ICS 35.240.40
A 11

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T XXXXX—XXXX

金融数据安全 数据生命周期安全规范

Financial Data Security - Security specification of data life cycle

（征求意见稿）

（本稿完成日期：2020 年 3 月 25 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

发 布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国人民银行提出。
本标准由全国金融标准化技术委员会（SAC/TC 180）归口。
本标准起草单位：。
本标准主要起草人：。

引　言

随着信息技术的发展，众多金融基础业务、核心流程、行业间往来等事务和活动均已运行在信息化支撑载体之上，金融业机构生产运行过程中产生的信息也逐步以不同形式转化为数字资产流转在金融业信息系统之中。随着大数据、人工智能、云计算等新技术在金融业的深入应用，数据逐步实现了从信息化资产到生产要素的转变，其重要性日益凸显。金融业机构数据泄露等安全威胁的影响逐步从机构内转移扩大至行业间，甚至影响国家安全、社会秩序、公众利益与金融市场稳定。如何在满足金融业务基本需求的基础上，强化金融行业数据保护能力，保障金融数据安全流动，已成为当前亟待解决的问题。

金融数据复杂多样，对数据实施生命周期安全管理，能够进一步明确数据生命周期各阶段的保护要求和保护目标，有助于金融业机构合理分配数据保护资源和成本，建立完善的数据生命周期防护机制。同时，合理、准确、完善的数据生命周期安全管理制度，能够促进金融数据在机构间、行业间的安全应用和共享，有利于金融行业数据价值的挖掘与实现。

为指导金融业机构合理制定和有效落实金融数据生命周期安全管理策略，进一步提高机构的数据管理和安全防护水平，确保金融数据的安全应用，编制本标准。

本标准凡涉及密码算法的相关内容，按国家密码管理部门及行业主管部门有关规定实施；凡涉及到采用密码技术解决保密性、完整性、真实性、不可否认性需求的，须遵循相关国家标准和行业标准。

金融数据安全 数据生命周期安全规范

1 范围

本标准从金融数据生命周期出发，规定了金融数据安全原则、安全防护要求、组织保障要求，数据安全工程要求以及信息系统运维保障要求等内容，建立了覆盖数据采集、传输、存储、使用、处理、交换、公开披露、数据跨境、删除及销毁各个过程的数据安全管理框架，为金融业机构开展数据生命周期安全防护工作提供指导。

本标准适用于金融业机构开展电子数据安全防护使用，并为第三方安全评估机构等单位开展数据安全检查与评估工作提供参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 50174-2017 数据中心设计规范

GB/T 25069—2010 信息安全技术 术语

GB/T 5271.1—2000 信息技术 词汇 第1部分：基本术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 4754-2017 国民经济行业分类

GM/Z 0001—2013 密码术语

GM/T 0002—2012 SM4分组密码算法

GB/T 37092-2018 密码模块安全检测要求

GB/T AAAA—AAAA《金融数据跨境安全要求》

JR/T 0158—2018 证券期货业数据分类分级指引

JR/T 0167—2018 云计算技术金融应用规范 安全技术要求

JR/T 0171—2020 个人金融信息保护技术规范

JR/T BBBB—BBBB 金融数据安全 数据安全分级指南

JR/T CCCC—CCCC 分布式数据库技术金融应用规范 安全技术

3 术语和定义

GB/Z 28828-2012及GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

3.1

信息（在信息处理中） information（in information processing）

关于客体（如事实、事件、事物、过程或思想，包括概念）的知识，在一定的场合中具有特定的意义。

[GB/T 5271.1-2000，定义01.01.01]

3.2

数据 data

信息的可再解释的形式化表示，以适用于通信、解释或处理。

注：可以通过人工或自动手段处理。

[GB/T 5271.1-2000，定义01.01.02]

3.3

隐私 privacy

个人所具有的控制或影响与之相关信息的权限，涉及由谁收集和存储、由谁披露。

[GB/T 25069—2010，术语2.1.63]

3.4

信息处理 information processing

对信息操作的系统执行，包括数据处理，也可包括诸如数据通信和办公自动化之类的操作。

注：术语“信息处理”不能用为“数据处理”的同义词。

[GB/T 5271.1-2000，定义01.01.05]

3.5

数据处理 data processing

自动数据处理 automatic data processing

数据操作的系统执行。

例：数据的数学运算或逻辑运算，数据的归并或分类，程序的汇编或编译，或文本的操作，诸如编辑、分类、归并、存储、检索、显示或打印。

注：术语“数据处理”不能用为“信息处理”的同义词。

[GB/T 5271.1-2000，定义01.01.06]

3.6

保密性 confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[GB/T 25069—2010，术语2.1.1]

3.7

完整性 integrity

保卫资产准确性和完整的特性。

[GB/T 25069—2010，术语2.1.42]

3.8

可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069—2010，术语2.1.20]

3.9

金融数据 financial data

金融业机构开展金融业务、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。

[JR/T BBBB—BBBB，术语3.10]

3.10

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。

3.11

个人金融信息主体 personal financial information

个人金融信息所标识的自然人。

注：改写GB/T 35273—2020，定义3.3。

3.12 **个人金融信息安全影响 personal information security impact assessment**

针对个人金融信息处理活动，检验其合法合规程度，判断其对个人金融信息主体合法权益造成损害的各种风险，以及评估用于保护个人金融信息主体的各项措施有效性的过程。

注：改写GB/T 35273—2020，定义3.9。

3.13

影响 impact

事件的后果。在信息安全中，一般指不测事件的后果。

[GB/T 25069—2010，术语2.3.105]

3.14

删除 delete

在金融产品和服务所涉及的系统中去除信息的行为，使其保持不可被检索、访问的状态。

注：改写GB/T 35273—2020，定义3.10。

3.15

明示同意 explicit consent

个人金融信息主体通过书面声明或主动作出肯定性动作，对其个人金融信息进行特定处理作出明确授权的行为。

注1：肯定性动作包括个人金融信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

注2：改写 GB/T 35273—2020，定义 3.6。

3.16

匿名化 anonymization

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

注1：个人金融信息经匿名化处理后所得的信息不属于个人金融信息。

注2：改写 GB/T 35273—2020，定义 3.14。

3.17

去标识化 de-identification

通过对个人金融信息的技术处理，使其在不借助额外信息的情况下，无法识别个人金融信息主体的过程。

注1：去标识化仍建立在个体基础之上，保留了个体颗粒度，采用假名、加密、加盐的哈希函数等技术手段替代对个人金融信息的标识。

注2：改写 GB/T 35273—2020，定义 3.15。

3.18

特权访问安全 Privileged access security

特权访问安全是一种帮助企业解决特权帐户相关问题的技术。

3.19

特权账户 Privilege account

是指涉及到企业核心数据资产的账号，特权账号存在于服务器、应用系统、数据库、中间件等。

3.20

未经授权的查看 unauthorized reading

未得到信息的所有者或有权授权人授权对信息的查看。

注1：未经授权的查看可能是善意的，也可能是恶意的；信息处理者无意泄露的未经授权的查看为信息泄露事件；攻击者通过使相关安全措施无效的措施有意获取的未经授权的查看为信息窃取事件。

注2：非法查看是对未经授权的查看的一种不严谨但在特定的语境下并无二义性的提法。

3.21

未经授权的变更 unauthorized altering

未得到信息的所有者或有权授权人授权对信息的变更。

注1：未经授权的变更典型地分为未经授权的增加（即增加全新的内容）、未经授权的更改（即修改现有的内容）或未经授权的删除（即删除原有的内容）三种情况，也可能是三种情况的组合。

注2：未经授权的变更可能是善意的，也可能是恶意的；往往表现为信息篡改事件、信息假冒事件、信息丢失事件等。

注3：非法变更是对未经授权的变更的一种不严谨但在特定的语境下并无二义性的提法。

4 缩略语

API	Application Programming Interface	应用程序接口
DLP	Data Leakage Prevention	数据防泄漏
DES-CBC	Data Encryption Standard-Cipher Block Chaining	数据加密标准-密码块链接

MD5	Message-Digest Algorithm 5	消息摘要算法5
TLS	Transport Layer Security	传输层安全协议
WORM	Write Once Read Many	一次写入多次读取
OCR	Optical Character Recognition	光学字符识别

5 概述

5.1 安全框架

金融数据生命周期是指金融业机构在开展业务和进行经营管理的过程中，对金融数据进行采集、传输、存储、使用、删除、销毁的整个过程，数据生命周期安全框架的示意如图1所示，遵循基本原则，以数据分级为基础，建立数据生命周期安全防护体系，并通过完善数据安全组织建设、明确数据安全工程与信息系统运维等环节的数据安全需求，全面保障金融业机构数据安全。

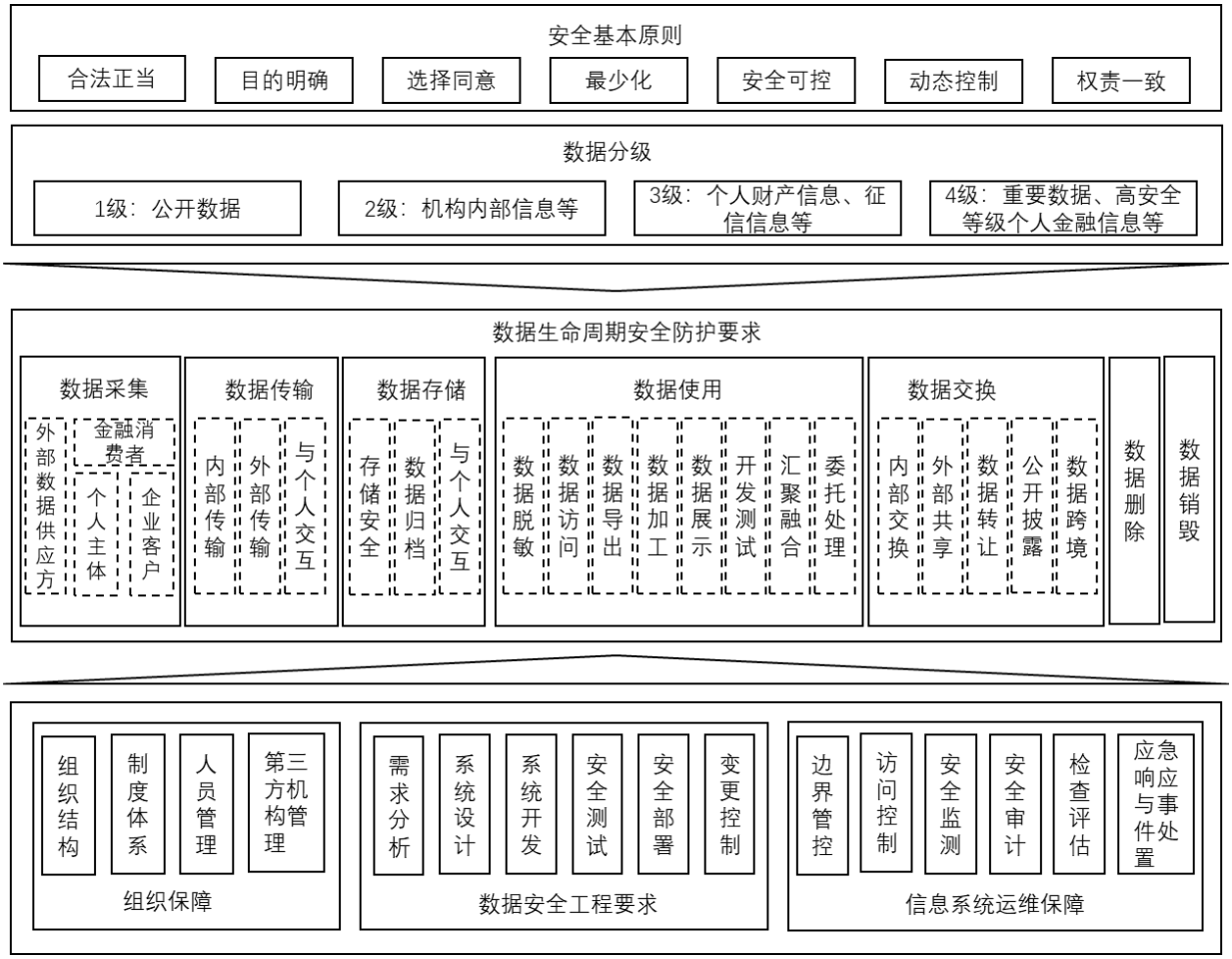

图1 数据生命周期安全框架示意图

数据安全原则确立数据安全防护工作的根本任务和基线要求，数据分级进一步明确数据安全防护工作的具体对象和防护重点，是构建数据生命周期安全框架的前提，也是金融机构建立全方位数据安全防护体系的前提条件。明确数据安全基本原则及数据的安全级别，有利于金融机构实施更为科学的数据安全方针、政策和总体部署，并进一步优化相关安全防护资源的合理配置。

数据生命周期安全防护要求是数据生命周期安全框架的核心，针对不同安全级别的数据，明确其在采集、传输、存储、使用、交换、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。结合金融业数据业务规则及金融数据的特点，建立覆盖金融数据生命周期全过程的安全防护机制，是金融机构数据安全防护工作的重中之重，也是确保金融数据安全的必经之路。

同时，组织保障、数据安全工程要求及信息系统运维保障也是数据生命周期安全框架必不可少的组成部分，共同构成确保数据生命周期安全防护机制能够有效落实和严格执行的基石。组织保障确保数据安全工作具有自决策层、管理层、执行层到监督层的完善管理体系，为数据安全相关工作的组织和落实奠定基础；数据安全工程要求将数据安全防控融入金融业机构信息系统建设、产品和服务研发等全过程中，确保从建设需求分析开始，就已将数据安全纳入全盘考虑的范畴；此外，在金融机构日常的运营过程中，信息系统运维过程的数据安全防控工作也不容忽视，加强在边界管控、访问控制、安全监测、安全审计、检查评估以及应急响应与事件处置等过程中的数据安全，能够有力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响应。

5.2 安全级别

金融数据安全级别可参照JR/T BBBB—BBBB《金融数据安全 数据安全分级指南》执行。根据安全性遭到破坏后的影响范围和影响程度，将金融数据的安全级别由高到低划分为4级、3级、2级、1级，涉及个人金融信息的参照JR/T 0171—2020中的C3、C2、C1分类，分别对应数据安全级别4级、3级、2级。金融业机构可根据实际管理情况，参照上述指南开展数据资产梳理及安全分级工作。

本标准所指金融数据安全，主要是指确保金融数据在其生命周期各阶段的安全性（保密性、完整性和可用性），通过采取相应措施，将数据安全性遭受破坏可能带来的安全影响（如安全隐患、声誉受损、财产丢失、设施损毁等）降至最低（或降至可接受的范围内）。其中，1级数据为公开数据，原则上无保密性要求，其安全防护需参考本标准有关完整性及可用性相关安全要求；2级至4级数据的安全防护，需在平衡安全需求与业务需求的基础上（如2级数据应优先考虑业务需求，4级数据应优先考虑安全需求），根据数据安全级别不同，有侧重地对数据进行适当保护安全防护，促进数据安全流动，深度挖掘并充分发挥金融数据的价值。

未经电子化的信息，依据档案文件等有关管理规范执行；涉及国家秘密的，依据国家有关法律法规执行，不在本标准规定的范围之内。证券行业数据安全分级工作可参照《证券期货业数据分类分级指引》执行。金融业机构境外分子公司及分支机构在境外开展业务过程中采集、产生的数据，其安全定级及数据保护工作可在参考当地法律法规及行业监管要求的前提下开展。

本标准中未明确具体安全级别的条款,为安全级别为1级至4级数据均应满足的数据安全通用要求，明确具体安全级别的条款，为该级别在满足数据安全通用要求基础上，需执行的附加安全要求。

6 数据安全原则

为防范和抵御金融数据安全风险，金融业机构在业务开展及日常经营管理过程中，应遵循以下数据安全基本要求：

a) 合法正当原则：金融数据的采集和应用应满足国家法律法规、部门规章、行业标准及监管政策等有关规定，确保数据采集和使用的合法性和正当性；
b) 目的明确原则：应制定金融数据安全防护策略，明确金融数据生命周期各阶段的安全防护目标和要求；
c) 选择同意原则：应向个人数据主体明示个人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；

d) 最小化原则：金融数据的采集应遵循最小够用；存储应根据内外部管理要求满足最小时限要求；使用仅应授予满足开展业务所必需的最小权限；
e) 全程可控原则：应通过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阶段的保密性、完整性和可用性，避免数据在全生命周期里被未授权访问、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应是一次性和静态的，应可基于业务需求、安全环境属性、系统用户行为等因素实施实时和动态的调整；
g) 权责一致原则：应明确本机构数据安全防护工作相关部门及其职责，有关部门及人员应积极落实相关措施，履行数据安全职责。因不履行或不当行使其职权等造成不良影响或损害的，均需承担相应的安全责任。

7 数据生命周期安全防护要求

7.1 数据采集

7.1.1 描述

数据采集是指金融业机构在提供金融产品和服务、开展经营管理等活动中，直接或间接从个人信息主体、企业客户及外部数据供应方采集数据的过程。数据采集过程，存在敏感数据泄露、数据源伪造、特权账户滥用等安全风险/问题，应采取技术措施加强数据采集过程的安全防护。

金融数据采集流程实现对数据的采集与提取、数据转换与标准化、信息交换与上传，并提供内置安全审计与监管等辅助工具。按照采集模式，可分为两种形式，包括从外部机构采集数据，从个人金融金融信息主体、企业客户等金融消费者处采集数据，详见附录A。

7.1.2 从外部数据供应方采集数据

金融业机构应：

a) 明确数据源、数据采集范围和频度，并开展数据安全影响评估；
b) 应制定数据供应商调查机制，并采用合同协议等方式，明确双方在数据安全方面的责任及义务，并确保外部供应商所提供数据的合法合规性和真实性；
c) 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；
d) 明确数据采集过程中个人信息和重要数据的知悉范围和安全管控措施，确保采集数据的合规性、完整性和真实性；
e) 应采取消息验证码、消息摘要等技术手段确保采集过程数据的完整性；
f) 采取自动化手段从网站或其他公开数据库间接收集数据时，应考虑网站和其他公开数据库的数据处理能力和网络承载能力，不能影响网站和公开数据库的正常运行；
g) 应对人工批量数据采集的环境进行安全管控，并通过人员权限管控、信息碎片化等方式，防止数据泄露；
h) 跟踪和记录 2 级及以上数据的采集过程，并采取技术措施确保所收集信息来源的可追溯性；
i) APP、WEB 等客户端不应留存 3 级及以上级数据，业务完成后应立即清除，并应及时对 cookies 等缓存进行清理；
j) 采集 3 级数据时，除以上条款外，还应结合口令密码、设备指纹、设备物理位置、网络接入方式、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；
k) 采集 4 级数据时，除以上条款外，还应满足：

1) 对采集全过程进行持续动态认证，确保数据采集设备或系统身份的真实性，必要时可实施阻断、二次认证等操作；
2) 对于采集数据进行数据级加密，并优先使用 SM 系列等国家商用密码算法；
3) 不应通过人工方式采集。

7.1.3 从金融消费者处采集数据

7.1.3.1 从个人金融信息主体采集数据

a) 从信息主体采集的信息属个人金融信息时，金融业机构应依据 JR/T 0171—2020《个人金融信息保护技术规范》6.1.1、7.1.1 相关要求，遵循合法、正当、必要的原则开展信息采集工作；
b) 通过纸质表单采集信息并转换为电子信息时，应满足以下要求：
   1) 所采集的信息应与提供的金融产品（或服务）直接相关，并与协议条款、隐私政策中约定收集的内容保持一致，不应超范围采集信息；
   2) 对表单的保存、传输、查阅、复制等操作进行严格授权审批，涉及 3 级以上数据的操作，应进行专项审批，并对表单（含纸质表单、电子化过程中以及电子化完毕后的表单）流转的全过程进行监控与审计；
   3) 在纸质表单电子化的过程中，应采取技术措施对电子化过程中的数据完整性、保密性进行控制；
   4) 纸质表单电子化工作若委托给第三方机构（包含外包服务机构与外部合作机构）处理时，应：
      (1) 对外包行为及第三方数据安全防护方案进行数据安全影响评估，确保受委托者具备足够的数据安全能力，并提供了足够的安全保护措施；
      (2) 应对第三方机构等受委托者进行监督，包括但不限于通过合同等方式规定受委托者的责任和义务，对受委托者进行安全检查和评估等。
c) 数据采集过程应符合 7.1.2 节中 c)至 k）所述要求；
d) 金融业机构在停止其提供的金融产品或服务时，应及时停止收集个人金融信息的活动。

7.1.3.2 从企业客户采集数据

金融业机构应：

a) 应采用合同协议等方式，明确数据采集的范围、频度、类型、用途等，并确保数据的合法合规性和真实性；
b) 基于不同业务目的所收集的企业客户信息，根据所用于的目的，开展数据安全影响评估，并采取相应的有效保护措施；
c) 数据采集过程应符合 7.1.2 节中 c)至 k）所述要求；
d) 通过纸质表单采集信息并转换为电子信息时，应满足 7.1.3.1 节中 b)所述要求。

7.2 数据传输

7.2.1 描述

数据传输是指金融业机构将数据从一个实体传输到另一个实体的过程，存在传输中断、篡改、伪造及窃取等安全风险，应采取数据传输加密、身份认证等技术措施加强数据传输过程的安全防护。金融数据传输涉及与金融机构相关联的全通信网络架构，按照传输模式，可分为金融机构内部数据传输

和金融机构与外部机构间的数据传输两种形式，不同传输形式和不同传输对象间所采用的数据传输技术方式也不同，金融机构数据传输模式详见附录B。

7.2.2 金融机构内部数据传输

金融机构内部数据传输，应满足如下要求：

a) 局域网内部应加强无线网络安全，生产网不应使用 WLAN，办公网使用 WLAN 应采用足够强度的安全防护措施，包括但不限于：
   1) 应通过绑定设备序列号或 MAC 地址（硬件地址）等硬件特征信息对无线接入点进行准入控制，合理设置传输功率，控制无线信号的覆盖范围；
   2) SSID 应采用规范的命名规则，且不应泄露机构、网络特性、物理位置等信息；
   3) 不应使用缺省 SSID，应进行信号隐藏，并禁用 SSID 广播，避免攻击者通过扫描直接获取无线网络信息；
   4) 应加强无线网络设备的管理帐号和口令安全，不应使用弱口令；
   5) 应采用双因素认证方式对接入用户进行身份校验；
   6) 接入端设备不应安装和使用无线网络密码分享等对数据安全有危害性的程序；
   7) 应控制移动智能终端在内网和互联网间的交叉使用；
   8) 短期使用和临时搭建的无线网络应及时拆除或关闭。
b) 海外专线应在租用专线的基础上，通过虚拟专网等技术确保传输线路的安全，确保其作为内部网络传输数据的安全性；
c) 传输通道建立前，应对通信双方进行身份鉴别和认证，确保数据传输双方是可信任的；
d) 对客户端应采取准入控制、身份认证等技术措施，防止非法或未授权终端接入网络；
e) 通过公开网络进行数据传输时应通过密钥、证书等密码技术手段进行双向认证，如使用安全套接字层或传输层安全（SSL/TLS）、互联网协议安全（IPSec）等协议；
f) 应对数据完整性进行验证，包括但不限于：
   1) 采用非密码技术，如奇偶校验、校验和等方式；
   2) 采用密码技术，如摘要、消息认证码、数字签名等方式。
g) 应采用设备冗余、线路冗余等措施，确保数据传输的可用性；
h) 应采用负载均衡、防入侵攻击等安全技术或设备来降低数据传输网络的可用性风险；
i) 应采用数字签名、时间戳等方式确保数据传输的抗抵赖性；
j) 通过物理介质传递生产数据时，应由专人押运确保物理介质安全到位，不应在无人监管下通过第三方（如民用物流公司等）进行传递；
k) 应使用安全的算法组合，禁用不安全的算法组合，如禁用基于 MD5、DES-CBC、SHA1 等算法组合；
l) 2 级数据传输应经过数据所有者授权审批，并留存数据传输相关日志；
m) 3 级级以上数据的传输，除满足以上要求外，还应采取报文级加密措施，禁止在通信数据中以明文形式出现；
n) 4 级数据的传输，除满足以上要求外，还应使用加密协议进行通道加密。

7.2.3 金融机构与外部机构数据传输

金融机构与外部机构数据传输，应满足如下要求：

a) 金融机构与外部机构之间的数据传输应优先选择专线、VPN 等技术；
b) 采取虚拟专网技术的传输链路，应对 VPN 用户和权限进行严格管理，采取适当强度的用户认证方式，并应按照“最小权限”原则对用户访问权限进行管控，防范非法接入行为；

c） 数据传输过程，应满足 7.2.2 中 c）至 k）所述要求；
d） 2 级数据外部传输应经过数据所有者授权审批，并使用加密协议进行通道加密或使用数据加密；
e） 3 级及以上数据原则上不应对外传输，若因业务需要确需传输或迁移时，除满足以上要求外，则应经数据所有者授权审批，并采用脱敏、去标识化或密码技术确保数据保密性；
f） 4 级数据中的个人金融信息原则上不应对外传输，国家法律法规及行业主管部门另有规定的除外。

7.2.4 金融机构与个人金融信息主体数据传输

金融机构与个人金融信息主体数据传输，应满足如下要求：
a） 使用公共网络进行通信的，应采取技术手段防范恶意第三方通过获得网络操控能力，避免发生 APT 攻击、DDOS、Worm 恶意软件攻击等网络攻击；
b） 金融业机构与金融消费者通过电子化渠道（如网上银行、手机银行、自主终端等）进行数据传输时应符合 JR/T 0171—2020 中 6.1.2 要求；
c） 数据传输过程，应满足 7.2.2 中 c）至 k）以及 7.2.3 中 d）至 f）所述要求。

7.3 数据存储

7.3.1 概述

数据存储是指金融业机构在提供金融产品和服务、开展经营管理等活动中，将数据进行持久化存储的过程，包括但不限于采用云存储服务、网络存储设备等载体存储数据。数据存储过程，可能存在敏感数据泄露、数据篡改、数据丢失、数据不可用等安全风险，应采取技术措施加强数据存储过程的安全防护。其中，数据存储应对数据存储设备及基础设施做好安全防护，包括落实数据存储设备的安全基线、接入鉴权机制等，以确保存储数据的可用性、完整性和持久性。

7.3.2 存储安全

数据存储的安全保障应满足以下要求：

a） 数据存储不应因存储形式或存储时效的改变而降低其安全保护强度；
b） 应依据最小化原则存储数据，不应以任何形式存储非业务必须的金融数据，存储时间应为业务必需的最短时间，国家法律法规与行业主管部门另有规定的除外；
c） 应定期对数据保存过程中可能产生的影响进行分风险评估，并采取相应安全防护措施；
d） 云环境数据存储和处理的物理设备应位于中国境内，并按照国家与金融主管部门规定对数据进行加密存储；
e） 分布式数据库存储应满足 JR/T CCCC—CCCC《分布式数据库技术金融应用规范 安全技术》标准要求；
f） 2 级及以上数据应采取技术措施保证存储数据的保密性，采取细粒度的访问控制与安全审计策略，必要时可采取固定处理终端、双人双岗控制等安全策略；
g） 3 级及以上数据存储时，应采用数字签名技术、数据鉴别码（DAC）等技术保证存储的数据完整性，使用数据时应进行数据完整性校验，并对数据完整性的破坏进行审计；
h） 应使用密码算法对 3 级数据及以上数据进行加密存储；
i） 文件系统中存放含有 3 级及以上数据的文件，宜采用整个文件加密存储方式进行保护。

7.3.3 数据归档

金融机构数据归档应满足以下要求：

a) 建立归档数据的压缩或加密策略，确保归档数据存储空间的有效利用和安全访问，数据安全保护等级与保护强度不应因数据归档而降低；
b) 依据数据生命周期和相关 IT 服务等级规范（SLA）建立不同的数据归档存储相关操作规程；
c) 应建立归档数据的安全策略和管控措施，防止非授权用户访问归档数据；
d) 建立在线/离线的多级数据归档架构，支持海量数据的有效归档、恢复和使用；
e) 定期采取必要的技术手段和管控措施查验归档数据完整性和可用性；
f) 建立归档数据安全审计与恢复制度，并指定专人负责。

7.3.4 备份和恢复

金融机构数据备份与恢复工作应满足以下要求：

a) 根据数据的安全级别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，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；生产中心应提供本地数据备份与恢复功能，采取实时备份与异步备份、增量备份与完全备份的方式；
b) 应建立同城与异地数据备份中心的远程数据备份与恢复功能，利用通信网络将关键数据定时批量传送至备用场地；
c) 云服务客户应在本地保存其业务数据的备份；
d) 数据备份方式应基于多冗余策略，可采用磁带、磁盘镜像、磁盘冷备等技术实现，备份频度及保存期限不低于相关监管和业务使用要求；
e) 应定期开展灾难恢复演练，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；
f) 应定期对备份数据的有效性进行检查，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，确保数据可用性；
g) 生产数据备份环境的物理和环境保护等级应参照 GB 50174-2017 执行；
h) 生产数据恢复到非生产环境后，应在申请使用时间到期后及时清理，防止未授权使用和访问；
i) 大数据平台应能提供数据整体迁移，并具备迁移数据的完整性检测能力。

7.4 数据使用

7.4.1 概述

数据使用是指金融业机构在提供金融产品和服务、开展经营管理等活动中，对金融数据进行访问、导出，以及分析、脱敏、加工、清洗等处理的过程。数据使用不得超出与收集数据时所声明的目的和范围，数据使用过程存在数据非授权访问、数据窃取、数据泄漏、数据损毁等安全风险的，应采取技术措施加强数据处理过程中的安全防护。

7.4.2 数据脱敏

数据脱敏是通过模糊化等方法对原始数据的处理，达到屏蔽重要数据、个人金融信息的一种数据保护方法。金融业机构数据脱敏应至少满足以下要求：

a) 应由数据所有者制定数据脱敏规范，明确数据脱敏规则、脱敏方法和使用限制等，如 4 级数据必须全部脱敏，3 级、2 级数据根据实际业务场景进行脱敏，1 级数据原则上可不做脱敏；
b) 应提供数据脱敏组件或技术手段，支持泛化、抑制、假名化、差分隐私等数据脱敏技术，宜提供统一的数据脱敏工具或服务组件，实现数据脱敏工具与数据权限管理系统的联动；

c） 应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；
d） 脱敏后的数据应与恢复文件隔离存储，本机构恢复原始数据的技术使用应由数据所有者申请，数据所有者、技术部门进行审核。

7.4.3 数据访问

7.4.3.1 基本要求

数据访问指各类主体对金融业机构数据资源的获取和使用，金融业机构应通过有效的管理和技术手段，按照预定策略控制各类主体的数据访问，具体要求如下：

a） 应综合考虑主体角色、可信级别、业务需要、时效性等因素，按最小化原则确定 2 级及以上数据的访问权限规则；3 级及以上数据访问还应建立访问权限申请和审核批准机制；
b） 应根据数据的不同安全级别，制定和明确数据访问控制过程中的相关安全措施，保障金融数据在被访问过程中的保密性和完整性，包括但不限于：
   1） 2 级及以上的数据访问应进行身份认证，对访问者实名认证，防止数据的非授权访问；3 级及以上的数据访问应实现多因素认证或二次授权；
   2） 2 级及以上的数据访问过程应留存相关操作日志。操作日志应至少包含明确的主体、客体、操作时间、具体操作类型、操作结果等；
   3） 3 级及以上的数据访问还应结合业务需要使用匿名、去标识化等手段，以满足最小化原则的要求。
c） 应对数据的访问权限和实际访问控制情况进行定期（最长不超过 6 个月）审计，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；
d） 应限制频繁查询数据人员（如柜员、客户经理等）的数据访问频率，严禁批量查询，确需批量查询的应通过相应审批并留存相关记录；
e） 应根据国家相关法律法规和金融主管部门云环境相关管理要求，制定本机构云环境使用安全规范。

7.4.3.2 特权访问安全要求

特权访问指通过不受原有访问控制措施限制的方式访问数据，例如使用数据库管理员权限访问数据，或使用可以在信息系统内执行所有功能、访问全量数据的特权账号等。特权访问的安全管理应遵循如下要求：

a） 特权账号应明确安全责任人，严格限定特权账号的使用地点，并配套多因素认证措施对使用者进行实名认证；
b） 应预先明确特权账号的使用场景和使用规则，并配套建立审批授权机制。可访问 3 级及以上数据的特权账号，在每次使用前均应按照事先建立的流程提出申请，经审批同意后方能使用；
c） 应详细记录特权账号的访问过程和操作记录，配备事后审计机制，并确保特权账号无法对操作日志进行修改和删除。

7.4.4 数据导出

数据导出指金融业机构在经营过程中因法律法规要求或业务需要将生产数据从信息系统中导出至终端、介质等较低等级安全域的情形。数据导出过程中，应遵循如下安全要求：

a） 金融业机构应根据最小化原则，确定数据的导出场景、导出数据范围和相应的权限规则；
b） 应通过风险评估、安全设计、流量监测、定期检查等手段确保数据导出涉及的协议、软件平台和传输信道的安全性；

c) 数据访问过程中执行导出操作的，访问主体的数据导出权限不得超过数据访问权限，3 级及以上数据的导出操作还应有明确的权限申请和审核批准机制；
d) 2 级及以上的数据导出操作应明确安全责任人，配备安全、完善的身份验证措施对导出操作人进行实名认证；3 级及以上数据的导出操作前还应使用多因素认证或二次授权机制，并将操作执行的网络地址限制在有限的范围内；
e) 2 级及以上的数据导出应有详细的操作记录，包括操作人、操作时间、操作结果、导出的数据对象等；
f) 3 级及以上的数据导出应使用去标识化、匿名化、加密等技术手段确保数据的保密性，国家相关法律法规和监管另有要求的除外；
g) 4 级数据原则上不能导出，确需导出的，除上述要求外，还应经金融业机构高级管理层批准，并配套数据跟踪溯源机制；
h) 数据导出应保存相关日志，日志留存时间最少为 6 个月。

7.4.5 数据加工

数据加工是指，基于金融业机构生产、业务系统中的原始数据，构建数据库表拼接、创建，数据字段的生成、衍生的过程。金融业机构数据加工应至少满足以下要求：

a) 明确原始数据数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容；
b) 原则上不允许对 4 级数据进行加工；
c) 3 级数据加工之前应进行数据安全评估；
d) 应采取必要的监控审计措施，确保实际加工操作符合安全规范，并对数据加工的保密性、完整性、可用性进行持续监督和评价，制定整改方案，监督整改；
e) 应完整记录数据加工过程的操作日志。

7.4.6 数据展示

数据展示是指金融业机构因业务需要，将数据资源显示的过程。金融业机构数据展示应至少满足以下要求：

a) 数据展示前，应事前评估展示需求（包括展示的条件、展示的对象和展示的内容），分析展示的必要性和安全性，具体要求如下：
   1) 应评估数据展示环境的安全性，避免因展示环境的安全缺陷导致数据泄露；
   2) 应在数据展示前对展示界面的访问权限做限制，仅允许获得授权的主体访问；
   3) 原则上不得展示非业务必须数据，确需展示时应屏蔽展示内容关键字段，因业务需要明文展示的，应通过相应的审批授权机制核实后方可展示，并形成审批记录。
b) 数据展示时，应确保展示数据的安全性，具体要求如下：
   1) 应对展示界面增加水印，水印内容应最少包括访问主体、访问时间；
   2) 应禁用展示界面复制、打印等可将展示数据导出的功能；
   3) 业务系统功能应对相关信息明文查询设计逐条查询功能，经审批获得授权后方可查看，并留存相关查询日志。
c) 数据展示后，应及时将展示数据从本地缓存中清除；
d) 2 级数据的展示应使通过数据所有者审批后方可展示；
e) 3 级数据的展示应在审批的基础上采用屏蔽、脱敏等措施防止信息泄露；
f) 4 级数据中属个人金融信息 C3 类数据的不得展示。

7.4.7 开发测试

开发测试是指以发现软件、程序错误，衡量软件、程序质量，并对其是否能满足设计要求进行评估的过程。金融业机构开发测试应至少满足以下要求：

a) 应制定开发测试规范，对前端及应用开发平台进行统一管理，在采集、传输、存储、处理客户敏感信息时应遵循“最小必需、授权审批”原则；
b) 应采取技术措施，实现开发测试环境与生产环境的有效隔离；
c) 应通过安全运维管理平台或数据提取专用终端获取数据，专用终端经审批后方可开通，操作流程可追溯，原则上不得涉及 4 级数据；
d) 开发测试等过程的数据，应事先采取去标识、匿名化等技术措施进行脱敏处理，防止数据处理过程中的个人金融信息泄露；
e) 使用外部的软件开发包/组件/源码开展开发测试工作前应进行安全评估；
f) 接入开发测试环境的内外部终端设备均应安装统一的终端安全管理软件；
g) 应制定开发测试安全审核流程，对数据源、需求、进行审核，以确保数据分析目的、分析操作等方面的正当性与合法性；
h) 应对开发测试过程进行日志记录，并定期进行安全审计；
i) 使用云环境进行开发测试的，非金融业机构设备接入开发测试环境应经过开发、运行部门审批，存储有开发测试数据的设备、介质带离金融业机构前应经过开发、运行部门审批；
j) 开发测试后的数据应参照本标准 7.10 节相关要求进行销毁。

7.4.8 汇聚融合

汇聚融合是指金融业机构因提供金融产品和服务、开展经营管理等活动，与机构内不同部门、控股子公司、控股机构及外部机构进行数据合作，产生新数据的过程。金融业机构数据汇聚融合应至少满足以下要求：

a) 汇聚融合后的数据应参照 JR/T BBBB-BBBB 进行重新定级，数据级别不应低于源数据等级；
b) 应根据数据汇聚融合后的类型、级别及所用于的目的，开展数据安全影响评估，并采取适当的技术保护措施；
c) 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明示同意；
d) 个人金融信息用于汇聚融合时，应开展个人金融信息安全影响评估，并采取适当的技术保护措施；
e) 4 级数据原则上不能用于汇聚融合，确有需要的，应经金融业机构高级管理层批准，建立数据跟踪溯源机制，并应制定审核机制，在数据汇聚融合后进行删除，审核和评估数据删除结果；
f) 跨金融牌照的汇聚融合应参照《金融控股公司监督管理试行办法》执行。
g) 应对匿名化或去标识化处理的数据集或其他数据集汇聚后重新识别出个人金融信息主体的风险进行识别和评价，并对数据集采取相应的保护措施；
h) 基于不同业务目的所收集的个人金融信息，根据汇聚融合后所用于的目的，开展安全影响评估，并采取有效的保护措施。

7.4.9 委托处理

委托处理指金融业机构因金融产品或服务的需要，将机构采集的数据（含机构内部生成的数据）委托给第三方机构（包含外包服务机构与外部合作机构）进行处理，并将处理结果反馈给金融业机构

的过程。此处委托处理的数据包括电子化数据、纸质单据 OCR 作业，以及纸质单据人工录入数据等。

金融业机构委托处理具体要求如下：

a) 金融业机构应依据本标准 8.4 节,落实委托处理活动中的第三方开展数据安全管理工作要求；

b) 受委托的第三方机构应满足外部监管机构的相关要求，金融业机构应对第三方机构开展事前尽职调查；

c) 委托行为不得超出 9.2 需求评审过程中确定的数据范围，若委托数据包含从企业客户采集的数据，其数据委托处理范围不得超出合同条款约定范围，若委托数据包含个人金融信息，则数据委托处理范围应符合 JR/T 0171—2020 中 6.1.4.1 节 a）款要求；

d) 应对委托行为进行数据安全评估(涉及个人金融信息的,应进行个人金融信息安全影响评估)，并确保受委托者具备足够的数据安全能力，且提供了足够的安全保护措施；

注1：数据安全评估（data security assessment），即针对数据处理活动,检验其安全及合法合规程度，评估数据安全保护措施有效性的过程。

e) 4 级数据不应进行委托处理；

f) 对委托处理的电子数据，应执行以下安全控制措施：

(1) 涉及个人金融信息的，应采用去标识化（不应仅使用加密技术）等方式进行脱敏处理；

(2) 涉及 2 级、3 级数据的，应对数据进行加密处理，并采取设置伪数据记录（行数据）、插入特征跟踪字段（列数据）、数字水印等 DLP 技术，降低数据被泄露、误用、滥用的风险；

(3) 若委托处理内容为市场或趋势分析等情况，应使用匿名化技术将明文数据进行匿名化处理；在选择匿名化技术时，宜结合委托处理业务需要，选择被猜解（或碰撞）风险相对较低的匿名化技术（包括但不限于 K-匿名）；若选择假名化技术，则应将其视同为明文数据，同时执行上述（2）款安全控制措施；

(4) 对委托处理的数据进行安全审计，若数据通过信息系统（包括 API、摆渡服务器）与委托方进行传递，则应在相应的控制节点（信息系统业务功能、API、服务器用户）设置安全审计功能，对数据的外发与回传进行审计；若数据以纸质介质方式与委托方进行传递，则应执行相应的内部授权审批程序，对传递数据的内容、用途、量级，数据接收方（细化至法人机构数据安全负责人）情况、使用时长、数据是否收回（或由对方进行销毁）等情况进行说明与审批，有关记录留档备查；

(5) 金融业机构与承接数据委托处理的第三方均在我国境内时，数据传输不应路由到境外网络。

g) 金融业机构应保存委托处理过程记录与有关数据的处理情况，以留档备查。

7.4.10 公开披露

金融业机构在提供金融产品（或服务）是过程中，因国家法律法规、行业主管部门规章，以及金融产品（或服务）业务需要，需在金融机构官方渠道公开披露数据时，应采取控制措施，保护披露数据的真实性与完整性。

金融业机构数据公开披露具体要求如下：

a) 应依据国家法律法规与行业主管部门规章，在金融业机构官方渠道披露数据；

b) 数据公开披露前，应依据金融业机构有关制度要求，对拟披露数据进行审核与审批，具体要求如下：

1) 数据安全管理部门会同有关业务部门，对拟披露数据的国家与行业法律法规遵从性、业务需求、数据脱敏方案进行审核；

2) 业务部门对披露渠道、披露时间（永久或固定时间段）、拟公开数据的真实性，以及数据脱敏效果进行确认；
3) 依据机构有关程序执行数据公开披露审批程序，过程记录留档。

c) 应采取技术措施对金融业机构公开披露数据的真实性与完整性进行安全防护，具体要求如下：
1) 通过金融业机构官方网站披露数据时，应采取包括网页防篡改等技术措施，防范披露数据篡改风险；
2) 通过金融业机构客户端应用软件披露数据时，客户端应用软件应符合 JR/T 0092—2019 有关安全技术要求。

d) 不应公开披露除 1 级外其他数据；
e) 个人金融信息的公开披露应符合 JR/T 0171—2020 中 6.1.4.3 与 7.1.3.1 节要求；
f) 应准确记录和保存数据的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等。

7.4.11 数据跨境

金融业机构在提供金融产品（或服务）过程中，因业务需要，确需向境外机构提供在中华人民共和国境内运营中收集和产生的数据时，应实施严格的数据出境安全管理措施，依法依规开展有关数据出境活动，并采取相关安全控制措施，保证出境数据的安全。

金融业机构数据出境具体要求如下：

a) 应依据国家法律法规与行业主管部门规章，以及 GB/T BBBB-BBBB《金融数据跨境安全要求》标准要求，制定数据出境安全管理规定，对数据出境的全过程制定明确的管理规程，并依据 GB/T BBBB-BBBB 对包括数据脱敏、加密传输、完整性保护、安全审计、防篡改、数据删除等安全控制措施提出明确的技术要求；
b) 应制定出境数据清单，梳理包括出境数据的业务场景、接收机构、数据接收方国家（或地区）数据保护法律法规情况、出境数据类型、规模（条数与量级）等情况，并明确出境数据是否涉及个人金融信息以及 4 级数据；
c) 依据国家法律法规与行业主管部门规章与技术标准，开展数据出境安全评估，确保境外数据接收方数据安全保护能力达到国家、行业有关部门与金融机构的安全要求；
d) 应与境外数据接收方通过签订协议、现场核查等方式，要求境外机构为所获得的数据履行保密义务，并依据金融机构要求履行有关安全审计、数据删除、事件处置、案件协查等责任义务；
e) 个人金融信息出境活动，应符合 JR/T 0171-2020 中 7.1.3.1 节 d)款要求；
f) 不得向外机构提供 4 级数据。

7.5 数据交换

7.5.1 描述

数据交换是指金融业机构在机构内部以及与外部机构进行数据交换的过程，包括机构内部交换、外部共享、数据转让等活动。

7.5.2 内部交换

数据内部交换指数据在金融业机构内不同区域、不同部门间的流转的过程。数据内部交换具体要求如下：

a) 数据内部流转应依据金融机构内部数据交换有关规定执行，并满足以下要求：

1) 数据内部交换应遵循“合法正当、目的明确、授权同意、业务确需、最小够用”原则，在进行数据内部交换前，数据采集部门与数据使用部门应对数据交换的业务需求进行确认；
2) 数据内部交换应执行授权审计程序，对数据的使用目的、数据内容、使用时间，匿名化或加密措施、使用后数据的处理方式（销毁）进行审核，有关记录留档备查；
3) 数据内部交换应采取匿名化技术将明文数据进行匿名化处理，匿名化措施的部署，应尽可能靠近数据源头，如数据库视图、应用系统底层 API 接口等；
4) 若因业务确需，需明文进行数据流转时，应：
   (1) 执行高级别的数据使用授权审批程序，对明文数据的使用目的、数据内容、使用时间，匿名化或加密措施、使用后数据的处理方式（销毁）进行审核，有关记录留档备查；
   (2) 应对数据进行加密处理，并采取设置伪数据记录（行数据）、插入特征跟踪字段（列数据）、数字水印等 DLP 技术，降低数据被泄露、误用、滥用的风险；
   (3) 或使用假名化技术，将数据进行脱敏处理，同时采取设置伪数据记录（行数据）、插入特征跟踪字段（列数据）、数字水印等 DLP 技术。

b) 个人金融信息的明文内部交换，应开展专门合规性审查，确保交换的场景、用途、方式等不违背金融业机构提供的隐私政策，不超出个人金融信息主体的授权范围，数据安全保护强度不因数据内部交换而降低；
c) 数据使用后，有关部门应对使用后的数据进行安全处置，具体要求如下：
   1) 数据使用部门应对其获得的数据进行删除处理，数据安全管理部门应对删除结果进行确认；
   2) 数据使用后产生的数据以及原始数据的衍生数据，应由数据安全管理部门会同原始数据采集部门、数据使用部门一同，明确数据属主与安全保护责任部门；数据安全管理部门与该数据的安全责任部门一同，对新产生的数据及原始数据的衍生数据开展数据安全定级工作。
d) 2 级及以上数据跨不同安全域流转时，应满足以下要求：
   1) 采取匿名化技术将明文数据进行匿名化处理；在选择匿名化技术时，宜结合数据使用部门业务需要，选择被猜解（或碰撞）风险相对较低的匿名化技术；
   2) 匿名化措施的部署，应尽可能靠近数据源头，如数据库视图、应用系统底层 API 接口等；
   3) 若因业务确需，需明文进行数据流转时，应：
      (1) 执行高级别的数据使用授权审批程序，对明文数据的使用目的、数据内容、使用时间，匿名化或加密措施、使用后数据的处理方式（销毁）进行审核，有关记录留档备查；
      (2) 应对数据进行加密处理，并采取设置伪数据记录（行数据）、插入特征跟踪字段（列数据）、数字水印等 DLP 技术，降低数据被泄露、误用、滥用的风险；
      (3) 或使用假名化技术，将数据进行脱敏处理，同时采取设置伪数据记录（行数据）、插入特征跟踪字段（列数据）、数字水印等 DLP 技术；
      (4) 禁止批量明文数据的跨安全域流转。

7.5.3 外部共享

数据外部共享指金融业机构在经营过程中，自身采集（含生成）的数据分发共享至外部合作单位的过程。金融业机构按照国家法律法规与行业主管部门规章要求，向行业主管与监管部门等有关机构履行数据报送义务的情况，也属于数据外部共享范畴。除按照国家法律法规与行业主管部门规章要求，

向行业主管与监管部门等有关机构履行数据报送义务外，金融业机构原则上不应进行数据外部共享，因业务确需（如转接清算等）与外部机构共享数据时，应充分重视信息安全风险。金融业机构数据外部共享具体要求如下：

a) 数据共享行为不得超出 9.2 需求评审过程中确定的数据范围，若共享数据包含从企业客户采集的数据，其数据共享范围不得超出合同条款约定范围，若共享数据包含个人金融信息，则数据委托处理范围应符合 JR/T 0171—2020 中 6.1.4.2 与 7.1.3.1 节要求；
b) 应对数据共享行为进行数据安全评估（涉及个人金融信息的，应进行个人金融信息安全影响评估），并确保数据接收方具备足够的数据安全能力，且提供了足够的安全保护措施；
c) 金融业机构 4 级数据不应与外部机构进行共享；
d) 金融业机构应与数据接收方签订书面协议，协议中应明确约定数据共享的内容和用途、外部合作方应承担的数据保护义务，并在协议中明确外部合作机构不得将获取的数据转移至任何第三方；
e) 金融业机构应向数据主体告知共享数据的目的、数据接收方的类型，并以合同条款的方式事先征得数据主体同意；
f) 金融业机构应帮助数据主体了解数据接收方数据的存储、使用等情况，在国际法律法规与行业主管部门有关规定及与数据主体约定的范围内，数据主体行使数据控制权利，金融业机构应配合响应其请求；
g) 对共享的电子数据，应执行以下安全控制措施：
    1) 利用自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）进行数据共享时，应通过标识、鉴别密文等信息有效验证调用者的身份，并定期检查和评估自动化工具和数据传输信道的安全性和可靠性；
    2) 通过应用系统、接口等共享数据的，应通过数据加密、攻击防护和流量监控等手段，有效防范网络监听、接口滥用等网络攻击和违规行为；
    3) 共享数据涉及个人金融信息时，依据业务需求应采用去标识化（含加密技术）等方式进行脱敏处理；
    4) 共享数据涉及 2 级、3 级数据时，应对数据进行加密处理，并采取设置伪数据记录（行数据）、插入特征跟踪字段（列数据）、数字水印等 DLP 技术，降低数据被泄露、误用、滥用的风险；
    5) 若数据共享需求为市场或趋势分析等情况，应使用匿名化技术将明文数据进行匿名化处理；在选择匿名化技术时，宜结合委托处理业务需要，选择被猜解（或碰撞）风险相对较低的匿名化技术（包括但不限于 K-匿名）；若选择假名化技术，则应将其视同为明文数据，同时执行上述（4）款安全控制措施；
    6) 应共享的数据进行安全审计，若数据通过信息系统（包括 API、摆渡服务器）与外部合作方进行传递，则应在相应的控制节点（信息系统业务功能、API、服务器用户）设置安全审计功能，对数据的外发与回传进行审计；若数据以纸质介质方式与外部合作方进行传递，则应执行相应的内部授权审批程序，对传递数据的内容、用途、量级，数据接收方（细化至法人机构数据安全负责人）情况、使用时长、数据是否收回（或由对方进行销毁）等情况进行说明与审批，有关记录留档备查；
    7) 金融业机构与外部合作方均在我国境内时，数据传输不应路由到境外网络；
    8) 数据外部共享应配套建立应急响应机制，在（疑似）发生数据外部共享相关的信息泄露事件或违规违约行为时，应及时切断其接入，并将该行为视为安全事件，执行事件处置程序。

h) 金融业机构按照国家法律法规与行业主管部门规章要求，向行业主管与监管部门等有关机构履行数据报送义务时，应采取措施对报送数据接收方的真实性、报送数据的保密性、真实性与完整性进行确认，具体要求如下：
   1) 应依据国家法律法规与行业主管部门规章要求，针对不同部门的数据报送要求，明确不同归口数据报送工作的责任部门与岗位，识别数据报送的渠道（API、服务器摆渡、人员手工报送等）、报送内容、报送频次，并建立针对性的数据报送控制程序与操作规程；
   2) 应按照数据接收方的数据安全保护要求，针对不同的报送渠道配置相应的数据安全保护措施，以保障报送数据的保密性与完整性，措施包括但不限于：
      (1) API 认证；
      (2) 服务器认证；
      (3) 使用加密通道传输数据；
      (4) 3 级以上数据采取双方认可的加密方式进行文件级（或报文级）加密；
      (5) 人员手工传递电子数据时，应对电子数据以双方认可的方式进行加密处理。
   3) 数据报送前，应开展以下工作：
      (1) 对数据的接收方、接收渠道进行确认；
      (2) 对拟报送数据的真实性、完整性进行复核，有时效性要求的数据，应对拟报送数据的时效进行复核。
   4) 数据报送时，应按照数据接收方的数据安全保护要求，采取相应的安全控制措施，保障报送数据的保密性与完整性；
   5) 应对数据报送的过程进行记录，留档备查。

7.5.4 数据转让

数据转让指金融业机构将自身采集（含生成）的数据所有权移交至外部机构，并后续不再承担该数据的所有权利和义务的过程。

金融业机构数据转让具体要求如下：

a) 除国家法律法规与行业主管部门规定有明确要求的，金融业机构不应转让数据；
b) 因机构收购、兼并、重组等情况，金融业机构主体变更而发生数据转让时，具体要求如下：
   1) 金融业机构将其提供的金融产品或服务移交至其他金融业机构的情况，应使用逐一传达（或公告）的方式通知数据主体知晓；
   2) 承接其金融产品或服务的金融业机构，应对其承接运营的金融产品或服务继续履行数据安全保护责任；如变更其在收购、兼并重组过程中获取的数据使用目的，应重新获得数据主体的明示同意（或授权）；
   3) 对于机构破产且无承接方的情况，金融业机构应将其情况及时报送行业主管部门，将数据移交至行业主管部门指定的机构进行继续保存，或依据行业主管部门的要求，对数据进行销毁处理，并将处理结果使用逐一传达（或公告）的方式通知数据主体知晓。
c) 个人金融信息的公开披露应符合 JR/T 0171—2020 中 6.1.4.2 与 7.1.3.1 节要求。

7.6 数据删除

金融业机构在执行数据删除工作时，应满足以下要求：

a) 应依据国家法律法规与行业主管部门规章，针对不同类型的数据设定其数据保存期，对于多不同保存期数据的集合，其保存期限选择其最长时限为该数据集合的保存期；
b) 超过保存期限的数据，应执行数据删除操作；

c） 应采取技术手段，在金融产品和服务所涉及的系统中去除待删除的数据，使其不可被检索和访问；
d） 开发测试、数据分析等金融机构内部数据使用需求执行完毕后，应由数据使用部门依据金融机构数据删除与销毁有关规定，对其使用的有关数据进行删除或销毁处理，记录处理过程，并将处理结果及时反馈至数据安全管理部门，由其进行数据删除或销毁情况确认；
e） 3 级及以上数据应建立数据删除的有效性复核机制，定期检查能否通过业务前台与管理后台访问已被删除数据；
f） 个人金融信息主体要求删除个人金融信息时，金融业机构应依据国家法律法规、行业主管部门有关规定以及与个人金融信息主体的约定予以响应。

7.7 数据销毁

数据销毁是指金融业机构在停止业务服务、数据使用以及存储空间释放再分配等场景下，对数据库、服务器和终端中的剩余数据以及硬件存储介质等采用数据擦除或者物理销毁的方式确保数据无法复原的过程。其中，数据擦除是指使用预先定义的无意义、无规律的信息多次反复写入存储介质的存储数据区域；物理销毁是指采用消磁设备、粉碎工具等设备以物理方式使存储介质彻底失效。在开展数据销毁活动过程中，存在因数据未彻底删除而导致的数据泄露风险，金融机构应采取安全控措施确保数据被安全有效的销毁。

数据销毁具体要求如下：

a） 应制定数据存储介质销毁操作规程，明确数据存储介质销毁场景、销毁技术措施，以及销毁过程的安全管理要求，并对已共享或者已被机构内部部门使用的数据提出有针对性的数据存储介质销毁管控规程；
b） 存储数据的介质如不再使用，应采用不可恢复的方式（如消磁、焚烧、粉碎等）对介质进行销毁处理；
c） 存储介质如还需继续使用，不应只采用删除索引、删除文件系统的方式进行信息销毁，应通过多次覆写等方式安全地擦除数据，确保介质中的数据不可再被恢复或者以其他形式加以利用，具体措施包括但不限于：
    1） 采用数据擦除方式销毁数据时，应明确定义数据填充方式与擦除次数（如全零、全一以及随机零一最少填写 7 次），并保证数据擦除所填充的字符完全覆盖存储数据区域；
    2） 数据擦除后的存储介质应通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据删除结果；
    3） 针对数据擦除后擦除失败的存储介质，应进一步采用物理方式进行销毁。
d） 应明确数据销毁效果评估机制，定期对数据销毁效果进行抽样认定，通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据删除结果；
e） 应对数据销毁全过程进行记录，并定期对数据销毁记录进行检查和审计；
f） 3 级及以上数据存储介质不应移作他用，销毁时应采用物理方式对其进行销毁处理；
g） 4 级数据存储介质的销毁应由参照保密管理规定，由相应的服务机构进行专门处理，并由金融业机构相应岗位人员对其进行全程监督；
h） 云环境下有关数据销毁应依据 JR/T 0167—2018 的 9.6 章节执行。

8 数据安全组织保障

8.1 组织结构

金融业机构应建立数据安全管理专门的组织体系，以保障数据生命周期安全防护要求的有效落实。数据安全管理体系架构如图2所示，应进一步明确相关组织架构和岗位设置。

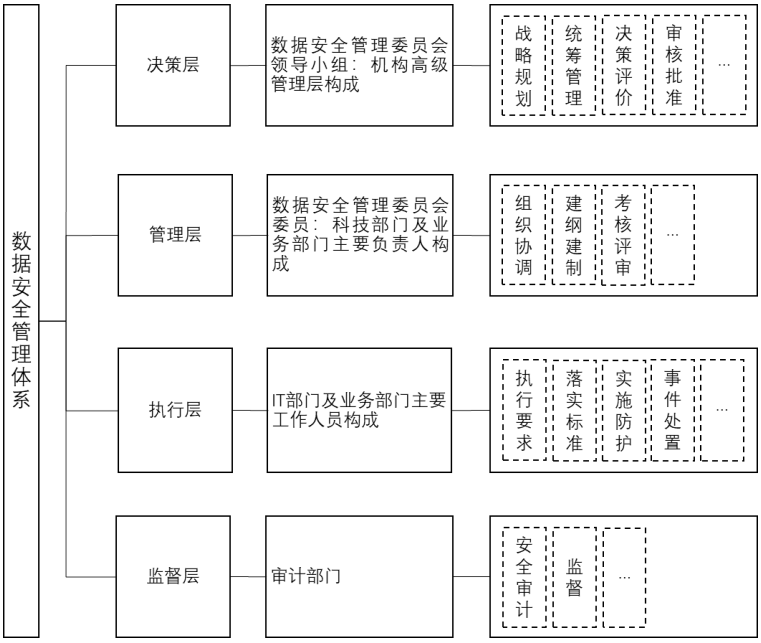

图 2 数据安全组织体系架构示意图

数据安全管理组织建设，应至少满足如下要求：

a) 应重视和加强顶层设计，建立覆盖决策、管理、执行、监督的数据安全管理组织结构，通过数据安全管理委员会的形式对数据安全工作进行统筹管理和实施，确保机构内部数据安全自顶向下管理的一致性；

b) 应设立由机构高级管理层组成的数据安全管理委员会领导小组，总体负责数据安全工作的统筹组织、指导推进和协调落实，明确数据安全管理部门，协调机构内部数据安全管理资源调配；

c) 委员会成员应至少包含主要部门主要负责人，负责数据安全相关工作的实施、相关政策和制度的制定评审工作，保障数据安全管理工作所需资源，并设立数据安全管理专职岗位，负责机构日常数据安全管理工作，具体如下：

   1) 制定、发布和维护本机构数据安全管理制度、规程与细则；
   2) 组织开展本机构数据分级工作，识别并维护数据资产清单；
   3) 制定、签发、实施、定期更新隐私政策和相关规程；
   4) 监督本机构内部，以及本机构与外部合作方数据安全管理情况；
   5) 在金融产品或服务上线发布前组织开展数据安全评估，避免未知（如与产品或服务功能及隐私政策不符）的数据收集、使用、共享等行为；
   6) 公布投诉、举报方式等信息，并及时受理数据安全相关投诉和举报。

注：主要部门应至少包括数据安全管理、信息科技（若数据安全管理与网络安全管理为不同部门时）、业务、法务、审计相关部门。

d) 业务部门、信息系统建设部门、信息系统运维部门应设立数据安全岗位，作为数据安全执行层，该岗位应履行以下工作职责：

   1) 根据机构数据安全相关策略和规程，落实本部门数据安全控制措施；
   2) 经授权审批程序后，为获得授权的各相关方分配数据权限；

3) 对本部门数据脱敏、对外提供等关键活动的数据安全控制有效性进行确认；
4) 配合执行数据相关安全评估及技术检测等工作；
5) 制定本部门数据安全应急预案，并定期开展数据安全应急演练，依据演练结果，修订数据安全应急预案；
6) 处置本部门有关数据安全事件；
7) 依据数据安全管理有关制度规范，记录本部门数据活动日志。

e) 应明确安全审计相关岗位，作为监督层，该岗位应履行以下工作职责：
1) 根据本机构数据相关业务实际情况，确定相应审计策略，包括但不限于审计周期、审计方式、审计形式等内容；
2) 监督数据安全政策、方针的执行；
3) 开展数据安全内部审计和分析，发现并反馈问题和风险，并对机构后续相关整改工作进行监督；
4) 配合开展外部审计相关的组织和协调工作。

8.2 制度体系

金融业机构应建立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职责，规范工作流程。制度体系的管理范畴应涵盖本机构、第三方机构（含外包服务机构与外部合作机构），并确保相关制度发布并传达给本机构员工及外部合作方。相关制度应至少包括数据安全政策、方针、制度、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案。

数据安全管理制度体系具体要求如下：

a) 应依据国家法律法规、行业制度规范，以及有关技术标准，制定本机构数据安全总体政策、方针，明确安全方针、安全目标和安全原则；
b) 应依据国家法律法规、行业制度规范，以及有关技术标准，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，该清单中应对数据级别进行识别和标注；
c) 应依据国家法律法规、行业制度规范，以及有关技术标准，制定数据安全管理制度及实施细则，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) 应制定本机构数据安全管理规定，提出本机构数据安全生命周期保护工作的总体策略；
2) 应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保护要求；
4) 建立数据脱敏（如屏蔽、去标识、匿名化等）管理规范和制度，应明确不同敏感级别数据脱敏规则、脱敏方法和脱敏数据的使用限制；
5) 建立第三方机构管理制度，并应至少满足本标准 8.4 所述要求；
6) 建立数据供方安全管理要求，对数据的来源的合法合规情况，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) 应建立数据采集、传输、存储、使用、汇聚融合、交换共享与转让、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) 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制度；
10) 建立安全事件应急响应机制，明确重大数据安全事件的处置流程及应对方法；
11) 建议数据安全事件管理与处置规程。

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。

8.3 人员管理

金融业机构应对数据安全管理相关人员进行管理，具体要求如下：

a) 在人员录用及日常管理方面，应满足以下要求：
   1) 录用员工前，应进行必要的背景调查，并与所有可访问机构 3 级以上数据的员工签署保密协议，或在劳动合同中设置保密条款；
   2) 应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：
      (1) 数据安全管理岗位、审计岗位；
      (2) 业务操作与信息技术操作特权账户所有者；
      (3) 数据各级权限审批岗位；
      (4) 重要（或关键）数据处理、交换岗位；
      (5) 信息系统开发、测试岗位人员；
      (6) 因业务需要，需高频和/或大批量接触（如采集、查询等操作过程）3 级及以上数据的岗位人员（如柜面、客户服务岗位等）；
      (7) 以及其他金融业机构识别的数据安全关键岗位。
   3) 在发生人员调离岗位时，应立即完成相关人员的数据的访问、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，应明确其继续履行有关信息的保密义务要求；
   4) 与员工终止劳动合同时，应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；
   5) 应建立外来人员管理制度,对允许被外部人员访问的系统和网络资源建立存取控制机制、认证机制，列明所有用户名单及其权限，加强对外来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培训计划，并至少满足以下要求：
   1) 应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法律法规、行业制度规范、技术标准、金融业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) 每年至少对数据安全管理专职与关键岗位人员进行一次数据安全专项培训；
   3) 应定期（至少每年一次）或在隐私政策发生重大变化时，对数据安全关键岗位上的相关人员开展专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程；
c) 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，并应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，签署保密协议，并定期对这些人员行为进行安全审查；
d) 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，并实行权利分离；必要时数据安全关键岗位（如特权账户所有者、关键数据处理与交换岗位等）应设立双人双岗，强化数据安全管理；
e) 系统开发人员、系统测试人员与运维人员之间不应相互兼岗。

8.4 第三方机构管理

金融业机构应对参与机构数据全生命周期过程中的第三方机构（包含外包服务机构与外部合作机构）进行管理，严控第三方数据安全风险，确保不因第三方机构合作或第三方的应用接入而危害机构数据安全。

第三方机构安全管理具体要求如下：

a) 建立第三方机构（包含外包服务机构与外部合作机构）管理制度，包括但不限于：
   1) 应对数据生命周期过程中相关的第三方机构进行审查与评估，评估其数据安全保护能力是否达到国家、行业主管部门与金融业机构的要求；
   2) 应通过协议或合同的方式，对第三方机构的数据使用行为进行约束，包括：
      (1) 不留存 3 级及以上数据；若因清分清算、差错处理等业务需要，确需留存 3 级及以上数（如支付账号）等信息，金融业机构应明确其保密义务与保密责任，并应根据安全要求落实安全控制措施，并将有关资料留档备查；
      (2) 明确要求第三方机构不得对金融业机构委托其加工处理的数据进行未经金融机构书面授权的存储、使用和共享等行为。
   3) 对可能访问金融业机构数据的第三方机构及其人员，金融业机构应要求第三方机构向有关人员传达金融业机构数据安全要求，与其签署保密协议，并对协议履行情况进行监督；
   4) 不应将存储 3 级及以上数据的数据库交由外部合作机构运维；
   5) 应定期对第三方机构的数据安全保护措施落实情况进行确认，确认的方式包括但不限于外部信息安全评估、现场检查等。
   6) 第三方机构在处理数据过程中发生数据安全事件（如数据泄露、被未经授权的访问或变更、损毁等），应及时依据双方约定的方式向金融业机构反馈；
   7) 国家法律法规与行业主管部门另有规定的，按照相关要求执行。
b) 当金融业机构在其产品或服务中接入具备数据处理功能的第三方产品或服务时，应对第三方的接入和涉及的产品和服务进行专门的数据安全管理，确保不因第三方的应用接入而危害机构数据安全，具体要求如下：
   1) 应对第三方产品或服务的接入进行安全评估，根据评估的结果确定是否接入该产品或服务，对于确定接入的产品或服务，应根据风险评估的结果实施适当的控制措施；
   2) 应明确第三方产品或服务接入的基本条件，要求第三方对接入的产品和服务的数据安全管理满足本框架的要求，并对其进行评价；
   3) 应与第三方产品或服务提供方签订合同或协议，约定双方的数据安全责任和义务，明确数据接收方的数据安全保护能力要求，以及履行的法律责任和合同的义务；
   4) 应对第三方嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的功能和安全性进行验证确认，如果第三方产品和服务发生变更，应重新进行验证确认；
   5) 应对第三方接入产品和服务的数据处理活动进行必要的监视，并保留记录，确保其满足合同或协议要求，发现第三方产品或服务没有落实安全管理要求和责任的，及时督促其整改，必要时停止接入；第三方接入产品和服务的数据处理过程中发现对金融机构个人金融信息的处理超出约定行为，应及时切断其接入，并将该行为视为安全事件，执行事件处置程序；
   6) 向用户直接提供服务的第三方产品或服务接入后应在用户界面清晰标识产品或服务的提供方。
c) 与第三方机构解除合作关系时，依据金融业机构的要求不再以任何方式保存从金融业机构获取的数据及相关衍生数据。

9 数据安全工程要求

9.1 描述

金融业机构在信息系统建设、产品和服务研发等过程中，应在需求分析、系统设计、系统开发、安全测试、安全部署、变更控制等信息系统建设的各个阶段，设立数据安全控制节点，建立由各有关部门（或岗位人员）参与的数据安全联席审核机制，明确并落实第7节数据生命周期安全要求。

9.2 需求分析

需求分析阶段，金融业机构信息系统建设需求提出部门、数据安全管理部门、网络安全管理部门（若数据安全管理与网络安全管理为不同部门时）、信息系统研发部门等关联部门应共同分析并确认信息系统建设所涉及的数据安全需求。

信息系统数据安全需求分析具体要求如下：

a) 信息系统建设需求提出部门负责依据金融产品（或服务）需求，制定信息系统建设数据安全需求文件，该文件应至少包含以下内容：
   1) 从金融产品（或服务）流程及规则、信息系统建设或改造、合同采购和第三方管理等方面提出数据保护需求；
   2) 说明数据的收集来源、合作方、数据提供方，以及是否涉及数据的转移、共享和对外提供；
   3) 识别产品中涉及处理个人金融信息的场景；
   4) 对拟进行的个人金融信息处理的说明（包括但不限于收集个人金融信息的范围、目的、规模、数量、数据等级、与其他数据的关联性等），并对拟进行的个人金融信息处理活动与个人金融信息处理目的之间的必要性（金融产品或服务业务开展之必要性、法律法规与行业规范遵从之必要性等）进行说明。
b) 数据安全管理部门对信息系统建设数据安全需求文件进行梳理，明确金融产品（或服务）需要满足的数据安全保护要求，需求文件梳理的输入至少应包括：
   1) 拟提供金融产品（或服务）国家（或地区）的数据安全有关政策、法律法规、国家和行业标准要求等；
   2) 数据保护应遵循的基本原则、行业认知及公众期待；
   3) 机构内部数据安全原则、规范和操作细则等；
   4) 金融产品（或服务）之前版本的遗留数据安全问题、外部风险来源等，以及已有数据安全事件的消减措施。
c) 数据安全管理部门会同有关部门（或岗位人员）对信息系统建设数据安全需求进行分析与评估，若评估后数据安全风险不可接受，则由信息系统建设需求提出部门调整需求文件后，再进行二次评估，需求分析与评估包括但不限于：
   1) 拟处理的数据的需求和目的；
   2) 拟处理的数据的类型和预期数量，以及数据收集、使用的方式和范围；
   3) 拟处理的数据的合法合规遵从性、业务确需与最小够用原则遵从性等；
   4) 梳理明确信息系统建设需求，以及在数据生命周期过程中可能涉及的其他相关信息系统；
   5) 拟处理的数据可能涉及的参与者及相关方，包括第三方的关系，若涉及数据供方，则应对数据供方的合法性、准确性与真实性进行评价；
   6) 合同条款、隐私政策符合性分析，明确是否需要对合同条款、隐私政策进行更新，以及更新的内容；

7） 金融产品（或服务）预期的业务处理流程、数据生命周期所涉及的过程；
8） 明确数据生命周期各个阶段的数据安全需求与安全功能要求，比如收集个人金融信息时需要用户授权同意、数据展示屏蔽等。

d） 针对待建信息系统所承载业务，应分析确认需要向合作方提供的主要数据范围、类型和级别，在满足国家法律法规及行业监管部门有关规定的基础上，采取必要的安全管控措施，包括：
1） 商业合作方：合作双方协商并通过商业合同或合作协议等具备法律效力的书面文件，明确规范双方互相提供的主要数据范围、业务类型、安全级别、技术接口、通信协议、保密规定、违约条款和安全管控措施等内容，合作双方严格按照合同规定履行各自的权利、责任和义务；
2） 行业组织或市场间机构：应按照行业组织或市场间机构发布的业务和技术规范，由合作双方通过商业合同或合作协议等具备法律效力的书面文件，明确规范双方互相提供的主要数据范围、业务类型、安全级别、保密规定、违约条款等内容，合作双方严格按照合同规定履行各自的权利、责任和义务；
3） 国家监管及有权机构：应严格按照行业监管机构或公检法等国家有权机关要求，提供必需的数据。

e） 对信息系统建设数据安全需求文件，需求分析及评估的过程应当保存记录。

9.3 系统设计

系统设计阶段，金融业机构系统研发部门负责根据信息系统需求分析书，组织有关部门（或岗位人员）设计信息系统建设方案，数据安全管理部门负责参与方案设计并进行数据安全评估。

信息系统数据安全系统设计具体要求如下：

a） 分析信息系统中涉及的数据信息生命周期阶段或数据理活动，明确各阶段（或处理活动）中的数据安全保护需求，为其设计对应的功能实现方案；在概要设计阶段应明确信息系统的数据保护策略，详细设计阶段应明确信息系统所使用的信息安全技术与数据安全功能；

b） 新系统数据安全方案设计步骤主要包括：
1） 对信息系统架构、业务过程、数据元素和数据流进行设计；
2） 对数据保护的各项功能要求进行分解，分解到信息系统架构设计的各个模块中；
3） 对数据保护的各项功能的实现选择技术路线，设计数据安全功能（如明示同意、展示屏蔽等）、APP 与 WEB 方式实现的隐私政策等；
4） 应分析业务功能、网络架构、系统部署、应用接口等系统运行环境对数据安全的影响，对数据网络安全保护功能（如身份鉴别、访问控制、数据加密、密钥管理、安全审计等）进行设计；
5） 应依据业务流程和交易规则，设计信息系统各类业务用户对于数据的控制功能（如业务角色的各类数据访问权限和规则、是否允许批量查询、是否允许数据批量导出后打印），针对数据未经授权的访问、泄露、篡改等风险，设计业务控制与安全审计功能，如：
(1) 不可执行无工单请求的个人金融信息查询操作；
(2) 查询未脱敏信息的只读与不可导出功能控制；
(3) 导出或打印 3 级数据的授权审批功能；
(4) 大数据分析的底层强制脱敏功能。
6） 设计信息系统配置部署方案。

c） 选择第三方 SDK/插件时，应在选择的 SDK/插件能满足相应功能和性能需求的基础上，考虑以下安全原则：

1) 合理性原则：涉及第三方 SDK 申请及使用的所有权限，均应且只应满足宿主产品所需要的功能；
2) 必要性原则：超出宿主产品所使用的功能，即使功能合理，也应当进行裁剪；
3) 辅助性原则：如果有替代方案可通过不采集个人信息或不使用敏感权限的前提下也能够实现所需功能，应当采取替代方案；
4) 最小化原则：在满足以上三个原则的情况下，针对宿主产品无使用场景，需要单独为第三方 SDK 申请的隐私敏感权限，应进行严格控制。

d) 数据安全管理部门应对信息系统建设方案进行数据安全评估，评估内容包括但不限于：
1) 根据金融产品（或服务）涉及的数据范围及类别、相关的政策法规及标准要求、各实现方案要求等，设定数据检查项，并对照检查项校验分析金融产品（或服务）的信息系统建设方案是否满足检查项要求；
2) 会同网络安全管理部门（若数据安全管理与网络安全管理为不同部门时）、信息系统运维部门对有关网络安全控制与信息系统运维需求设计进行符合性评价。

e) 有关设计讨论的过程、设计方案、设计评估结论等文档应留档保存。

9.4 系统开发

系统开发阶段主要工作为落实信息系统设计中的数据安全设计要求，以保证数据安全策略实现的阶段。本阶段主要由信息系统研发部门负责根据系统数据安全设计方案，以及有关概要设计、详细设计等文档，进行系统开发，实现数据安全策略，并形成开发过程文档。

信息系统数据安全系统开发具体要求如下：

a) 应落实信息系统中的数据安全需求与设计，并在每个开发的迭代周期，检查数据安全功能实现的效果；
b) 内部自研的数据脱敏工具包应支持研发人员调用实现不同场景的个人信息脱敏处理；
c) 应执行安全的编码策略，包括但不限于：
1) 保证开发环境的安全性，使用官方渠道下载的开发工具；
2) 避免将敏感数据直接嵌入到程序，如加密密钥、后端服务器敏感信息等；
3) 应优化代码逻辑，剔除应用中的无效编码；
4) 设立统一的日志管理接口，避免在日志中记录敏感信息；
5) 控制用户输入数据的类型、长度，进行恶意代码过滤等；
6) 对于接收到的外部数据、加载的外部文件，进行完整、有效性检验；
7) 依据安全编码规范进行安全开发；
8) 采用测试工具完成代码安全基准测试。

d) 系统开发阶段，应考虑第三方 SDK/代码安全，包括但不限于：
1) 实现过程中充分考虑数据采集、处理、传输、存储、删除是否符合预期，包括嵌入第三方 SDK/插件或相关组件等涉及间接收集或处理个人信息的场景；
2) 系统 API 使用安全，宜使用官方推荐版本的 API 接口，不使用系统废弃的 API；对关键操作身份校验和权限检查，避免遗漏安全限制操作；
3) 对第三方 SDK/插件进行安全评估。

9.5 安全测试

测试审核阶段的数据重在对数据保护举措的核实。在此阶段，需要对前阶段已定义的数据保护各项要求的执行情况进行客观测试与评价，反映预期个人信息设计要求。本阶段主要由信息系统研发部门对数据安全控制措施的信息系统应用实现情况进行测试，信息系统建设需求提出部门参与本阶段工

作，与信息系统研发部门一同，对业务操作层面的数据安全控制措施应用情况进行验证测试。数据安全管理部门对测试报告中数据安全的合规执行情况进行确认。

信息系统数据安全安全测试具体要求如下：

a) 信息系统研发部门测试团队应建立数据安全测试用例，对系统设计开发文档、系统数据安全需求说明书及数据安全评估过程文档的内容进行验证及测试，并形成系统数据安全测试报告。包括但不限于：
   1) 创建并维护数据安全安全测试用例，包括但不限于：
      (1) 数据安全测试用例应覆盖数据安全全生命周期的安全防护控制措施，并应能够覆盖信息系统数据安全需求、设计方案等系统特性数据安全控制措施与数据安全功能；
      (2) 创建并维护个人金融信息隐私保护测试用例，测试用例应覆盖隐私保护有关功能与安全控制措施；
      (3) 应依据数据安全评估报告以及信息系统各阶段迭代过程中数据安全事件改进措施，设计并维护测试用例。
   2) 依据测试计划开展数据安全测试测试，将测试过程与测试结果形成记录，包括但不限于：
      (1) 依据测试用例开展数据安全全生命周安全功能测试，对信息系统的数据安全功能进行验证，确保系统功能实现符合代码开发要求与系统设计要求，不存在逻辑错误与安全功能漏洞；
      (2) 依据测试用例开展个人金融信息隐私保护功能测试，对隐私保护系统功能进行验证，确保系统隐私保护功能实现符合代码开发要求与系统设计要求，确保个人金融信息采集、使用等过程有关明示同意、展示屏蔽、数据脱敏等功能实现符合有关要求；
      (3) 使用静态及动态方式对系统内外部接口、第三方插件（含 SDK）集成情况进行数据安全专项测试，对外部接口数据交互情况进行测试，涉及集成第三方插件进行数据采集、对外提供等重点环节，应进行动态调试与监控（时长不小于 24 小时）确保数据采集、对外提供方式与内容不存在系统功能设计外的任何请求；
      (4) 依据机构网络安全要求，执行有关网络安全功能与专项安全测试。

b) 信息系统建设需求提出部门应配合信息系统研发部门测试团队完成业务操作层面的数据安全控制措施应用情况测试，依据测试用例，宜使用去标识化后的生产数据对业务操作层面的数据安全保护功能进行测试，包括但不限于：
   1) 业务用户角色设计与访问控制功能的有效性验证，确保有关访问控制策略不会被绕过；
   2) 业务用户有关数据使用申请、查询、使用、归档、销毁等阶段中数据安全功能的有效性验证，确保不存在因逻辑漏洞、编码缺陷等问题导致的数据被未经授权的查看和变更；
   3) 业务用户有关数据使用过程的操作审计功能有效性进行验证。

c) 数据安全管理部门对测试报告中数据安全的合规执行情况进行确认，并对个人金融信息隐私保护测试情况进行审核；

d) 在安全测试阶段，信息系统建设需求提出部门应会同信息系统研发部门对测试中的不符合项进行说明或整改。包括但不限于：
   1) 测试中发现数据安全问题，信息系统研发部门测试团队应进行记录，涉及系统设计需求相关应及时反馈信息系统建设需求提出部门；若发现有高安全等级数据安全缺陷，应及时反馈数据安全管理部门与网络安全管理部门（若数据安全管理与网络安全管理为不同部门时），对安全缺陷进行分析、评估风险，制定加固方案与整改措施；
   2) 在测试阶段，安全技术团队和业务人员等相关方进行评审，在整改后的审核环节重点评估整改方案的有效性，以及整改方案是否会带来新的数据安全风险。

e) 安全测试与整改过程应进行记录，有关测试报告、评审意见应留档保存。

9.6 发布部署

发布部署阶段指信息系统研发部门项目组交付信息系统版本，并将系统的交付版本部署配置到生产环境的过程。发布部署参与方主要包括信息系统研发部门、信息系统建设需求提出部门、数据安全管理部门、信息系统运维部门，分别负责信息系统版本的发布与交付、信息系统需求确认、信息系统上线数据安全评审与个人信息安全影响评估报告签发、信息系统上线部署等工作。

信息系统数据安全发布部署具体要求如下：

a) 发布准备阶段数据安全要求如下：
   1) 对于业务连续性要求较高的数据安全功能与安全控制措施,应优先采用灰度发布的方式，对数据安全功能与控制措施进行验证，灰度发布方式包括但不限于：
      (1) 准生产或演练环境中使用脱敏后的生产数据进行功能验证；
      (2) 小范围在部分用户中上线发布新功能，测试可能对业务的实际影响。
   2) 待灰度发布验证通过后，依据业务方策略进行扩展发布；
   3) 信息系统研发部门项目组应证明信息系统已符合数据安全要求,方可进入系统发布阶段。
b) 发布评审阶段数据安全要求如下：
   1) 信息系统版本发布前，应由信息系统建设需求提出部门内部评审，审视版本发布质量达标情况，检查各项活动执行情况是否达到质量要求；
   2) 发布前应对数据安全与个人金融信息合规措施进行复审，确保有关安全功能与控制措施已符合系统发布要求，评审内容包括但不限于：
      (1) 上线发布前已通过完成网络安全测试，测试结果无未修改的高安全等级问题，有关风险可接受的安全问题，已制定风险跟踪方案或计划；
      (2) 上线发布前是否完成数据安全测试，测试结果无未修改的高安全等级问题，有关风险可接受的安全问题，已制定风险跟踪方案或计划；
      (3) 上线发布前是否进行个人金融信息合规评审。
c) 个人金融信息影响评估阶段数据安全要求如下：
   1) 若在信息系统版本上线前开展过个人金融信息安全影响评估，在系统版本发布前应由信息系统建设需求提出部门及数据安全管理部门，会同有关岗位人员（如法务团队）评审并正式签发个人信息安全影响评估报告；
   2) 个人金融信息安全影响评估报告应明确写明评估结果，结果通常为：通过、通过但有异常、需上报问题。
d) 安全部署阶段数据安全要求如下：
   1) 明确数据安全保护相关的信息系统环境配置规范、系统上线验收标准；
   2) 由信息系统运维部门将系统版本部署到相应环境，并由验收团队根据产品的需求分析、方案设计、合规要求等对产品、环境配置等进行验收；
   3) 完成信息系统交付的版本在生产网环境的部署。
e) 发布部署过程应进行记录，有关数据安全审批意见、个人金融信息安全影响评估报告、发布过程记录应留档保存。

9.7 变更控制

变更控制是指系统上线后对系统进行修正、改造、升级的过程，变更评审需区分数据变更、数据结构变更、以及程序变更三个类型。

信息系统数据安全变更控制具体要求如下：

a) 应对数据安全变更场景与业务需求进行识别，对包括数据采集、数据外部供方的变化、数据

使用方式的变化、数据汇聚融合、数据对外提供、脱敏机制变化等重要环节，建立数据变更控制程序，对数据安全功能与安全控制措施进行评审；

b) 数据结构变更若涉及表结构的增删改，应对以下内容进行评审：
   1) 是否引入新的数据接口，已有接口是否会扩大数据暴露的范围；
   2) 对外接口涉及敏感信息时是否有相应授权；
   3) 数据结构的变化是否对原有数据脱敏、加密等控制措施造成影响；
   4) 新增的敏感数据是否已经做好相应的安全防护；
c) 系统功能（或程序）变更涉及应用系统功能模块新增或已有系统功能模块升级改造的情况，应对以下内容进行评审：
   1) 如新增系统功能模块，应对其应用逻辑层面的安全策略、规则和技术、数据安全和技术安全设计策略是否合理进行评审；
   2) 如在已有系统功能模块架构升级时，应对已有架构调整对数据保密性、完整性、可用性是否有影响，系统架构调整是否导致数据安全防护等级提升，架构调整是否影响已有授权关系等内容进行评审。

10 信息系统运维保障

10.1 描述

信息系统运维是指通过对信息系统的网络、服务器及服务等进行运营和维护，保障信息系统及其所承载服务正常运行并及时发现风险，确保系统及服务在成本、稳定性、连续性、效率等方面达成一致可接受的状态。

10.2 边界管控

边界管控应满足以下安全要求：

a) 应在内网边界部署防火墙，按照“最小权限”原则控制外部机构的访问权限；
b) 互联网区和外联接入区为不可控区域，应在边界进行足够强度的安全防控措施；
c) 内部可控区域应与不可控区域进行隔离，在不可控区域和可控区域间应根据应用需求和数据传输需要逐一开通访问关系，默认为禁止访问；
d) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间应采取可靠的技术隔离手段；
e) 设备接入和开通数据传输接口应严格落实安全生产相关要求，并应制定接入生产网络和开通数据传输接口相关审批流程；
f) 应保证跨越边界数据流通过边界设备提供的受控接口进行通信；
g) 应能对非授权设备私自连接到内部网络，以及内部网络私自连接到外部网络的行为进行检查，准确定位接入点，并对其进行有效阻断；
h) 机构建立互联网 WLAN 时，接入终端应经过审批授权，采取无线网络终端设备准入控制措施，防止终端通过 WLAN 非法接入内部网络，并应采取技术手段防止操作系统管理权限被非法破解的终端设备接入内网 WLAN；
i) 终端通过互联网接入内网时，应采取前置机等方式在边界网络区域落地，实现技术隔离，避免直接透传至内部网络。

10.3 访问控制

10.3.1 访问控制策略设计

访问控制策略应满足以下安全要求：

a) 应依据数据的不同类型与安全级别设计不同的访问控制策略：
   1) 应依据“业务必需、最小权限、职责分离”的原则，设计数据库系统与文件系统的用户鉴别和访问控制策略，并对各类系统用户的设计其工作必需的最小访问权限；
   2) 应依据“知所必需、最小权限、职责分离”的原则，设计业务系统用户对系统业务功能与相应系统业务数据的访问控制策略，并对各类业务系统用户的访问控制实现方式和具体授权机制进行明确说明；
   3) 对数据库系统、存储系统、文件管理系统与存储介质管理有关管理员用户，应建立管理员身份标识与鉴别机制，并对其防控权限与操作规程进行详细说明；
b) 应建立面向数据应用的安全控制机制，包括访问控制时效的管理和验证，以及应用接入数据存储的合法性和安全性取证机制，宜建立基于用户行为或设备行为的数据存储安全监测与控制机制。

10.3.2 物理环境访问控制

放置数据存储系统与存储介质的物理环境应布置以下访问控制机制：

a) 金融机构数据存储系统应部署于机构数据中心高安全等级区域，存储系统服务器与带库等设备机房出入口应部署措施控制、鉴别和记录进入的人员；
b) 第三方人员访问存储系统服务器与带库区域应执行严格的授权审批程序，由金融机构人员全程陪同，并限制和监控其活动范围；
c) 对包括备份介质在内的存储介质的出入库应采取措施进行出入库控制，并由金融机构内部指定岗位人员完成，未经授权，任何存储介质不得带离磁带库房。

10.3.3 信息系统与介质访问控制

访问金融数据的业务应用系统应依据以下要求部署系统访问控制机制：

a) 用户角色的定义和权限设计应遵循以下原则：
   1) 参考业务职能，确定系统中需设置的各类用户角色（如操作人员、管理人员、审计人员等）和权限；
   2) 用户角色定义和权限设计能够体现职责分离的安全制约原则，如经办人员和审计人员权限分离；
   3) 应严格限制系统中缺省用户的权限。
b) 用户角色的访问范围和方式要求：
   1) 应控制用户对业务功能能够达到的访问范围，如功能菜单、业务文件、数据库表、表中的业务数据字段和其他资源；
   2) 控制用户对业务数据能够执行的访问方式，如读、写、删除、创建等。
c) 系统应具备登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

10.3.4 数据存储系统的访问控制

数据存储系统（包括文件系统）应依据以下要求设计存储介质的访问控制机制:

a) 存储系统应设计访问控制策略，并实现访问控制，对访问对象的访问范围和操作权限不超出预定义的范围，且满足最小授权原则；

b） 存储系统访问控制机制应对业务面和管理面各自可访问的资源策略进行配置，并对业务面和管理面的相互访问进行隔离；
c） 存储 3 级及以上数据的系统应采用多因素身份认证技术对用户进行身份鉴别；
d） 应使用存储访问控制模块部署数据用户身份标识与鉴别策略、数据访问控制策略、数据扩容及复制策略，并执行相关安全控制措施；
e） 应对访问存储业务的应用进行鉴别，对应用进行唯一标识，并将标识和与其相关的所有可审计事件相关联。鉴别信息不应明文存储，且鉴别数据不应被未授权查阅和篡改。不应存在可绕过鉴别机制的访问方式。

10.4 安全监测

10.4.1 数据溯源

金融业机构宜对数据生命周期过程中的数据查询、修改、删除等环节的相关操作进行跟踪记录，确保数据相关操作行为可追溯，并应至少满足以下要求：

a） 应制定数据溯源的策略和机制，明确溯源数据的安全存储、分析使用等管理制度；
b） 应标识外部数据的合法来源；
c） 宜建立数据资产地图，按需对特定数据对象进行标记和跟踪，构建和维护数据血缘关系；
d） 应对关键溯源数据进行备份，并采取技术手段对溯源数据进行安全保护；
e） 应采取技术访问控制、加密等技术措施保证溯源数据的安全性、完整性和保密性；
f） 应记录数据操作过程，出现数据泄露事件后可进行溯源；
g） 宜构建数据溯源的安全模型，增强数据操作的可追溯性；

10.4.2 流量分析

金融业机构流量分析应参考以下要求：

a） 宜采取流量分析技术对数据采集、数据交换、处理等关键节点进行监测；
b） 宜对比分析异常情况，如不安全的采集设备与采集内容、非授权时段访问敏感数据、多次尝试、批量下载等及时发现风险问题并进行处置；
c） 宜对比分析流量变化和规律，形成总结报告，并对安全防护措施进行针对性调整；
d） 应对互联网出口流量进行实时检测，发现流量异常、未经授权等行为并及时处置。

10.4.3 异常行为检测

金融业机构应建立日常数据泄露监控机制，宜充分利用大数据技术，主动预防、发现和终止数据泄露行为，有效防范和化解风险，异常行为检测至少应包含以下内容：

a） 应建立异常行为检测指标，对异常行为进行识别、跟踪和监控；
b） 宜采取措施检测数据传输过程，记录并阻断数据未经授权或高风险的数据下载和传输等行为，防止数据泄露；
c） 应采取措施检测用户上网行为，防止未经授权将数据传输或存储到互联网上；
d） 应采取措施检测用户终端，防止未经授权的设备接入金融业机构内部网络；
e） 应利用系统运行日志、上网行为、终端等安全系统日志监控资源，结合业务操作日志，对数据的异常使用、用户异常行为进行分析，形成数据安全分析报告，及时反馈相关部门。

10.4.4 态势感知

金融业机构宜能够有效感知内部安全风险并能够准确定位响应，态势感知至少应满足以下要求：

a) 应大量收集外部情报，如舆情信息等，用以辅助安全风险分析；
b) 宜在内部各个关键节点，通过安全设备、探针等检测相关信息，包括但不限于设备指纹、上网行为日志、业务操作日志、数据库日志、流量日志；
c) 宜对用户、行为、设备进行画像，通过算法模型检测内部潜在的账户盗用、数据滥用、数据外发、数据爬取等安全风险和威胁，并进行可视化展示。

10.5 安全审计

金融业机构信息应记录数据操作行为日志，并针对日志进行审计分析，识别并告警可疑行为，具体审计内容应至少包含以下要求：

a) 应制定数据审计日志的管理规范，明确数据审计日志的存储、分析、检查等要求；
b) 安全审计范围应覆盖至每个有权使用数据的用户，包括但不限于数据库管理员、数据库用户、操作系统管理员、操作系统用户、存储介质管理员、存储介质用户等；
c) 审计日志应包括时间、用户、IP 地址、操作对象、操作行为和操作结果等相关信息；
d) 审计日志不应记录 3 级及以上数据；
e) 宜搭建数据安全审计系统，提供对审计记录数据进行统计、查询、分析及生成审计报表的功能，收集和清洗相关日志，实现统一日志管理，建立审计策略并执行相关检查，形成审计报告反馈相关部门；
f) 网络安全事件等相关网络日志的留存时间应不少于 6 个月；
g) 审计日志留存时间应不少于 6 个月；
h) 应对数据生命周期全过程进行安全审计；
i) 应定期对 3 级及以上数据生命周期全过程进行内部审计；
j) 应安排专人定期查看日志，对事件日志、告警事件进行分析和处理，并对发现的安全事件和可疑问题进行处置；
k) 应对审计日志数据进行保护，防止未授权的访问和输出；
l) 应对审计日志数据进行备份，避免受到非预期的删除、修改或覆盖等。

10.6 检查评估

金融业机构定期或不定期开展数据安全检查和评估，检查评估包含但不限于以下管理要求：

a) 应建立数据安全检查评估机制，定期制定数据安全检查评估计划；
b) 在产品或服务发布前，或业务功能发生重大变化时，应进行数据安全影响评估；
c) 在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大数据安全事件时，应进行数据安全影响评估；
d) 形成数据安全影响评估报告，并以此采取措施降低风险及可能带来的损失；
e) 每年至少应开展一次全面的数据安全检查评估，评估方式包括但不限于自评估、外部第三方机构评估等；
f) 数据安全检查宜采取多种形式，如自查、内部检查和外部检查等；
g) 针对检查评估过程中发现的问题，应指定责任部门，制定适宜的整改计划，并跟踪落实；
h) 妥善留存有关安全评估报告，确保可供相关方查阅，并以适宜的形式对外公开；
i) 应采取技术措施确保检查评估记录和检查报告的安全留存。

10.7 应急响应与事件处置

金融业机构应制定可行的应急响应预案，及时处置数据安全事件告警，并在重大事件发生时立即启动应急响应，包含但不限于以下管理要求：

a) 制定应急响应与事件处置规范，建立完善的应急响应与事件处置和问责机制，做好应急预案，组织应急演练，确保在紧急情况下重要信息资源的可用性；
b) 应建立与公安机关等外部相关机构沟通协调机制，加强金融业机构内部各职能部门间的合作与沟通，协同处理数据安全事件；
c) 应依据国家法律法规和金融主管部门规定、事件性质、影响范围等，对安全事件进行分级；
d) 应制定安全策略，对不同级别的安全事件进行相应处置，重大事件发生后应及时启动应急响应机制；
e) 应汇聚安全事件相关信息，形成调查记录和事件清单，还原事件过程并留存相关证据；
f) 应按照金融主管部门有关规定，向金融主管部门上报事件及其处置情况；
g) 发生客户个人金融信息相关数据泄露事件，金融业机构应履行客户告知义务，并及时采取补救措施；
h) 事件处置结束后，应分析和总结原因和存在的问题，调整数据安全策略，避免事件再次发生，并形成总结报告。

注：个人金融信息相关数据泄露事件：即金融业机构通过不同渠道获取的个人客户、员工、对公客户关联自然人的数据的安全保护措施被破坏，导致转移中的、存储的或其他处理中的个人数据被意外或非法的销毁、丢失、篡改、未经授权访问等。

附 录 A
（资料性附录）金融业机构数据采集模式

金融数据采集流程实现对数据的采集与提取、信息数据转换与标准化、信息交换与上传，并提供内置安全审计与监管等辅助工具。按照采集模式，可分为两种形式，包括金融机构从外部机构采集数据，从金融消费者（包括个人金融信息主体与企业客户）处采集，如图2所示。

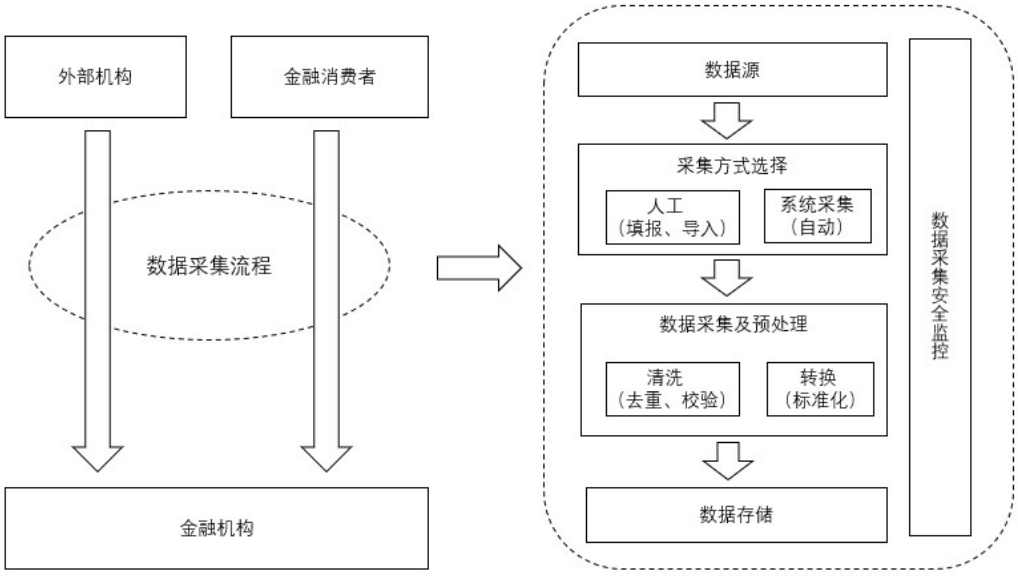

图2 金融机构数据采集模式

金融数据采集流程可涉及：

a) 确定原始数据采集源及内容：通过分析业务所需的数据，明确数据采集标准范围及属性。
   1) 金融机构从外部机构采集的数据源包括但不限于：关系数据库、XML、CSV、Excel、结构化文本、非结构化文件等；
   2) 金融机构从金融消费者采集的数据源包括但不限于：账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息和其他反映特定个人金融信息主体某些情况的信息。
b) 确定数据采集方式：通过分析数据源类型，根据可操作性、成本导向等原则选定所采用的方式技术：
   1) 金融机构从外部机构采集数据的方式包括但不限于：通过与外部机构合作，使用特定系统接口等相关方式采集数据；
   2) 金融机构从金融消费者采集数据的方式包括但不限于：通过金融业机构柜面（含纸质单据）、信息系统、金融自助设备、受理终端、客户端软件等方式采集。
c) 数据采集及预处理：确定采集方式后，采集的数据需要经过清洗和标准化转换后，加载存储到数据库中；
d) 采集监控：对数据采集过程、结果、明细、性能、异常进行实时动态监控，帮助及时了解运转情况。

附 录 B
（资料性附录）金融机构数据传输模式

金融数据传输涉及与金融机构相关联的全通信网络架构，按照传输模式，可分为金融机构内部数据传输和金融机构与外部机构间的数据传输两种形式，不同传输形式和不同传输对象间所采用的数据传输技术方式也不同。

首先，金融机构内部数据传输包括本机构同一数据中心节点内部或其同一分、子机构内部的数据传输、本机构及其分、子机构之间的数据传输，以及本机构内部不同数据中心之间的数据传输。其中，同一数据中心节点内部的数据传输，以及同一分、子机构内部的数据传输，通常采用本地局域网或WLAN方式实现；本机构与其分、子机构之间的数据传输，以及分、子机构之间的数据传输，通常采用VPN或基于专线技术的机构内骨干网方式实现；本机构内部不同数据中心间的数据传输，通常采用VPN、城域网或基于专线技术的机构内骨干网方式实现。

其次，金融机构与外部机构间的数据传输包括金融机构与外部机构之间数据传输，以及金融机构与金融消费者之间的数据传输。其中，与外部机构间的数据传输通常采用专线或VPN的方式实现；与金融消费者之间的数据传输通常采用有线互联网、移动互联网、第三方互联网应用的方式实现。

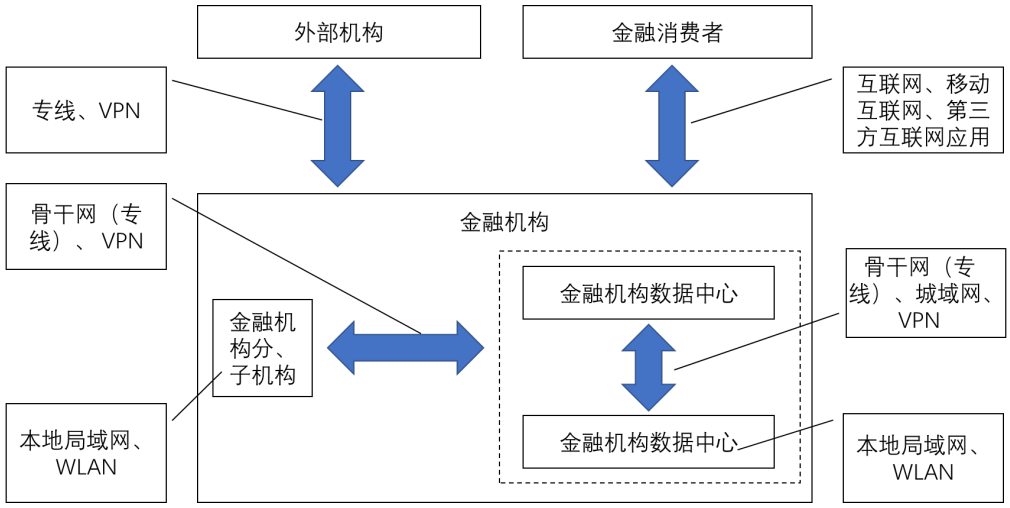

图3 金融机构数据传输模式

骨干网是指一个机构内用来连接多个区域或地区的高速网络，按照区域大小可规划出多个层级的骨干网，本地局域网是指在一个中心内部的园区网，骨干网用来连接分布在跨广域网、城域网的多个本地局域网。

专线传输方式一般指网络运营商针对企业用户提供的、具有固定IP、独享带宽点到点的传输线路，如ADSL、SDH、帧中继、DDN、ATM 、电话拨号等。

VPN是指建立在运营商公共网络基础上的，采用隧道技术建立的虚拟专用网络。

有线互联网是指通过特定的信息采集与共享的传输通道，利用电话拨号、ADSL、WLAN等接入技术完成用户与IP广域网的高带宽、高速度的物理连接网络。此类网络容易被攻击者利用有线传输的漏洞、布网的缺陷或者错误配置窃取敏感信息，需要注意对信息进行有效的数据保护。

移动互联网是指通过3G、4G、5G等移动通信技术基础上建立起的网络，此类网络容易被攻击者利用无线协议的漏洞，布网的缺陷或简陋配置窃取传输信息，在应用过程中需要注意对信息进行有效的数据保护。

第三方互联网应用是指第三方应用软件通过互联网、移动互联网借助API等技术接入并使用金融机构服务的形式。第三方应用软件通常是由独立的科技公司或个人开发并发放的。

附 录 C
（资料性附录）数据脱敏

C.1 概述

金融机构开展金融数据安全防护工作过程中，敏感信息的保护是其中尤为重要的一个环节。金融行业机构类型众多且数量庞大，随着我国信息化与数字化建设进程的不断加快，金融产品与服务的形式和内容也愈加创新多样。金融机构在业务开展和日常运营的过程中，积累了大量的数据，这些数据大多直接关联金融消费者的财产和信息安全，甚至关乎国家经济建设与社会稳定，具有较强的敏感性。因此，敏感信息的保护已成为金融业数据安全应用过程中需首要解决的问题。金融业敏感信息通常包括国家法律法规中的敏感信息、业务数据中的敏感信息，以及个人金融信息中的敏感信息等，在实际应用过程中，需要根据实际业务场景、数据安全级别等因素，选择适当的数据脱敏方式防止敏感信息的泄露，此外，个人金融信息常用去标识化技术实现个人金融信息主体的隐私保护。

C.2 定义与说明

C.2.1 数据脱敏

数据脱敏指通过一定方法消除信息系统数据中的敏感信息，保留业务所需的数据特征或内容，改变它的部分数值的数据处理过程，能够在很大程度上解决敏感数据在非可信环境中使用的问题，防止数据泄密，同时又可保证系统测试、业务监督等相关的处理不受影响。借助数据脱敏技术，消除敏感信息，并使脱敏后的信息保留其原始个人金融信息格式和属性，以确保应用程序可在使用脱敏个人金融信息的开发与测试过程中正常运行。

C.2.2 数据去标识化

数据去标识化指通过一定方法去除标识信息和个人信息主体之间的关联性，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。去标识化是隐私保护数据发布的主要工具之一，通过去除数据集中隐私属性和数据主体之间的关联关系，并且具有足够的防止重识别能力后，数据集的某些属性就可以共享发布，供外部业务系统进行处理分析。

C.2.3 两者的区别与联系

数据去标识化的主要目标是去除标识信息，防止重标识导致标识信息泄露，数据脱敏的主要目标是消除敏感信息，防止数据因为不当使用而进行泄露，两者在处理原始数据过程中可能存在相同的技术如遮蔽、删除，但是在数据类型、使用场景等方面还是略有不同，如表C.1所示。

表 C.1 数据脱敏与数据去标识化的对比

对比项	数据脱敏	数据去标识化
目标	消除敏感信息	去除标识信息
数据类型	个人、企业重要数据等敏感数据	个人隐私数据居多

对比项	数据脱敏	数据去标识化
使用场景	数据使用、数据研发、数据测试、数据共享等居多	数据发布、数据披露等居多
使用技术	数据删除、数据替换、数据抑制、数据随机化等	统计技术、密码技术、抑制技术、假名化技术、泛化技术、随机化技术和数据合成技术等
使用模型	---	K-匿名模型和差分隐私模型等

C.3 数据脱敏基本原则

数据脱敏不但要确保消除掉敏感信息，还需尽可能平衡数据脱敏所花费的代价、使用方的业务需求等多个因素。所以，为了确保数据脱敏的过程、代价可控，得到的结果正确且满足业务需要，在实施数据脱敏时，应从技术和管理两方面出发，需要遵循以下六大基本原则：

a) **有效性**:应保证数据脱敏过程的有效性，原始数据数据脱敏处理后，原始信息中包含的敏感信息已被消除，无法通过处理后的数据得到敏感信息，防止使用非敏感数据进行推断、重建、还原敏感原始数据；

b) **真实性**:应保证数据脱敏过程的真实性，脱敏后的数据应尽可能真实地体现原始数据的特征如数据格式、类型、长度、大小、唯一性等，且应尽可能多保留原始数据中的有意义信息；

c) **高效性**:应保证数据脱敏过程的高效性，通过借助程序实现脱敏自动化工作，并可进行重复执行。在不影响有效性的前提下，平衡脱敏的力度与所花费的代价，将数据脱敏的工作控制在一定的时间和经济成本内；

d) **可重现**:即相同源数据在配置相同算法和参数的情况下，脱敏后的数据应保持一致，随机类的算法除外；

e) **关联性**:对于结构化和半结构化数据，在同一数据表中某字段与另外字段有对应关系，如果脱敏算法破坏了这种关系，该字段的使用价值将不复 存在。通常在进行数据统计需要参考量的情况下，数据的关联性要求较高；

f) **可配置性**:应保证数据脱敏过程的可配置性，由于不同场景下的安全要求不同，数据脱敏时的处理方式和处理字段也不尽相同。因此需通过配置的方式，按照输入条件不同，生成不同的脱敏结果，从而可按数据使用场景等因素为不同的最终用户提供不同的脱敏数据。

C.4 数据脱敏技术分类

数据脱敏技术由于使用场景的不同分为动态数据脱敏和静态数据脱敏，静态数据脱敏一般用在非生产环境，将敏感数据从生产环境抽取并脱敏后用于培训、分析、测试、开发等非生产环境。动态数据脱敏一般用在生产环境，将敏感数据实时进行脱敏后用于应用访问等生产环境。

C.4.1 静态数据脱敏

静态数据脱敏用于处理静止的数据，即根据生产系统真实数据的生成规划创建可在内部和外部使用的符合真实数据规则但又与真实数据不同的数据，防止敏感数据意外泄露。静态数据脱敏主要特点：

a) 适应性，即可为任意格式的敏感数据脱敏；

b) 一致性，即数据脱敏后保留原始数据字段格式和属性；

c) 复用性，即可重复使用数据脱敏规则和标准，通过定制数据隐私策略满足不同业务需求。

C.4.2 动态数据脱敏

动态脱敏是针对某些特定应用屏蔽数据的方法，可随时对敏感字段进行脱敏，实时防止未授权用户访问敏感信息。动态数据脱敏主要特点：

a) 实时性，即能够实时地对用户访问的敏感数据进行动态脱敏、加密和提醒；
b) 多平台，即通过定义好的数据脱敏策略实现跨平台间、不同应用程序或者应用环境间的访问限制；
c) 可用性，即能够保证脱敏数据的完整，满足业务系统的数据需要。

C.5 常见数据脱敏技术

常见的脱敏技术主要包括扰乱技术、泛化技术、有损技术和抑制技术四类，主要如下：

C.5.1 扰乱技术

扰乱是指通过加入噪声的方式对原始数据进行干扰，以实现对原始数据的扭曲、改变，扰乱后的数据仍保留着原始数据的分布特征，具体的技术方法包括但不限于：

a) 重排：将原始数据按照特定的规则进行重新排列，例如将序号 12345 重排为 54321；
b) 替换：按照特定规则对原始数据进行替换，常见的替换方式包括常数替换、查表替换、参数化替换等；
c) 唯一值映射：将数据映射成一个唯一值，允许根据映射值找回原始值，支持正确的聚合或者连接操作；
d) 序映射：将数据映射成新值，同时保持数据顺序；
e) 均化：针对数值性的敏感数据，在保证脱敏后数据集总值或平均值与原数据集相同的情况下，改变数值的原始值；
f) 散列：即对原始数据取散列值，使用散列值来代替原始数据；
g) 固定偏移：将数据值增加 n 个固定的偏移量，隐藏数值部分特征；
h) 局部混淆：保持前面 n 为不变，混淆其余部分；
i) 乱序：对敏感数据进行重新随机分布，混淆原有值和其他字段的联系；
j) 混洗：主要通过对敏感数据进行跨行随机互换来打破其与本行其他数据的关联关系，从而实现脱敏；
k) 随机化：采用随机数据代替真值，保持替换值的随机性以模拟样本的真实性。例如用随机生成的姓和名代替真值；
l) 重写：参考原数据的特征，重新生成数据。重写与整体替换较为类似，但替换后的数据与原始数据通常存在特定规则的映射关系，而重写生成的数据与原始数据则一般不具有映射关系。例如对员工工资，可使用在一定范围内随机生成的方式重新构造数据。

C.5.2 泛化技术

泛化是指在保留原始数据局部特征的前提下使用一般值替代原始数据，泛化后的数据具有不可逆性，具体的技术方法包括但不限于：

a) 数据截断：直接舍弃业务不需要的信息，仅保留部分关键信息，例如将手机号码 13500010001 截断为 135；

b) 偏移取整：按照一定粒度对数据如时间进行向上或向下偏移取整，可在保证数据一定分布特征的情况下隐藏原始时间，例如将时间 20200322 18:08:19 按照 10 秒钟粒度向下取整得到 20200322 08:08:10，如将金额 5123.62 元按照百位粒度向上取证得到 5100 元；
c) 分档规整：将数据按照大小规整到预定义的多个档位，例如将客户资产按照规模分为高、中、低三个级别，将客户资产数据用这三个级别代替；
d) 变换：指对数值和日期类型的源数据，通过随机函数进行可控的调整(例如对于数值类型数据随机增减 20%;对于日期数据，随机增减 200 天)，以便在保持原始数据相关统计特征的同时，完成对具体数值的伪装。

C.5.3 有损技术

有损是指通过损失部分数据的方式来保护整个敏感数据集,适用于数据集的全部数据汇总后才构成敏感信息的场景，具体的技术方法包括但不限于：

a) 限制返回行数：仅仅返回可用数据集合中一定行数的数据，例如商品配方数据，只有在拿到所有配方数据后才具有意义，可在脱敏时仅返回一行数据；
b) 限制返回列数：仅仅返回可用数据集合中一定列数的数据，例如在查询人员基本信息时，对于某些敏感列，不包含在返回的数据集中；
c) 删除：直接删除敏感数据或将其置为空。

C.5.4 抑制技术

抑制是指通过隐藏数据中部分信息的方式来对原始数据的值进行转换，又称为隐藏技术，具体的技术方法包括但不限于：

a) 掩码屏蔽：用通用字符替换原始数据中的部分信息，例如将手机号码 13500010001 经过掩码得到 135****0001，掩码后的数据长度与原始数据一样。

C.6 脱敏方法的应用场景

下表列举了各类常见的脱敏方法及其应用场景并提供了部分脱敏示例，在实施数据脱敏作业时，可结合自身敏感数据现状和脱敏需求，灵活应用各类脱敏技术。

表C.2数据脱敏场景示例

序号	脱敏技术	脱敏方法	应用场景	方法描述	数据示例
1	扰乱	重排	保证数据集的业务属性的前提下，适用于群体信息统计的场景	将数据库的某一列值进行重排	22,31,27—> 31,27,22
2		替换	替换方法能够彻底的脱敏单类数据，但往往也会使相关字段失去业务含义	如统一将女性用户名替换为 F，对内部人员可以完全保持信息完整性，但易破解，常见的替换方式包括常数替换、查表替换、参数化替换.	李四—> F

序号	脱敏技术	脱敏方法	应用场景	方法描述	数据示例
3		散列	散列的脱敏方式最常用于敏感数据存储场景	将输入映射为 1 个 hash 值，常用作将不定长数据为固定长度的字符串，常用的 hash 算法，如 MD5、SHA-256、SHA-1、HMAC	123456—> e10adc3949ba59abbe56e057f20f883e
4		唯一值映射	唯一值映射可以保持表内表间关系，多用于开发测试场景	将数据映射成一个唯一值，允许根据映射值找回原始值，支持正确的聚合或者连接操作	Simth—> CLemetz
5		加密	适用于机密性要求高，不需要保持业务属性的场景	DES/3DES/AES 等加密算法实现脱敏，支持逆运算。安全程度取决于采用哪种加密算法，一般根据实际情况而定。	123456—> U2FsdGVkX19yci4oGpXvMfQJmzBfe9jV
6		固定偏移	根据特定业务场景，无需保持数据的业务属性的一种脱敏方式	将数据值增加 1 个固定的偏移量，隐藏数值部分特征	253—> 1253
7		局部混淆		保持前面 n 位不变，混淆其余部分	123@163.com—> 123344@163.com
8		乱序		对敏感数据进行重新随机分布，混淆原有值和其他字段的联系	将敏感字段重新分布
9		均化	保证数据集的业务属性的前提下，适用于群体信息统计的场景	针对数值性的敏感数据，在保证脱敏后数据集总值或平均值与原数据集相同的情况下，改变数值的原始值	保持脱敏数据集某个数值相同的情况下进行脱敏
10		随机化	不需要保持业务属性的场景	采用随机数据代替真值，保持替换值的随机性以模拟样本的真实性。例如用随机生成的姓和名代替真值。	“张三”—> “李四”
11		混洗	一般混洗方法用于大数据集合、且需要保留待脱敏数据特定特征的场景;对于小数据集，混洗形成的目标数据有可能通过其他信息被还原，在使用的时候需要特别慎重。	主要通过对敏感数据进行跨行随机互换来打破其与本行其他数据的关联关系，从而实现脱敏。	对敏感数据进行跨行随机互换
12		排序映射	需要保持一定的数据业务属性，并进行排序的场景	将数据映射成新值，同时保持数据顺序	500—> 25000
13	泛化	规整	保证数据集的业务属性，适用于群体信息统计的场景	将数据按照大小规整到预定义的多个档位	（0，60）、（60，90）、（90，100）—> 及格、良好、优秀
14		偏移取整		数据或者日期进行向上或者向下取整	28—> 20

序号	脱敏技术	脱敏方法	应用场景	方法描述	数据示例
15		变换	数值变化通过调整变动幅度可以有效控制目标数据的统计特征和真实度，是常用的脱敏方法。	指对数值和日期类型的源数据，通过随机函数进行可控的调整(例如对于数值类型数据随机增减 20%;对于日期数据，随机增减 200 天)，以便在保持原始数据相关统计特征的同时，完成对具体数值的伪装。	通过随机函数进行脱敏数据进行可控的调整
16		截断		将数据尾部截断，只保留前半部分	021123456—> 021
17	有损	限制返回行数	适用于过滤某些敏感行数或者列数的场景	仅仅返回可用数据集合中一定行数的数据	商品配方数据，只有拿到所有配方数据才有意义，可在脱敏时仅返回 1 行数据
18		限制返回列数		仅仅返回可用数据集合中一定列数的数据	查询人员基本信息时，对于某些敏感列，不包含在返回数据集中
19		删除	无需使用到该类敏感数据的场景	直接删除敏感数据或将其置为空。	直接删除敏感数据
20	抑制	掩码屏蔽	这种方法可以在很大程度上脱敏的同时，保持原有数据感观，也是一种广泛使用的方法。	保持数据长度不变，但只保留数据信息	13905710571—> 139****0571

C.7 常见的去标识化技术模型

常用的去标识化技术包括统计技术、密码技术、抑制技术、假名化技术、泛化技术、随机化技术和数据合成技术，常用的去标识化模型包括K-匿名模型和差分隐私模型等。下表给出了常见去标识化技术模型特性的对比情况。

表 C.3 常用的去标识化技术

技术类别	技术子类	输出数据类型	数据真实性保持	适用数据类型	适用属性类型	降低隔离风险	降低关联风险	降低推导风险	降低可分辨风险	计算消耗
统计技术	抽样	微数据	√	不详	不详	部分	部分	部分	部分	低
	聚合	统计数据	不详	连续数据	敏感属性	√	√	√	部分	低/中[1]
密码技术	确定性加密	微数据	√	所有	标识和敏感属性	×	部分	×	×	中
	保序加密	微数据	√	所有	标识和敏感属性	×	部分	×	×	中/高

技术类别	技术子类	输出数据类型	数据真实性保持	适用数据类型	适用属性类型	降低隔离风险	降低关联风险	降低推导风险	降低可分辨风险	计算消耗
	同态加密	微数据	√	所有	标识和敏感属性	×	×	×	×	高
	保留格式加密	微数据	√	所有	标识和敏感属性	×	×	×	×	高
	同态秘密共享	微数据	√	所有	标识和敏感属性	×	×	×	×	高
抑制技术	屏蔽	微数据	√	分类数据	局部标识符	√	部分	×	×	低
	局部抑制	微数据	√	分类数据	标识符	部分	部分	部分	部分	低
	记录抑制	微数据	√	不详	不详	部分	部分	部分	部分	低
	抽样	微数据	√	不详	不详	部分	部分	部分	部分	低
假名化技术	独立于标识符的假名	微数据	√	分类数据	直接标识符	×	部分	×	×	低[2]/中
	基于密码技术的标识符派生假名	微数据	√	分类数据	直接标识符	×	部分	×	×	低[2]/中
泛化技术	取整	微数据	√	连续数据	标识和敏感属性	×	部分	部分	部分	低
	顶层与底层编码	微数据	√	有序数据	标识和敏感属性	×	部分	部分	部分	低
随机化技术	噪声添加	微数据	×	连续数据	标识和敏感属性	部分	部分	部分	部分	低
	置换	微数据	×	所有	标识和敏感属性	部分	部分	部分	部分	中
	微聚集	微数据	×	连续数据	准标识和敏感属性	×	部分	部分	部分	中
数据合成技术		统计数据	不详	连续数据	敏感属性	√	√	√	部分	低/中[3]
差分隐私模型		微数据	×	所有	标识和	√	√	部分	√	中/高

技术类别	技术子类	输出数据类型	数据真实性保持	适用数据类型	适用属性类型	降低隔离风险	降低关联风险	降低推导风险	降低可分辨风险	计算消耗
					敏感属性					[4]
K-匿名模型		微数据	√	所有	所有	√	部分	×	部分	高
l-多样性模型		微数据	√	所有	所有	√	部分	×	部分	高
t-接近模型		微数据	√	所有	所有	√	部分	×	部分	高

C.8 去标识化模型和技术选择参考因素

不同类型数据需要采用不同的去标识化技术，所以需要确定数据的类型和业务特性后，选择合适的去标识化模型和技术，以下为选择的参考因素：

a) 是否需要对重标识风险进行量化；
b) 聚合数据是否够用；
c) 数据是否可删除；
d) 是否需要保持唯一性；
e) 是否需要满足可逆性；
f) 是否需要保持原有数据值顺序；
g) 是否需要保持原有数据格式，如数据类型、长度等保持不变；
h) 是否需要保持统计特征，如平均值、总和值、最大值、最小值等；
i) 是否需要保持关系型数据库中的实体完整性、参照完整性或用户自定义完整性；
j) 是否可以更改数据类型，比如在针对字符串类型的“性别”（男/女）进行去标识化时，是否可以变成数字类型表示（1/0）；
k) 是否需要满足至少若干个属性值相同，以加强数据的不可区分性；
l) 是否可以对属性值实施随机噪声添加，对属性值做小变化；
m) 去标识化的成本约束。

参 考 文 献

[1] 数据安全管理办法（征求意见稿）

[2] 关键信息基础设施安全保护条例（征求意见稿）

[3] 信息安全等级保护商用密码管理办法（国密局发〔2007〕11号）

[4] 中国人民银行网络数据安全保护指南（银办发〔2019〕7号）

[5] GB/T 37939—2019 信息安全技术 网络存储安全技术要求

[6] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[7] JR/T 0158-2018 证券期货业数据分类分级指引

[8] GM/T 0002-2012 SM4分组密码算法

[9] JR/T 0149—2016 中国金融移动支付 支付标记化技术规范

[10] Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST Special Publication 800-171, Revision 1, 2016

[11] Assessing Security Requirements for Controlled Unclassified Information,NIST Special Publication 800-171A, 2018

[12] Information technology-Security techniques-Privacy enhancing data de-identification terminology and classification of techniques, ISO/IEC 20889:2018

[13] Information technology-Security techniques-Specification for digital redaction, ISO/IEC 27038:2014