员、数据库管理员、网络管理员、业务操作人员均应设置口令密码，并每半年更换，口令密码的强度应满足不同安全性要求。（F3）**

e) **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，未经科技部门主管领导许可，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。（F3）**

f) **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。（F3）**

g) **确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F3）**

h) **应支持各类环境中密码设备使用、管理权限分离。（F3）**

#### 8.1.10.10 变更管理

本项要求包括：

a) **变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认。（F3）**

b) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

c) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。

d) 应建立中止变更并从失败变更中恢复的程序，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。

e) **变更前应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。（F3）**

f) **如果需要对生产环境进行重大变更，应按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同意后，再进行变更操作，以确保生产系统的安全。（F3）**

g) **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。（F3）**

#### 8.1.10.11 备份与恢复管理

本项要求包括：

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和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

d) **应每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。（F3）**

e) **应每季度对备份数据的有效性进行检查，备份数据要实行异地保存。（F3）**

f) **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。（F3）**

g) **灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。（F3）**

h) **应建立健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后重续运行操作指引、各系统灾难切换操作手册。（F3）**

i) **金融机构应根据信息系统的灾难恢复工作情况，确定审计频率，应每年至少组织一次内部灾难恢复工作审计。（F3）**

j) **应定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。（F3）**

k) **应建立灾难备份系统，主备系统实际切换时间应少于RTO时间，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。（F3）**

#### 8.1.10.12 安全事件处置

本项要求包括：

a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件。

b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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等。

c) 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。

d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

#### 8.1.10.13 应急预案管理

本项要求包括：

a) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容，**业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字确认。（F3）**

b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。

c) 应**每年**对系统相关的人员进行应急预案培训，并进行应急预案的演练。**（F3）**

d) **在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。（F3）**

e) **突发事件应急处置领导小组应统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。（F3）**

f) **突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F3）**

g) **实施报告制度和启动应急预案的单位应实行重大突发事件24小时值班制度。（F3）**

h) 应定期对原有的应急预案重新评估，修订完善。

i) **应急演练结束后，应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。（F3）**

#### 8.1.10.14 外包运维管理

本项要求包括：

a) 应确保外包运维服务商的选择符合国家的有关规定。

b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。
c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确。
d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。
e) **应要求外包运维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。（F3）**
f) **应制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F3）**

## 8.2 云计算安全扩展要求

### 8.2.1 安全物理环境

#### 8.2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

### 8.2.2 安全通信网络

#### 8.2.2.1 网络架构

本项要求包括：

a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统。
b) 应实现不同云服务客户虚拟网络之间**及同一云服务客户不同虚拟网络之间**的隔离。**（F3）**
c) **应实现云计算平台的业务网络与管理网络安全隔离。（F3）**
d) 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。
e) 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略。
f) 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

### 8.2.3 安全区域边界

#### 8.2.3.1 访问控制

本项要求包括：

a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
c) **应实现虚拟机之间、虚拟机与资源管理和调度平台之间、虚拟机与外部网络之间的安全访问控制。（F3）**
d) **应对云计算平台管理员访问管理网络进行访问控制。（F3）**

#### 8.2.3.2 入侵防范

本项要求包括：

a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。
d) 应在检测到网络攻击行为、异常流量情况时进行告警。

e) **应检测和防护云计算平台内部虚拟机发起的针对云计算平台的攻击，能够定位发起攻击的虚拟机，记录攻击类型、攻击时间、攻击流量等信息。（F3）**
f) **云服务客户通过互联网提供金融服务时，应支持DoS/DDoS攻击防护，通过清洗DoS/DDoS攻击流量，保障网络、服务器及上层应用的可用性。（F3）**
g) **云服务客户通过互联网提供金融服务时，应支持检测Web应用漏洞，拦截SQL注入、XSS攻击等多种Web应用攻击行为。（F3）**

#### 8.2.3.3 安全审计

本项要求包括：

a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。
b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

### 8.2.4 安全计算环境

#### 8.2.4.1 身份鉴别

本项要求包括：

a) 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。
b) **应支持云服务客户密码策略管理，密码策略管理应支持密码复杂度策略、密码有效期策略，云服务客户账号的初始密码应支持随机生成，云服务客户首次登录支持强制修改初始密码。（F3）**
c) **应支持为云服务客户随机生成虚拟机登录口令或云服务客户自行设置登录口令。（F3）**
d) **应支持云服务客户以密钥对方式登录虚拟机时，自主选择云计算平台生成密钥对或自行上传密钥对。（F3）**
e) **应支持云服务客户自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别。（F3）**

#### 8.2.4.2 访问控制

本项要求包括：

a) 应保证当虚拟机迁移时，访问控制策略随其迁移。
b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。

#### 8.2.4.3 入侵防范

本项要求包括：

a) 应能检测虚拟机之间的资源隔离失效，并进行告警。
b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警。
c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。
d) **应能够检测虚拟机对宿主机资源的异常访问，并进行告警。（F3）**

#### 8.2.4.4 恶意代码防范

本项要求包括：

a) **应支持对后门、木马、蠕虫、webshell等恶意代码的静态检测和行为检测，并对检测出的恶意代码进行控制和隔离。（F3）**
b) **应支持云服务客户自行安装防恶意代码软件，并支持更新防恶意代码软件版本和恶意代码库。（F3）**

#### 8.2.4.5 镜像和快照保护

本项要求包括：

a) 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。
b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。
c) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。
d) **应保证虚拟机镜像和快照文件备份在不同物理服务器。（F3）**
e) **应支持自动虚拟机快照功能，保证系统能根据快照恢复。（F3）**

#### 8.2.4.6 数据完整性和保密性

本项要求包括：

a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。
b) 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限。
c) 应使用校验技术或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
d) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。

#### 8.2.4.7 数据备份恢复

本项要求包括：

a) 云服务客户应在本地保存其业务数据的备份。
b) 应提供查询云服务客户数据及备份存储位置的能力。
c) 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致。
d) 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。
e) **应周期性测试云计算平台的备份系统和备份数据，支持故障识别和备份重建。（F3）**

#### 8.2.4.8 剩余信息保护

本项要求包括：

a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除。
b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除，**不能通过软件工具恢复。（F3）**
c) **对于更换或报废的存储介质，应采取安全删除、强化消磁或者物理损坏磁盘等方式，防止恢复已清除数据。（F3）**

### 8.2.5 安全管理中心

#### 8.2.5.1 集中管控

本项要求包括：

a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配。
b) 应保证云计算平台管理流量与云服务客户业务流量分离。
c) 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计。

d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等运行状况的集中监测，**监测内容包括CPU利用率、带宽使用情况、内存利用率、存储使用情况等。（F3）**

e) **应对异常行为集中监控分析并告警。集中监控服务质量，并可导出集中监控报告。应支持远程监控的可视化展示。（F3）**

#### 8.2.6 安全建设管理

##### 8.2.6.1 云服务商选择

本项要求包括：

a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。

b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标。

c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。

e) 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。

##### 8.2.6.2 供应链管理

本项要求包括：

a) 应确保供应商的选择符合国家有关规定。

b) 应将供应链安全事件信息或威胁信息及时传达到云服务客户。

c) 应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

d) **应分析外包服务或采购产品对云服务安全性的影响。（F3）**

#### 8.2.7 安全运维管理

##### 8.2.7.1 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

##### 8.2.7.2 网络和系统安全管理

**云服务商应制定相关策略，持续监控设备、资源、服务以及安全措施的有效性，并将安全措施有效性的监控结果定期提供给云服务客户。（F3）**

##### 8.2.7.3 应急预案管理

**云服务商应将应急预案提前告知云服务客户。（F3）**

### 8.3 移动互联安全扩展要求

#### 8.3.1 安全物理环境

##### 8.3.1.1 无线接入点的物理位置

本项要求包括：

a) 应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。
b) **应为营业网点的无线接入设备的安装选择合理位置，避免被非法破坏、替换。（F3）**

### 8.3.2 安全通信网络

#### 8.3.2.1 通信传输

本项要求包括：

a) **应在移动终端与服务器之间建立安全的信息传输通道，例如使用有效安全版本的TLS或IPSec等协议。（F3）**
b) **客户端应用软件与服务器应进行双向认证，可通过密钥、证书等密码技术手段实现服务器与客户端应用软件之间的安全认证。（F3）**
c) **通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字证书技术。（F3）**
d) **通过客户端应用软件发起的资金类交易报文或客户敏感信息变更报文，应能够防止重放攻击。（F3）**

### 8.3.3 安全区域边界

#### 8.3.3.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

#### 8.3.3.2 访问控制

无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

#### 8.3.3.3 入侵防范

本项要求包括：

a) 应能够检测到非授权无线接入设备和非授权移动终端的接入行为。
b) 应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为。
c) 应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态。
d) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等。
e) 应禁止多个AP使用同一个认证密钥。
f) 应能够阻断非授权无线接入设备或非授权移动终端。

### 8.3.4 安全计算环境

#### 8.3.4.1 移动终端管控

本项要求包括：

a) 应保证移动终端安装、注册并运行终端管理客户端软件。
b) 移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。

#### 8.3.4.2 移动应用管控

本项要求包括：

a) 应具有选择应用软件安装、运行的功能。

b) 应只允许指定证书签名的应用软件安装和运行。
c) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。

#### 8.3.4.3 访问控制

本项要求包括：

a) **客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。（F3）**
b) **应采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问。（F3）**
c) **客户端应用软件在授权范围内，不应访问非业务必需的文件和数据。（F3）**

#### 8.3.4.4 安全审计

**客户端应用软件运行日志中不应打印支付敏感信息，不应打印完整的敏感数据原文。（F3）**

#### 8.3.4.5 入侵防范

本项要求包括：

a) **客户端应用软件应对软件接口进行保护，防止其他应用对客户端应用软件接口进行非授权调用。（F3）**
b) **客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。（F3）**
c) **客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。（F3）**
d) **客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。（F3）**

### 8.3.5 安全建设管理

#### 8.3.5.1 移动应用软件采购

本项要求包括：

a) 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。
b) 应保证移动终端安装、运行的应用软件由指定的开发者开发。

#### 8.3.5.2 移动应用软件开发

本项要求包括：

a) 应对移动业务应用软件开发者进行资格审查。
b) 应保证开发移动业务应用软件的签名证书合法性。

### 8.3.6 安全运维管理

#### 8.3.6.1 配置管理

应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

## 8.4 物联网安全扩展要求

### 8.4.1 安全物理环境

#### 8.4.1.1 感知节点设备物理防护

本项要求包括：

a) 感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动、**使用环境与外壳防护等级（IP 代码）范围一致。（F3）**
b) 感知节点设备在工作状态所处物理环境应能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域）。
c) 感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等。
d) 关键感知节点设备应具有可供长时间工作的电力供应(关键网关节点设备应具有持久稳定的电力供应能力）。
e) **感知节点设备的部署应遵循封闭性原则，降低设备被非法拆除、非法篡改的风险。（F3）**

#### 8.4.1.2 感知网关节点设备物理安全要求

本项要求包括：

a) **感知网关节点设备应具有持久稳定的电力供应措施。（F3）**
b) **应保证感知网关节点设备所在物理环境具有良好的信号收发能力（如避免信道遭遇屏蔽）。（F3）**
c) **感知网关节点设备应具有定位装置。（F3）**

### 8.4.2 安全区域边界

#### 8.4.2.1 接入控制

本项要求包括：

a) 应保证只有授权的感知节点可以接入，**应保证感知节点、感知网关节点及处理应用层任意两者间相互鉴别和授权，非授权的感知节点、感知网关节点、处理应用层不能相互接入。（F3）**
b) **每个感知节点和感知网关节点应具备传感网络中唯一标识，且该标识不应被非授权访问所篡改。（F3）**
c) **具有指令接收功能的感知节点设备，应保证只有授权过的系统、终端可以对感知节点下发指令。（F3）**
d) **由第三方平台提供感知节点、感知网关节点中转接入时，第三方平台的安全保护等级应不低于接入的物联网系统的安全保护等级。（F3）**

#### 8.4.2.2 入侵防范

本项要求包括：

a) 应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为。
b) 应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。
c) **当感知网关节点检测到攻击行为时，应上报攻击源 IP、攻击类型、攻击时间等信息。（F3）**
d) **可编程的感知节点、网关节点禁止运行未授权的代码。（F3）**

### 8.4.3 安全计算环境

#### 8.4.3.1 感知节点设备安全

本项要求包括：

a) 应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。
b) 应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F3）**

c) 应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F3）**
d) **应具有保存密码、密钥、设备标识等安全相关数据的安全单元。（F3）**
e) **针对可编程的感知节点设备，应进行代码安全审计。（F3）**

#### 8.4.3.2 网关节点设备安全

本项要求包括：

a) 应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F3）**
b) 应具备过滤非法节点和伪造节点所发送的数据的能力。
c) 授权用户应能够在设备使用过程中对关键密钥进行在线更新。
d) 授权用户应能够在设备使用过程中对关键配置参数进行在线更新。
e) **对于具有数据处理能力的网关节点设备，授权用户应能够在设备使用过程中对相关处理逻辑进行在线更新。（F3）**
f) **对于具有数据处理能力的网关节点设备，应具备计算逻辑主动校验功能，防止处理逻辑被恶意篡改。（F3）**
g) **应具有保存密码、密钥、设备标识等安全相关数据的安全单元。（F3）**
h) **应进行代码安全审计。（F3）**

#### 8.4.3.3 抗数据重放

本项要求包括：

a) 应能够鉴别数据的新鲜性，避免历史数据的重放攻击。
b) 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

#### 8.4.3.4 数据融合处理

应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。

#### 8.4.3.5 访问控制

**未经过鉴别和授权的感知节点、感知网关节点、处理应用层不应相互访问。（F3）**

### 8.4.4 安全运维管理

#### 8.4.4.1 感知节点管理

本项要求包括：

a) 应指定人员**或使用自动化巡检手段**，定期**检查**感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护，**针对可编程的智能设备，应定期扫描处理逻辑、进行固件更新维护操作。（F3）**
b) 应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。
c) 应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。
d) **应在经过充分测试评估后，在不影响关键感知节点、感知网关节点安全稳定运行的情况下进行补丁、固件更新等工作。（F3）**
e) **关键感知节点、感知网关节点应通过安全传输通道进行固件与补丁更新，在检测到异常时应能将结果上报至安全管理中心。（F3）**

f) **针对监控类的感知节点设备，应设置安全阈值，对如设备长时间静默、电压过低、仓库温湿度与噪音等环境要素超过安全范围等情况，进行在线预警。（F3）**

g) **应对感知节点状态进行监测，发现异常时应定位处理。（F3）**

# 9 第四级安全要求

## 9.1 安全通用要求

### 9.1.1 安全物理环境

#### 9.1.1.1 物理位置选择

本项要求包括：

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内。

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

c) **机房应避开火灾危险程度高的区域，周围100米内不得有加油站、燃气站等危险建筑。（F4）**

#### 9.1.1.2 物理访问控制

本项要求包括：

a) 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

b) 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。

c) **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。（F4）**

#### 9.1.1.3 防盗窃和防破坏

本项要求包括：

a) 应将设备或主要部件**放入机柜中**进行固定**放置并配备安全锁，**并设置明显的不易除去的标识。**（F4）**

b) 应将通信线缆铺设在隐蔽安全处。

c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统，**机房主要出入口应安装如红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。（F4）**

d) **应建立机房视频监控系统和动环监控系统，并对监控内容进行记录，对机房风冷水电设备、消防设施、门禁系统等重要设施实行24小时全面监控，视频监控记录和门禁系统出入记录至少保存3个月。（F4）**

#### 9.1.1.4 防雷击

本项要求包括：

a) **机房所在建筑应设置防直击雷装置，根据要求装设建筑避雷针、避雷线、避雷网、避雷带等避雷装置，并定期对防雷设施进行维护和防雷检测。（F4）**

b) 应将各类机柜、设施和设备等通过接地系统安全接地。

c) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

d) **机房应通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。（F4）**

#### 9.1.1.5 防火

本项要求包括：

a) 机房应设置火灾自动消防系统，能够**通过在机房内、基本工作房间内、活动地板下、吊顶里及易燃物附近部位设置烟感、温感等多种方式**自动检测火情、自动报警，并自动灭火。**（F4）**
b) 机房及相关的工作房间和辅助房应采用具有**至少 2 级**耐火等级的建筑材料。**（F4）**
c) 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
d) **机房应备有一定数量的对电子设备影响小的手持式灭火器，消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发。（F4）**
e) **机房内部通道设置、装修装饰材料、设备线缆等应满足消防要求，并对机房进行消防验收，纸张、磁带和胶卷等易燃物品要放置于金属制的防火柜内。（F4）**
f) **主机房宜采用管网式洁净气体灭火系统，也可采用高压细水雾灭火系统，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动，凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。（F4）**
g) **应定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练。（F4）**
h) **机房应设置消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用，在机房通道上应设置显著的消防标志。（F4）**

#### 9.1.1.6 防水和防潮

本项要求包括：
a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
b) 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。
c) **为便于地下积水的转移，漏水隐患区域地面周围应设排水沟或地漏等排水设施，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。（F4）**
d) 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。
e) **应对温湿度调节设备安装漏水报警装置，并设置防水堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。（F4）**

#### 9.1.1.7 防静电

本项要求包括：
a) 应采用防静电地板或地面并采用必要的接地防静电措施。
b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
c) **主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。（F4）**
d) **进入机房应采取防尘措施，如准备鞋套，减少带入机房的灰尘。（F4）**

#### 9.1.1.8 温湿度控制

本项要求包括：
a) 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。
b) **机房应采用专用温湿度调节设备，并应满足机房监控系统的要求。（F4）**
c) **温湿度调节设备的工作能力应满足机房负载要求，并应保有一定的余量。（F4）**

#### 9.1.1.9 电力供应

本项要求包括：
a) 应在机房供电线路上配置稳压器和过电压防护设备。
b) 应**按照双路供电的原则**设置冗余或并行的电力电缆线路为计算机系统供电。**（F4）**
c) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

d) 应提供应急供电设施，**以备供电系统临时停电时启用，并确保应急供电设施能在UPS供电时间内到位，每年需进行应急供电设施的模拟演练，并定期对备用电力供应设备进行检修和维护，确保其能正常使用。（F4）**

e) **UPS供电系统的冗余方式应采用N+1、N+2、2N、2(N+1)等方式，负载功率小于单机UPS额定功率的80%，并通过两路独立市电提供UPS输入，未建立备用发电机应急供电系统的单位，UPS后备时间至少2小时，已建立备用发电机应急供电系统的单位，UPS后备时间应满足至少15分钟以上。（F4）**

f) **计算机系统供电应与其他供电分开，机房内要求采用机房专用插座，市电、UPS电源插座分开，满足负荷使用要求。（F4）**

g) **计算机系统应选用铜芯电缆，避免铜、铝混用，若不能避免时，应采用铜铝过渡头连接。（F4）**

h) **机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。（F4）**

i) **机房重要区域、重要设备应提供UPS单独供电，核心区域、重要设备应由不同的UPS提供双回路供电。（F4）**

#### 9.1.1.10 电磁防护

本项要求包括：

a) 电源线和通信线缆应隔离铺设，避免互相干扰。

b) 应对关键区域和关键设备**以及磁介质**实施电磁屏蔽。**（F4）**

### 9.1.2 安全通信网络

#### 9.1.2.1 网络架构

本项要求包括：

a) 应保证网络设备的业务处理能力满足业务高峰期需要，**如：业务处理能力能满足业务高峰期需要的 50%以上。（F4）**

b) 应保证网络各个部分的带宽满足业务高峰期需要。

c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。

d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性，**双线路设计时，宜由不同的电信运营商提供。（F4）**

f) 应按照业务服务的重要程度分配带宽，优先保障重要业务。

g) **应使用前置设备实现跨机构联网系统与入网金融机构业务主机系统的隔离，防止外部系统直接对入网金融机构业务主机的访问和操作。（F4）**

h) **应使用专用网络用于金融机构间的重要信息交换，与公用数据网络隔离。（F4）**

i) **机构应至少通过两条主干链路接入跨机构交易交换网络，并可根据实际情况选择使用专用的通信链路。两条主干链路应具有不同的路由，当一条链路发生异常时，另一条链路应能承载全部的交易数据。（F4）**

#### 9.1.2.2 通信传输

本项要求包括：

a) 应采用密码技术保证通信过程中数据的完整性，**并按照国家密码管理部门与行业有关要求使用密码算法。（F4）**

b) 应采用密码技术保证通信过程中数据的保密性，**并按照国家密码管理部门与行业有关要求使用密码算法。（F4）**
c) 应在通信前基于密码技术对通信的双方进行验证或认证。
d) 应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。

#### 9.1.2.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

### 9.1.3 安全区域边界

#### 9.1.3.1 边界防护

本项要求包括：

a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制。
c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制。
d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
e) 应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断。
f) 应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。

#### 9.1.3.2 访问控制

本项要求包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。
d) 应能根据会话状态信息为进出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。（F4）**
e) 应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。
f) **对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。（F4）**
g) **应每季度检查并锁定或撤销网络设备中不必要的用户账号。（F4）**

#### 9.1.3.3 入侵防范

本项要求包括：

a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。
c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。
d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
e) **应采取技术手段对高级持续威胁进行监测、发现。（F4）**
f) **入侵检测的管理系统应做到分级管理，对系统的部署做到逐级分布。（F4）**

g) **应采用联动防护机制，及时识别网络攻击行为，并实现快速处置。（F4）**

#### 9.1.3.4 恶意代码和垃圾邮件防范

本项要求包括：

a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

#### 9.1.3.5 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b) **应记录无线网络接入行为，形成日志进行留存，保存时间不少于6个月。（F4）**

c) 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) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，**审计记录保存时间不少于6个月。（F4）**

e) **所有的审计手段需要具备统一的时间戳，保持审计的时间标记一致。（F4）**

#### 9.1.3.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

### 9.1.4 安全计算环境

#### 9.1.4.1 身份鉴别

本项要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，**应实现身份鉴别信息防窃取和防重用。静态口令应在8位以上，由字母、数字、符号等混合组成，至少每90天更换口令一次，不允许新设定的口令与前三次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定期更换。（F4）**

b) 应具有登录失败处理功能，应配置并启用结束会话、**限制登录间隔**、限制非法登录次数和当登录连接超时自动退出等相关措施。**（F4）**

c) **操作系统和数据库系统应设置鉴别警示信息，当出现越权访问或尝试非法访问时，系统会自动提示未授权访问。（F4）**

d) 当进行远程管理时，**应对终端进行身份标识和鉴别，采用密码技术**防止鉴别信息在网络传输过程中被窃听。**（F4）**

e) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

#### 9.1.4.2 访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限。

b) 应重命名或删除默认账户，修改默认账户**和预设账户**的默认口令。**（F4）**

c) **应用系统应强制首次登录的用户修改默认账户或预设账户的默认口令。（F4）**

d) **宜通过技术手段定期检测是否存在多余的、过期的账户。（F4）**

e) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。
f) 应授予管理用户所需的最小权限，实现管理用户的权限分离。
g) **应严格限制默认账户或预设账户的权限，如默认账户或预设账户的权限应为空权限或某单一功能专用权限等。（F4）**
h) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。
i) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。
j) 应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。

#### 9.1.4.3 安全审计

本项要求包括：

a) 应启用安全审计功能，审计应覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
b) 审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等。
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，**审计记录保存时间应不少于6个月。（F4）**
d) 应对审计进程**或程序**进行保护，防止未经授权的中断。**（F4）**
e) **对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息，以便能够及时发现可能的问题。（F4）**
f) **审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正确性。（F4）**

#### 9.1.4.4 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序。
b) 应关闭不需要的系统服务、默认共享和高危端口。
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。
d) 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内容符合系统设定要求。
e) 应能**通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时发**现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。**（F4）**
f) 应能够检测到对**所有**节点进行入侵的行为，并在发生严重入侵事件时提供报警。**（F4）**
g) **所有安全计算环境设备应全部专用化，生产设备不得进行与业务不相关的操作。（F4）**
h) **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或间接反馈到前台界面。（F4）**

#### 9.1.4.5 恶意代码防范

本项要求包括：

a) 应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
b) **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。（F4）**

#### 9.1.4.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

#### 9.1.4.7 数据完整性

本项要求包括：

a) 应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

b) 应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

c) 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。**证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录，交易系统还应能够详细记录用户合规交易数据，如业务流水号、账户名、IP地址、交易指令等信息以供审计，并能够追溯到用户。（F4）**

#### 9.1.4.8 数据保密性

本项要求包括：

a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据**和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护其存储过程中的保密性。（F4）**

#### 9.1.4.9 数据备份恢复

本项要求包括：

a) 应提供重要数据的本地数据备份与恢复功能，**采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指标（如RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放，数据保存期限依照国家相关规定。（F4）**

b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。

d) 应建立异地灾难备份中心，提供业务应用的实时切换。

e) **对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。（F4）**

f) **为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果。（F4）**

g) **数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以1个月为周期的数据冗余。（F4）**

h) **异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资源（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。（F4）**

#### 9.1.4.10 剩余信息保护

本项要求包括：

a） 应保证**操作系统、数据库系统和应用系统用户**鉴别信息所在的存储空间被释放或重新分配前得到完全清除，**无论这些信息是存放在硬盘上还是内存中。（F4）**

b) 应保证**操作系统、数据库系统和应用系统用户**存有敏感数据的存储空间被释放或重新分配前得到完全清除，**无论这些信息是存放在硬盘上还是内存中。（F4）**

#### 9.1.4.11 个人信息保护

本项要求包括：

a) **金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。（F4）**

b) 应仅采集和保存业务必需的用户个人**金融**信息。 **（F4）**

c) **应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限，**应禁止未授权访问和非法使用用户个人**金融**信息。**（F4）**

d) **金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F4）**

e) **金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸面（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F4）**

f) **应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F4）**

g) **开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F4）**

### 9.1.5 安全管理中心

#### 9.1.5.1 系统管理

本项要求包括：

a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

c) **应每月对设备的配置文件进行备份，发生变动时应及时备份。（F4）**

d) **应使用自动化监控平台对设备运行状况进行实时监测，运维人员应每天定期查看并记录系统运行状况。（F4）**

e) **应每月检验网络设备软件版本信息，并通过有效测试验证进行相应的升级，同时留存测试验证相关记录。（F4）**

#### 9.1.5.2 审计管理

本项要求包括：

a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。

b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

c) **应严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审计用户的权限分离，避免非授权的删除、修改或覆盖。（F4）**

#### 9.1.5.3 安全管理

本项要求包括：

a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。

b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

#### 9.1.5.4 集中管控

本项要求包括：

a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。

b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。

c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。

d) 应对分散在各个设备上的**安全事件、**审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。**（F4）**

e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

f) 应能对网络中发生的各类安全事件进行识别、报警、分析**、响应和处置。（F4）**

g) 应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。

h) **应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。（F4）**

### 9.1.6 安全管理制度

#### 9.1.6.1 安全策略

应制定**全机构范围**网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等，**并编制形成网络安全方针制度文件。（F4）**

#### 9.1.6.2 管理制度

本项要求包括：

a) 应对安全管理活动中的各类管理内容建立安全管理制度。

b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。

c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

#### 9.1.6.3 制定和发布

本项要求包括：

a) **金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应负责制定适用辖内的安全管理制度。（F4）**

b) 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。

c) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。

#### 9.1.6.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度

进行修订。

#### 9.1.7 安全管理机构

##### 9.1.7.1 岗位设置

本项要求包括：

a) **网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。（F4）**

b) 应**设立由本机构领导、业务与技术相关部门主要负责人组成的**网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权，**负责协调本机构及辖内网络安全管理工作，决策本机构及辖内网络安全重大事宜。（F4）**

c) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。

d) 应设立系统管理员、审计管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

e) **应设立专门的网络安全审计岗位，负责网络安全审计制度和流程的实施，制订和执行网络安全审计计划，对网络安全整个生命周期和重大事件等进行审计。（F4）**

f) **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，信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。（F4）**

g) **除网络安全管理部门外，其他部门均应指定至少一名网络安全员，协助网络安全管理部门开展本部门的网络安全管理工作。（F4）**

##### 9.1.7.2 人员配备

本项要求包括：

a) 应配备一定数量的系统管理员、审计管理员和安全管理员等。

b) 应配备专职安全管理员，不可兼任。

c) 关键事务岗位应配备多人共同管理。

d) **应定期对网络安全重要岗位人员进行轮换。（F4）**

##### 9.1.7.3 授权和审批

本项要求包括：

a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。

b) 应针对**系统投入运行、重要资源（如敏感数据等资源）的访问、**系统变更、重要操作、物理访问和系统接入等事项建立审批程序，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。**（F4）**

c) 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。

d) **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。（F4）**

e) **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。（F4）**

##### 9.1.7.4 沟通和合作

本项要求包括：

a) 应加强各类管理人员、组织内部机构以及网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。

b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。
c) 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。

#### 9.1.7.5 审核和检查

本项要求包括：

a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
b) 应定期进行全面安全检查，检查内容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。
c) **应建立对门户网站内容发布的审核、管理和监控机制。（F4）**
d) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，对安全检查结果进行通报并报上一级机构科技部门备案。（F4）**
e) **应制定违反和拒不执行安全管理措施规定的处罚细则。（F4）**

### 9.1.8 安全管理人员

#### 9.1.8.1 人员录用

本项要求包括：

a) 应指定或授权专门的部门或人员负责人员录用。
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。
c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
d) 应从内部人员中选拔从事关键岗位的人员。
e) **应对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。（F4）**
f) **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，不应从事网络安全管理工作。（F4）**

#### 9.1.8.2 人员离岗

本项要求包括：

a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
b) 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，**并保证离岗人员负责的信息技术系统的口令立即更换。（F4）**

#### 9.1.8.3 人员考核

本项要求包括：

a) **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。（F4）**
b) **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。（F4）**
c) **应建立保密制度，并定期或不定期的对保密制度执行情况进行检查或考核。（F4）**
d) **应对考核结果进行记录并保存。（F4）**

#### 9.1.8.4 安全意识教育和培训

本项要求包括：

a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

b) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。
c) **每年应至少对网络安全管理人员进行一次网络安全培训。（F4）**
d) 应定期对不同岗位的人员进行技术技能考核。
e) **应对安全教育和培训的情况和结果进行记录并归档保存。（F4）**

#### 9.1.8.5 外部人员访问管理

本项要求包括：

a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。
c) **应对允许被外部人员访问的金融机构计算机系统和网络资源，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。（F4）**
d) 外部人员离场后应及时清除其所有的访问权限。
e) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权的**增加、删除、修改、查询数据等**操作，不得复制和泄露**金融机构的任何信息。（F4）**
f) 对关键区域或关键系统不允许外部人员访问。

### 9.1.9 安全建设管理

#### 9.1.9.1 定级和备案

本项要求包括：

a) 应将备案材料报主管部门和相应公安机关备案。
b) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。
c) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。
d) 应保证定级结果经过相关部门的批准。

#### 9.1.9.2 安全方案设计

本项要求包括：

a) 应根据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) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。
c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
d) **使用上一级机构信息系统资源或对其他机构信息系统资源与配置造成影响的区域性建设项目，项目建设方案应分别通过上一级机构业务与科技部门的审核、批准。（F4）**

#### 9.1.9.3 产品采购和使用

本项要求包括：

a) 应确保网络安全产品采购和使用符合国家的有关规定。
b) 应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。
c) **各机构购置扫描、检测类网络安全产品应报本机构科技主管部门批准、备案。（F4）**
d) 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。
e) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。
f) **扫描、检测类网络安全产品仅限于本机构网络安全管理人员使用。（F4）**

g) **应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取整改措施并按规定程序报告。（F4）**
h) **应定期对各类网络安全产品产生的日志和报表进行备份存档，至少保存6个月。（F4）**
i) **应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。（F4）**
j) **应在本地配置网络安全产品。（F4）**

#### 9.1.9.4 自行软件开发

本项要求包括：

a) 应将开发环境与实际运行环境物理分开，**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**，测试数据和测试结果受到控制。**（F4）**
b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。
c) 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。
d) 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
e) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制。
f) 应在软件开发过程中对**代码规范、代码质量、代码安全性进行审查，**在软件安装前对可能存在的恶意代码进行检测。**（F4）**
g) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。
h) **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。（F4）**

#### 9.1.9.5 外包软件开发

本项要求包括：

a) 应在软件交付前检测其中可能存在的恶意代码。
b) 应保证开发单位提供软件设计文档和使用指南。
c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
d) **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。（F4）**
e) **应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F4）**
f) **应要求外包服务商每年至少开展一次网络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。（F4）**

#### 9.1.9.6 工程实施

本项要求包括：

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) 应制定安全工程实施方案控制工程实施过程。
c) **针对涉及到新旧数据系统切换的工程实施，应选择对客户影响较小的时间段进行。系统切换时间超过一个工作日，需至少提前5个工作日发布提示公告，并提供应急服务途径。（F4）**
d) 应通过第三方工程监理控制项目的实施过程。
e) **应制定灾难备份系统集成与测试计划并组织实施，通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求。（F4）**
f) **系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。（F4）**

#### 9.1.9.7 测试验收

本项要求包括：

a) 应**根据设计方案或合同要求等**制订测试验收方案，并依据测试验收方案实施测试验收，**应详细记录测试验收结果**，形成测试验收报告。**（F4）**

b) 应**由项目承担单位（部门）或公正的第三方制订安全测试方案，**进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容，**并将测试报告报科技部门审查。（F4）**

c) **新建应用系统投入生产运行前，原则上应进行不少于1个月的模拟运行和不少于3个月的试运行。（F4）**

d) **对于在生产系统上进行的测试工作，应先进行风险分析和告知，同时制定详细的系统测试方案、数据备份与系统恢复措施、应急处置措施后，经系统用户和主管领导审批同意后，才能开展测试工作，以确保生产系统的安全。（F4）**

#### 9.1.9.8 系统交付

本项要求包括：

a) 应制定交付清单，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) **建设单位应在完成建设任务后将建设过程文档和运维文档全部移交科技部门。（F4）**

c) 应对负责运行维护的技术人员进行相应的技能培训。

d) **外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将采用的关键安全技术措施和核心安全功能设计对外公开。（F4）**

#### 9.1.9.9 等级测评

本项要求包括：

a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。

b) 应在发生重大变更或级别发生变化时进行等级测评。

c) **应选择公安部认可的全国等级保护测评机构推荐目录中的测评单位进行等级测评，并与测评单位签订安全保密协议。（F4）**

#### 9.1.9.10 服务供应商选择

本项要求包括：

a) **应评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。（F4）**

b) 应确保服务供应商的选择符合国家的有关规定。

c) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。

d) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

### 9.1.10 安全运维管理

#### 9.1.10.1 环境管理

本项要求包括：

a) **机房布线应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F4）**

b) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，**每天巡查机房运行状况，**定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理，**填写机房值班记录、巡视记录。（F4）**

c) 应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作出规定。

d) **进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。（F4）**
e) **机房管理员应经过相关培训，掌握机房各类设备的操作要领。（F4）**
f) **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F4）**
g) **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单位主管领导批准后实施。（F4）**
h) **应设置弱电井，并留有足够的可扩展空间。（F4）**
i) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
j) 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等。

#### 9.1.10.2 资产管理

本项要求包括：

a) 应编制并保存与保护对象相关的资产清单，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。
c) 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。

#### 9.1.10.3 介质管理

本项要求包括：

a) 应将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，并根据存档介质的目录清单定期盘点。
b) **所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F4）**
c) 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，做好防信息泄漏控制措施**，并对介质的归档和查询等进行登记记录。**（F4）**
d) **对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开，如是电子文档则应进行电子化审批流转登记管理。（F4）**
e) **对载有敏感信息存储介质的销毁，应报有关部门备案，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。（F4）**
f) **应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F4）**
g) **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科技部门指定的同城或异地安全区域。（F4）**
h) **应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。（F4）**
i) **应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F4）**

#### 9.1.10.4 设备维护管理

本项要求包括：

a) 应对各种设备（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、维修和服务的审批、维修过程的监督控制等。
c) **设备确需送外单位维修时，应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。（F4）**

d) **制定规范化的故障处理流程，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）。（F4）**

e) **新购置的设备应经过验收，验收合格后方能投入使用。（F4）**

f) **应制定设备管理规范，根据设备使用年限，及时进行更换升级，落实设备使用者的安全保护责任。（F4）**

g) 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。

h) **需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复性销毁处理，同时备案；信息消除处理仅限于废止设备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。（F4）**

#### 9.1.10.5 漏洞和风险管理

本项要求包括：

a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

#### 9.1.10.6 网络和系统安全管理

本项要求包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。

b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。

c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。

d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。

e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容，**重要运维操作要求至少两人在场，保留记录，并由操作和复核人员进行确认，维护记录和确认记录应至少妥善保存6个月。（F4）**

f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。

g) **金融行业网间互联安全应实行统一规范、分级管理、各负其责的安全管理模式，未经金融机构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。（F4）**

h) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。

i) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

j) **应制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部门（岗）开启远程访问服务，经过审批后才可开通，操作过程中应保留不可篡改的审计日志，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。（F4）**

k) **各机构应以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。（F4）**

l) **网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不应对外公开，未经科技主管部门授权，任何外部机构与人员不应检测或扫描机构内部网络。（F4）**

m) **所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。（F4）**

n) **网络系统应采取定时巡检、定期检修和阶段性评估的措施，业务高峰时段和业务高峰日要加强巡检频度和力度，确保硬件可靠、运转正常。（F4）**

o) **系统管理员不应兼任业务操作人员，系统管理员不应对业务数据进行任何增加、删除、修改等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门审批，并详细记录维护内容、人员、时间等信息。（F4）**

p) **每季度应至少进行一次漏洞扫描，对发现的网络安全漏洞及时进行修补，扫描结果应及时上报。（F4）**

q) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。

r) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

s) **网络和系统管理员应对网络和系统变更进行详细的记录。（F4）**

#### 9.1.10.7 恶意代码防范管理

本项要求包括：

a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。

b) **客户端应统一安装病毒防治软件，设置用户口令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。（F4）**

c) 应定期验证防范恶意代码攻击的技术措施的有效性。

#### 9.1.10.8 配置管理

本项要求包括：

a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

#### 9.1.10.9 密码管理

本项要求包括：

a) 应遵循密码相关的国家标准和行业标准。

b) **选用的密码产品和加密算法应符合国家相关密码管理政策规定，应优先使用国产密码算法。（F4）**

c) 应使用国家密码管理主管部门认证核准的密码技术和产品。

d) 应采用硬件密码模块实现密码运算和密钥管理。

e) **应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理。（F4）**

f) **系统管理员、数据库管理员、网络管理员、业务操作人员均应设置口令密码，至少每3个月更换一次，口令密码的强度应满足不同安全性要求。（F4）**

g) **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，未经科技部门主管领导许可，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。（F4）**

h) 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。（F4）
i) 确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F4）
j) 应支持各类环境中密码设备使用、管理权限分离。（F4）

9.1.10.10 变更管理

本项要求包括：

a) 变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并得到客户的确认。（F4）
b) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。
c) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。
d) 应建立中止变更并从失败变更中恢复的程序，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。
e) 变更前应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。（F4）
f) 如果需要对生产环境进行重大变更，应按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同意后，再进行变更操作，以确保生产系统的安全。（F4）
g) 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。（F4）

9.1.10.11 备份与恢复管理

本项要求包括：

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) 应制定数据备份与恢复相关安全管理制度，对备份信息的备份方式、备份频度、存储介质、保存期等进行规范。（F4）
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
d) 应每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性和灾难发生时的可获取性。（F4）
e) 应每季度对备份数据的有效性进行检查。备份数据要实行异地保存。（F4）
f) 灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾难恢复策略。（F4）
g) 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。（F4）
h) 应定期开展灾难恢复培训，在条件许可的情况下，由相关部门统一部署，至少每年进行一次灾难恢复演练，包括异地备份站点切换演练和本地系统灾难恢复演练；异地备份站点切换：在异地建立热备份站点，当主站点因发生灾难导致系统不可恢复时异地备份站点能承担起主

**站点的功能，本地系统灾难恢复：当本地系统发生异常中断时能够在短时间恢复和保障业务数据的可运行性。（F4）**

i) **金融机构应根据信息系统的灾难恢复工作情况，确定审计频率，应每年至少组织一次内部灾难恢复工作审计。（F4）**

j) **应安排专人负责灾难恢复预案的日常维护管理。（F4）**

k) **应建立灾难备份系统，主备系统实际切换时间应满足实时切换，灾备系统处理能力应不低于主用系统处理能力的50%，通信线路应分别接入主备系统。有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。（F4）**

9.1.10.12 安全事件处置

本项要求包括：

a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件。

b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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。

d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

e) 应建立联合防护和应急机制，负责处置跨单位安全事件。

9.1.10.13 应急预案管理

本项要求包括：

a) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容，**业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字确认。（F4）**

b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。

c) 应**每年**对系统相关的人员进行应急预案培训，并进行应急预案的演练。**（F4）**

d) 应定期对原有的应急预案重新评估，修订完善。

e) 应建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练。

f) **在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练。（F4）**

g) **突发事件应急处置领导小组应统一领导应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。（F4）**

h) **突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F4）**

i) **实施报告制度和启动应急预案的单位应实行重大突发事件24小时值班制度。（F4）**

j) **应急演练结束后，应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。（F4）**

9.1.10.14 外包运维管理

本项要求包括：

a) 应确保外包运维服务商的选择符合国家的有关规定。

b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

c） 应保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确。

d） 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。

e） **应要求外包运维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。（F4）**

f） **应制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F4）**

## 9.2 云计算安全扩展要求

### 9.2.1 安全物理环境

#### 9.2.1.1 基础设施位置

本项要求包括：

a） 应保证云计算基础设施位于中国境内。

b） **对于团体云部署模式，应保证用于服务金融行业的云计算数据中心的物理服务器与其他行业物理隔离。（F4）**

c） **应保证云计算平台的运维和运营系统部署在中国境内。（F4）**

### 9.2.2 安全通信网络

#### 9.2.2.1 网络架构

本项要求包括：

a） 应保证云计算平台不承载高于其安全保护等级的业务应用系统。

b） 应实现不同云服务客户虚拟网络之间**及同一云服务客户不同虚拟网络之间**的隔离。**（F4）**

c） **应实现云计算平台的业务网络与管理网络安全隔离。（F4）**

d） 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。

e） 应具有根据云服务客户业务需求自主设置安全策略的能力，包括**划分安全区域、**定义访问路径、选择安全组件、配置安全策略。**（F4）**

f） 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

g） 应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问。

h） 应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式。

i） 应为第四级业务应用系统划分独立的资源池。

j） **对于团体云部署模式，应保证除广域网外为金融行业服务的网络物理硬件不与其他行业共享。（F4）**

k） **应支持云服务客户监控所拥有各网络节点间的流量。（F4）**

### 9.2.3 安全区域边界

#### 9.2.3.1 访问控制

本项要求包括：

a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
c) **应实现虚拟机之间、虚拟机与资源管理和调度平台之间、虚拟机与外部网络之间的安全访问控制。（F4）**
d) **应对云计算平台管理员访问管理网络进行访问控制。（F4）**
e) **应支持云服务客户通过VPN访问云计算平台。（F4）**
f) **应支持云服务客户自行在虚拟网络边界设置访问控制规则。（F4）**
g) **应支持云服务客户自行划分子网、设置访问控制规则。（F4）**

#### 9.2.3.2 入侵防范

本项要求包括：

a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。
d) 应在检测到网络攻击行为、异常流量情况时进行告警。
e) **应检测和防护云计算平台内部虚拟机发起的针对云计算平台的攻击，能够定位发起攻击的虚拟机，记录攻击类型、攻击时间、攻击流量等信息。（F4）**
f) **云服务客户通过互联网提供金融服务时，应支持DoS/DDoS攻击防护，通过清洗DoS/DDoS攻击流量，保障网络、服务器及上层应用的可用性。（F4）**
g) **云服务客户通过互联网提供金融服务时，应支持检测Web应用漏洞，拦截SQL注入、XSS攻击等多种Web应用攻击行为。（F4）**

#### 9.2.3.3 安全审计

本项要求包括：

a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。
b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

### 9.2.4 安全计算环境

#### 9.2.4.1 身份鉴别

本项要求包括：

a) 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。
b) **应支持云服务客户密码策略管理，密码策略管理应支持密码复杂度策略、密码有效期策略，云服务客户账号的初始密码应支持随机生成，云服务客户首次登录支持强制修改初始密码。（F4）**
c) **应支持为云服务客户随机生成虚拟机登录口令或云服务客户自行设置登录口令。（F4）**
d) **应支持云服务客户以密钥对方式登录虚拟机时，自主选择云计算平台生成密钥对或自行上传密钥对。（F4）**
e) **应支持云服务客户自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别。（F4）**
f) **应支持集中管理云服务客户鉴别凭证。（F4）**
g) **应支持修改云服务客户鉴别凭证前验证云服务客户身份。（F4）**
h) **应支持检测云服务客户账户异常并通知云服务客户。（F4）**

#### 9.2.4.2 访问控制

本项要求包括：

a) 应保证当虚拟机迁移时，访问控制策略随其迁移。
b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。
c) **应禁止云服务商或第三方未授权操作云服务客户资源。（F4）**

#### 9.2.4.3 入侵防范

本项要求包括：

a) 应能检测虚拟机之间的资源隔离失效，并进行告警。
b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警。
c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。
d) **应能够检测虚拟机对宿主机资源的异常访问，并进行告警。（F4）**
e) **应对虚拟机启动和运行过程进行完整性保护。（F4）**
f) **应对虚拟机重要配置文件进行完整性保护。（F4）**

#### 9.2.4.4 恶意代码防范

本项要求包括：

a) **应支持对后门、木马、蠕虫、webshell等恶意代码的静态检测和行为检测，并对检测出的恶意代码进行控制和隔离。（F4）**
b) **应支持云服务客户自行安装防恶意代码软件，并支持更新防恶意代码软件版本和恶意代码库。（F4）**

#### 9.2.4.5 镜像和快照保护

本项要求包括：

a) 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。
b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。
c) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。
d) **应保证虚拟机镜像和快照文件备份在不同物理服务器。（F4）**
e) **应支持自动虚拟机快照功能，保证系统能根据快照恢复。（F4）**

#### 9.2.4.6 数据完整性和保密性

本项要求包括：

a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。
b) 应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限。
c) 应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
d) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。
e) **应支持云服务客户选择第三方密钥加解密数据，密钥支持云服务客户自管理、云服务商管理和第三方机构管理。（F4）**
f) **应支持云服务客户对云计算平台上的数据进行加密存储。（F4）**

#### 9.2.4.7 数据备份恢复

本项要求包括：

a) 云服务客户应在本地保存其业务数据的备份。
b) 应提供查询云服务客户数据及备份存储位置的能力。

c) 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致。
d) 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。
e) **应周期性测试云计算平台的备份系统和备份数据，支持故障识别和备份重建。（F4）**

#### 9.2.4.8 剩余信息保护

本项要求包括：
a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除。
b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除，**不能通过软件工具恢复。（F4）**
c) **对于更换或报废的存储介质，应采取安全删除、强化消磁或者物理损坏磁盘等方式，防止恢复已清除数据。（F4）**

### 9.2.5 安全管理中心

#### 9.2.5.1 集中管控

本项要求包括：
a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配。
b) 应保证云计算平台管理流量与云服务客户业务流量分离。
c) 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计。
d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等运行状况的集中监测，**监测内容包括CPU利用率、带宽使用情况、内存利用率、存储使用情况等。（F4）**
e) **应对异常行为集中监控分析并告警。集中监控服务质量，并可导出集中监控报告。应支持远程监控的可视化展示。（F4）**

### 9.2.6 安全建设管理

#### 9.2.6.1 云服务商选择

本项要求包括：
a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。
b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标。
c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
e) 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。

#### 9.2.6.2 供应链管理

本项要求包括：
a) 应确保供应商的选择符合国家有关规定。
b) 应将供应链安全事件信息或威胁信息及时传达到云服务客户。

c) 应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

d) **应分析外包服务或采购产品对云服务安全性的影响。（F4）**

e) **与供应商签订的服务水平协议中的相关指标，不低于拟与客户所签订的服务水平协议中的相关指标。（F4）**

f) **当变更供应商时，对供应商变更带来的安全风险进行评估，采取有效措施控制风险。（F4）**

#### 9.2.7 安全运维管理

##### 9.2.7.1 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

##### 9.2.7.2 网络和系统安全管理

**云服务商应制定相关策略，持续监控设备、资源、服务以及安全措施的有效性，并将安全措施有效性的监控结果定期提供给云服务客户。（F4）**

##### 9.2.7.3 应急预案管理

**云服务提供商应将应急预案提前告知云服务客户。（F4）**

### 9.3 移动互联安全扩展要求

#### 9.3.1 安全物理环境

##### 9.3.1.1 无线接入点的物理位置

本项要求包括：

a) 应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

b) **应为无线接入设备的安装选择合理位置，避免被非法破坏、替换。（F4）**

#### 9.3.2 安全通信网络

##### 9.3.2.1 通信传输

本项要求包括：

a) **应在移动终端与服务器之间建立安全的信息传输通道，例如使用有效安全版本的TLS或IPSec等协议。（F4）**

b) **客户端应用软件与服务器应进行双向认证，可通过密钥、证书等密码技术手段实现服务器与客户端应用软件之间的安全认证。（F4）**

c) **通过客户端应用软件发起的资金类交易报文，应确保交易报文的不可抵赖性，在有条件的情况下应采用数字证书技术。（F4）**

d) **通过客户端应用软件发起的资金类交易报文或客户敏感信息变更报文，应能够防止重放攻击。（F4）**

#### 9.3.3 安全区域边界

##### 9.3.3.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

#### 9.3.3.2 访问控制

无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

#### 9.3.3.3 入侵防范

本项要求包括：

a) 应能够检测到非授权无线接入设备和非授权移动终端的接入行为。
b) 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。
c) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。
d) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。
e) 应禁止多个 AP 使用同一个认证密钥。
f) 应能够阻断非授权无线接入设备或非授权移动终端。

### 9.3.4 安全计算环境

#### 9.3.4.1 移动终端管控

本项要求包括：

a) 应保证移动终端安装、注册并运行终端管理客户端软件。
b) 移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。
c) 应保证移动终端只用于处理指定业务。

#### 9.3.4.2 移动应用管控

本项要求包括：

a) 应具有选择应用软件安装、运行的功能。
b) 应只允许指定证书签名的应用软件安装和运行。
c) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。
d) 应具有接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。

#### 9.3.4.3 访问控制

本项要求包括：

a) **客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。（F4）**
b) **应采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问。（F4）**
c) **客户端应用软件在授权范围内，不应访问非业务必需的文件和数据。（F4）**

#### 9.3.4.4 安全审计

**客户端应用软件运行日志中不应打印支付敏感信息，不应打印完整的敏感数据原文。（F4）**

#### 9.3.4.5 入侵防范

本项要求包括：

a) **客户端应用软件应配合业务交易风险控制策略，以安全的方式将相关信息上送至风险控制系统（F4）**

b) **客户端应用软件应对软件接口进行保护，防止其他应用对客户端应用软件接口进行非授权调用。（F4）**
c) **客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。（F4）**
d) **客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。（F4）**
e) **客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。（F4）**

#### 9.3.5 安全建设管理

##### 9.3.5.1 移动应用软件采购

本项要求包括：
a) 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。
b) 应保证移动终端安装、运行的应用软件由指定的开发者开发。

##### 9.3.5.2 移动应用软件开发

本项要求包括：
a) 应对移动业务应用软件开发者进行资格审查。
b) 应保证开发移动业务应用软件的签名证书合法性。

#### 9.3.6 安全运维管理

##### 9.3.6.1 配置管理

应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

### 9.4 物联网安全扩展要求

#### 9.4.1 安全物理环境

##### 9.4.1.1 感知节点设备物理防护

本项要求包括：
a) 感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动、**使用环境与外壳防护等级（IP 代码）范围一致。（F4）**
b) 感知节点设备在工作状态所处物理环境应能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域）。
c) 感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等。
d) 关键感知节点设备应具有可供长时间工作的电力供应(关键网关节点设备应具有持久稳定的电力供应能力）。
e) **感知节点设备的部署应遵循封闭性原则，降低设备被非法拆除、非法篡改的风险。（F4）**

##### 9.4.1.2 感知网关节点设备物理安全要求

本项要求包括：
a) **感知网关节点设备应具有持久稳定的电力供应措施。（F4）**

b) **应保证感知网关节点设备所在物理环境具有良好的信号收发能力（如避免信道遭遇屏蔽）。（F4）**

c) **感知网关节点设备应具有定位装置。（F4）**

### 9.4.2 安全区域边界

#### 9.4.2.1 接入控制

本项要求包括：

a) 应保证只有授权的感知节点可以接入，**应保证感知节点、感知网关节点及处理应用层任意两者间相互鉴别和授权，非授权的感知节点、感知网关节点、处理应用层不能相互接入。（F4）**

b) **每个感知节点和感知网关节点应具备传感网络中唯一标识，且该标识不应被非授权访问所篡改。（F4）**

c) **具有指令接收功能的感知节点设备，应保证只有授权过的系统、终端可以对感知节点下发指令。（F4）**

d) **由第三方平台提供感知节点、感知网关节点中转接入时，第三方平台的安全保护等级应不低于接入的物联网系统的安全保护等级。（F4）**

#### 9.4.2.2 入侵防范

本项要求包括：

a) 应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为。

b) 应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

c) **当感知网关节点检测到攻击行为时，应上报攻击源 IP、攻击类型、攻击时间等信息。（F4）**

d) **可编程的感知节点、网关节点禁止运行未授权的代码。（F4）**

### 9.4.3 安全计算环境

#### 9.4.3.1 感知节点设备安全

本项要求包括：

a) 应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。

b) 应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F4）**

c) 应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力，**至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F4）**

d) **应具有保存密码、密钥、设备标识等安全相关数据的安全单元。（F4）**

e) **针对可编程的感知节点设备，应进行代码安全审计。（F4）**

#### 9.4.3.2 网关节点设备安全

本项要求包括：

a) 应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力，**能够对感知终端进行鉴别，至少支持基于网络标识、MAC 地址、通信协议、通信端口、口令其一的身份鉴别机制。（F4）**

b) 应具备过滤非法节点和伪造节点所发送的数据的能力。

c) 授权用户应能够在设备使用过程中对关键密钥进行在线更新。

d) 授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

e) **对于具有数据处理能力的网关节点设备，授权用户应能够在设备使用过程中对相关处理逻辑进行在线更新。（F4）**
f) **对于具有数据处理能力的网关节点设备，应具备计算逻辑主动校验功能，防止处理逻辑被恶意篡改。（F4）**
g) **应具有保存密码、密钥、设备标识等安全相关数据的安全单元。（F4）**
h) **应进行代码安全审计。（F4）**

#### 9.4.3.3 抗数据重放

本项要求包括：

a) 应能够鉴别数据的新鲜性，避免历史数据的重放攻击。
b) 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

#### 9.4.3.4 数据融合处理

本项要求包括：

a) 应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。
b) 应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令。

#### 9.4.3.5 访问控制

**未经过鉴别和授权的感知节点、感知网关节点、处理应用层不应相互访问。（F4）**

### 9.4.4 安全运维管理

#### 9.4.4.1 感知节点管理

本项要求包括：

a) 应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护，**针对可编程的智能设备，应定期扫描处理逻辑、进行固件更新维护操作。（F4）**
b) 应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。
c) 应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。
d) **应在经过充分测试评估后，在不影响关键感知节点、感知网关节点安全稳定运行的情况下进行补丁、固件更新等工作。（F4）**
e) **关键感知节点、感知网关节点应通过安全传输通道进行固件与补丁更新，在检测到异常时应能将结果上报至安全管理中心。（F4）**
f) **针对监控类的感知节点设备，应设置安全阈值，对如设备长时间静默、电压过低、仓库温湿度与噪音等环境要素超过安全范围等情况，进行在线预警。（F4）**
g) **应对感知节点状态进行监测，发现异常时应定位处理。（F4）**

# 附 录 A
（规范性附录）
## 关于金融行业安全通用要求、安全扩展要求和增强性安全要求的选择和使用

由于等级保护对象承载的业务不同，对其安全关注点会有所不同，有的更关注信息的安全性，即更关注搭线窃听、假冒用户等可能导致的信息泄密、非法篡改；有的更关注业务的连续性，即更关注保证系统连续正常的运行，免受对系统未授权的修改、破坏而导致系统不可用引起业务中断。

不同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求是有差异的，即使相同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求也有差异。等级保护对象的安全保护等级由业务信息安全性等级和系统服务保证性等级较高者决定（见 GB/T 22240—2020），因此，对某一个定级后的等级保护对象的安全保护的侧重点可以有多种组合。

等级保护对象定级后，可能形成的定级结果组合见表 A.1。

**表 A.1 各等级保护对象定级结果组合**

| 安全保护等级 | 等级保护对象定级结果组合 |
|---|---|
| 第二级 | S1A2，S2A2，S2A1 |
| 第三级 | S1A3，S2A3，S3A3，S3A2，S3A1 |
| 第四级 | S1A4，S2A4，S3A4，S4A4，S4A3，S4A2，S4A1 |

安全保护措施的选择应依据上述定级结果，本部分中的技术安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄露、破坏和免受未授权的修改的信息安全类要求（简记为 S）；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 A）；其它安全保护类要求（简记为 G）。本部分中所有安全管理要求和安全扩展要求均标注为 G,安全要求及属性标识见表 A.2。

表 A.2　安全要求及属性标识

| 技术/管理 | 分类 | 安全控制点 | 属性标识 |
|---|---|---|---|
| 安全技术要求 | 安全物理环境 | 物理位置选择 | G |
| | | 物理访问控制 | G |
| | | 防盗窃和防破坏 | G |
| | | 防雷击 | G |
| | | 防火 | G |
| | | 防水和防潮 | G |
| | | 防静电 | G |
| | | 温湿度控制 | G |
| | | 电力供应 | A |
| | | 电磁防护 | S |
| | 安全通信网络 | 网络架构 | G |
| | | 通信传输 | G |
| | | 可信验证 | S |
| | 安全区域边界 | 边界防护 | G |
| | | 访问控制 | G |
| | | 入侵防范 | G |
| | | 可信验证 | S |
| | | 恶意代码防范 | G |
| | | 安全审计 | G |
| | 安全计算环境 | 身份鉴别 | S |
| | | 访问控制 | S |
| | | 安全审计 | G |
| | | 可信验证 | S |
| | | 入侵防范 | G |
| | | 恶意代码防范 | G |
| | | 数据完整性 | S |
| | | 数据保密性 | S |
| | | 数据备份恢复 | A |

表A.2（续）

| 技术/管理 | 分类 | 安全控制点 | 属性标识 |
| --- | --- | --- | --- |
| 安全技术要求 | 安全计算环境 | 剩余信息保护 | S |
| | | 个人信息保护 | S |
| | 安全管理中心 | 系统管理 | G |
| | | 审计管理 | G |
| | | 安全管理 | G |
| | | 集中管控 | G |
| 安全管理要求 | 安全管理制度 | 安全策略 | G |
| | | 管理制度 | G |
| | | 制定和发布 | G |
| | | 评审和修订 | G |
| | 安全管理机构 | 岗位设置 | G |
| | | 人员配备 | G |
| | | 授权和审批 | G |
| | | 沟通和合作 | G |
| | | 审核和检查 | G |
| | 安全管理人员 | 人员录用 | G |
| | | 人员离岗 | G |
| | | 安全意识教育和培训 | G |
| | | 外部人员访问管理 | G |
| | 安全建设管理 | 定级和备案 | G |
| | | 安全方案设计 | G |
| | | 产品采购和使用 | G |
| | | 自行软件开发 | G |
| | | 外包软件开发 | G |
| | | 工程实施 | G |
| | | 测试验收 | G |
| | | 系统交付 | G |
| | | 等级测评 | G |

表A.2（续）

| 技术/管理 | 分类 | 安全控制点 | 属性标识 |
| --- | --- | --- | --- |
| 安全管理要求 | 安全建设管理 | 服务供应商管理 | G |
| | 安全运维管理 | 环境管理 | G |
| | | 资产管理 | G |
| | | 介质管理 | G |
| | | 设备维护管理 | G |
| | | 漏洞和风险管理 | G |
| | | 网络与系统安全管理 | G |
| | | 恶意代码防范管理 | G |
| | | 配置管理 | G |
| | | 密码管理 | G |
| | | 变更管理 | G |
| | | 备份与恢复管理 | G |
| | | 安全事件处置 | G |
| | | 应急预案管理 | G |
| | | 外包运维管理 | G |

对于确定了安全保护等级的定级系统，选择和使用基本安全要求时，可以按照以下过程进行：

a) 明确定级系统应该具有的安全保护能力，根据等级保护对象的安全保护等级选择安全要求。方法是根据本部分，第二级系统选择第二级安全要求，第三级系统选择第三级安全要求，第四级系统选择第四级安全要求，以此作为出发点。

b) 根据等级保护对象的定级结果，基于表A.1和表A.2对安全要求进行调整。根据系统服务保证性等级选择相应等级的系统服务保证类（A类）安全要求；根据业务信息安全性等级选择相应等级的业务信息安全类（S类）安全要求；根据系统安全等级选择相应级别的安全通用要求（G类）和安全扩展要求（G类）。例如，某金融云平台系统根据S2、A3定为三级系统，那么可按照S2类安全要求、A3类安全要求、G3安全通用要求和G3云计算安全扩展项要求进行系统建设。

c) 根据等级保护对象采用新技术和新应用的情况，选用相应级别的安全扩展要求作为补充。采用云计算技术的选用云计算安全扩展要求，采用移动互联技术的选用移动互联安全扩展要求，采用物联网技术的选用物联网安全扩展要求，采用大数据平台系统的选用大数据安全扩展要求。

d) 针对金融行业等级保护对象的特点，分析可能在某些方面的特殊安全保护能力要求，选择较高级别的安全要求或其他标准的增强性安全要求（如金融行业增强性安全要求）。对于本部分中提出的安全要求无法实现或有更加有效的安全措施可以替代的，可以对安全要求进行调整，调整的原则是保证不降低整体安全保护能力。

总之，保证不同安全保护等级的对象具有相应级别的安全保护能力，是安全等级保护的核心。选用

本部分中提供的安全通用要求和安全扩展要求是保证等级保护对象具备一定安全保护能力的一种途径和出发点，在此出发点的基础上，可以参考等级保护的其他相关标准和安全方面的其他相关标准，调整和补充安全要求，从而实现等级保护对象在满足等级保护安全要求基础上，又具有自身特点的保护。

# 附 录 B
（规范性附录）
关于等级保护对象整体安全保护能力的要求

网络安全等级保护的核心是保证不同安全保护等级的对象具有相适应的安全保护能力。本部分第5章提出了不同级别的等级保护对象的安全保护能力要求，第7章～第9章分别针对不同安全保护等级的对象应该具有的安全保护能力提出了相应的安全通用要求和安全扩展要求。

依据本部分分层面采取各种安全措施时，还应考虑以下总体性要求，保证等级保护对象的整体安全保护能力。

a） 构建纵深的防御体系。

本部分从技术和管理两个方面提出安全要求，在采取由点到面的各种安全措施时，在整体上还应保证各种安全措施的组合从外到内构成一个纵深的安全防御体系，保证等级保护对象整体的安全保护能力。应从通信网络、网络边界、局域网络内部、各种业务应用平台等各个层次落实本部分中提到的各种安全措施，形成纵深防御体系。

b） 采取互补的安全措施。

本部分以安全控制的形式提出安全要求，在将各种安全控制落实到特定等级保护对象中时，应考虑各个安全控制之间的互补性，关注各个安全控制在层面内、层面间和功能间产生的连接、交互、依赖、协调、协同等相互关联关系，保证各个安全控制共同综合作用于等级保护对象上，使得等级保护对象的整体安全保护能力得以保证。

c） 保证一致的安全强度。

本部分将安全功能要求，如身份鉴别、访问控制、安全审计、入侵防范等内容，分解到等级保护对象的各个层面，在实现各个层面安全功能时，应保证各个层面安全功能实现强度的一致性。应防止某个层面安全功能的减弱导致整体安全保护能力在这个安全功能上削弱。例如，要实现双因子身份鉴别，则应在各个层面的身份鉴别上均实现双因子身份鉴别；要实现基于标记的访问控制，则应保证在各个层面均实现基于标记的访问控制，并保证标记数据在整个等级保护对象内部流动时标记的唯一性等。

d） 建立统一的支撑平台。

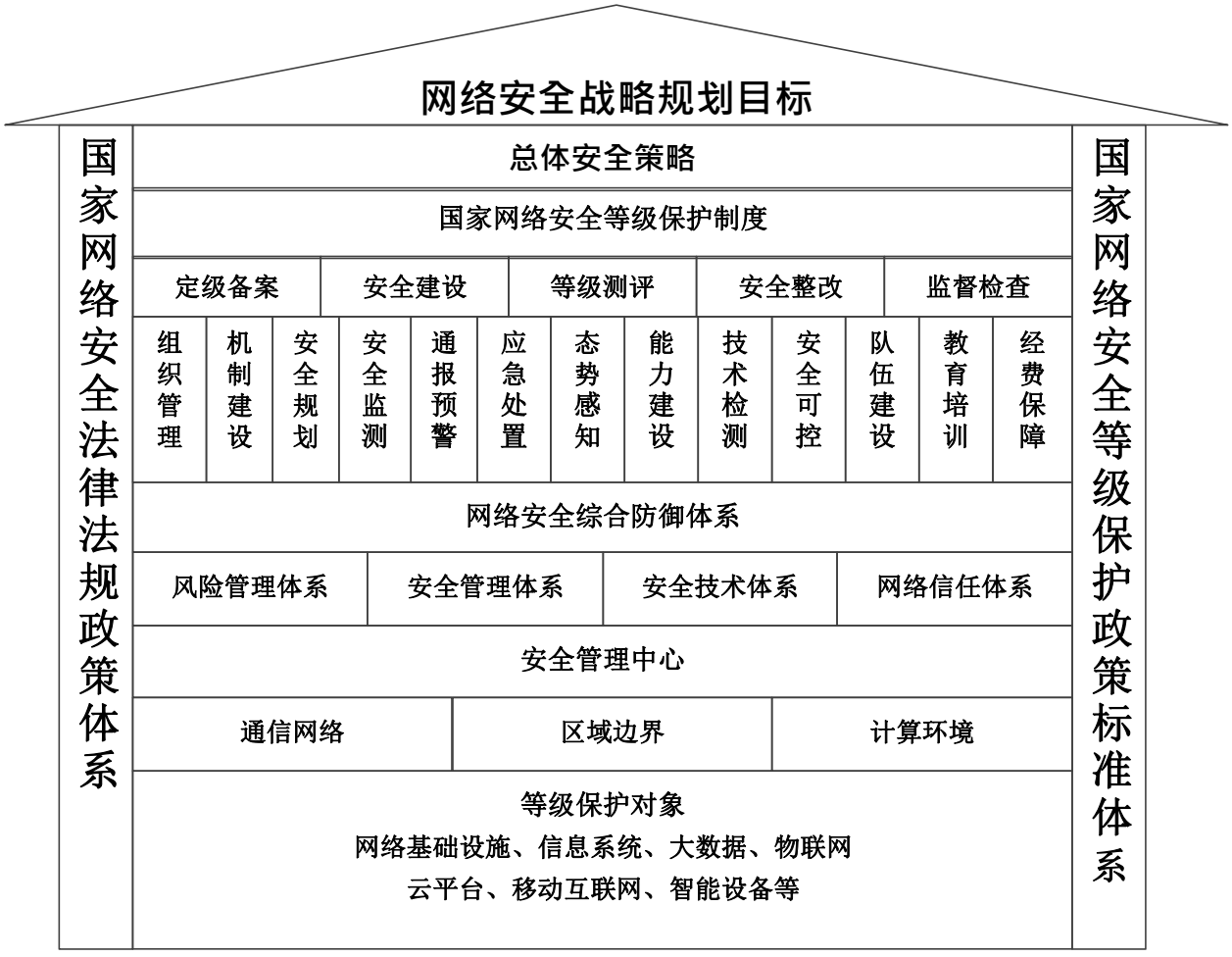
本部分针对较高级别的等级保护对象，提到了使用密码技术、可信技术等，多数安全功能（如身份鉴别、访问控制、数据完整性、数据保密性等）为了获得更高的强度，均应基于密码技术或可信技术，为了保证等级保护对象的整体安全防护能力，应建立基于密码技术的统一支撑平台，支持高强度身份鉴别、访问控制、数据完整性、数据保密性等安全功能的实现。

e） 进行集中的安全管理。

本部分针对较高级别的等级保护对象，提到了实现集中的安全管理、安全监控和安全审计等要求，为了保证分散于各个层面的安全功能在统一策略的指导下实现，各个安全控制在可控情况下发挥各自的作用，应建立集中的管理中心，集中管理等级保护对象中的各个安全控制组件，支持统一安全管理。

# 附 录 C
（规范性附录）
等级保护安全框架和关键技术使用要求

在开展网络安全等级保护工作中应首先明确等级保护对象，等级保护对象包括通信网络设施、信息系统（包含采用移动互联等技术的系统）、云计算平台/系统、大数据平台/系统、物联网系统等；确定了等级保护对象的安全保护等级后，应根据不同对象的安全保护等级完成安全建设或安全整改工作；应针对等级保护对象特点建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系。应依据国家及金融行业网络安全等级保护政策和标准，开展组织管理、机制建设、安全规划、安全监测、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、队伍建设、教育培训和经费保障等工作。等级保护安全框架见图C.1。




图C.1 等级保护安全框架

应在较高级别等级保护对象的安全建设和安全整改中注重使用一些关键技术：

a) 可信计算技术。

应针对计算资源构建保护环境，以可信计算基（TCB）为基础，实现软硬件计算资源可信；针对信息资源构建业务流程控制链，基于可信计算技术实现访问控制和安全认证，密码操作调用和资源的管理等，构建以可信计算技术为基础的等级保护核心技术体系。

b） 强制访问控制。

应在高等级保护对象中使用强制访问控制机制，强制访问控制机制需要总体设计、全局考虑，在通信网络、操作系统、应用系统各个方面实现访问控制标记和策略，进行统一的主客体安全标记，安全标记随数据全程流动，并在不同访问控制点之间实现访问控制策略的关联，构建各个层面强度一致的访问控制体系。

c） 审计追查技术。

应立足于现有的大量事件采集、数据挖掘、智能事件关联和基于业务的运维监控技术，解决海量数据处理瓶颈，通过对审计数据快速提取，满足信息处理中对于检索速度和准确性的需求；同时，还应建立事件分析模型，发现高级安全威胁，并追查威胁路径和定位威胁源头，实现对攻击行为的有效防范和追查。

d） 结构化保护技术。

应通过良好的模块结构与层次设计等方法来保证具有相当的抗渗透能力，为安全功能的正常执行提供保障。高等级保护对象的安全功能可以形式表述、不可被篡改、不可被绕转，隐蔽信道不可被利用，通过保障安全功能的正常执行，使系统具备源于自身结构的、主动性的防御能力，利用可信技术实现结构化保护。

e） 多级互联技术。

应在保证各等级保护对象自治和安全的前提下，有效控制异构等级保护对象间的安全互操作，从而实现分布式资源的共享和交互。随着对结构网络化和业务应用分布化动态性要求越来越高，多级互联技术应在不破坏原有等级保护对象正常运行和安全的前提下，实现不同级别之间的多级安全互联、互通和数据交换。

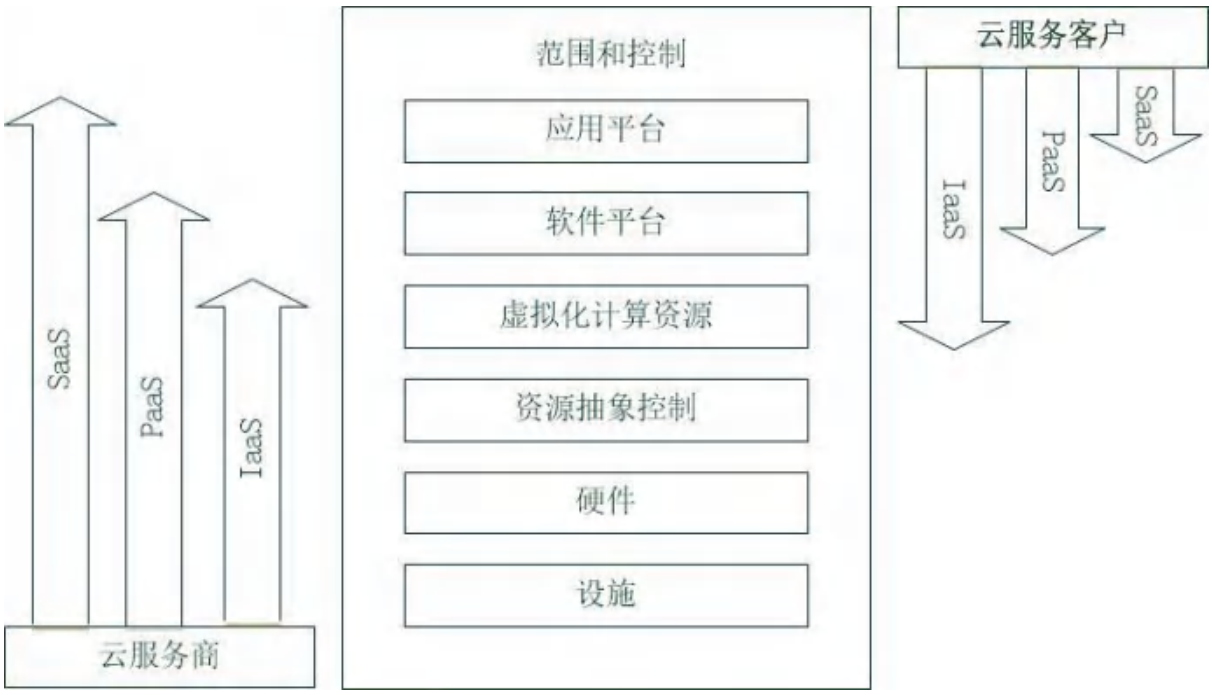
# 附 录 D
（资料性附录）
## 云计算应用场景说明

本部分中将采用了云计算技术的信息系统，称为云计算平台/系统。金融行业云计算平台的特征是云服务客户所提供的金融服务种类众多，数据体量大，受到破坏、泄露或篡改会对国家安全、社会秩序或公共利益造成较大影响，所以金融行业云计算平台所定安全保护等级应不低于第三级，部署在金融行业云计算平台上的云服务客户应用服务自主定级。本部分7.2章节中的第二级云计算安全扩展要求指标仅适用于部署在云平台上的第二级云服务客户应用服务。

云计算平台/系统由设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成。云服务的服务模式包括IaaS、PaaS和SaaS三种基本的云计算服务模式。

云计算服务模式与控制范围的关系如图D.1所示，在不同的服务模式中，云服务商和云服务客户对计算资源拥有不同的控制范围，控制范围则决定了安全责任的边界。在IaaS模式下，云计算平台/系统由设施、硬件、资源抽象控制层组成；在PaaS模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；在SaaS模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件。不同服务模式下云服务商和云服务客户的安全管理责任有所不同。

对于云服务客户，在IaaS、PaaS、SaaS模式下，应在其安全责任边界内依据相应等级网络安全保护要求，从安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理九方面落实有关安全要求，具体安全要求遵循相应等级的安全通用要求。




图D.1 云计算服务模式与控制范围的关系

本部分中不同的云服务模式安全管理责任主体见表D.1。

**表 D.1 安全管理责任主体**

| 层面 | 安全要求 | 安全组件 | 责任主体 | | |
|---|---|---|---|---|---|
| | | | IaaS | PaaS | SaaS |
| 安全物理环境 | 物理位置选择 | 数据中心及物理设施 | 云服务商 | 云服务商 | 云服务商 |
| 安全通信网络 | 网络架构 | 物理网络 | 云服务商 | 云服务商 | 云服务商 |
| | | 虚拟网络安全域 | 云服务客户 | 云服务商 | 云服务商 |
| 安全区域边界 | 访问控制、入侵防范、安全审计、边界防护 | 物理网络及附属设备、虚拟网络管理平台、虚拟网络安全域 | 云服务商、云服务客户 | 云服务商 | 云服务商 |
| 安全计算环境 | 身份鉴别、访问控制、入侵防范、恶意代码防范、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护 | 物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像等；云管理平台（含运维和运营）、镜像、快照等 | 云服务商 | 云服务商 | 云服务商 |
| | | 虚拟网络设备、虚拟安全设备、虚拟机等 | 云服务客户 | 云服务商 | 云服务商 |
| | | 云服务客户应用系统及相关软件组件、云服务客户应用系统配置、云服务客户业务相关数据 | 云服务客户 | 云服务客户 | 云服务客户 |
| 安全管理中心 | 审计管理、集中管控 | 审计设备/措施 | 云服务商、云服务客户 | 云服务商、云服务客户 | 云服务商、云服务客户 |
| 安全管理机构和人员 | 授权和审批 | 授权和审批流程、文档等 | 云服务商 | 云服务商 | 云服务商 |
| 安全建设管理 | 云服务商选择、供应链管理 | 供应链管理流程 | 云服务商 | 云服务商 | 云服务商 |
| | | 云服务商选择及管理流程 | 云服务客户 | 云服务客户 | 云服务客户 |
| 系统安全运维管理 | 云计算环境管理、网络和系统安全管理、应急预案管理 | 云计算环境、网络和系统安全、应急预案管理的相关流程、策略和数据 | 云服务商 | 云服务商 | 云服务商 |

# 附 录 E
（资料性附录）
## 移动互联应用场景说明

采用移动互联技术的等级保护对象其移动互联部分由移动应用、移动终端、无线网络和后台系统四部分组成，移动应用是安装移动终端上，包括个人金融客户端、金融业务专用应用和移动办公应用程序；移动终端包括个人移动终端、金融业务专用终端和移动办公设备，其中金融业务专用终端包括智能POS、业务处理Pad等；移动终端通过无线通道连接无线接入设备接入，无线通道包括无线设备和移动网络；无线接入网关通过访问控制策略限制移动终端的访问行为，如图E.1所示，后台的移动终端管理系统负责对移动终端的管理，包括向客户端软件发送移动设备管理、移动应用管理和移动内容管理策略等。移动互联安全扩展要求主要针对移动应用、移动终端和无线网络部分提出安全要求，移动互联网络拓扑简图，如图E.2。

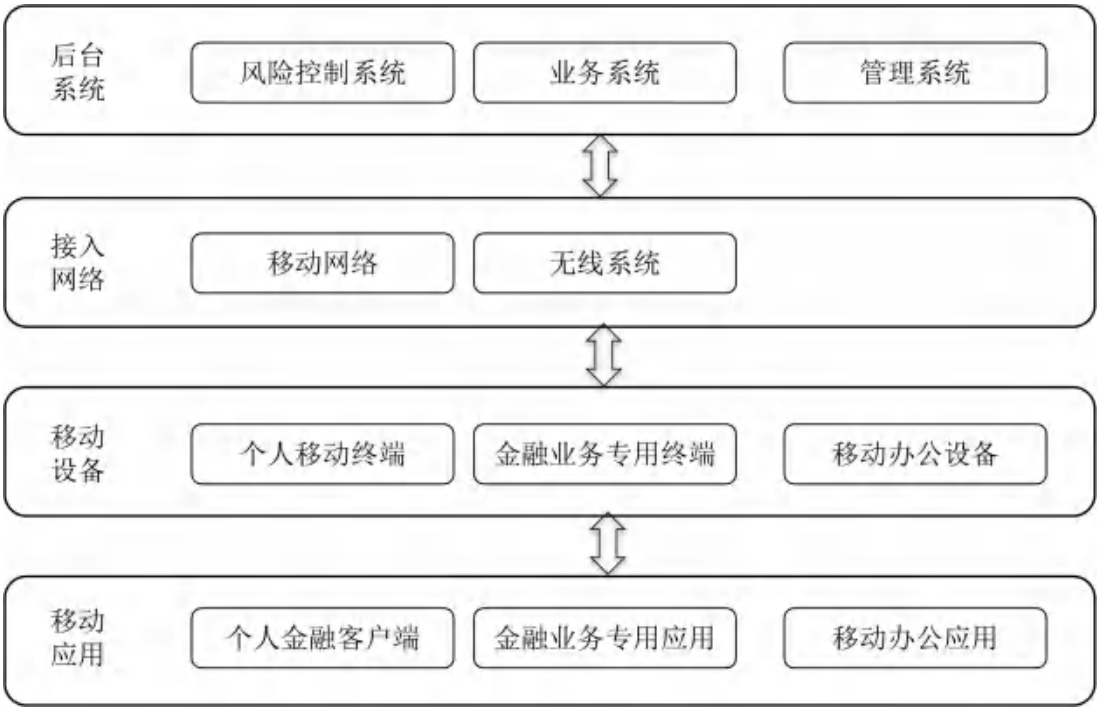



图 E.1 移动互联应用架构

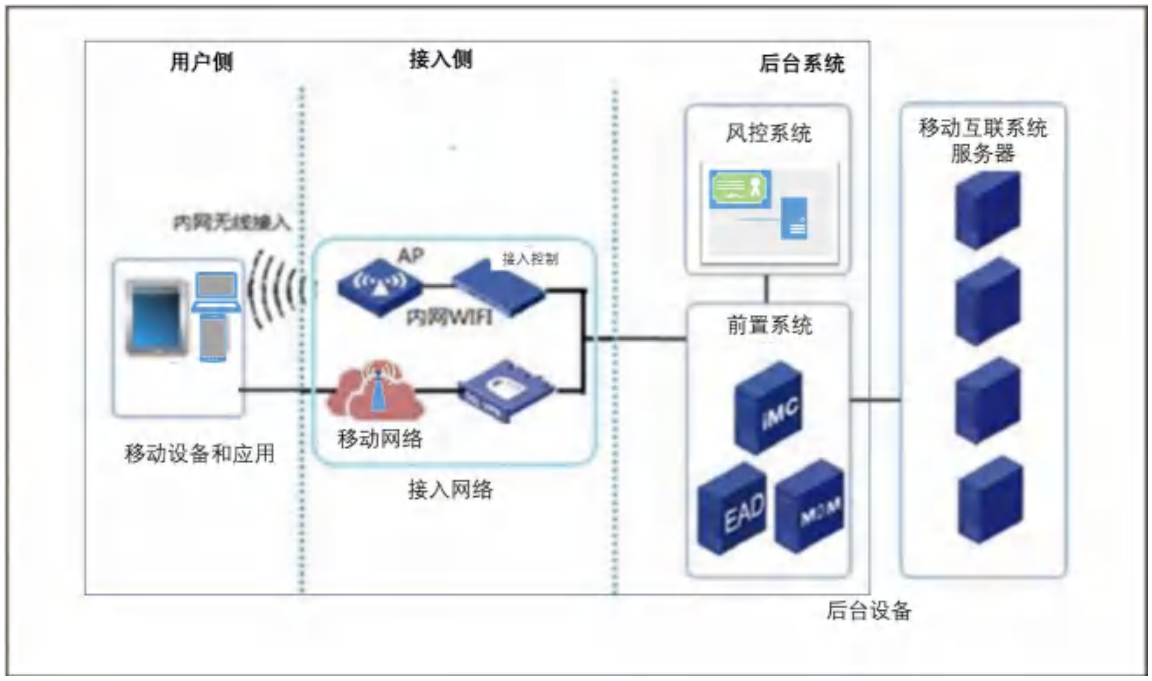



图 E.2 移动互联网络拓扑简图

# 附 录 F
（资料性附录）
物联网应用场景说明

物联网通常从架构上可分为三个逻辑层，即感知层、网络传输层和处理应用层。其中感知层包括传感器节点和传感网网关节点，或RFID标签和RFID读写器，也包括这些感知设备及传感网网关、RFID标签与阅读器之间的短距离通信（通常为无线）部分；网络传输层包括将这些感知数据远距离传输到处理中心的网络，包括互联网、移动网等，以及几种不同网络的融合；处理应用层包括对感知数据进行存储与智能处理的平台，并对业务应用终端提供服务。对大型物联网来说，处理应用层一般是云计算平台和业务应用终端设备。物联网构成示意图如图F.1所示。对物联网的安全防护应包括感知层、网络传输层和处理应用层，由于网络传输层和处理应用层通常是由计算机设备构成，因此这两部分按照安全通用要求提出的要求进行保护，本部分的物联网安全扩展要求针对感知层提出特殊安全要求，与安全通用要求一起构成对物联网的完整安全要求。传感网络中若终端感知节点能够直接通过网络传输层连接处理应用层则不需要通过感知网关节点连接。

具有感知层、网络传输层、处理应用层的物联网应符合物联网扩展要求。没有感知节点设备、系统通过API进行对接视同于通用信息系统。

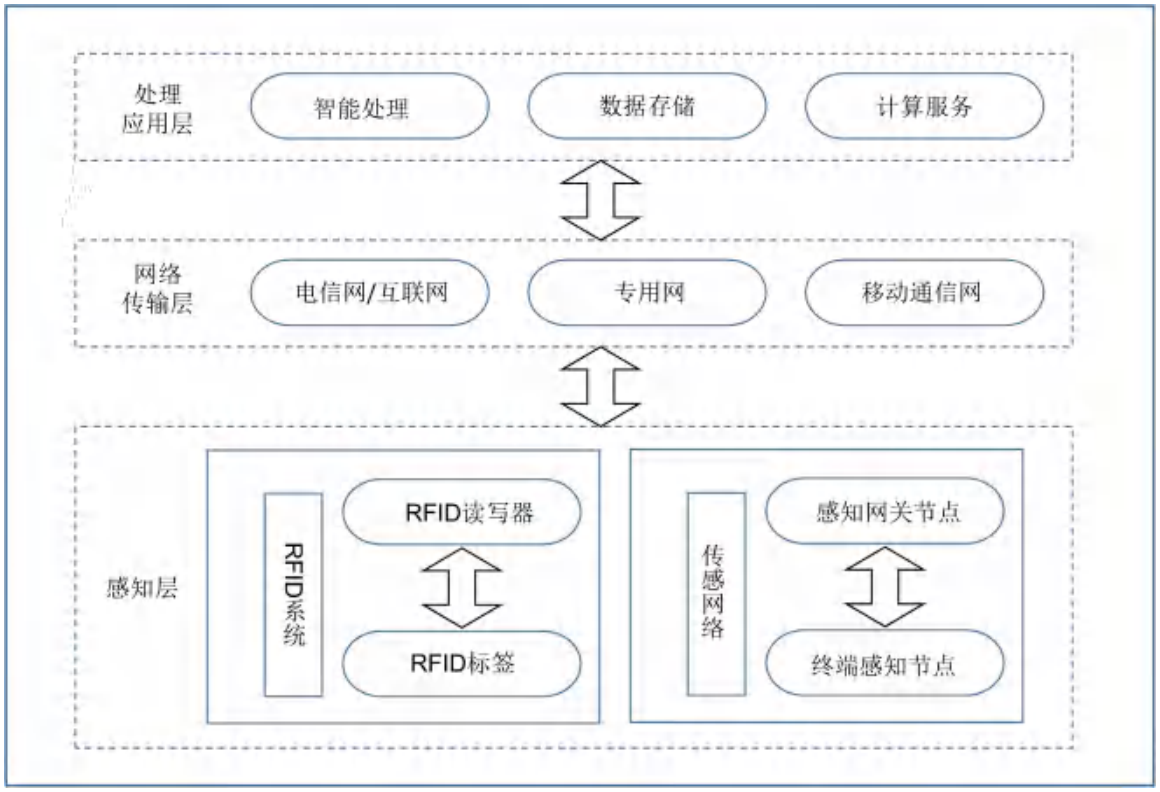



图 F.1 物联网构成

# 附 录 G
（资料性附录）
大数据应用场景说明

## G.1 大数据概述

本部分中将采用了大数据技术的信息系统，称为大数据系统。大数据系统通常由大数据平台、大数据应用以及处理的数据集合构成，金融机构的大数据系统参考模型见图G.1。由于金融行业大数据系统的特征是数据体量大、种类多、聚合快、价值高，受到破坏、泄露或篡改会对国家安全、社会秩序或公共利益造成较大影响，故**金融行业大数据系统所定的保护等级应不低于第三级**。

大数据安全涉及大数据平台的安全和大数据应用的安全。

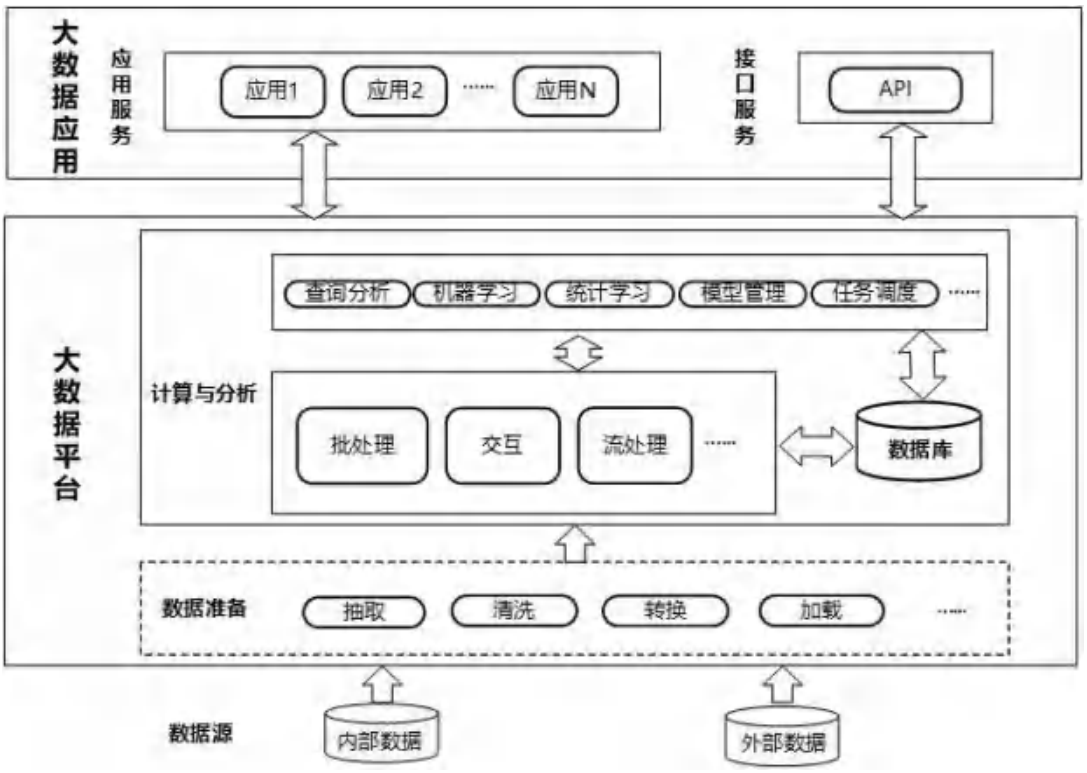



图 G.1 大数据系统架构

大数据应用是基于大数据平台对数据的处理过程，通常包括数据采集、数据存储、数据应用、数据交换和数据销毁等环节，上述各个环节均需要对数据进行保护，通常需考虑的安全控制措施包括数据采集授权、数据真实可信、数据分类标识存储、数据交换完整性、敏感数据保密性、数据备份和恢复、数据输出脱敏处理、敏感数据输出控制以及数据的分级分类销毁机制等。大数据平台是为大数据应用提供资源和服务的支撑集成环境。金融行业的大数据平台包括数据准备、计算与分析，其中数据准备层可由大数据平台实现，也可由数据源实现。计算与分析应支持分布式计算、实时计算或并行计算的方式进行数据处理。金融行业的大数据应用包含应用服务、接口服务以及应用服务结合接口服务三种类型。大数据系统除按照本部分的要求进行保护外，还需要考虑其特点，参照本附录补充和完善安全控制措施。

以下给出大数据系统可补充的安全控制措施供参考。

## G.2 第二级可参考安全控制措施

金融行业大数据系统所定保护等级应不低于第三级，故本部分无第二级大数据安全要求。

## G.3 第三级可参考安全控制措施

### G.3.1 安全物理环境

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

### G.3.2 安全通信网络

本项要求包括：

a) 应保证大数据平台不承载高于其安全保护等级的大数据应用。
b) 应保证大数据平台的管理流量与系统业务流量分离。

### G.3.3 安全计算环境

本项要求包括：

a) 大数据平台应**对导入的数据源进行统一管理，并**对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。**（F3）**
b) 大数据平台应能对不同客户的大数据应用实施标识和鉴别，**身份标识应具有唯一性。（F3）**
c) 大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力。
d) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理，**包括注册/认证、权限设置、工具升级、注销。（F3）**
e) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行。
f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术，**静态脱敏包括采用统计、抑制、假名化、泛化、随机化等技术，大数据应用应根据需求对敏感数据进行展示屏蔽。（F3）**
g) 对外提供服务的大数据平台，平台或**内部其他系统**只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；**授权的颗粒度应达到表级或文件级。（F3）**
h) 应**依据**数据分类分级安全管理**要求，针对大数据应用的数据提供相应的安全保护措施。（F3）**
i) 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求。
j) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证与安全保护策略保持一致。
k) **应授予大数据平台的用户、工具或服务组件最小权限，实现组件的管理和服务权限分离，访问控制粒度应达到表级或文件级。（F3）**
l) **大数据平台在数据建模分析时，需确保敏感数据和个人金融信息位于安全区域，包括但不限于数据隔离区、数据沙箱等。（F3）**
m) 涉及重要数据接口、重要服务接口的调用，应实施访问控制，**访问权限在自有的授权管理机制基础上，实现细粒度的权限管控，如表级或文件级的授权控制**，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。**（F3）**
n) 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复。
o) **应对数据主体访问大数据平台进行限制，限制内容包含单次数据查看量、数据查看频次、总查看次数等。（F3）**

p) **针对大数据应用导出的数据文件，应根据安全需求对数据文件进行脱敏、水印或加密等。（F3）**
q) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求。
r) 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。

### G.3.4 安全建设管理

本项要求包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。
c) 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。
d) **大数据平台的安全整体规划和安全方案设计内容应包含所提供的数据安全防护能力，并形成配套文件，确保其安全规划符合网络安全法等国家法律法规相关要求。（F3）**

### G.3.5 安全运维管理

本项要求包括：

a) 应**具备数字资产统一注册、管理和使用监控能力并**建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。**（F3）**
b) **应维护大数据平台使用和维护的数字资产清单，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。（F3）**
c) 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施。
d) 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程。
e) 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。
f) **应建立数据安全管理规范，**对访问大数据平台的用户进行约束和规范。**（F3）**
g) **重要、敏感数据的采集、传输、存储、处理、使用环境应严格控制开源、共享软件的使用，严控开源、共享软件的来源，并对其代码进行安全审计，确保安全、可靠。（F3）**

## G.4 第四级可参考安全控制措施

### G.4.1 安全物理环境

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

### G.4.2 安全通信网络

本项要求包括：

a) 应保证大数据平台不承载高于其安全保护等级的大数据应用。
b) 应保证大数据平台的管理流量与系统业务流量分离。

### G.4.3 安全计算环境

本项要求包括：

a) 大数据平台应**对导入的数据源进行统一管理，并**对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别。**（F4）**
b) 大数据平台应能对不同客户的大数据应用实施标识和鉴别，**身份标识应具有唯一性。（F4）**
c) 大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力。
d) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理，**包括注册/认证、权限设置、工具升级、注销。（F4）**
e) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行。
f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术，**静态脱敏包括采用统计、抑制、假名化、泛化、随机化等技术，大数据应用应根据需求对敏感数据进行展示屏蔽。（F4）**
g) 对外提供服务的大数据平台，平台**或内部其他系统**只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；**授权的颗粒度应达到记录或字段级。（F4）**
h) 应**依据**数据分类分级安全管理**要求，针对大数据应用的数据提供相应的安全保护措施。（F4）**
i) 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求，**访问控制粒度达到记录或字段级。（F4）**
j) 大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证与安全保护策略保持一致。
k) **应授予大数据平台的用户、工具或服务组件最小权限，实现组件的管理和服务权限分离，访问控制粒度应达到记录或字段级。 （F4）**
l) **大数据平台在数据建模分析时，需确保敏感数据和个人金融信息位于安全区域，包括但不限于数据隔离区、数据沙箱等。（F4）**
m) 涉及重要数据接口、重要服务接口的调用，应实施访问控制，**访问权限在自有的授权管理机制基础上，实现细粒度的权限管控，如记录或字段级的授权控制**，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。**（F4）**
n) 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复。
o) **应对数据主体访问大数据平台进行限制，限制内容包含单次数据查看量、数据查看频次、总查看次数等。（F4）**
p) **针对大数据应用导出的数据文件，应根据安全需求对数据文件进行脱敏、水印或加密等。（F4）**
q) **应对大数据应用导出的数据条数以及累计导出的总条数进行限制。（F4）**
r) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求。
s) 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。
t) 大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。

### G.4.4 安全建设管理

本项要求包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。
c) 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。

d) **大数据平台的安全整体规划和安全方案设计内容应包含所提供的数据安全防护能力，并形成配套文件，确保其安全规划符合网络安全法等国家法律法规相关要求。（F4）**

G.4.5 安全运维管理

本项要求包括：

a) 应**具备数字资产统一注册、管理和使用监控能力并**建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程。**（F4）**

b) **应维护大数据平台使用和维护的数字资产清单，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。（F4）**

c) 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施。

d) 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程。

e) 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。

f) **应建立数据安全管理规范，对访问大数据平台的用户进行约束和规范。（F4）**

g) **重要、敏感数据的采集、传输、存储、处理、使用环境应严格控制开源、共享软件的使用，严控开源、共享软件的来源，并对其代码进行安全审计，确保安全、可靠。（F4）**

# 附 录 H
（资料性附录）
敏感数据和个人金融信息类别

## H.1 敏感数据类别

敏感数据是指一旦泄露可能会对用户或金融机构造成损失的数据，包括但不限于：

a) 个人金融信息中的用户鉴别信息与用户鉴别辅助信息,具体见个人金融信息类别中的C3类别信息。

b) 若用户鉴别辅助信息与账号结合使用可直接完成支付，则属于 C3 类别信息。

c) 金融业务中的支付敏感信息。

**注：**支付敏感信息指的是金融业务中涉及支付主体隐私和身份识别的重要信息。包括但不限于银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

d) 系统敏感数据，如系统的密钥、关键的系统管理数据。

e) 其他需要保密的敏感业务数据。

f) 关键性的操作指令。

g) 系统主要配置文件。

h) 其他需要保密的数据。

## H.2 个人金融信息类别

根据JR/T 0171—2020中4.2的规定，信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为C3、C2、C1三个类别。具体如下：

a) C3 类别信息主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害，包括但不限于：

1) 银行卡磁道数据（或芯片等效信息）、卡片验证码（CVN 和 CVN2）、卡片有效期、银行卡密码、网络支付交易密码。

2) 账户（包括但不限于支付账号、证券账户、保险账户）登录密码、交易密码、查询密码。

3) 用于用户鉴别的个人生物识别信息。

b) C2 类别信息主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害，包括但不限于：

1) 支付账号及其等效信息，如支付账号、证件类识别标识与证件信息（身份证、护照等）、手机号码。

2) 账户（包括但不限于支付账号、证券账户、保险账户）登录的用户名。

3) 用户鉴别辅助信息，如动态口令、短信验证码、密码提示问题答案、动态声纹密码；若用户鉴别辅助信息与账号结合使用可直接完成用户鉴别，则属于 C3 类别信息。

4) 直接反映个人金融信息主体金融状况的信息，如个人财产信息（包括网络支付账号余额）、借贷信息。

5) 用于金融产品与服务的关键信息，如交易信息（如交易指令、交易流水、证券委托、保险理赔）等。

6） 用于履行了解你的客户（KYC）要求，以及按行业主管部门存证、保全等需要，在提供产品和服务过程中收集的个人金融信息主体照片、音视频等影像信息。

7） 其他能够识别出特定主体的信息，如家庭地址等。

c） C1 类别信息主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响，包括但不限于：

1） 账户开立时间、开户机构。

2） 基于账户信息产生的支付标记信息。

3） C2 和 C3 类别信息中未包含的其他个人金融信息。

个人金融信息主体因业务需要（如贷款）主动提供的有关家庭成员信息（如身份证号、手机号、财产信息等），应依据 a)～c)敏感程度类别进行分类，并实施针对性的保护措施。

两种或两种以上的低类别信息经过组合、关联和分析后可能产生高敏感程度的信息。同一信息在不同的服务场景中可能处于不同的类别，应依据服务场景以及该信息在其中的作用对信息的类别进行识别，并实施针对性的保护措施。

# 参 考 文 献

[1] GB/T 22240—2020 网络安全等级保护定级指南
[2] GB/T 25070—2019 网络安全等级保护安全设计技术要求
[3] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[4] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求
[5] GB/T 37093—2018 信息安全技术 物联网感知层接入通信网的安全要求
[6] GB/T 37721—2019 信息技术大数据分析系统功能要求
[7] JR/T 0011 银行集中式数据中心规范
[8] JR/T 0013 金融业星型网间互联安全规范
[9] JR/T 0023 证券公司信息技术管理规范
[10] JR/T 0026 银行业计算机信息系统雷电防护技术规范
[11] JR/T 0044 银行业信息系统灾难恢复管理规范
[12] JR/T 0055.4 银行卡联网联合技术规范第4部分：数据安全传输控制
[13] JR/T 0060 证券期货业信息系统安全等级保护基本要求
[14] JR/T 0067 证券期货业信息系统安全等级保护测评要求
[15] JR/T 0068—2019 网上银行系统信息安全通用规范
[16] JR/T 0166—2018 云计算技术金融应用规范技术架构
[17] JR/T 0167—2018 云计算技术金融应用规范安全技术要求
[18] 中国证券业协会.证券公司集中交易安全管理技术指引(中证协发〔2006〕81号),2006-08-01
[19] 中国证券业协会.证券营业部信息技术指引（中证协发〔2009〕154号），2009-09-07
[20] 中国保监会.保险业重大突发事件应急处理规定（保监会令〔2003〕3号），2003-12-18