

ICS 03.060

CCS A 11

团体标准

T/NIFA 21—2023

金融数据安全技术防护规范

Financial data security

technical protection specification

2023—11—10 发布

2023—11—10 实施

中国互联网金融协会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语与定义 1

4 缩略语 4

5 金融数据安全技术总则 4

 5.1 概述 4

 5.2 目标 5

 5.3 原则 5

6 金融数据安全技术防护框架 5

7 金融数据基础安全 6

 7.1 制度规范 6

 7.2 人员管理 7

 7.3 金融数据资产管理 8

 7.4 金融数据分类分级 8

8 金融数据全生命周期安全 10

 8.1 数据采集安全 10

 8.2 数据传输安全 10

 8.3 数据存储安全 11

 8.4 数据使用安全 12

 8.5 数据交换安全 17

 8.6 数据销毁安全 18

9 金融数据安全监管与运维 18

 9.1 边界管控 18

 9.2 访问控制 19

 9.3 数据安全监测 19

 9.4 数据安全审计 21

 9.5 数据安全评估 21

 9.6 安全事件应急处置 22

附录 A（资料性）自动化数据分类分级技术 23

附录 B（资料性）数据脱敏技术 25

附录 C（资料性）数据加密技术 27

附录 D（资料性）用户实体行为分析技术 29

附录 E（资料性）安全级别定义 31

参考文献 32

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》和GB/T 20004.1—2016《团体标准化 第1部分：良好行为指南》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网金融协会提出。

本文件由中国互联网金融协会归口。

本文件起草单位：中国互联网金融协会、同盾科技有限公司、海问律师事务所、奇富科技股份有限公司、重庆富民银行股份有限公司、中互金认证有限公司。

本文件主要起草人：单强、陆书春、朱勇、王新华、唐晓军、李阜新、马丹、高建锋、周良、陈克举、赵新、邓康、杨建媛、李娜、马元朋、王睿、刘志刚、邬肖玢。

金融数据安全技术防护规范

1 范围

本文件规定了金融数据安全技术防护的目标和原则，明确了相关制度规范、数据全生命周期安全、数据安全监管和运维方法等内容，确立了金融机构在开展业务和进行经营管理过程中的数据安全技术防护方案。

本文件适用于金融机构开展金融数据安全技术防护使用，并为第三方评估机构单位开展金融数据安全防护检查与评估工作提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语与定义

GB/T 35273—2020和GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

金融数据 financial data

金融机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类数据。

注：该类数据可用传统数据处理技术或大数据处理技术进行组织、存储、计算、分析和管理的。

[来源：JR/T 0197—2020，3.10，有修改]

3.2

个人信息 personal information

以电子或其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

[来源：GB/T 35273—2020，3.1，有修改]

3.3

个人金融信息 personal financial information

金融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1：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。

注2：改写GB/T 35273—2020，定义3.1。

[来源：JR/T 0185—2020，3.9]

3.4

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

注1：敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息等。

注2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇的，属于个人敏感信息。

[来源：GB/T 41479—2022，3.7]

3.5

敏感数据 sensitive data

由权威机构确定的受保护的信息数据。

注：敏感信息数据的泄露、修改、破坏或丢失会对人或事产生可预知的损害。

[来源：GB/T 39477—2020，3.7]

3.6

重要数据 important data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

3.7

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019，3.1]

3.8

保密性 confidentiality

信息对未授权的个人、实体或进程不可用或不可泄露的性质。

[来源：GB/T 25069—2022，3.41]

3.9

完整性 integrity

准确和完整的性质。

[来源：GB/T 25069—2022，3.612]

3.10

可用性 availability

可由经授权实体按需访问和使用的性质。

[来源：GB/T 25069—2022, 3.345]

3.11

真实性 authenticity

一个实体是其所声称实体的性质。

[来源：GB/T 25069—2022, 3.769]

3.12

数据生命周期 data lifecycle

数据从产生，经过数据采集、数据传输、数据存储、数据使用（包括访问、导入与导出、加工、展示、开发测试、汇聚融合、公开披露、转让等）、数据交换，直至数据销毁等各种生存形态的演变过程。

[来源：GB/T 35274—2017, 3.2, 有修改]

3.13

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或关联，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

[来源：GB/T 35273—2020, 3.14]

3.14

数据脱敏 data desensitization

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

[来源：GB/T 37988—2019, 3.12]

3.15

数据沙箱 data sandbox

一种通过实现数据所有权和数据使用权分离，以确保数据流通过程安全可控的产品或平台。

3.16

数据水印 digital watermarking

一种将特定的数字信号嵌入数据产品中以保护数字产品版权、完整性防复制或去向追踪的技术。

[来源：GB/T 36303—2018, 3.1, 有修改]

3.17

访问控制 access control

一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。

[来源：GB/T 25069—2022, 3.147]

3.18

溯源信息 provenance information

数据处理过程中记录的可以实现追踪数据来源的信息。

[来源: GB/T 39477—2020, 3.10]

3.19

多方安全计算 secure multi-party computation

多方安全计算主要研究针对无可信第三方情况下,安全地进行多方协同的计算问题。即在一个分布式网络中,多个参与实体各自持有秘密数据,各方希望以这些数据为输入共同完成对某函数的计算,而要求每个参与实体除计算结果、预期可公开的信息外均不能得到其他参与实体的任何输入信息。

注:多方安全计算的常用技术有混淆电路(Garbled Circuit)、不经意传输(Oblivious Transfer)、秘密分享(也称为秘密分割,Secret Sharing)、同态加密(Homomorphic Encryption)等。

3.20

联邦学习 federated learning

一种多个参与方在保证各自原始私有数据不出数据方定义的私有边界的前提下,协作完成某项机器学习任务的机器学习模式。

4 缩略语

下列缩略语适用于本文件:

API: 应用程序接口(Application Programming Interface)

DES—CBC: 数据加密标准—密码块链接(Data Encryption Standard—Cipher Block Chaining)

DLP: 数据泄露防护(Data Leakage Protection)

IP: 网际互连协议(Internet Protocol)

MAC: 媒体访问控制(Media Access Control)

MD5: 消息摘要算法(Message—Digest Algorithm 5)

SHA1: 安全散列算法(Secure Hash Algorithm 1)

SSL: 安全套接层协议(Secure Socket Layer)

TLS: 安全传输层协议(Transport Layer Security)

UEBA: 用户实体行为分析(User and Entity Behavior Analytics)

5 金融数据安全技术总则

5.1 概述

金融数据安全技术防护旨在对金融数据资产进行全面梳理,并指导金融机构设置数据安全防护措施。数据安全防护管理是建立统一、完善的数据生命周期安全保护框架的基础工作,能够为金融机构制定有针对性的数据安全管控措施提供支撑。

- a) 组织保障: 数据安全组织保障是数据安全技术防护框架必不可少的组成部分,确保数据安全工作具有包括决策层、管理层、执行层以及监督层的完善管理体系,是确保数据安全防护机制能够有效落实和严格执行的基石;
- b) 核心保障: 数据生命周期安全防护要求是数据安全技术防护框架的核心,针对不同数据类型的安全防护要求,明确其在采集、传输、存储、使用、删除以及销毁等数据生命周期各个环节的安全防护要求,是金融机构开展数据安全防护工作的基本依据;
- c) 运维保障: 在金融机构日常运营过程中,加强在监测运维过程中的数据安全风险防控能力,可保障数据安全防护机制的有效执行,和数据安全问题的及时发现与应对。

5.2 目标

数据安全防护的目标是保障金融数据及其应用过程中的运营合规、风险可控和价值实现,主要包括:

- a) 运营合规: 建立符合法律法规和行业监管的数据运营管理体系,保障数据及其应用的合规;
- b) 风险可控: 建立数据风险管控机制,确保数据及其应用满足风险偏好和风险容忍度;
- c) 价值实现: 构建数据价值实现体系,促进数据资产化和数据价值实现。

5.3 原则

为防范和抵御金融数据安全风险,金融机构在开展业务及日常经营管理过程中,遵循以下数据安全基本原则:

- a) 合法合规原则: 满足国家法律法规及行业主管部门有关规定,确保金融数据全生命周期活动的合法性和正当性;
- b) 目的明确原则: 制定金融数据安全防护策略,明确金融数据生命周期各环节的安全防护目标和要求;
- c) 授权保密原则: 向个人金融信息主体明示数据采集和处理的目的、方式、范围、规则等,制定完善的隐私政策,在进行数据采集和处理前征得其授权同意,对所涉及的信息进行严格保密;
- d) 最小够用原则: 金融机构应仅处理个人金融信息主体授权同意的金融数据,处理的金融数据为业务所必需的最小金融数据类型和数量;
- e) 全程可控原则: 采取与金融数据安全级别相匹配的安全管控机制和技术措施,确保金融数据在全生命周期各环节的保密性、完整性和可用性,避免数据在全生命周期内被未经授权访问、破坏、篡改、泄漏或丢失等;
- f) 动态控制原则: 金融数据的安全控制策略和安全防护措施不是一次性和静态的,可基于业务需求、安全环境属性、系统用户行为等因素实施实时和动态调整;
- g) 权责一致原则: 明确本机构数据安全防护工作相关部门及其职责,有关部门及人员积极落实相关措施,履行数据安全防护职责。

6 金融数据安全技术防护框架

金融数据安全技术防护框架(见图1)包含以下四部分:

- a) 金融数据安全总则: 包含金融数据安全防护的任务、目标和原则;
- b) 金融数据全生命周期安全: 包含数据采集、数据传输、数据存储、数据使用、数据交换和数据销毁;
- c) 金融数据基础安全: 包含制度规范、人员管理、数据资产管理和数据分类分级;
- d) 金融数据检测及运维安全: 包含边界管控、访问控制、数据安全监测、数据安全审计、数据安全评估和安全事件应急处置。

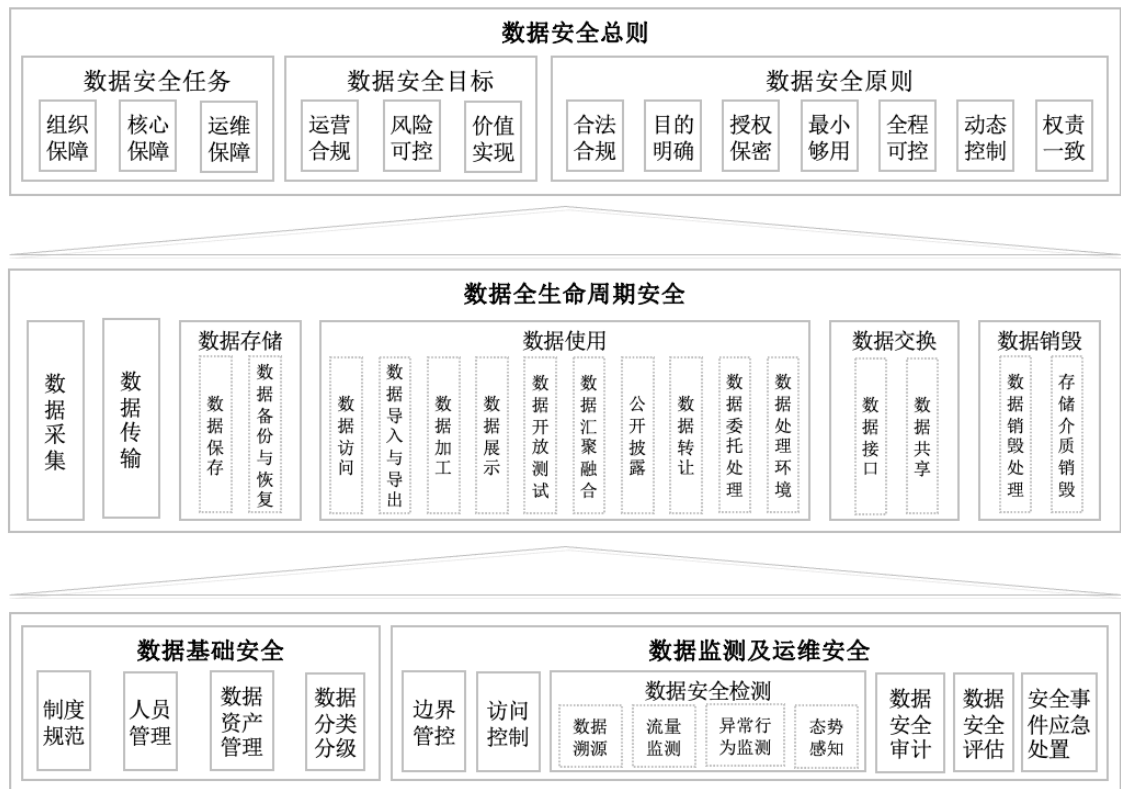


图1 金融数据安全技术防护框架

7 金融数据基础安全

7.1 制度规范

金融机构应建立统一的金融数据安全管理制度体系，明确各层级部门与相关岗位数据安全工作的职责，规范工作流程。数据安全管理制度体系要求如下：

- a) 应依据国家与行业主管和监管部门要求，结合机构自身风险管控策略和偏好、安全建设预算等因素，制定本机构数据安全总体安全策略、方针、目标、原则；
- b) 应制定本机构数据分级规程，识别并维护本机构数据资产清单，并标注相应的数据级别；
- c) 应制定数据安全管理制度及实施细则并定期评价更新，确保基于数据分级的数据安全制度体系覆盖机构数据全生命周期，并对有关制度的有效性进行定期评价与更新，具体要求如下：
 - 1) 制定本机构数据安全管理制度，提出本机构数据安全生命周期保护工作的总体策略；
 - 2) 针对不同安全级别的数据，制定相应的安全策略和保障措施；
 - 3) 建立金融数据安全日常管理及操作流程，对数据生命周期各阶段的数据保护工作提出具体要求；
 - 4) 建立合理、统一的密码使用和密钥管理技术规范和制度；
 - 5) 建立数据脱敏技术规范和制度，明确不同安全级别数据脱敏规则、脱敏方法和脱敏数据的使用限制，配置脱敏数据识别和脱敏效果验证服务组件或技术手段，确保数据脱敏的有效性和合规性，对数据的脱敏操作过程留存日志记录，用于审核违规使用、审核脱敏完整性；
 - 6) 建立数据供应方安全管理要求，确定数据来源合法合规，对数据的真实性、有效性进行管理；

- 7) 建立数据出境安全控制要求与操作程序；
 - 8) 建立数据采集、传输、存储、使用、删除及销毁相关审核规程，宜采用电子化手段实现审核流程；
 - 9) 制定数据采集的操作规程，规范数据采集的渠道、数据格式、流程和方式；
 - 10) 建立数据安全评估、个人金融信息安全影响评估以及内外部数据安全检查与评估制度；
 - 11) 建立数据安全事件管理、处置规程和应急响应等机制，明确重大数据安全事件的处置流程及应对方法。
- d) 应定期审核和更新金融数据安全管理制度；
- e) 在本机构组织架构发生重大调整或数据相关服务发生重大变化时，应及时对金融数据安全策略与规程进行评估，并按需进行修订和更新。

7.2 人员管理

金融机构应对涉及数据安全的人员进行管理，具体要求如下：

- a) 人员录用及日常管理方面：
- 1) 录用员工前，进行必要的背景调查；
 - 2) 对数据安全关键岗位制定统一的保密协议，并与可接触机构3级及以上数据的员工以及从事数据安全关键岗位的员工签署保密协议；
 - 3) 识别机构数据安全关键岗位，并与其签署数据安全岗位责任协议，数据安全关键岗位包括但不限于：
 - 数据安全岗位、审计岗位；
 - 业务操作与信息技术操作特权账户所有者；
 - 数据各级权限审批岗位；
 - 重要数据处理岗位；
 - 信息系统开发、测试岗位人员；
 - 因业务需要，需高频和（或）大批量接触3级及以上数据的岗位人员；
 - 外部数据采购岗位；
 - 其他金融机构识别的数据安全关键岗位。
 - 4) 发生人员调离岗位时，立即完成相关人员数据访问、使用等权限的配置调整，并明确有关人员后续的数据保护管理权限和保密责任；若有关人员调整后的岗位不涉及数据的访问与处理的，明确其继续履行有关信息的保密义务要求；
 - 5) 与员工终止劳动合同时，立即终止并收回其对数据的访问权限，明确并告知其继续履行有关信息的保密义务要求，并签订保密承诺书；
 - 6) 建立外部人员管理制度，对允许被外部人员访问的系统和网络资源建立数据存取控制机制、认证机制，列明所有外部用户名单及其权限，加强对外部人员的数据安全要求和培训，必要时签署保密协议。
- b) 在人员培训和教育方面，应制定数据安全相关岗位人员的安全专项培训计划：
- 1) 按照培训计划定期开展数据安全意识教育与培训，培训内容包括但不限于国家有关法律法规、行业规章制度、技术标准，以及金融机构内部数据安全有关制度与管理规程等内容，并对培训结果进行评价、记录和归档；
 - 2) 对密切接触高安全等级数据的人员定期开展数据安全意识教育和培训，培养办公数据定期删除意识，并定期开展数据删除自查工作；
 - 3) 每年至少对数据安全专职与关键岗位人员进行1次数据安全专项培训；
 - 4) 至少每年1次或在隐私政策发生重大变化时，对数据安全关键岗位上的人员开展专业化培

训和考核，确保人员熟练掌握隐私政策和相关规程。

- c) 在数据安全技术方面，应具备以下能力：
 - 1) 应熟悉国内外主流的数据安全产品和工具，如DLP、脱敏工具、加密平台、数据溯源和态势感知平台等，能判断当前组织的需求；
 - 2) 在数据生命周期中，应能评估潜在数据安全风险，包括但不限于数据泄露风险、数据篡改风险、数据滥用风险等，并能制定有效、合理降低数据风险的解决方案或措施；
 - 3) 应对敏感数据流动做好审计工作，具备风险排查能力，以及快速处置数据篡改和数据泄露的能力；
 - 4) 应对当前数据安全体系进行技术验证，可采用白盒、灰盒和黑盒等安全测试和对抗，确保数据安全防御形成一个持续迭代更新的良性循环系统；
 - 5) 应了解国内外前沿的数据安全和隐私保护技术，如加密技术、差分隐私和UEBA等，能在恰当时期引入组织需要的技术，降低数据安全和隐私保护的风险。
- d) 在数据相关人员管理及关键岗位设置方面，应进一步加强管理，对接触高安全等级金融数据的人员及其岗位进行审批和登记，并定期对这些人员的行为进行安全审查；
- e) 数据库管理员、操作员及安全审计人员等岗位应设立专人专岗，并实行职责分离；必要时特权账户所有者、关键数据处理岗位等数据安全关键岗位应设立双人双岗，强化数据安全管控。

7.3 金融数据资产管理

金融数据资产管理应执行国家及行业监管要求，并结合金融机构实际情况，具体要求如下：

- a) 应明确数据资产安全责任主体及相关方；
- b) 应通过技术工具实现数据资产的自动识别与发现，包括但不限于：资产扫描、元数据接口对接、数据字典导入等方式，收集、发现数据资产。其中，资产扫描方式以任务形式对指定网段内的各类数据库进行嗅探，自动发现数据库资产并进行备案，再通过对指定数据库进行扫描，识别库中的表名、表描述、字段名、字段描述、字段类型、字段长度与样本数据；数据字典导入和接口方式可通过文件导入或与元数据系统的接口对接方式获取数据资产；
- c) 对于密钥类数据资产，应明确密钥管理安全要求，并构建密钥管理系统，实现对密钥的全生命周期（生成、存储、使用、分发、更新、销毁等）的安全管理；
- d) 应建立组织统一的金融数据资产管理系统，通过技术工具实现对数据资产的统一管理，明确数据资产标识和数据资产相关管理方的属性标识；
- e) 应建立便于索引和查询的金融数据资产清单，并及时更新数据资产相关信息；
- f) 应通过数据资产管理系统量化金融业务机构数据资产的整体情况，包括但不限于数据资产的数据量、各等级数据资产的分布情况等，从而便于数据资产管理人员进行组织整体数据资产现状的统计；
- g) 应能够量化评估金融机构内部数据资产相关管理者在相关数据安全流程中的参与情况，并根据评估结果调整管理者的职责。

7.4 金融数据分类分级

7.4.1 分类分级原则

- a) 数据分类在实施中遵循以下原则：
 - 1) 科学性：数据分类宜充分考虑数据的业务属性、多维特征和行业特点，按照其相互间内在逻辑关联对数据进行科学分类；
 - 2) 实用性：数据类目设置宜与现有管理和分类相兼容，降低分类和数据保护的实施难度；
 - 3) 稳定性：数据类目划分宜选择数据对象最稳定的本质特性作为依据；

- 4) 拓展性：数据分类应充分考虑业务拓展需求，前瞻性规划设计；
 - 5) 规范性：数据类目名称应能准确、简洁表达数据特征和内容，内涵、外延清晰。
- b) 数据分级在实施中遵循以下原则：
- 1) 安全性：数据的级别划分应围绕数据安全保护展开，确保数据安全地流通和使用；
 - 2) 依从性：数据的级别划分应符合法律法规要求，满足监管部门相关规定；
 - 3) 可执行性：数据的级别划分客观明了，易于理解，依据数据特征和定级规则即可判定数据的级别，具有良好的可操作性；
 - 4) 时效性：数据级别具有一定的时效性，数据级别可能会因业务发展、安全策略等变化而有所变化，定期审计改进；
 - 5) 合理性：数据级别划分合理，不宜将所有数据集集中于某几个级别，不将重要数据的级别划分过低。一般将数据安全级别划分为5个级别，从高到低划分为5级、4级、3级、2级、1级。

7.4.2 分类分级实施方法

- a) 数据分类的实施方法，构建从总到分的树形逻辑体系和框架：
- 1) 以金融基础数据标准分类框架的主题为划分维度，确定一级子类；
 - 2) 在一级子类基础上，参考基础数据标准分类框架的标准大类，结合本机构数据特点，综合考虑数据安全分类管理的需求，再细分类别，形成二级子类；
 - 3) 在二级子类基础上，根据具体的业务内容，再逐个类别确定具体的数据元，形成三级子类；
 - 4) 四级子类，基于三级子类的数据进行细分。
- b) 数据分级的实施方法，主要根据影响对象和影响程度的组合进行定级：
- 1) 数据分级的时机：应根据实际工作的需要选择分级的最佳时机。分级的最佳时机为提供数据服务前；分级的最差时机为提供数据服务时；
 - 2) 数据分级的粒度：由一个或多个字段组成的数据集合；
 - 3) 数据分级的范围：本机构的金融信息资源，参与数据分类的数据都要分级。

7.4.3 分类分级流程

数据分类分级包括发起、审核、更新等流程环节。相关人员应遵循客观、独立和审慎的原则，在充分进行分析的基础上，遵循既定的标准，保证分类分级的质量。

- a) 数据分类流程，一般分为以下四个阶段：
- 1) 数据分类准备，全面梳理业务条线和业务内容，掌握数据资源的体量、类型、分布、业务含义等基本属性，明确业务划分的颗粒度；
 - 2) 数据分类实施，确定组织或机构的业务主题、业务领域，参考本文件的数据分类方法进行类别设置，并按照分类的业务含义对数据资源进行划分归类；
 - 3) 数据分类审核，审核并优化数据分类评定的过程和结果，确保数据分类结果与业务主题、业务领域、业务内容的要求一致；
 - 4) 分类结果发布，发布符合数据分类要求的分类结果并投入使用。
- b) 数据安全分级的流程，一般分为以下五个阶段：
- 1) 数据分级准备，对数据资源进行盘点，明确数据分级的粒度、范围；
 - 2) 数据的分级，根据数据的影响对象、影响程度，确定数据安全遭到破坏后可能会影响的对象和影响的程度，基于该结果对数据定级；
 - 3) 数据分级审核，审核并优化数据安全级别评定过程和结果，确保数据安全级别划分与数据安全保护目标一致；
 - 4) 分级结果发布，发布符合数据安全目标和要求的分级结果；

- 5) 分级审计变更, 依据安全性和时效性原则, 及时对数据的内容、时效性和使用场景等需进行数据安全级别修订的情形, 实施审计和变更。

7.4.4 分类分级工具

分类分级工具应符合以下要求:

- a) 应优先采用技术工具, 运用字段名、字段描述、内容关键字、正则表达式、自然语言识别等规则匹配, 进行数据特征的智能识别, 并与数据分类分级模板中的明细分类建立映射关系, 快速实现数据分类分级;
- b) 宜基于已分类分级的数据资产结果集, 将结果中的表名、字段名、字段描述、数据特征等作为向量, 进行机器学习建模, 持续进行模型优化, 形成数据分类分级模型知识库, 构建全自动数据分类分级工具;
- c) 数据分类分级的识别中, 在数据含义单一、量小情况下, 可采用人工手段;
- d) 应根据业务和使用场景的变化对数据级别进行动态调整;
- e) 应对数据分类分级的变更进行记录, 并通知相关数据的使用方;
- f) 对数据分类分级结果应定期组织的审计评估, 确保数据分类分级的正确性。

8 金融数据全生命周期安全

8.1 数据采集安全

数据采集安全应符合以下要求:

- a) 应明确数据采集的目的、方式、范围和保存期限。当涉及敏感个人信息时, 应明确采集的必要性及对个人的影响, 不应收集与提供服务无关的个人信息;
- b) 个人信息的采集应取得用户授权同意;
- c) 应建立数据采集工具, 统一设置采集策略, 记录详细的日志, 确保数据采集授权过程的完整记录, 支持对数据采集和获取操作过程的可追溯性;
- d) 应规定数据采集的渠道及外部数据源鉴定方式, 并对采集来源方式、数据范围和类型进行记录;
- e) 通过移动端采集数据时, 应实现终端数据安全防护, 防止数据泄露, 如将数据与宿主机硬盘进行隔离等方式;
- f) 应支持对采集全过程的加密通信, 从发起数据采集请求, 数据采集授权到采集数据传输的通信过程应采取双向加密传输;
- g) 采集数据时, 应对数据采集设备或系统的真实性进行验证; 当采集敏感数据时, 还应结合口令密码、设备指纹、网络接入方式、设备物理位置、设备风险情况等多种因素对数据采集设备或系统的真实性进行增强验证;
- h) 数据采集涉及敏感信息时, 应在数据传输前根据数据使用需要对原始数据进行脱敏或加密处理, 降低数据传输过程中的风险;
- i) 存储采集的数据时, 应对采集到的数据根据数据安全级别和使用需要进行加密后存储, 并对所存储的数据定期进行备份, 保证存储数据的安全性, 防止所存储的数据遭到窃取和破坏;
- j) 应采用摘要、消息认证码、数字签名、数据证书技术手段或管控措施, 对采集和获取到的数据进行完整性校验, 防止采集前后数据被篡改;
- k) 应基于合规评估的数据采集策略, 包括但不限于原则、频度、范围等, 实现数据合规性监控与告警。

8.2 数据传输安全

数据传输安全应符合以下要求：

- a) 应明确金融数据传输安全管理规范，明确数据传输安全要求，如传输通道加密、数据内容加密、签名验签、身份鉴别、数据传输接口安全等；
- b) 应建立传输数据完整性校验机制，如效验码、消息摘要、数字签名等，并采用技术手段实现数据容错或恢复；
- c) 应明确需要进行传输加密的业务场景，并进行数据加密传输，如TLS/SSL、数字签名、时间戳等方式，确保数据传输的保密性和不可抵赖性；
- d) 当传输敏感数据时，应支持对数据进行字段级加密，并采用安全的传输协议进行传输；
- e) 应提供统一的数据加密模块供开发传输功能的人员调用，根据不同数据类型和安全级别进行数据加密处理，保证组织内数据加密功能的统一性；
- f) 应选用安全的密码算法，禁用如MD5、DES—CBC、SHA1等在未加密情况下的不安全的算法；
- g) 应采用安全技术或部署相关设备，如防火墙、负载均衡、防入侵攻击、数据防泄漏检测与防护等设备，保证网络可用性及防止数据泄露；
- h) 应提供对传输通道两端进行主体身份鉴别、认证的技术方案和工具，确保数据传输双方是可信的；
- i) 应部署技术工具，对通道安全、密码算法配置、密钥管理等保护措施进行审核及监控；
- j) 应采用有效的技术手段及时发现数据传输中的安全问题，对传输的数据进行安全拦截，并构建自动化应急能力；
- k) 宜构建全链路的数据流转的监控体系，能够实时了解数据的流向、传输情况；
- l) 应对关键的网络传输链路、网络设备节点实行冗余建设，保证数据传输可靠性和网络传输服务可用性；
- m) 应在数据传输完成后立即清除不再使用的历史缓存数据；
- n) 应详细记录数据传输过程日志，如传输链路建立成功与失败、监控异常与安全事件等。

8.3 数据存储安全

8.3.1 数据保存安全

数据保存安全应符合以下要求：

- a) 应制定数据安全保存的标准与规范，保证数据保存物理安全和环境安全；
- b) 应建立各类金融数据存储系统的安全配置规则，明确各类数据存储系统的账号权限管理、访问控制、日志管理、加密管理、版本升级等方面的要求；
- c) 应采用必要的技术手段支撑存储介质及逻辑存储空间的安全管理，如权限管理、身份鉴别、访问控制等，防止存储媒体的不当使用而可能引发的数据泄露风险；
- d) 应建立开放可伸缩的数据存储架构，根据安全级别、重要性、使用频率等因素，将数据分域分级存储；
- e) 应建立隔离存储授权和操作规范，确保具备多租户数据存储安全隔离能力；
- f) 应建立数据存储加密架构，满足应用层、数据平台层、操作系统层、数据存储层等不同层次的数据存储加密需求；
- g) 应建立数据分片和分布式存储安全规范和规则，采用必要的技术手段，保证分布式存储下分片数据完整性、一致性和保密性保护要求；
- h) 敏感数据应采取技术措施保证存储数据的保密性，必要时可采取多因素认证、固定处理终端、固定处理程序或工具、双人双岗控制等安全策略；
- i) 存储重要数据和个人信息等敏感金融数据，应采用加密、安全存储、访问控制、安全审计等安全措施；

- j) 应提供数据存储系统配置扫描工具，定期对重要的数据存储系统进行安全配置扫描，确保符合安全基线要求；
- k) 应将可用于恢复识别个人的信息与去标识化后的信息分开存储，并加强访问控制；
- l) 个人生物识别信息应与个人身份信息分开存储，在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份后，不应存储可提取个人生物识别信息的原始图像；
- m) 在我国境内产生的金融数据原则上应在我国境内存储，国家及行业主管部门另有规定的除外。

8.3.2 数据备份与恢复

数据备份与恢复应符合以下要求：

- a) 应根据金融数据的安全级别和对系统运行的影响，明确数据备份与恢复操作规程，制定数据备份和数据恢复策略，包含数据备份和恢复的范围、备份频率、备份方式与工具、日志记录、数据保存期限等；
- b) 生产数据应采取实时备份与异步备份、增量备份与完全备份的方式，提供本地数据备份与恢复功能；
- c) 应建立数据备份与恢复的统一技术工具，包括但不限于数据备份、数据快照、实时捕获、数据库复制、长期保存、容灾接管等技术，支持本地和异地数据灾备，保证数据备份、数据恢复的自动执行；
- d) 应建立备份数据的安全技术手段，包括但不限于对备份数据的访问控制、压缩或加密管理；
- e) 数据备份应基于多冗余策略，可采用定期磁带、远程镜像、磁盘冷备、热备、双活等技术，备份频度及保存期限不低于相关监管和业务使用要求；
- f) 应制定数据恢复方案，明确恢复成功的业务及系统指标，定期进行数据恢复演练，并对技术方案中关键技术的可行性进行验证测试，记录并保存验证结果；
- g) 应采取必要的技术手段定期对备份数据的完整性和可用性进行检查，对主要备份业务数据进行恢复验证，确保数据可用性；
- h) 对过期存储数据及其备份数据应采用彻底删除或匿名化的方法进行处理，保证数据已被完全清除、无法恢复或无法识别到个人；
- i) 应确保存储架构具备数据存储跨机柜、跨机房、跨地域的容错部署能力。

8.4 数据使用安全

8.4.1 数据访问

数据访问应符合以下要求：

- a) 金融机构应综合各类主体角色、信用等级、业务需求和数据时效性等因素，按最小化原则，针对金融数据的不同安全级别，制定相应的权限管理策略；
- b) 应建立精细粒度的访问权限申请和审核批准机制，并通过访问控制组件或访问控制代理技术对访问的终端设备、应用程序、操作、IP地址等多种因素综合进行访问控制，拒绝不符合策略规则的访问和操作行为；
- c) 应建立统一的身份鉴别授权访问控制的防护技术，包括：身份鉴别、基于多因素身份认证登录、二次授权等，并应支持特权账户和敏感数据相隔离，保障金融数据在被访问过程中的保密性和完整性；
- d) 应对数据的访问权限和实际访问控制情况进行定期审计，至少每半年1次对访问权限规则和已授权清单进行复核，及时清理已失效的账号和授权。

8.4.2 数据导入与导出

数据导入与导出应符合以下要求：

- a) 金融机构应综合数据量、增长速度、业务需求、性能等因素，根据最小够用原则，明确数据导入导出场景、数据范围及相关规程；
- b) 应依据金融数据分类分级要求建立符合金融业务规则的数据导入导出安全相关的授权策略、不一致处理策略和流程控制策略；
- c) 应建立数据导入导出安全评估机制和授权审批流程；
- d) 应对请求数据导入导出的终端、用户或服务组件等采取多因素鉴别技术进行身份鉴别，以验证其身份的真实性和合法性；
- e) 数据导入时，应使用安全扫描技术，确认是否被恶意感染，如木马植入、病毒等信息；
- f) 数据导出时，应使用安全传输通道，如IPsec VPN、SFTP或本地传输机制等，并使用数据加密、数据脱敏等技术手段防止数据泄露；
- g) 应记录金融数据的导入导出行为，包括操作人、操作时间、操作结果、数据类型及安全级别等，留存时间不少于6个月，确保可追溯。应定期进行审计，确保未超出数据授权使用范围；
- h) 在导入导出完成后应对数据导入导出通道的缓存数据进行清除，保证不可被恢复；
- i) 应为导入导出通道提供冗余备份的能力，确保数据导入导出的安全可靠；
- j) 应具有数据导入过程保护和回退机制，保障获取过程中产生问题时能有效还原和恢复数据。

8.4.3 数据加工

8.4.3.1 数据加工分析要求

数据加工分析应符合以下要求：

- a) 应明确原始数据加工过程中的数据获取方式、访问接口、授权机制、数据使用、处理结果安全等内容，明确数据分析工具使用算法，以及该算法使用数据范围及方式；
- b) 制定金融数据加工过程的相关安全管理规范，确保数据加工操作前后数据间的映射关系，应能通过数据血缘等方式保留溯源的信息；
- c) 应采用数据加密、数据脱敏等技术措施，保证数据加工过程的数据安全性；
- d) 针对个人信息数据的分析中，应采用多种技术手段降低数据分析过程中的隐私泄露风险，如差分隐私保护、K-匿名、数据沙箱等；
- e) 应对算法本身进行风险评估，以确定该算法输出的分析结果不会涉及到用户个人隐私和组织的敏感信息；
- f) 应记录并保存数据加工过程中个人信息、重要数据等敏感数据的操作行为，包括但不限于处理人员、处理系统IP地址、处理时间和处理方式等；
- g) 应对数据加工分析过程进行必要的监督和安全审核，采取必要的技术手段和管控措施，避免信息泄漏风险，确保数据加工分析过程的安全性；
- h) 应采用必要的技术手段，在数据有恢复需求时，保证数据加工过程中产生的数据问题能有效的还原和恢复数据；
- i) 应具备数据一致性检测及故障处理能力。

8.4.3.2 数据加工者要求

重要数据加工处理者、赴境外上市的数据加工处理者、向境外提供个人信息和重要数据的数据加工处理者，应当每年开展一次数据安全评估。一般数据安全评估框架包括：评估内容和范围、评估方法、评估结果、评估报告。

- a) 评估内容和范围：应明确各相关部门的金融数据全生命周期采集、传输、存储、处理、交换以及销毁各个阶段的安全管理评估范围，包括但不限于：

- 是否明确了对应的安全管控岗位和人员；
 - 是否采取了权限管理、访问控制、加密管理等安全技术防护手段；
 - 是否规定了数据脱敏规则、方法、处理流程；
 - 是否对数据处理、使用、删除以及权限申请等流程进行了规范；
 - 是否对相关操作进行了完整的日志记录；
 - 是否落实了定期的安全检查工作制度；
 - 是否落地了数据安全风险事件的自动监控和风险预警功能；
 - 是否明确了数据安全风险事件处置流程、方法以及应急预案等。
- b) 评估方法：在评估过程中采用的评估方法包括但不限于：
- 文档查验：依据金融数据安全管理规定等相关文档材料，查验各相关部门的金融数据安全管理的实际落实情况是否满足金融数据安全规定中数据全生命周期各个阶段的安管理的要求；
 - 配置核查：登录与金融相关的数据管理信息系统和应用系统，检查对应系统平台的实际配置情况是否与金融数据安全规定中数据全生命周期各个阶段的安管理要求保持一致；
 - 工具测试：利用技术工具对与金融数据相关的信息系统以及应用系统等进行实操测试，验证对应系统平台的管理能力是否符合相关评估内容所述技术能力、功能流程等安全管控要求；
 - 旁站验证：通过对与金融数据相关的应用界面、数据展示界面、数据存储界面、数据操作日志记录、数据处理流程、防护机制等进行查验，评估金融数据安全措施是否有效。
- c) 评估结果：应依据金融数据安全实际管理情况与金融数据安全规定中的数据全生命周期各个阶段的安管理要求进行对比分析，对数据产生方、数据应用方、数据管理方以及系统研发方实际的数据安全管理能力进行综合判定：
- 若金融数据全生命周期各个阶段的实际安全管理情况与金融数据安全规定90%（含）以上符合，则对应的评估结果应判定为“符合”；
 - 若金融数据全生命周期各个阶段的实际安全管理情况与金融数据安全规定60%（含）～90%符合，则对应的评估结果应判定为“基本符合”；
 - 若金融数据全生命周期各个阶段的实际安全管理情况与金融数据安全规定60%以下符合，则对应的评估结果应判定为“不符合”。
- d) 评估报告：根据评估结果编写评估报告，评估报告中应对评估内容、方法、结果、问题等进行总结和分析。同时，数据产生方、数据应用方以及系统研发方应将评估报告汇总提交至数据管理方，由数据管理方按照实际评估结果对金融数据安全具体落实情况进行汇总分析，并依据评估结果内容对金融数据安全规定中的安全管控措施进行调整。

8.4.4 数据展示

数据展示应符合以下要求：

- a) 数据展示前，应事前评估展示需求，包括展示的形式、条件、内容和目标等，并根据展示数据的类型和敏感等级，制定相应的安全策略；
- b) 数据展示时，应对应用系统桌面、运维终端、客户端应用软件、柜面受理设备、自助终端设备等界面展示增加水印，水印内容应最少包括数据所有者、访问主体、访问时间和使用用途；
- c) 数据展示时，应禁用展示界面复制、打印、截屏等可将展示数据导出的功能；
- d) 数据展示时，应对敏感数据进行逐条授权、逐条查询、分级防护或具备对查询相关授权、次数、频率、总量等指标的实时监测预警能力，并留存相关查询日志；
- e) 对于敏感数据的展示应在审批授权的基础上采用屏蔽、变形、替换、随机、格式保留加密（FPE）和强加密算法（如AES）等多种脱敏算法，防止数据泄露；

- f) 数据展示后，应及时将展示数据从本地缓存中清除。

8.4.5 数据开发测试

数据开发测试应符合以下要求：

- a) 应采取技术措施，实现生产环境数据和开发测试环境数据的有效隔离；
- b) 应通过技术手段控制数据的获取范围，包括对象、数据量等，并结合敏感数据的类型和匿名化的效果，以及该数据在开发测试过程中的用途和要求，制定数据脱敏策略；
- c) 在生产数据进入开发测试环境之前进行脱敏处理，确保经过脱敏后的数据不再带有敏感信息，防止数据处理过程中的数据泄露；
- d) 应对脱敏后的数据质量进行评估，保持源数据特征，满足开发测试对数据的仿真要求，不影响业务使用；
- e) 在开发测试等过程使用的数据，应采用伪行水印、伪列水印等技术，植入数据水印信息，在保证不干扰开发测试的情况下，对数据使用行为进行溯源，防止数据泄露；
- f) 应对开发测试中提供的算法模型的可用性、一致性、合规性、安全性进行审核；
- g) 使用外部的软件开发包、组件、第三方代码等开展开发测试工作前应进行数据安全评估；
- h) 应对开发测试过程进行日志记录，并定期进行安全审计。

8.4.6 数据汇聚融合

数据汇聚融合应符合以下要求：

- a) 汇聚融合的数据不应超出收集时所声明的使用范围，因业务需要确需超范围使用的，应再次征得个人金融信息主体的明示同意；
- b) 汇聚融合后产生的数据应采用智能化分类分级技术，重新确定数据安全级别；
- c) 应根据汇聚融合后可能产生的数据内容、数据用途、数据安全级别等开展数据安全影响评估，并采取有效的技术保护措施；
- d) 涉及第三方机构合作的，应以合同协议等方式明确用于汇聚融合的数据内容和范围、数据汇聚融合方式、结果用途和知悉范围、各合作方数据保护职责和义务，以及数据保护要求和技术规范等；
- e) 多个数据归属方在融合使用数据的过程中，应采用多方安全计算、联邦学习、数据加密等技术，保证各自数据不被泄漏，有效实现多方数据的使用价值；
- f) 原则上不应用于汇聚融合的数据，因业务需要确需汇聚融合的，应建立审批授权机制并采用数据跟踪溯源技术；
- g) 应对脱敏后的数据集或其他数据集经汇聚融合后重新识别出敏感数据的风险进行识别和评估，并采用有效的技术手段，对数据集进行安全保护；
- h) 宜建设数据安全隐私计算平台，促进金融机构和第三方机构数据进行数据融合、数据密文共享、联合计算、联合建模，使数据在各业务线之间流通，打通跨域数据的应用价值链。

8.4.7 公开披露

数据公开披露应符合以下要求：

- a) 应明确公开披露数据的内容、使用范围及规范，发布者与使用者的权利和义务；
- b) 数据公开披露前，应对拟披露的数据进行审核与审批，对拟披露数据的合规性、业务需求、披露渠道、披露时间、数据脱敏方案进行审核；
- c) 通过金融机构官方网站披露数据时，应具备防范网站页面的源代码暴露、网页防篡改、穷举登录尝试、重放攻击、SQL注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/325013104314011120>