附件
ICS 35.240.40
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0223—2021

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

2021－04－08 发布　　2021－04－08 实施

中国人民银行　　发 布

目　　次

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》的规定起草。

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。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：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、国家金融IC卡安全检测中心（银行卡检测中心）、中国建设银行股份有限公司、兴业银行股份有限公司、中国农业银行股份有限公司、招商银行股份有限公司、恒丰银行股份有限公司、中国银行股份有限公司、网联清算有限公司、平安银行股份有限公司、中国保险行业协会、华为技术有限公司、北京钱袋宝支付技术有限公司、蚂蚁科技集团股份有限公司、全知科技（杭州）有限责任公司、北京安华金和科技有限公司、奇安信科技集团股份有限公司、杭州安恒信息技术股份有限公司、深圳云安宝科技有限公司、哈尔滨工业大学（深圳）数据安全研究院、上海淇毓信息科技有限公司、北京天融信网络安全技术有限公司、深信服科技股份有限公司、北京神州绿盟科技有限公司、北京长亭未来科技有限公司、上海艾芒信息科技有限公司、华控清交信息科技（北京）有限公司、成方金融科技有限公司、中国人民银行广州分行、中国人民银行南京分行、中国人民银行营业管理部、中国人民银行哈尔滨中心支行、深圳市长亮科技股份有限公司、北京中金国盛认证有限公司、平安保险（集团）股份有限公司、阿里云计算有限公司。

本文件主要起草人：李伟、陈立吾、沈筱彦、车珍、曲维民、昝新、夏磊、方怡、马晓伟、渠韶光、陈聪、居崑、杨波、刘静芳、刘超、栾家阳、吴远松、王照坤、赵志蛟、俞吴杰、邱斌、郑超、王福舟、陈雪秀、陈俊、郭林、母延燕、严敏瑞、康雪婷、冷杉、兰安娜、宋铮、王昕、朱通、王勰思、杨海峰、唐力、林玉波、张晨晖、周亚超、林鹭、韩培义、姚磊、刘川意、王安滨、温树海、包英明、李建彬、徐省委、訾然、张帆、马男、张帆、杜宁、王云河、王蜀洪、安鸿飞、唐辉、高强裔、侯漫丽、黎凯伦、任军远、戴辰、薛金川、曹正阳、辜敏、陈裕源、王衍强、任妍、王炤宇。

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，金融业机构生产运营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中。随着大数据、人工智能、云计算等新技术在金融业深入应用，金融数据逐步实现从信息化资产到生产要素的转变，其重要性日益凸显。数据泄露、滥用、篡改等安全威胁的影响逐步从机构内转移扩大至机构间和行业间，甚至影响国家安全、社会秩序、公众利益和金融市场稳定。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，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、行业间安全应用和共享，有利于数据价值挖掘与实现。

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，进一步提高金融业机构的数据管理和安全防护水平，确保金融数据安全应用，编制本文件。

本文件凡涉及密码技术的相关内容，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，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

本文件规定了金融数据生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，建立覆盖数据采集、传输、存储、使用、删除及销毁过程的安全框架。

本文件适用于指导金融业机构开展电子数据安全防护工作，并为第三方测评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—2010　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

GB 50174—2017　数据中心设计规范

JR/T 0092—2019　移动金融客户端应用软件安全管理规范

JR/T 0158—2018　证券期货业数据分类分级指引

JR/T 0171—2020　个人金融信息保护技术规范

JR/T 0197—2020　金融数据安全　数据安全分级指南

3　术语和定义

GB/T 35273—2020和GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

数据处理　data processing

自动数据处理　automatic data processing

数据操作的系统执行。

示例：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。

[来源：GB/T 5271.1—2000，01.01.06]

3.2

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。

[来源：GB/T 25069—2010，2.1.1]

3.3

完整性 integrity

保卫资产准确和完整的特性。

[来源：GB/T 25069—2010，2.1.42，有修改]

3.4

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。

[来源：GB/T 25069—2010，2.1.20]

3.5

真实性 authenticity

确保主体或资源的身份正是所声称的特性。

注：真实性适用于用户、进程、系统和信息之类的实体。

[来源：GB/T 25069—2010，2.1.69，有修改]

3.6

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。

[来源：JR/T 0197—2020，3.10]

3.7

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。

[来源：GB/T 35273—2020，3.1，有修改]

3.8

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。

[来源：GB/T 35273—2020，3.3，有修改]

3.9

个人金融信息安全影响评估 personal financial 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。

[来源：GB/T 35273—2020，3.9，有修改]

3.10

影响 impact

事件的后果。

注：在信息安全中，一般指不测事件的后果。

[来源：GB/T 25069—2010，2.3.105，有修改]

3.11

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。

[来源：GB/T 35273—2020，3.10，有修改]

3.12

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：肯定性动作包括个人金融信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

[来源：GB/T 35273—2020，3.6，有修改]

3.13

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：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。

[来源：GB/T 35273—2010，3.14，有修改]

3.14

特权访问安全 privileged access security

一种帮助企业解决特权账户相关问题的技术。

3.15

特权账户 privileged account

涉及到企业核心数据资产的账号。

注：特权账号存在于服务器、应用系统、数据库、中间件等。

4 缩略语

下列缩略语适用于本文件：

ADSL：非对称数字用户线路（Asymmetric Digital Subscriber Line）

AES：高级加密标准（Advanced Encryption Standard）

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

APP：应用程序（Application）

ATM：异步传输模式（Asynchronous Transfer Mode）

CSV：逗号分隔值（Comma-Separated Values）

DDN：数字数据网（Digital Data Network）

DES-CBC：数据加密标准-密码块链接（Data Encryption Standard-Cipher Block Chaining）
ETL：抽取-转换-装载（Extract-Transform-Load）
HMAC：哈希运算消息认证码（Hash-based Message Authentication Code）
IP：网际互连协议（Internet Protocol）
MD5：消息摘要算法（Message-Digest Algorithm 5）
MSTP：多业务传送平台（Multi-Service Transport Platform）
OCR：光学字符识别（Optical Character Recognition）
RSA：公钥密码算法（Rivest-Shamir-Adleman）
SDH：同步数字体系（Synchronous Digital Hierarchy）
SHA1：安全散列算法（Secure Hash Algorithm 1）
SSID：服务集标识（Service Set Identifier）
VPN：虚拟专用网络（Virtual Private Network）
WEB：全球广域网（World Wide Web）
WLAN：无线局域网（Wireless Local Area Network）
XML：可扩展标记语言（Extensible Markup Language）

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（见图1）遵循数据安全原则，以数据安全分级为基础，建立覆盖数据生命周期全过程的安全防护体系，并通过建立健全数据安全组织架构和明确信息系统运维环节中的数据安全需求，全面加强金融业机构数据安全保护能力。

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、删除以及销毁等数据生命周期各个环节的安全防护要求，是金融业机构开展数据安全防护工作的基本依据。结合金融数据业务规则及金融数据特点，建立覆盖金融数据生命周期全过程的安全防护机制，是金融业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。

数据安全组织保障、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。数据安全组织保障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，为数据安全相关工作的组织和落实奠定基础。在金融业机构日常运营过程中，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、应急响应与事件处置等过程中的数据安全风险防控能力，可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应对。

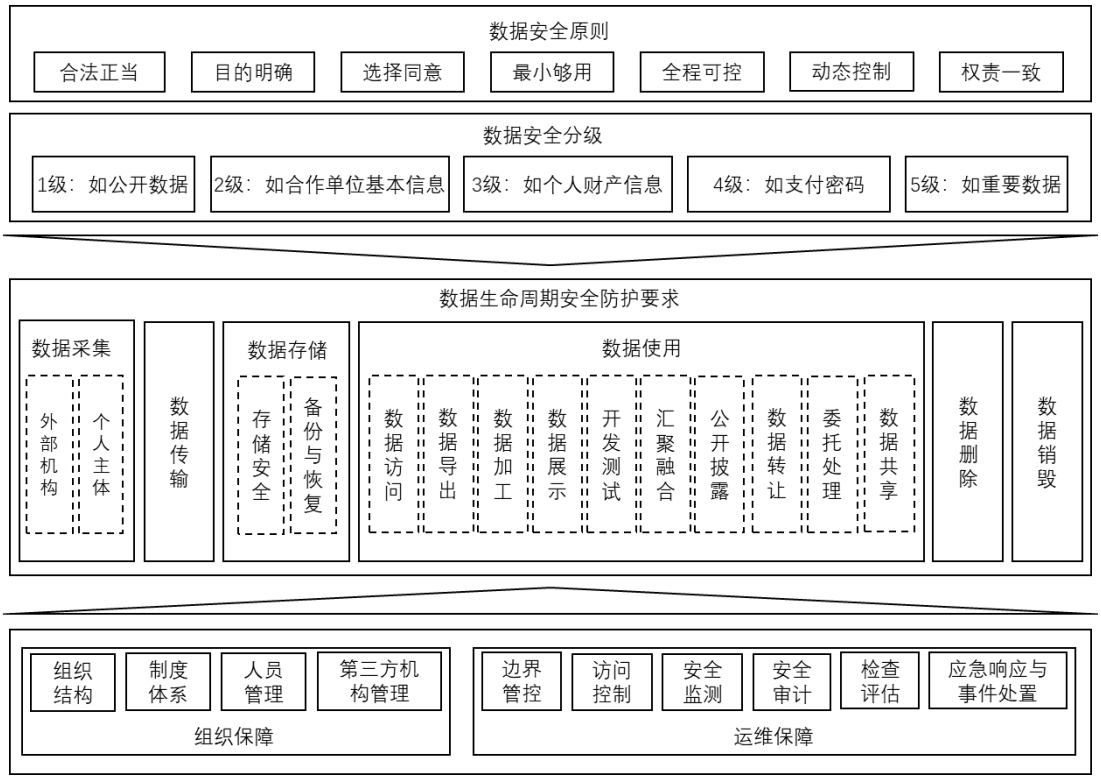


图 1　数据生命周期安全框架

5.2　分级保护

金融数据安全级别按照JR/T 0197—2020相关要求，根据安全性遭到破坏后的影响范围和影响程度，将金融数据安全级别由高到低划分为5级、4级、3级、2级、1级。

本文件所指金融数据安全，主要是指确保金融数据在其生命周期各阶段的安全性，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，其安全防护应参考本文件有关完整性及可用性安全要求；2级至4级数据的安全防护应在平衡安全需求与业务需求的基础上，根据数据安全级别不同，有侧重地采取适当的安全防护措施，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，5级数据的保护按照国家及行业主管部门的有关要求执行。

证券行业数据安全分级和数据安全保护工作按照JR/T 0158—2018等证券行业相关要求执行，云环境的数据安全应符合国家和行业主管部门的相关要求。金融业机构境外分、子公司和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应按照数据跨境相关要求执行。

涉及个人金融信息的内容，除满足本文件要求外，还应按照JR/T 0171—2020相关要求执行。

注：本文件中未明确具体安全级别的条款，为安全级别为1级至4级数据均应满足的通用安全要求；已明确具体安全级别的条款，为该级别数据保护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，金融业机构在开展业务及日常经营管理过程中，遵循以下数据安全基本要求：

a)　合法正当原则：应确保金融数据全生命周期各环节数据活动的合法性和正当性。

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环节的安全防护目标和要求。
c) 选择同意原则：应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。
d) 最小够用原则：金融业机构应仅处理个人金融信息主体授权同意的金融数据，且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：应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，履行数据安全防护职责。

7 数据生命周期安全防护

7.1 数据采集

7.1.1 概述

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，直接或间接从个人金融信息主体，以及企业客户、外部数据供应方等外部机构获取数据的过程。数据采集过程存在数据泄露、数据源伪造、特权账户滥用、数据篡改等安全风险。

数据采集过程实现数据的采集与提取、转换与标准化、信息上传，并提供内置安全审计与监管等辅助工具。按照采集模式，可分为从外部机构和从个人金融信息主体采集数据，见附录A。

7.1.2 从外部机构采集数据

金融业机构从外部机构采集数据，安全要求如下：

a) 应通过合同协议等方式，明确双方在数据安全方面的责任及义务，明确数据采集范围、频度、类型、用途等，确保外部机构数据的合法合规性和真实性，必要时提供相关个人金融信息主体的授权。
b) 从外部数据供应方处采集数据，应制定数据供应方约束机制，并明确数据源、数据采集范围和频度，并事前开展数据安全影响评估。

注：数据安全影响评估（data security impact assessment）：针对数据处理活动，检验其合法合规程度，判断其对相关方合法权益造成损害的各种风险，以及评估相关保护措施有效性的过程。

c) 采集的企业客户数据应与提供的金融产品或服务直接相关，并与合同协议条款、隐私政策中约定采集的内容保持一致，不应超范围采集数据。
d) 应明确数据采集过程中个人金融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) 通过系统批量采集的数据应采用摘要、消息认证码、数字签名等密码技术确保采集过程数据的完整性。
f) 应对人工批量采集数据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，防止采集过程出现数据泄露。
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。

h） 应对数据采集过程进行日志记录，并采取技术措施确保信息来源的可追溯性。

i） 采集 3 级及以上数据时，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。

j） 采集 4 级数据时，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的真实性，必要时可实施阻断、二次认证等操作。

2） 对采集的数据进行数据加密。

3） 不应通过人工方式采集。

7.1.3 从个人金融信息主体处采集数据

金融业机构从个人金融信息主体处采集数据，安全要求如下：

a） APP、WEB 等客户端相关业务完成后不应留存 3 级及以上数据，并及时对缓存进行清理。

b） 采集的个人金融信息应与提供的金融产品或服务直接相关，并与合同协议条款、隐私政策中约定采集的内容保持一致，不应超范围采集数据。

c） 通过纸质表单采集数据并转换为电子数据时，满足以下要求：

1） 对表单的保存、查阅、复制等操作进行严格审批授权，涉及 3 级及以上数据的操作，应进行专项审批，并对表单流转的全过程进行监控与审计。

2） 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。

d） 数据采集过程应符合 7.1.2 d）～j）所述要求。

e） 金融业机构在停止其提供的金融产品或服务时，应立即停止数据收集活动及数据分析应用活动，相关国家及行业主管部门另有规定的按照相关规定执行。

7.2 数据传输

数据传输是指金融业机构将数据从一个实体发送到另一个实体的过程，存在数据传输中断、篡改、伪造及窃取等安全风险。金融数据传输涉及与金融业机构相关联的全通信网络架构和通信方式，按照传输模式（见附录B），可分为金融业机构内部数据传输、金融业机构与外部机构或金融客户的数据传输两种形式，不同传输形式和不同传输对象采用的数据传输技术方式也不同。数据传输安全要求如下：

a） 采取措施加强数据传输过程中的网络和数据安全，满足以下基本要求：

1） 应加强软件开发安全管理，保障数据传输工具的安全性，工具上线前应开展必要的渗透测试、支持库漏洞查找等工作，以防止工具使用过程中遭受恶意破坏、功能篡改、信息窃取等攻击。

2） 应采用防火墙、入侵检测等安全技术或设备，确保数据传输网络的安全性。

3） 不同网络区域或者安全域之间应进行安全隔离和访问控制。

4） 终端应采取准入控制、终端鉴别等技术措施，防止非法或未授权终端接入内部网络。

5） 应对通信双方进行身份认证，确保数据传输双方是可信任的。

6） 应采用数字签名、时间戳等方式，确保数据传输的抗抵赖性。

7） 应采用密码技术或非密码技术等方式，确保数据的完整性。

8） 应选用安全的密码算法，禁用如 MD5、DES-CBC、SHA1 等不安全的算法。

9） 2 级及以上数据的内部传输，应事先经过审批授权明确当前授权的范围、频次、有效期等，避免出现一次性授权、打包授权等情况。

10） 2 级及以上数据的对外传输，应事先经过审批授权并采取数据加密、安全传输通道或安全传输协议进行数据传输。

11）3 级及以上的数据内部传输，应采取数据加密、安全传输通道或安全传输协议进行数据传输。
12）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的，应经过事先审批授权，并采取技术措施确保数据保密性。
13）4 级及以上数据传输，应对数据进行字段级加密，并采用安全的传输协议进行传输。
14）4 级数据中的个人金融信息原则上不应对外传输，国家及行业主管部门另有规定的除外。
15）应在数据传输不完整时清除传输缓存数据。
16）应在数据传输完成后立即清除传输历史缓存数据。
17）应定期检查或评估数据传输的安全性和可靠性。
18）向国家机关、行业主管和监管单位传输数据，应按照国家及行业相关管理要求进行传输。

b） 通过内部无线网络传输数据，在满足 7.2 a）基本要求的基础上，还应满足以下要求：
1） 采用绑定设备序列号或硬件地址（MAC 地址）等管控措施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 采用规范的命名规则，不泄露机构名称、网络特性、物理位置等信息，禁止使用缺省的 SSID，生产环境应禁用 SSID 广播，避免攻击者通过扫描直接获取无线网络信息。
3） 采用安全、可靠的加密协议，对无线通信信道进行安全加密。
4） 确保无线网络设备的物理安全，禁用不必要的服务，强化无线网络设备的管理账号和口令安全，禁止使用弱口令，建立安全管理基线。
5） 加强无线网络用户管理，禁止多人使用同一账号，采用双因素认证方式对接入用户进行身份校验，停用长时间未登录使用无线网络的账号。
6） 采取措施控制移动智能终端在内网和互联网交叉使用的风险，加强应用安全和数据泄露防护，防范恶意代码传播。
7） 明确短期使用及临时搭建的无线网络使用期限，期满后应及时拆除或关闭。

c） 通过运营商网络传输数据，在满足 7.2 a）基本要求的基础上，2 级及以上数据还应采用专线或 VPN 等技术确保传输通道的安全，确保数据传输的安全性。

d） 通过物理介质批量传递 3 级及以上数据时应对数据进行加密或脱敏，并由专人负责收发、登记、编号、传递、保管和销毁等，传递过程中可采用密封、双人押送、视频监控等确保物理介质安全到位，传递过程中物理介质不应离开相关责任人、监控设备等的监视及控制范围，且不应在无人监管情况下通过第三方进行传递，国家及行业主管部门另有规定的除外。

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，将数据进行持久化保存的过程，包括但不限于采用磁盘、磁带、云存储服务、网络存储设备等载体存储数据。数据存储过程，可能存在数据泄露、篡改、丢失、不可用等安全风险。

7.3.2 存储安全

数据存储的安全要求如下：

a） 数据存储不应因存储形式或存储时效的改变而降低安全保护强度。

b） 应根据安全级别、重要性、量级、使用频率等因素，将数据分域分级存储。

c） 应依据最小够用原则存储数据，不应以任何形式存储非业务必需的金融数据，存储时间应为业务必需的最短时间，国家及行业主管部门另有规定的除外。

d) 应定期对数据存储过程中可能产生的影响进行风险评估，并采取相应安全防护措施。
e) 脱敏后的数据应与用于还原数据的恢复文件隔离存储，使用恢复原始数据的技术应经过严格审批，并留存相关审批及操作记录。
f) 应采取一定措施确保数据存储的完整性，存储 3 级及以上数据时，应采用密码技术、权限控制等技术措施保证数据完整性。
g) 2 级及以上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。
h) 3 级数据的存储应采取加密等技术措施保证数据存储的保密性。
i) 保存 3 级及以上数据的信息系统，其网络安全建设及监督管理宜满足网络安全等级保护 3 级要求。
j) 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。
k) 4 级及以上数据应使用密码算法加密存储。
l) 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。
m) 在我国境内产生的 5 级数据应仅在我国境内存储。
n) 应对数据存储区域进行规划，并对不同区域之间的数据流动进行安全管控。

7.3.3 备份和恢复

数据备份与恢复工作安全要求如下：

a) 根据数据的安全级别和数据对系统运行的影响，制定数据备份策略和恢复策略，备份策略应至少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、备份周期或频率、备份范围等。
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。
d) 数据备份应基于多冗余策略，可采用磁带、磁盘镜像、磁盘冷备、热备、双活等技术实现，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和可用性进行检查，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) 生产数据备份存放环境及其物理设施的安全保护等级应按照 GB 50174—2017 的要求执行。
h) 大数据平台应提供数据整体迁移功能，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，进行数据的访问、导出、加工、展示、开发测试、汇聚融合、公开披露、数据转让、委托处理、数据共享等活动。数据使用不应超出数据采集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、窃取、泄漏、篡改、损毁等安全风险。

7.4.2 数据访问

7.4.2.1 基本要求

数据访问指金融业机构内外部各类主体对数据进行查询和变更的过程，数据访问控制安全要求如下：

a) 应综合考虑主体角色、信用等级、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。

b) 3级及以上数据访问应建立访问权限申请和审核批准机制，并宜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、系统进行控制，以及实际操作和申请操作进行验证，保证实际操作与申请并审批的操作是一致的。

c) 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，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问。

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应实现多因素认证或二次授权，并应结合业务需要对数据采取脱敏和控制访问数据行数的技术措施，以满足最小化原则要求。

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。

e) 应通过访问控制等措施限制频繁查询数据人员的数据访问频率，如柜员、客户经理、客服人员等确需批量查询的应通过相应审批并留存相关记录，并宜提供访问控制组件与审批结果的自动联动能力。

7.4.2.2 特权访问安全要求

特权访问指不受访问控制措施限制的数据访问，例如使用数据库管理员权限访问数据，或使用可在信息系统内执行所有功能、访问全量数据的特权账号等。特权访问的安全要求如下：

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。

c) 可访问3级及以上数据的特权账号，在每次使用前应进行审批授权，并宜采取措施确保实际操作与所获授权的操作是一致的，防止误执行高危操作或越权使用等违规操作。

d) 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。

7.4.3 数据导出

数据导出是指数据从高等级安全域流动至低等级安全域的过程，如数据从生产系统至运维终端、移动存储介质等情形。数据导出安全要求如下：

a) 金融业机构应根据最小够用原则，确定数据导出场景、导出数据范围和相应的权限规则。

b) 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。

c) 2级及以上的数据导出应有详细操作记录，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。

d) 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。

e） 3 级及以上数据的导出操作前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。
f） 3 级及以上的数据导出应使用加密、脱敏等技术手段防止数据泄露，国家及行业主管部门另有规定的除外。
g） 4 级数据原则上不应导出，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。

7.4.4 数据加工

数据加工是金融业机构基于市场分析、业务优化、风险管控等需求，对数据进行清洗、转换、分析、挖掘等操作。数据加工安全要求如下：

a） 应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） 3 级及以上数据加工之前应进行数据安全评估，并采用加密、脱敏等技术措施，保证数据加工过程的数据安全性。
c） 除业务必须外，不应对 4 级数据进行加工。
d） 应对数据加工过程进行必要的监督和检查，确保加工过程的数据安全性。
e） 应完整记录数据加工过程的操作日志。

7.4.5 数据展示

数据展示是指金融业机构通过业务运营平台、运维终端、客户端应用软件、银行卡受理设备、自助终端设备等界面显示数据的过程。数据展示安全要求如下：

a） 数据展示前，应事前评估展示需求，包括展示的条件、环境、权限、内容等，确定展示的必要性和安全性。
b） 数据展示时，应确保展示数据的安全性，具体要求如下：
    1） 对应用系统桌面、移动运维终端、柜面受理设备等界面展示增加水印，水印内容应最少包括访问主体、访问时间。
    2） 禁用展示界面复制、打印等可将展示数据导出的功能。
    3） 业务系统对 2 级及以上数据明文查询实现逐条授权、逐条查询，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功能，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 级数据的展示应事先通过审批授权后方可展示。
e） 3 级数据的展示应在审批的基础上采用屏蔽等技术措施防止信息泄露。
f） 4 级及以上数据不应明文展示，国家及行业主管部门另有规定的除外。

7.4.6 开发测试

开发测试是指金融业机构使用金融数据完成软件、系统、产品等开发和测试的过程。开发测试安全要求如下：

a） 应采取技术措施，实现开发测试环境数据与生产环境数据的有效隔离。
b） 应通过安全运维管理平台或数据提取专用终端获取数据，专用终端应事先经过审批授权后方可开通，原则上不应涉及 4 级数据。
c） 通过管理平台或专用终端获取 3 级及以上数据时，应通过技术手段控制数据的获取范围，包括对象、数据量等，并能对获取的数据按照策略进行脱敏处理，保证生产数据经过脱敏处理后才能被提取。

d) 开发测试等过程的数据，应事先进行脱敏处理，防止数据处理过程中的数据泄露，国家及行业主管部门另有规定的除外。
e) 使用外部的软件开发包、组件、源码等开展开发测试工作前应进行数据安全评估。
f) 接入开发测试环境的内外部终端设备应进行统一安全管理，宜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) 非本机构设备接入开发测试环境应经过开发部门以及设备使用部门审批，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部门以及设备使用部门审批。

7.4.7 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，在机构内部不同部门之间或本机构与外部机构之间，进行多源或多主体的数据汇集、整合等产生数据的过程。数据汇聚融合安全要求如下：

a) 汇聚融合的数据不应超出采集时所声明的使用范围，因业务需要确需超范围使用个人金融信息的，应事先再次征得个人金融信息主体明示同意。
b) 汇聚融合前应根据汇聚融合后可能产生的数据内容、所用于的目的、范围等开展数据安全影响评估，并采取适当的技术保护措施。
c) 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、结果用途和知悉范围、各合作方数据保护责任和义务，以及数据保护要求等，并采用技术手段如多方安全计算、联邦学习、数据加密等技术降低数据泄露、窃取等风险。
d) 4级数据原则上不应用于汇聚融合，因业务需要确需汇聚融合的，应建立审批授权机制并具备数据跟踪溯源能力后方可汇聚融合。
e) 应对脱敏后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。
f) 汇聚融合后产生的数据以及原始数据的衍生数据，应重新明确数据所属单位和安全保护责任部门，并确定相应数据的安全级别。

7.4.8 公开披露

公开披露是指金融业机构在提供金融产品或服务的过程中，因国家有关规定、行业主管部门规章，以及金融产品或服务业务需要，在其指定渠道公开数据的行为。数据公开披露安全要求如下：

a) 应依据国家有关规定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，对拟披露数据的合规性、业务需求、数据脱敏方案进行审核。
    2) 机构业务部门对披露渠道、披露时间、拟公开数据的真实性，以及数据脱敏效果进行确认，披露时间指永久或固定时间段。
    3) 依据机构有关程序执行数据公开披露审批程序，其审批过程和记录留档。
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，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，按照 JR/T 0092—2019 相关要求执行。

d) 3级及以上数据原则上不应公开披露，国家及行业主管部门另有规定的除外。
e) 应准确记录和保存数据的公开披露情况，包括公开披露的日期、规模、目的、范围等。

7.4.9 数据转让

数据转让指金融业机构将数据移交至外部机构，不再享受该数据相关权利和不再承担该数据相关义务的过程。数据转让安全要求如下：

a) 除以下情况外，原则上不应转让数据：
   1) 满足国家与行业主管部门要求。
   2) 已通过合同协议等有关约定获得数据转让相关授权的。
   3) 在金融业机构出现收购、兼并、重组等情形时，依照国家及行业有关规定履行义务。
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，具体安全要求如下：
   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时，应通过逐一传达或公告的方式向个人金融信息主体等履行告知义务。
   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，应重新获得个人金融信息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，并将处理结果通过逐一传达或公告的方式向个人金融信息主体等履行告知义务。

7.4.10 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，在不改变该数据相关权利和义务的前提下，将数据委托给第三方机构进行处理，并获取处理结果的过程。此处委托处理也包括纸质单据OCR作业、纸质单据人工录入等。委托处理安全要求如下：

a) 应依据本文件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国家及行业主管部门的相关要求，金融业机构应对第三方机构开展事前尽职调查。
c) 委托行为不应超出事前已获得授权及合同协议约定的数据使用范围。
d) 应根据委托处理的数据内容、范围、目的等，对数据委托处理行为进行数据安全影响评估，涉及个人金融信息的，应进行个人金融信息安全影响评估，并采取相应的有效保护措施。
e) 应对被委托方数据安全防护能力进行数据安全评估，并确保被委托方具备足够的数据安全防护能力，提供了足够的安全保护措施。

注：数据安全评估（data security assessment）：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。

f) 不应对4级数据进行委托处理。
g) 对委托处理的金融数据，安全要求如下：
   1) 个人金融信息应事先采用数据脱敏（见附录C）等技术防止个人金融信息泄露，因业务确需，以及国家及行业主管部门另有规定的除外。
   2) 涉及2级、3级数据的，应对数据进行加密处理，并采取数据标记、数据水印（见附录D）等技术，降低数据被泄露、误用、滥用的风险。

3) 因业务确需无法对数据进行脱敏或加密处理的，应明确相应授权审批机制，事前对委托处理的内容通过专项审批，并采取技术措施防止数据被泄露、误用和滥用。

h) 对委托处理的数据进行安全审计，要求如下：

1) 数据通过信息系统与委托方进行传递时，则应在相应的控制节点设置安全审计功能，对数据的外发与回传进行审计，其中信息系统包括 API、摆渡服务器，控制节点包括信息系统业务功能、API、服务器用户。

2) 数据以纸质介质或磁盘等存储介质与委托方进行传递时，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，其中数据接收方细化至法人机构数据安全负责人。

i) 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。

7.4.11 数据共享

数据共享是指金融数据在不同部门或机构之间进行分享，包含与行业主管部门的数据分享，各方均承担该数据相关权利和义务的过程。数据共享安全要求如下：

a) 数据内部共享是指发生在金融业机构内部，在本部门职能需要之外进行的数据共享，安全要求如下：

1) 应梳理数据共享的各类场景，明确各类场景的安全要求和责任部门，并建立相应的审核批准机制，对数据使用目的、内容、使用时间、技术防护措施、数据使用后的处置方式等进行审批，并留存相关记录。

2) 在数据共享前，应开展数据安全影响评估，对共享的数据内容、数据范围、时间周期、传输方式、用途、安全管控手段等要素进行评估，涉及个人金融信息的不应超出其授权范围，数据安全保护强度不因数据共享而降低。

3) 应对 2 级以及上的数据共享过程留存日志记录，记录内容包括但不限于共享内容、共享时间、防护技术措施等。

4) 采取以下措施确保 3 级及以上数据共享的安全性：

——原则上应对 3 级及以上数据进行脱敏；

——若因业务确需，无法对数据进行脱敏的，应对共享内容通过专项审批，并对数据进行加密、选用安全可靠的传输协议或在安全可控的环境中进行共享；

——脱敏方式的选取宜充分结合数据共享场景、业务需要和安全风险评估结果，选择被猜解或碰撞风险相对较低的脱敏技术；

——脱敏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。

5) 不应共享 4 级数据。

6) 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，应通过身份认证、数据加密、反爬虫机制、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，并定期检查和评估自动化工具安全性和可靠性。

7) 数据使用部门应根据共享前约定的数据使用期限，对数据进行安全处置，数据共享方应对处置结果进行确认。

b) 数据外部共享指金融业机构在经营过程中，在本机构职能需要之外与外部机构进行的数据共享，安全要求如下：

1) 应满足 7.4.1 a）所述安全要求。

2) 应与数据接收方通过合同协议等方式，明确双方在数据安全方面的责任及义务，并约定共享数据的内容和用途、使用范围等。

3) 应定期对数据接收方的数据安全保护能力进行评估，确保数据接收方具备足够的数据安全保护能力，当数据接收方丧失数据安全保护能力时，应启动应急响应程序。
4) 应向个人金融信息主体等告知共享数据的目的、数据接收方的类型，并事先征得相应授权。
5) 应帮助个人金融信息主体等了解数据接收方数据的存储、使用等情况。
6) 对共享数据，应执行以下安全控制措施：
   ——共享数据涉及2级、3级数据时，应对数据进行加密处理，并采取数据标记、数据水印等技术，降低数据被泄露、误用、滥用的风险；
   ——应定期对共享的数据进行安全审计；
   ——应配套建立应急响应机制，必要时应及时切断数据共享。
7) 按照国家及行业主管部门有关要求，向行业主管和监管部门等有关机构履行数据报送义务时，应采取有效措施确保数据接收方的身份真实性、数据的保密性、真实性与完整性。

7.5 数据删除

数据删除是指在金融产品和服务所涉及的系统及设备中去除数据，使其保持不可被检索、访问的状态。金融业机构在执行数据删除工作时，安全要求如下：

a) 应依据国家及行业主管部门有关规定及与个人金融信息主体约定的时限等，针对不同类型的数据设定其数据保存期，对于多个不同保存期数据的集合，保存期限选择最长时限为该数据集合的保存期。
b) 超过国家及行业主管部门有关规定、内部规章及合同协议所述保存期限的数据，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。
d) 开发测试、数据分析等金融业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业机构数据删除有关规定，对其使用的有关数据进行删除，记录处理过程，并将处理结果及时反馈至内部数据安全管理部门，由其进行数据删除情况确认。
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，应依据国家及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。
g) 在停止其提供的金融产品或服务时，应对其在提供该金融产品或服务过程中所收集的个人金融信息进行删除或匿名化处理，与个人金融信息主体另有约定的除外，国家及行业主管部门另有规定的按照相关规定执行。
h) 金融产品或服务的用户主动提出删除其数据的情形，如账户注销，应对其相应信息进行删除，与个人金融信息主体另有约定的除外，国家及行业主管部门另有规定的按照相关规定执行。

7.6 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。数据销毁安全要求如下：

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数据销毁，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被利用，具体措施包括但不限于：
   1) 采用数据擦除方式销毁数据时，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) 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，验证数据销毁结果。
   3) 针对数据擦除后擦除失败的存储介质，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) 应采取双人制实施数据销毁，分别作为执行人和复核人，并对数据销毁全过程进行记录，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，销毁时应采用物理销毁的方式对其进行处理，如消磁或磁介质、粉碎、融化等。
g) 4 级数据存储介质的销毁应参照国家及行业涉密载体管理有关规定，由具备相应资质的服务机构或数据销毁部门进行专门处理，并由金融业机构相应岗位人员对其进行全程监督。

8 数据安全组织保障

8.1 组织结构

金融业机构应设立数据安全管理委员会，建立自上而下的覆盖决策、管理、执行、监督四个层面的数据安全管理体系（见图2），明确组织架构和岗位设置，保障数据生命周期安全防护要求的有效落实，要求如下：

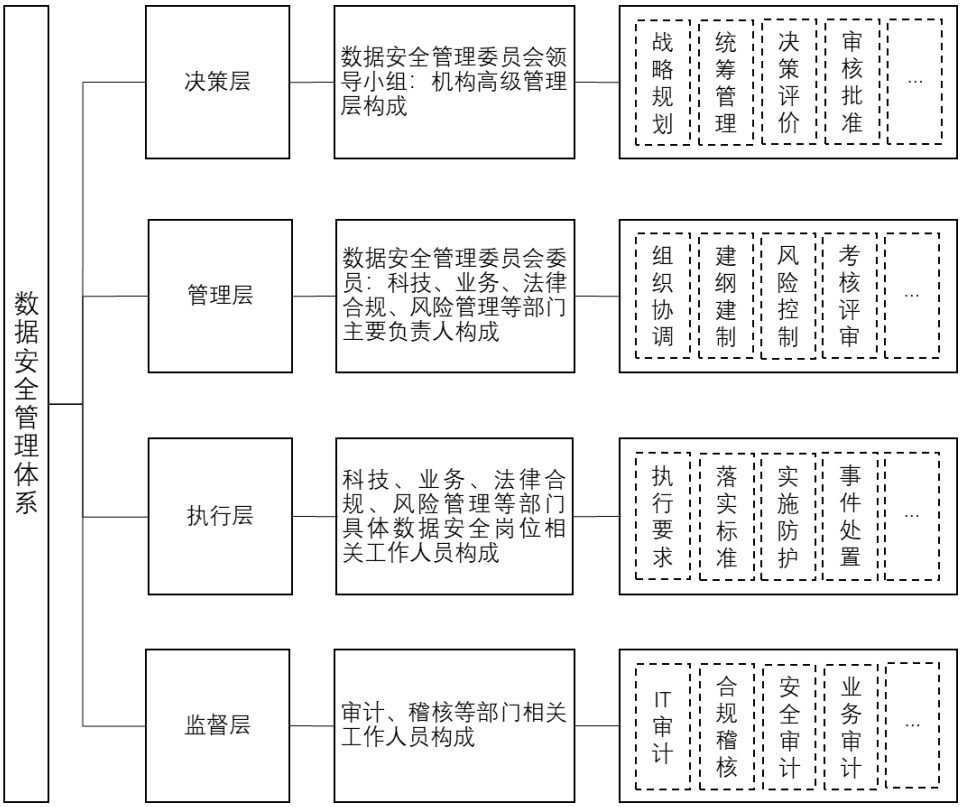


图 2　数据安全管理体系

a) 应设立由金融业机构高级管理层组成的领导小组，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。

b) 委员会成员应至少包含主要部门的主要负责人，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，负责日常数据安全管理工作，具体如下：

   1) 主要部门应至少包括数据安全管理、信息科技、业务、法务、合规、风险管理、稽核审计、人事部门等相关部门。
   2) 制定、发布和更新本机构数据安全管理制度、规程与细则。
   3) 组织开展本机构数据分级工作，识别并维护数据资产清单。
   4) 制定、签发、实施、定期更新隐私政策和相关规程。
   5) 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。
   6) 在金融产品或服务上线发布前组织开展数据安全评估，避免不当的数据采集、使用、共享等行为，如与产品或服务功能及隐私政策不符等情况。

c) 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，作为数据安全管理的执行层，该岗位应履行以下工作职责：

   1) 根据数据安全相关策略和规程，落实本部门数据安全防护措施。
   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。

d) 应明确安全审计、合规稽核、风险管理等相关岗位，作为数据安全管理的监督层，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，确定相应审计策略及规范，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) 公布投诉、举报方式等信息，并及时受理数据安全和隐私保护相关投诉和举报。
4) 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。
5) 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) 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) 建立第三方机构管理制度，并至少满足本文件 8.4 所述要求。
7) 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。
8) 建立数据出境安全控制要求与操作程序。
9) 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。
10) 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。
11) 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。
12) 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。

8.3 人员管理

金融业机构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，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：
      ——数据安全管理岗位、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；
      ——其他金融业机构识别的数据安全关键岗位。
   4) 在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，并至少满足以下要求：
   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) 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管理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，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，强化数据安全管理。

8.4 第三方机构管理

金融业机构应对参与本机构数据全生命周期过程中的第三方机构进行管理，确保不因与第三方机构合作或第三方应用接入而危害数据安全。第三方机构安全管理具体要求如下：

a) 建立第三方机构管理制度，包括但不限于：
   1) 应建立第三方机构审查与评估机制，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) 通过合同协议等方式，对第三方机构的数据使用行为进行约束，包括：
      ——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级及以上数据，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；
      ——未经金融业机构书面授权，第三方机构不应对金融业机构委托其加工处理的数据进行存储、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) 应对第三方机构进行监督，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，定期对受委托者进行安全检查和评估等。
   7) 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。
   8) 国家及行业主管部门另有规定的，应按照相关要求执行。
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，应对接入和涉及的第三方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。
   2) 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。
   3) 应与第三方产品或服务提供方签订合同协议，明确双方在数据安全方面的责任及义务，并明确数据接收方应具备的数据安全保护能力要求。
   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。
   6) 金融业机构发现第三方接入产品和服务在数据处理过程中，对金融业机构个人金融信息的处理超出约定行为，或存在其他违规行为时，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，向监管部门上报。
   7) 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。
   8) 与第三方机构解除合作关系时，应要求第三方机构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，国家及行业主管部门另有规定的除外；若涉及向用户直接提供服务的第三方产品或服务，应在与第三方机构解除合作关系时，明确告知用户金融业机构已解除与第三方机构合作关系。

9 信息系统运维保障

9.1 边界管控

边界管控安全要求如下：

a) 应在内网边界按照“最小权限”原则严格控制外部机构的访问权限，管控措施包括但不限于：防火墙、入侵防御、应用安全防护、API 网关、数据安全防护等。
b) 互联网区和外联接入区为不可控区域，应在内部可控区域与不可控区域之间进行隔离，并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。
c) 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技术手段进行隔离。
d) 应明确生产网络接入和数据传输接口开通相关审批流程。
e) 数据跨边界传输应通过边界设备提供的受控接口进行通信。
f) 对使用 API 进行数据跨域流动的边界，应使用 API 防护技术，对 API 使用者进行身份认证，并对 API 访问行为进行检查，对异常访问行为采取限速、阻断等措施。
g) 应使用设备主动发现等技术及时发现非授权设备私自连接到内部网络的情况，使用网络访问行为管理技术对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) 在内部建立 WLAN 时，接入终端应经过事先审批授权，采取网络准入控制措施，防止终端非法接入内部网络，并应采取终端合规检查、终端安全状态感知等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，应采取代理或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。
j) 应通过多因素认证技术，标识和验证使用者身份，使用设备证书确定设备身份，根据终端常用位置和目前位置、设备属性、安全状态、访问行为等信息动态授权其访问权限。

9.2 访问控制

9.2.1 访问控制策略

访问控制策略安全要求如下：

a) 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，并对各类系统用户设计其工作必需的最小访问权限。
    2) 应依据“业务必需、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) 访问控制策略应使用白名单机制，明确定义允许的行为。
    4) 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。

9.2.2 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，访问控制机制安全要求如下：

a) 数据存储系统应部署在高安全等级区域，存储系统服务器与带库等设备机房出入口应部署电子门禁、视频监控等措施控制、鉴别和记录进入的人员。
b) 第三方机构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，使用明显标识标志其访客身份，由金融业机构人员全程陪同，记录出入时间，并限制和监控其活动范围。
c) 应对包括备份介质在内的存储介质出入库采取措施进行出入库控制，并由金融业机构内部指定岗位人员完成，未经金融业机构授权，任何存储介质不应带离磁带库房。

9.2.3 信息系统与介质访问控制

访问金融数据的业务应用系统访问控制机制安全要求如下：

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经办人员、操作人员、管理人员、审计人员等权限。
   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) 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应满足以下要求：
   1) 控制用户对业务功能的访问范围，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、设置抑制时间和网络登录连接超时自动退出等措施。
d) 对于承载 4 级及以上数据的信息系统，业务系统以及所承载的基础设施的访问，应结合访问者身份及系统安全状态进行访问授权和控制。

9.2.4 数据存储系统的访问控制

数据存储系统存储介质的访问控制机制，安全要求如下：

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平面和管理平面各自可访问的资源策略进行独立配置，并对业务平面和管理平面的相互访问进行隔离。
c) 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。
d) 应对访问存储业务的应用进行鉴别，对应用身份进行唯一标识，并将标识和与其相关的所有可审计事件相关联，且不应存在可绕过鉴别机制的访问方式。
e) 存储 3 级及以上数据的系统应采用数字证书、多因素身份认证等技术对用户进行身份鉴别，并完整记录用户行为，供事后审计。

9.3 安全监测

9.3.1 数据溯源

金融业机构宜具备数据溯源能力，对数据生命周期过程中数据的采集、查询、修改、删除、共享等相关操作进行跟踪，通过留存金融数据流动记录等方式，确保金融数据相关操作行为可追溯。数据溯源安全要求如下：

a) 应制定金融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) 应标识外部数据的来源合法性，并对外部数据的真实性和准确性等数据质量进行评估。
c) 宜建立金融数据资产地图，从数据类型、数据量级、数据特征等维度对金融数据进行盘点和梳理，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) 应记录数据操作过程及关键数据要素，在出现数据泄露事件后可根据泄露的数据进行溯源。
e) 宜构建数据溯源的安全模型，增强数据操作的可追溯性。
f) 应对关键溯源数据进行备份，并采取技术手段对溯源数据和备份数据进行安全保护。
g) 应采取访问控制、加密等技术措施保证溯源数据的安全性。
h) 应以泄露数据为线索，建立对高安全等级数据事件记录进行检索溯源的机制，支持对接口、IP、账号、时间进行溯源集中度分析，定位追踪到相关责任人。
i) 应建立以批量泄露数据、多类型数据作为线索进行溯源的能力，加强基于数据线索的数据溯源分析能力，加强数据溯源的时效性和准确率。
j) 宜建立主体溯源分析能力，对涉及高安全等级数据的疑似泄露事件进行影响范围评估，做好同范围内尚未泄露的数据安全保护工作。

9.3.2 流量分析

金融业机构业务流量分析安全要求如下：

a) 宜采取流量分析技术对数据采集、传输、处理、分析等关键节点进行监测。
b) 应部署以数据为中心的数据流量分析系统，识别并分析高安全等级数据流动情况，包括流动类型、流动范围、数据载体、日均量级、数据账号访问情况、数据流向等信息，并对异常流量、行为等进行告警。
c) 应对比分析流量中数据流动异常情况如不安全的采集设备与采集内容、非授权时段访问高安全等级数据、未授权访问、频繁访问、超量数据传输、多次尝试、批量下载等，及时发现风险问题并进行处置。
d) 宜对比分析数据流量变化和规律，构建数据流动流量基线和高安全等级数据流动基线，及时形成总结报告，并对安全防护措施进行针对性调整。
e) 应对互联网出口流量进行实时检测，发现数据流量异常、数据流向未经授权等行为并及时处置。

9.3.3 异常行为监测

金融业机构应建立日常数据泄露、数据篡改、数据窃取、数据非法使用的风险监控机制，主动预防、发现和终止数据泄露异常行为，有效防范和化解风险，异常行为检测安全要求如下：

a) 应建立异常行为监测指标，包括 IP、账号、数据、使用场景等多个维度，对异常行为事件进行识别、发现、跟踪和监控。
b) 应采取措施监测用户数据访问行为，防止未经授权的数据传输或下载。
c) 宜采取措施监测数据传输过程，并联动管理系统和安全防护设备，记录并预警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。
d) 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，对数据异常使用、用户异常行为进行分析，形成数据安全分析报告，并对异常情况及时处置。

9.3.4 态势感知

金融业机构宜具备有效感知内部数据安全风险并准确定位响应的能力，态势感知安全要求如下：

a) 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、管理平台的审批日志、业务操作日志、数据库日志、流量日志。
b) 宜对账号、IP、数据接口、数据系统、数据设备进行画像，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、数据篡改、数据窃取、数据爬取等安全风险和威胁，并进行可视化展示各类风险和数据流动态势。
c) 宜结合实时安全漏洞资讯、错报等信息对态势感知平台的底层规则进行及时更新。

9.4 安全审计

金融业机构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，审计方式包括但不限于内部审计、外部审计等，具体审计内容安全要求如下：

a) 应制定日志数据管理与安全审计规范，明确日志的存储、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、业务管理员、业务使用者、存储介质用户等。
c) 日志记录内容应包括时间、用户、IP 地址、操作对象、操作内容、操作行为和操作结果等相关信息。
d) 日志内容中不应出现 4 级及以上数据。
e) 包含 3 级数据的日志，对其访问应进行访问控制。
f) 宜搭建数据安全审计系统，对日志进行统一管理和处理，建立并执行审计策略，提供对审计记录进行统计、查询、分析及生成审计报表的功能，形成审计报告反馈相关部门。
g) 应对日志进行备份，避免受到非预期的删除、修改或覆盖等。
h) 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置，并对发现的安全事件和可疑问题进行相应的处置和响应。
i) 应对数据生命周期全过程进行日志记录并开展以数据为中心的安全审计。
j) 应定期对 3 级及以上数据生命周期全过程进行内部审计。
k) 审计记录应至少包括时间的日期和时间、事件类型、主体身份、事件内容、事件结果等。
l) 应对审计记录进行安全保护，防止未授权的访问和输出。
m) 应具备审计记录分权管理能力，可针对不同的角色和组设置审计范围，各组无法看到自己管理的审计范围以外的数据，保证审计数据的安全。
n) 日志和审计记录的留存时间应不少于 6 个月。

9.5 检查评估

金融业机构定期或不定期开展数据安全相关检查和评估，包括合规审查、安全巡检、安全评估等方面，安全要求如下：

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，应及时做好数据安全评估。
c) 在国家及行业主管部门的相关要求发生变化时，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，应进行数据安全评估。
d) 应形成数据安全评估报告，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 1 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，执行管理和技术并重的检查原则，并通过技术工具对相关管理检查内容进行验证和确认。

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） 应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。

9.6 应急响应与事件处置

金融业机构制定应急响应预案，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，安全要求如下：

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） 应依据国家及行业主管部门规定、事件性质、影响范围等，对安全事件进行分级管理。

c） 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。

d） 应按照金融主管部门有关规定，向金融主管部门上报数据安全事件及其处置情况。

e） 发生金融数据泄露事件时，金融业机构应及时采取补救措施，并按照合同协议等有关约定履行客户及合作方告知义务。

f） 数据用于生产事件重现或排查等用途时，应建立相应的数据保护规则，并事前经过审批授权并采取相应的技术保护措施，降低数据泄露、丢失等安全风险。

g） 事件处置结束后，应分析和总结原因和存在的问题，形成调查记录和事件清单，调整数据安全策略，避免事件再次发生，并形成总结报告。

注：金融数据泄露事件：即金融业机构自身的数据安全保护措施被破坏或存在缺陷，导致转移中的、存储的或其他处理中的金融数据被意外或非法销毁、丢失、篡改及未经授权访问等情况。

附 录 A
（资料性）
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、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，可分为从外部机构和从个人金融信息主体处采集数据，见下图。

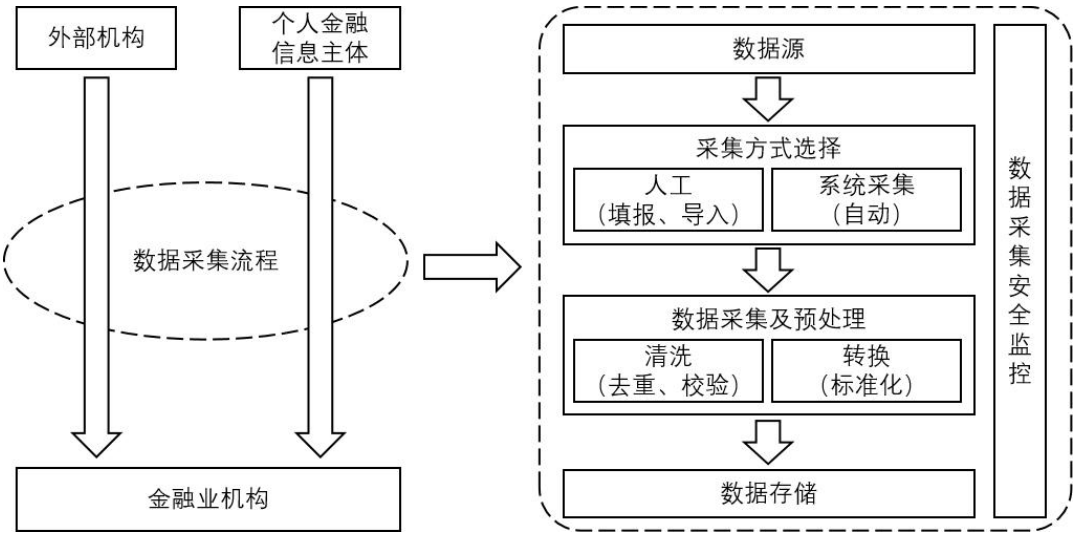


图 金融数据采集模式

金融数据采集流程可涉及：

a) 确定采集的原始数据源及内容：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) 从外部机构采集的数据源包括但不限于：数据库、XML、CSV、Excel、结构化文本、非结构化文件等。
   2) 从金融客户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采集的方式技术。
   1) 从外部机构采集数据的方式包括但不限于：与外部机构合作，通过使用特定系统接口等方式。
   2) 从金融客户采集数据的方式包括但不限于：通过金融业机构柜面、信息系统、自助设备、受理终端、客户端软件等方式。
c) 数据采集及预处理：确定采集方式后，采集的数据经过清洗和标准化转换，存储到数据库中。
d) 数据采集安全监控：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）
数据传输模式

金融数据传输涉及与金融业机构相关联的全通信网络架构。按照传输模式，可分为金融业机构内部数据传输、金融业机构与外部机构或金融客户的数据传输两种，不同传输模式和不同传输对象间所采用的数据传输技术也不同，见下图。

金融业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、子机构内部数据传输，本机构与分、子机构数据传输，以及本机构内部不同数据中心之间数据传输。其中，同一数据中心节点内部数据传输，以及同一分、子机构内部数据传输，通常采用本地局域网方式；本机构与其分、子机构数据传输，以及分、子机构之间数据传输，通常采用VPN或基于专线技术的机构内骨干网方式；本机构内部不同数据中心的数据传输，通常采用VPN、城域网或基于专线技术的机构内骨干网方式。

金融业机构外部数据数据传输包括金融业机构与外部机构数据传输，以及金融业机构与金融客户数据传输。其中，与外部机构数据传输通常采用专线或VPN的方式；与金融客户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、无线互联网等方式。

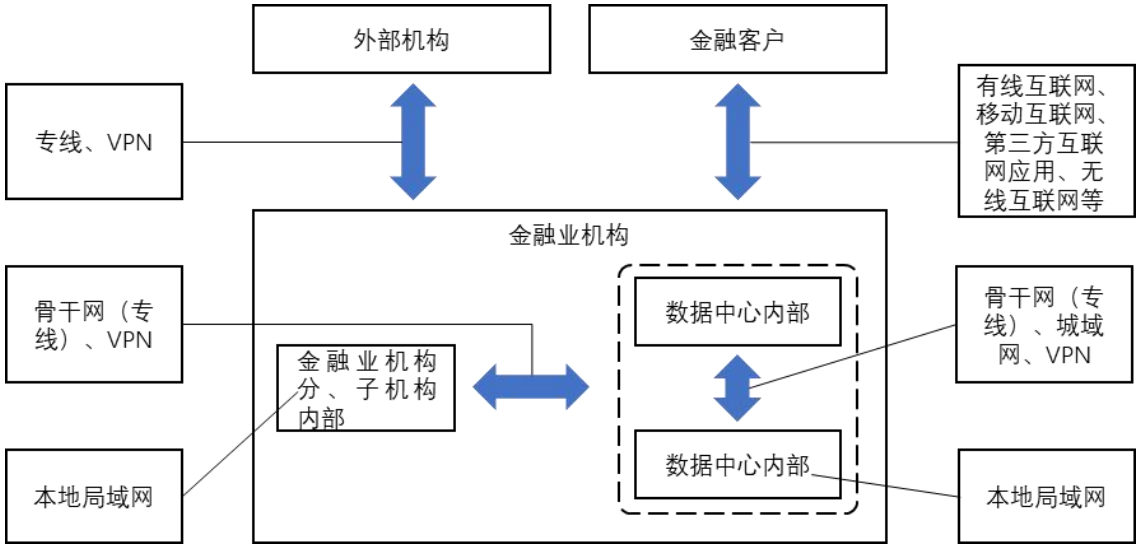


图 金融业机构数据传输模式

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、MSTP、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高安全等级信息，需要注意对信息进行有效的保护。

移动互联网是指通过3G、4G、5G等移动通信技术建立的网络，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业机构服务的形式。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）
数据脱敏

C.1 概述

金融业机构在开展金融数据安全防护工作过程中，对敏感信息的保护是其中尤为重要的环节。金融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多样。金融业机构在业务开展和日常运营过程中，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数据安全，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，对敏感信息的保护已成为金融数据安全应用过程中需首要解决的问题。金融敏感信息通常包括国家规定的敏感信息、业务数据的敏感信息，以及个人金融信息的敏感信息等，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泄露。

C.2 数据脱敏的定义

数据脱敏是指从原始环境向目标环境进行敏感数据交换时，通过一定的方法消除原始环境中数据的敏感性，并保留目标环境业务所需的数据特性或内容的数据处理过程，常用数据脱敏方法技术见表C.1。本附录中数据脱敏主要针对金融行业中的个人金融信息和金融重要数据，其中个人金融信息的脱敏是金融领域隐私保护的一种常见的方式，金融业机构借助数据脱敏技术，消除个人金融信息敏感性，有效保证个人金融信息在企业数据分析、监管协作、开放测试等过程中的安全性。

表C.1 常用数据脱敏方法技术

序号	脱敏方法	脱敏技术	描述	举例说明
1	泛化	规整	将数据按照大小规整到预定义的多个档位	客户产生的业务费用按照金额多少分为高、中、低三个级别 如：0-10 万、10-30 万、30 万及以上→低、中、高
2		偏移取整	数据或者日期进行向上或者向下取整	将时间按照 10 秒钟粒度向下取整 如：20200322 18:08:19→20200322 18:08:10
3		截断	将数据尾部截断，只保留前半部分	保留手机号码前七位，截断剩余部分 如：13500010001→1350001
4	抑制	掩码屏蔽	保持数据长度不变，但只保留数据信息	掩盖手机号码的第四位到第七位 如：13500010001→135****0001
5	扰乱	重排	将原始数据按照特定的规则重新排列，对于跨行数据，采用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	大数据集合且需要保留待脱敏数据特定特征场景下，对数据进行重排 如：22，31，27→31，27，22

序号	脱敏方法	脱敏技术	描述	举例说明
6		加密	对脱敏数据进行对称加密算法、非对称加密算法等加密算法处理，使外部用户只能看到无意义的加密后数据，同时在特定场景下，可提供解密能力，使具有密钥的相关方可获得原始数据	常用对称加密算法，如 DES、3DES、AES 等 常用非对称加密算法，如 RSA、DSA 等 如：123456→U2FsdGVkX19yci4oGpXvMfQJmzBfe9jV
7		替换	如统一将女性性别替换为 F，对内部人员可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	敏感数据都替换为唯一的常数值； 从中间表中随机或按照特定算法选择数据进行替代； 以敏感数据作为输入，通过特定函数形成新的替换数据； 如：女→F
8		散列	对原始数据取散列值，使用散列值来代替原始数据	常用 hash 算法，如 SHA-256、HMAC 等 如：123456→ebe56e057f20f88310adc3949ba59abe
9		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	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；对手机号码，可在一定范围内按照规则随机生成构造数据
10		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	根据数据值的业务场景，增加 1 个固定偏移量； 如：253→1253
11		局部混淆	保持数据中的 n 位不变，混淆其余部分	保持座机号码区号不变的情况下，对其余部分进行混淆 如：0571-123456→0571-328192
12		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	保持余额的总额不变的情况下，对数据进行脱敏
13	有损	限制行数	仅返回可用数据集合中一定行数的数据	后台系统不具备开放式查询能力，严格限制批量查询
14		限制列数	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，不返回如余额、消费记录等敏感列

C.3 数据脱敏基本原则

数据脱敏要确保消除数据的敏感性，尽可能平衡数据脱敏花费的代价、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及代价可控，得到的结果正确且满足业务需要，在实施数据脱敏时，遵循以下原则：

a) 有效性：指数据脱敏过程的有效性，原始数据经脱敏处理后，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) 高效性：指数据脱敏过程的高效性，通过借助计算机程序实现脱敏自动化，并可重复执行，在不影响有效性的前提下，平衡脱敏的力度和代价，将数据脱敏工作控制在一定的时间和经济成本内。

c) 可重现：即相同原始数据在配置相同算法和参数的情况下，脱敏后的数据具有一致性，随机类的算法除外。

d) 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，数据的关联性较高。

e) 可配置性：指数据脱敏过程的可配置性，由于不同场景下的安全需求不同，数据脱敏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需求提供不同的脱敏数据。

C.4 数据脱敏方法技术

C.4.1 泛化

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，具体的技术方法包括但不限于：

a) 截断：直接舍弃业务不需要的信息，仅保留部分关键信息，数据截断后的结果往往无法较好地保持原有业务属性，因此在对数据截断时，根据数据特点酌情选择截断位数。

示例：1）将手机号码12300010001截断为1230001。

2）把身份证号码123184198501184115截断为198501184115。

b) 偏移取整：按照一定粒度对数据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数据原始属性，偏移取整的方法主要通过舍弃一定的精度来保证原始数据的安全性，可一定程度上保持数据业务特性上的分布密度，适用于粗略统计分析的场景。

示例：1）将时间20200322 18:08:19按照10秒钟粒度向下取整得到20200322 18:08:10。

2）将金额5123.62元按照百位粒度向上取证得到5100元。

c) 规整：将数据按照大小规整到预定义的多个档位，规整的方法尽管保持了一定的业务含义，但是很大程度上会丧失数据原有的精度，可根据实际的业务需要选择泛化技术的实现方法。

示例：1）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。

2）客户产生的业务费用按照金额多少分为高、中、低三个级别，将客户业务费用用这三个级别代替。

C.4.2 抑制

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。

a) 掩码屏蔽：指保留部分信息，对敏感数据的部分内容用通用字符（如“X、*”等）进行统一替换，从而使得敏感数据保持部分内容公开，但对信息持有者来说易于辨别。

示例：1）将手机号码12300010001经过掩码得到123****0001。

2）把身份证号码123184198501184115经过掩码得到为123184000000004115。

b） 个人金融信息在通过计算机屏幕、客户端应用软件等界面展示过程中，采取信息掩码屏蔽或截词等技术措施对数据实施脱敏，从而降低数据泄露的风险。

示例：将银行卡号码1234701202106563320经过掩码得到1234**********3320。

C.4.3 扰乱

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，对于跨行数据，采用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。

1） 采用按照一定顺序打乱数据位序等方式进行重排。

2） 重排可在相当大范围内保证部分业务数据信息，如有效数据范围、数据统计特征等，使脱敏后数据看起来跟原始数据更一致，与此同时也牺牲了一定的安全性，一般重排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，重排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。

b） 加密：对脱敏数据进行对称加密算法、非对称加密算法等常规加密算法处理，使外部用户只能看到无意义的加密后的数据，同时在特定场景下，可提供解密能力，使具有密钥的相关方可获得原始数据。

1） 采用对称或非对称加密算法对数据进行加密存储。

2） 加密其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，这种方法的缺点是：加密本身需要一定的计算能力，对于大数据集来源会产生很大资源开销。一般加密后数据与原始数据格式差异较大，“真实性”较差。

c） 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。

1） 常数替换：所有敏感数据都替换为唯一的常数值，具有不可逆性。

2） 查表替换：从中间表中随机或按照特定算法选择数据进行替代。

3） 参数化替换：以敏感数据作为输入，通过特定函数形成新的替换数据。

d） 散列：即对原始数据取散列值，使用散列值来代替原始数据。

1） 使用散列函数对客户密码等信息进行计算得到散列值，以此替换原始数据。

2） 为了保证散列的安全性，避免采用弱安全性散列函数如 MD5、SHA1，对于原文空间有限的散列，实际的应用场景中通常采用加入随机因子的方法提高安全性，散列函数常用于密码等敏感信息存储的场景。

e） 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。

f） 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。

g） 局部混淆：保持前面 n 位不变，混淆其余部分。

h） 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。

i） 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，这种方法通常用于成本表、工资表等场合。

C.4.4 有损

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，金融后台系统不具备开放式查询能力，根据业务场景需要采用合适的有损技术可达到限制批量查询的效果。具体的有损技术方法包括但不限于：

a) 限制行数：仅仅返回可用数据集合中一定行数的数据，多应用于不具备开放式查询能力的后台系统、严格限制批量查询等场景。

b) 限制列数：仅仅返回可用数据集合中一定列数的数据，可应用于人员基本信息查询时，限制或禁止返回的数据集中包含某些敏感列。

C.5 数据脱敏应用分类

C.5.1 概述

数据脱敏根据数据脱敏的实时性和应用场景的不同，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.5.2 静态数据脱敏

静态数据脱敏旨在通过类似ETL技术的处理方式，按照脱敏规则一次性完成大批量数据的变形转换处理，静态脱敏示意图见图C.1。静态脱敏通常会在将生产环境中的敏感数据交付至开发、测试或者外发环境时使用，在降低数据敏感程度的同时，能够最大程度上保留原始数据集所具备的数据内在关联性等可挖掘价值。

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，通过定制数据隐私政策满足不同业务需求。

图C.1 静态脱敏示意图

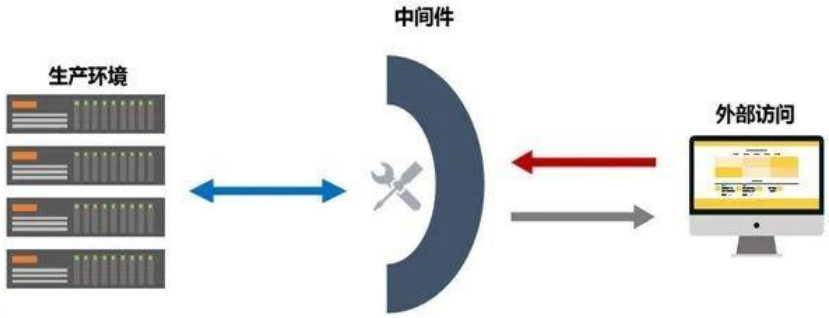
C.5.3 动态数据脱敏

动态数据脱敏旨在通过类似网络代理的中间件技术，按照脱敏规则对于外部申请访问的数据进行即时处理并返回脱敏后结果，动态脱敏示意图见图C.2。动态脱敏通常会在数据对外提供查询服务的场景中使用，在降低数据敏感程度的同时，最大程度上降低了需求方获取脱敏后数据的延迟，请求实时产生的数据也能即时得到脱敏后结果。动态数据脱敏主要特点如下：

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平台间、不同应用程序或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。



图C.2 动态脱敏示意图

C.6 数据脱敏应用场景

数据脱敏的应用场景主要分为技术场景和业务场景，技术场景主要包括开发测试、数据分析、数据科学研究、生产、数据交换、运维等场景，业务场景包括但不限于信贷风险评估、骗保识别、精准营销、消费信贷等场景，常用数据脱敏应用场景见表C.2。

表C.2 常用数据脱敏应用场景

序号	场景分类	脱敏场景	场景描述	动态脱敏	静态脱敏
1	技术场景	开发测试应用场景	金融行业开发使用的业务系统中存在大量的客户敏感信息，如姓名、年龄、手机号码、银行卡号码、地址、工作信息等，在系统建设前期，往往需要使用上述信息进行开发测试，此时需要使用脱敏技术来保证客户敏感信息不被泄露。		√
2		数据分享应用场景	数据分享应用场景在一些特定需求下，部分隐私数据需要提供给其他机构或企业，但对其他隐私数据可进行抑制、扰乱等操作。		√
3		数据科学研究应用场景	数据科学研究应用场景，其主要目的是通过数据进行研究，因此需要保留数据本身的一些特征。研究时需要保留的数据特征可能是用户的年龄信息、性别信息、地区信息、行为记录等。但不需要保证保留用户身份信息和全部的敏感字段，只需要保留研究所必须的内容即可。		√
4		生产应用场景	生产场景主要指各类业务场景，当涉及访问敏感数据时，需要对部分敏感数据做脱敏，这种场景下往往采用掩码屏蔽的方式对数据进行脱敏。	√	

序号	场景分类	脱敏场景	场景描述	动态脱敏	静态脱敏
5		数据交换应用场景	数据交换场景主要是通过API接口方式向特定平台提供数据，与生产应用场景相比，数据请求时会附带用户信息，需要对部分用户信息进行脱敏。	√	
6		运维应用场景	运维人员需要对数据库进行监控、维护，但对内部数据是不需要进行了解的，对于高敏感的数据采取脱敏的措施。	√	
7	业务场景	精准营销	融合金融业务数据和外部可信数据，借助大数据技术构建金融个人客户画像（人口统计学特征、消费能力数据、兴趣数据、风险偏好等）和企业客户画像（企业的生产、流通、运营、财务、销售和客户数据、相关产业链上下游等数据），并有效的开展精准营销，包括根据客户的实时状态来进行营销；不同业务或产品的交叉推荐；根据客户的喜欢进行服务或者产品进行个性化推荐等。这类大数据应用前台一般采用掩码屏蔽的方式对数据进行脱敏，后台一般采用干扰等方式对数据进行脱敏。	√	√
8		骗保识别	借助大数据手段，保险企业可结合内部、第三方和社交媒体数据进行早期异常值检测，包括了客户的健康状况、财产状况、理赔记录等，通过建设保险欺诈识别模型，大规模的识别近年来发生的所有赔付事件，并及时采取干预措施，减少先期赔付，显著提升骗保识别的准确性与及时性，这类大数据应用前台一般采用掩码屏蔽的方式对数据进行脱敏，后台一般采用干扰等方式对数据进行脱敏。	√	√
9		风控管理	基于企业内外部交易和历史数据，利用客户基本信息、账号基本信息、交易历史、客户历史行为模式、正在发生行为模式等，结合智能规则引擎，实时或准实时预测和分析欺诈等非法行为，主要用于信贷业务和欺诈防范，并与目前的征信建设相结合，如商户评分模型及审批规则、行业风险识别模型、人民银行征信报告评分模型、个人信用分析模型、风险客户预警模型、贷后实时监控模型、反欺诈模型等。这类大数据应用前台一般采用掩码屏蔽的方式对数据进行脱敏，后台一般采用干扰等方式对数据进行脱敏。	√	√
10		智能投顾	基于客户的风险偏好、海量个人投资者真实投资交易信息的深入挖掘分析、交易行为分析，依靠大数据量化模型，洞悉交易个人投资者交易行为的变化、投资信心的状态与发展趋势、对市场的预期以及当前的风险偏好等信息，给客户更高的投资方案和投资产品推荐等投资顾问服务。这类大数据应用前台一般采用掩码屏蔽的方式对数据进行脱敏，后台一般采用干扰等	√	√

序号	场景分类	脱敏场景	场景描述	动态脱敏	静态脱敏
			方式对数据进行脱敏。		

C.7 隐私数据脱敏方法参考

C.7.1 联系人姓名的脱敏

联系人姓名的脱敏方法示例见表C.3。

表C.3 联系人姓名的脱敏方法示例

敏感数据类型		联系人姓名
格式		联系人姓名与身份证姓名格式一致，为若干个汉字
开发测试应用场景	脱敏技术	查表替换
	脱敏规则	根据姓名字典表替换成具有姓名特征的随机化姓名
	脱敏示例	张三→李四；王五→牛六；令狐冲→欧阳峰
数据分享应用场景	脱敏技术	局部混淆、掩码屏蔽、数据截断等
	脱敏规则	局部混淆为例：保持姓不变，名部分随机
	脱敏示例	张三→张华，李德峰→李得风；独孤求败→独孤峰；阿不都沙拉克→阿布都杰克
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	3 个字内隐藏第 1 个字，4-6 个字隐藏前 2 个字，大于 6 个字隐藏第 3-6 个字，隐藏字用*号代替
	脱敏示例	张三→*三，李德峰→*德峰；独孤求败→**求败；阿不都沙拉克→阿不****
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	局部混淆、掩码屏蔽、数据截断等
	脱敏规则	局部混淆为例：保持姓不变，名部分随机
	脱敏示例	张三→张华，李德峰→李得风；独孤求败→独孤峰；阿不都沙拉克→阿布都杰克

C.7.2 企业户名的脱敏

企业户名的脱敏方法示例见表C.4。

表C.4 企业户名的脱敏方法示例

敏感数据类型		企业户名
格式		企业类户名与营业执照一致，为公司名称，由若干个汉字组成
开发测试应用场景	脱敏技术	局部混淆
	脱敏规则	保留后 6 位，其余部分混淆

敏感数据类型		企业户名
	脱敏示例	阿里拉拉科技有限公司→眺望远方科技有限公司
数据分享应用场景	脱敏技术	限制列数、掩码屏蔽、局部混淆等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	按长度分阶梯保留：长度 4 个字及以下的，首尾各保留 1 个字；长度 5-6 个字的，首尾各保留 2 个字；长度 7 个字及以上奇数的，隐去中间 3 个字；长度 8 个字及以上偶数，隐去中间 4 个字；隐藏字用*号代替
	脱敏示例	北京大学→北**学；中国农业银行→中国**银行；青岛金星化工厂→青岛***化工厂；青岛金龙印染有限公司→青岛金****限公司
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	掩码屏蔽
	脱敏规则	按长度分阶梯保留：长度 4 个字及以下的，首尾各保留 1 个字；长度 5-6 个字的，首尾各保留 2 个字；长度 7 个字及以上奇数的，隐去中间 3 个字；长度 8 个字及以上偶数，隐去中间 4 个字；隐藏字用*号代替
	脱敏示例	北京大学→北**学；中国农业银行→中国**银行；青岛金星化工厂→青岛***化工厂；青岛金龙印染有限公司→青岛金****限公司

C.7.3 身份证号码的脱敏

身份证号码的脱敏方法示例见表C.5。

表C.5 身份证号码的脱敏方法示例

敏感数据类型		身份证号码
格式		18 位数字，号段 3 位+归属地编号 4 位+流水号 4 位
开发测试应用场景	脱敏技术	查表替换
	脱敏规则	根据身份证号码映射表替换成随机的身份证号码
	脱敏示例	123100199903032000→123424198702112909
数据分享应用场景	脱敏技术	限制列数
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留前 12 位，后 6 位用*代替

敏感数据类型		身份证号码
	脱敏示例	123001988032013 87→123000198803******
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	限制列数
	脱敏规则	隐藏或删除姓名字段
	脱敏示例	/

C.7.4 护照号码的脱敏

护照号码的脱敏方法示例见表C.6。

表C.6 护照号码的脱敏方法示例

敏感数据类型		护照号码
格式		1 位字母+8 位数字，字母代表护照种类，数字为流水号
开发测试应用场景	脱敏技术	唯一值映射
	脱敏规则	通过唯一值映射将护照映射为非真实的护照号码
	脱敏示例	G12345678→G87654321
数据分享应用场景	脱敏技术	限制列数
	脱敏规则	隐藏或删除本字段
	脱敏示例	/
数据科学研究应用场景	脱敏技术	限制列数
	脱敏规则	隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留 1 位字母和最后 3 位数字，其余用*代替
	脱敏示例	G12345678→G*****678
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	数据截断、局部混淆、掩码屏蔽等
	脱敏规则	数据截断为例：保留前 4 位，截断剩余位数
	脱敏示例	G12345678→G123

C.7.5 地址的脱敏

地址的脱敏方法示例见表C.7。

表C.7 地址的脱敏方法示例

敏感数据类型	地址
格式	格式不固定，为不定长的字符串

敏感数据类型		地址
开发测试应用场景	脱敏技术	查表替换
	脱敏规则	根据地址映射表替换成随机的地址
	脱敏示例	浙江省杭州市南街胡同口→江苏省南京市北街弄堂里
数据分享应用场景	脱敏技术	数据截断
	脱敏规则	保留省市，其余截断
	脱敏示例	浙江省杭州市西湖区胡同口→浙江省杭州市
数据科学研究应用场景	脱敏技术	数据截断
	脱敏规则	保留省市区（县），其余截断
	脱敏示例	浙江省杭州市西湖区胡同口→浙江省杭州市西湖区
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	按长度分阶梯保留：长度 5 个字及以下的，保留第 1 个字和最后 2 个字；长度 6-9 个字的，保留最后 5 个字；长度为 10 个字及以上的，隐去最后 5 个字之前的 4 个字；隐藏字用*代替
	脱敏示例	浙江省杭州市西湖区胡同口→浙江省****湖区胡同口
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	数据截断
	脱敏规则	保留省市区（县），其余截断
	脱敏示例	浙江省杭州市西湖区胡同口→浙江省杭州市西湖区

C.7.6 车牌号码的脱敏

车牌号码的脱敏方法示例见表C.8。

表C.8 车牌号码的脱敏方法示例

敏感数据类型		车牌号码
格式		1 个汉字+1 个字母+5 位字母和数字组合流水号，流水号前为地区编码
开发测试应用场景	脱敏技术	查表替换
	脱敏规则	根据车牌号码映射表替换成随机的车牌号码
	脱敏示例	鲁 AB1234→鲁 A84321
数据分享应用场景	脱敏技术	数据截断
	脱敏规则	保留前 2 位地区编码，其余截断
	脱敏示例	鲁 AB1234→鲁 A
数据科学研究应用场景	脱敏技术	数据截断
	脱敏规则	保留前 2 位地区编码，其余截断
	脱敏示例	鲁 AB1234→鲁 A
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留地区编码和流水号最后 2 位，其余用*代替
	脱敏示例	鲁 AB1234→鲁 A**234

敏感数据类型		车牌号码
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留地区编码和流水号最后 2 位，其余用*代替
	脱敏示例	鲁 AB1234→鲁 A**234

C.7.7 联系电话（固定电话）的脱敏

联系电话（固定电话）的脱敏方法示例表C.9。

表C.9 联系电话（固定电话）的脱敏方法示例

敏感数据类型		联系电话（固定电话）
格式		区号+3-4 位区域信息+4 位流水号
开发测试应用场景	脱敏技术	查表替换
	脱敏规则	根据固定电话特征表替换成随机的固定电话
	脱敏示例	0531-12345678→0531-43214231
数据分享应用场景	脱敏技术	数据截断、局部混淆、掩码屏蔽等
	脱敏规则	数据截断为例：保留前 4 位，截断剩余位数
	脱敏示例	0531-12345678→0531
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	区号不隐藏，7-8 位电话号码保留最后 3 位，其余用*代替
	脱敏示例	0531-12345678→0531-*****678
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	数据截断、局部混淆、掩码屏蔽等
	脱敏规则	数据截断为例：保留前 4 位，截断剩余位数
	脱敏示例	0531-12345678→0531

C.7.8 联系电话（手机号码）的脱敏

联系电话（手机号码）的脱敏方法示例见表C.10。

表C.10 联系电话（手机号码）的脱敏方法示例

敏感数据类型		联系电话（手机号码）
格式		11 位数字，号段 3 位+归属地编号 4 位+流水号 4 位
开发测试应用场景	脱敏技术	查表替换

敏感数据类型		联系电话（手机号码）
	脱敏规则	根据手机号码特征表替换成随机的手机号码
	脱敏示例	12319007127→12329193818
数据分享应用场景	脱敏技术	限制列数
	脱敏规则	隐藏或删除企业户名字段
	脱敏示例	/
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留前 3 位和最后 3 位，其余用*代替
	脱敏示例	12300172387→123*****387
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	数据截断、局部混淆、掩码屏蔽等
	脱敏规则	以数据截断为例：保留前 3 位，截断剩余位数
	脱敏示例	12300172387→123

C.7.9 日期时间的脱敏

日期时间的脱敏方法示例表C.11。

表C.11 日期时间的脱敏方法示例

敏感数据类型		日期时间
格式		年月日时分秒
开发测试应用场景	脱敏技术	查表替换
	脱敏规则	根据日期映射表替换成对应的日期
	脱敏示例	2020 年 1 月 28 日 13 时 24 分 15 秒→1999 年 2 月 10 日 12 时 33 分 1 秒
数据分享应用场景	脱敏技术	数据截断、局部混淆、掩码屏蔽等
	脱敏规则	以数据截断为例：保留年月信息，截断剩余部分
	脱敏示例	2020 年 1 月 28 日 13 时 24 分 15 秒→2020 年 1 月
数据科学研究应用场景	脱敏技术	偏移取整
	脱敏规则	将时间按照分钟粒度取整
	脱敏示例	2020 年 1 月 28 日 13 时 24 分 15 秒→2020 年 1 月 28 日 13 时 24 分
生产应用场景	脱敏技术	数据截断、局部混淆、掩码屏蔽等
	脱敏规则	以数据截断为例：保留年月日，截断剩余位数
	脱敏示例	2020 年 1 月 28 日 13 时 24 分 15 秒→2020 年 1 月 28 日
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	

敏感数据类型		日期时间
运维应用场景	脱敏技术	数据截断、局部混淆、掩码屏蔽等
	脱敏规则	以数据截断为例：保留年月日，截断剩余位数
	脱敏示例	2020 年 1 月 28 日 13 时 24 分 15 秒→2020 年 1 月 28 日

C.7.10 电子邮箱的脱敏

电子邮箱的脱敏方法示例见表C.12。

表C.12 电子邮箱的脱敏方法示例

敏感数据类型		电子邮箱
格式		电子邮箱名+@+电子邮件服务器地址
开发测试应用场景	脱敏技术	局部混淆
	脱敏规则	混淆电子邮箱名，保留@+电子邮件服务器地址的部分
	脱敏示例	tony@xxx.com→martin@xxx.com
数据分享应用场景	脱敏技术	掩码屏蔽
	脱敏规则	“@”前小于等于 5 位的，隐藏前 2 位；大于 5 位的，保留前 3 位，其余用*号代替
	脱敏示例	tony@xxx.com→**ny@xxx.com
数据科学研究应用场景	脱敏技术	掩码屏蔽
	脱敏规则	“@”前小于等于 5 位的，隐藏前 2 位；大于 5 位的，保留前 3 位，其余用*号代替
	脱敏示例	tony@xxx.com→**ny@xxx.com
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	“@”前小于等于 5 位的，隐藏前 2 位；大于 5 位的，保留前 3 位，其余用*号代替
	脱敏示例	tony@xxx.com→**ny@xxx.com
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	掩码屏蔽
	脱敏规则	“@”前小于等于 5 位的，隐藏前 2 位；大于 5 位的，保留前 3 位，其余用*号代替
	脱敏示例	tony@xxx.com→**ny@xxx.com

C.7.11 密码的脱敏

密码的脱敏方法示例见表C.13。

表C.13 密码的脱敏方法示例

敏感数据类型		密码
格式		5-30 位不定长大写字母、小写字母、数字、下划线、减号、点的组合
开发测试应用场景	脱敏技术	限制列数
	脱敏规则	隐藏或删除本字段
	脱敏示例	/
数据分享应用场景	脱敏技术	限制列数

敏感数据类型		密码
	脱敏规则	隐藏或删除本字段
	脱敏示例	/
数据科学研究应用场景	脱敏技术	限制列数
	脱敏规则	隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	全遮盖
	脱敏示例	123456>******
数据交换应用场景	脱敏技术	限制列数
	脱敏规则	隐藏或删除本字段
	脱敏示例	/
运维应用场景	脱敏技术	限制列数
	脱敏规则	隐藏或删除本字段
	脱敏示例	/

C.7.12 金融账号的脱敏

金融账号的脱敏方法示例表C.14。

表C.14 金融账号的脱敏方法示例

敏感数据类型		金融账号
格式		5-30 位不定长大写字母、小写字母、数字等字符的组合
开发测试应用场景	脱敏技术	唯一值映射
	脱敏规则	通过唯一值映射将金融账号映射为非真实的金融账号
	脱敏示例	victlr1011→htilrh2038
数据分享应用场景	脱敏技术	掩码屏蔽
	脱敏规则	分段屏蔽，每隔 2 位用*替换 2 位
	脱敏示例	victlr1011→vi**lr**11
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	分段屏蔽，每隔 2 位用*替换 2 位
	脱敏示例	victlr1011→vi**lr**11
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	限制列数、局部混淆、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除姓名字段
	脱敏示例	/

C.7.13 银行卡号码的脱敏

银行卡号码的脱敏方法示例见表C.15。

表C.15 银行卡号码的脱敏方法示例

敏感数据类型		银行卡号码
格式		13-19 位数字，开户行编号+卡种编号+流水号
开发测试应用场景	脱敏技术	唯一值映射
	脱敏规则	通过唯一值映射将银行卡号码映射为非真实的银行卡号码
	脱敏示例	1234567890123456789→1234890123113433320
数据分享应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留前 6 位和最后 4 位，中间用*代替
	脱敏示例	1234567890123456789→123456**********6789
数据科学研究应用场景	脱敏技术	限制列数
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留前 6 位和最后 4 位，中间用*代替
	脱敏示例	1234567890123456789→123456**********6789
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	掩码屏蔽、数据截断、局部混淆等
	脱敏规则	掩码屏蔽为例：保留前 4 位和最后 4 位，中间用*代替
	脱敏示例	1234567890123456789→123456**********6789

C.7.14 存折账号的脱敏

存折账号的脱敏方法示例见表C.16。

表C.16 存折账号的脱敏方法示例

敏感数据类型		存折账号
格式		14-19 位数字，开户行编号+存折类型编号+流水号
开发测试应用场景	脱敏技术	唯一值映射
	脱敏规则	通过唯一值映射将存折账户映射为非真实的存折账户
	脱敏示例	12345601100413825→12345*********3825
数据分享应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留前 4 位和最后 4 位，中间用*代替
	脱敏示例	12345601100413825→1234*********3825
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/

敏感数据类型		存折账号
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留前 4 位和最后 4 位，中间用*代替
	脱敏示例	12345601100413825→1234*********3825
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	掩码屏蔽、数据截断、局部混淆等
	脱敏规则	掩码屏蔽为例：保留前 4 位和最后 4 位，中间用*代替
	脱敏示例	12345601100413825→1234*********3825

C.7.15 增值税税号的脱敏

增值税税号的脱敏方法示例见表C.17。

表C.17 增值税税号的脱敏方法示例

敏感数据类型		增值税税号
格式		15-20 位不定长数字，2 位省市代码+4 位地区代码+2 位经济性质代码+2 位行业代码+流水号
开发测试应用场景	脱敏技术	唯一值映射
	脱敏规则	通过唯一值映射将增值税税号映射为非真实的增值税税号
	脱敏示例	12345600609102381D→xxx123006022123411
数据分享应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留前 4 位和最后 4 位，中间用*代替
	脱敏示例	12345600609102381D→1234**********381D
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留前 4 位和最后 4 位，中间用*代替
	脱敏示例	12345600609102381D→1234**********381D
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	掩码屏蔽、数据截断、局部混淆等
	脱敏规则	掩码屏蔽为例：保留前 4 位和最后 4 位，中间用*代替
	脱敏示例	12345600609102381D→1234**********381D

C.7.16 增值税账号的脱敏

增值税账号的脱敏方法示例见表C.18。

表C.18　增值税账号的脱敏方法示例

敏感数据类型		增值税账号
格式		8-28 位数字，为银行对公账户，开户行编号+卡种编号+流水号
开发测试应用场景	脱敏技术	唯一值映射
	脱敏规则	通过唯一值映射将增值税账号映射为非真实的增值税账号
	脱敏示例	12345616627053002257→12345616627078622384
数据分享应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留最后 4 位，其余用*代替
	脱敏示例	12345616627053002257→**********2257
数据科学研究应用场景	脱敏技术	限制列数、掩码屏蔽等
	脱敏规则	限制列数为例：隐藏或删除本字段
	脱敏示例	/
生产应用场景	脱敏技术	掩码屏蔽
	脱敏规则	保留最后 4 位，其余用*代替
	脱敏示例	12345616627053002257→**********2257
数据交换应用场景	脱敏技术	同生产应用场景
	脱敏规则	
	脱敏示例	
运维应用场景	脱敏技术	掩码屏蔽、数据截断、局部混淆等
	脱敏规则	掩码屏蔽为例：保留最后 4 位，其余用*代替
	脱敏示例	12345616627053002257→**********2257

附 录 D
（资料性）
数据水印

D.1 概述

金融业机构在开展金融数据安全防护工作过程中，越来越多的数据库数据通过网络进行存储和发布，这些数据往往包含各类敏感信息，即使脱敏后仍然有巨大的社会价值与经济价值，如果不采取有效的安全控制和版权保护措施，会给攻击者可乘之机。在缺乏数据库完整性验证的有效措施时，一旦出现数据泄露，后果也是无法想象的。因此，需要使用数据水印技术在数据交换及数据使用中的分发共享、委托处理等环节标明数据的来源、分发对象、分发时间、分发途径及使用范围等。当出现数据泄露事件时，可从植入的数据水印信息中还原上述信息，达到追溯泄露途径、追责泄露人员的目的，避免相同类型的数据泄露事件发生。

D.2 数据水印的定义

数据水印是指从原始环境向目标环境进行敏感数据交换时，通过一定的方法向数据中植入水印标记，从而使数据具有可识别分发者、分发对象、分发时间、分发目的等因素，同时保留目标环境业务所需的数据特性或内容的数据处理过程。数据水印具有隐蔽性、可追溯性、确定性等特点。

D.3 数据水印基本原则

数据水印为了能够进行分发追溯，同时又要避免植入水印干扰正常数据的使用，设计基本原则如下：

a) 可追溯性：保证植入数据中水印的有效性，当包含了数据水印内容的数据泄露时，可追溯出其中包含的信息。
b) 仿真性：保证植入数据水印的真实性，数据水印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，且不会破坏原有数据的可读性。
c) 部分有效性：保证用于追溯信息的包含数据水印的泄露数据并不需要全部内容，只需要部分数据，即可追溯完整水印信息。
d) 可配置性：保证数据水印过程的可配置性，由于需要植入的水印不同，数据水印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，生成不同的水印结果。
e) 安全性：嵌入在原始数据中的水印是不可除的，且能够提供完整的版权证据，数据水印不会因为数据的某种改动而导致水印信息丢失的能力，数据水印能保持完整性或仍能被准确鉴别。

D.4 数据水印技术方法

D.4.1 伪行水印

伪行水印指在对某些外发数据添加水印时，通过添加人为生成的若干整行信息，并从中挑选某些字段植入水印信息的技术。这些筛选的植入水印的字段一般常见于身份证号码、电话号码、银行卡号码、交易金额等字段。

伪行水印主要处理步骤为：基于对数据表结构分析和数据类型分析，识别主键表和外键表；确定主键值的处理方式，自动生成或者手动生成；识别敏感数据字段，在伪行水印库中选取添加的数据类型与敏感字段匹配；对其他数据字段进行同类型数据的生成；选择生成数据的分组策略，分组策略主要解决伪行数据生成的行数及伪行数据在原始数据中如何分布；根据设置生成伪行数据，并在伪行数据中自动嵌入水印标记，伪行水印处理步骤见图 D.1。

图D.1　伪行水印处理步骤

D.4.2　伪列水印

伪列水印指通过对分发数据中，人为构造增加一列，并在其中植入水印的机制。

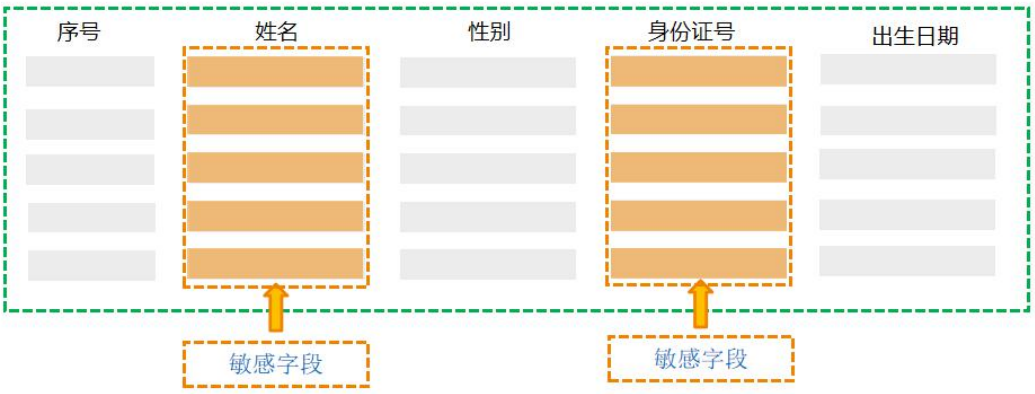
伪列水印主要处理步骤为：基于对数据表结构分析和数据类型分析，在伪列水印库中选取添加的数据类型，然后根据水印的类型，系统生成与原始数据量一致的伪列数据，并在伪列的数据中自动插入水印标记，伪列水印处理步骤见图 D.2。

图D.2　伪列水印处理步骤

D.4.3　脱敏水印

脱敏水印指在增加行和列的情况下，通过对原始数据中某些字段按照一定的水印植入规则进行脱敏变形，产生的脱敏后数据植入了水印信息的技术。

脱敏水印主要处理步骤为：基于对数据表结构分析和敏感数据发现分析，识别敏感字段。根据识别的敏感字段，选择相应的数据变形算法，对数据进行变形处理，在数据过程中添加水印标识到变形后的数据中。在数据置换的数据变形方式下，对数据置换的可逆编码记录并结合水印标记信息生成新的变形后数据，生成带有水印标记信息的数据，脱敏水印处理步骤见图 D.3。



图D.3　脱敏水印处理步骤

D.4.4　水印添加

水印添加的一般步骤如下：

a）　数据初始化，数据库表包含有多个元组，每个元组的数据模式可用 R=（Pk，F1，F2…Fn，Fk），其中 R 代表元组，Pk 代表主键，Fk 为外键，F1，F2…Fn 为属性；在属性中包含有部分敏感信息，定义 C 为数据库中包含敏感属性的表的集合，对 C 进行数据抽取形成数据子集 S，S 中含有 1 个或多个表，S 中表的属性含有敏感信息，S 中表之间具有一定的关系，比如主外键表。

b）　定义伪行伪列字段规则，字段规则根据敏感数据属性含义和数据类型进行定义；敏感数据属性定义会根据数据属性含义和数据类型结合，敏感数据属性往往具有明显的数据特征和数据类型；首先将分离出敏感数据属性，根据敏感数据属性的类型、值域范围及限定规则，抽象出敏感数据属性的规则，数据值型数据将通过正则表达式方式抽取数据属性规则，字符型属性可通过正则表达式方式或进行值域范围分解抽取数据属性规则。

c）　对数据进行字段规则配置，选择数据子集 S 中 1 个或多个表的属性，进行伪行字段或者伪列字段规则配置；首先选择指定的表，根据表中的已有字段属性分布情况，选择采用伪行或伪列方式嵌入水印信息；选择伪行时，对表中已有字段属性进行规则定义，选择字段属性配置对应的伪行字段规则，由于表中字段属性会很多，限制至少两个字段属性需要配置，其余字段属性按默认值，配置生成的数据行比例因子；选择伪列时，直接配置对应的伪列字段规则，生成的数据行比例因子为 1。

d）　水印数据的生成，根据选择的字段规则，进行水印数据的生成；伪行或伪列水印处理根据字段规则配置生成数据行或数据列，生成的数据中对应规则配置的数值型数据按正则表达式构建数据值，并通过随机数值组合生成水印标记信息并嵌入到数据值中；字符型数据按值域范围获取数据字典数据构建数据值，并通过值域数据字典对应的数值编码生成水印标记信息并嵌入到数据值中。

e）　水印数据的嵌入，水印数据的插入处理；伪行水印处理时，按照配置的数据行比例因子，在原始数据中按照一定的间隔比例将水印数据分散的插入到原始数据中；伪列水印处理时，对原始数据增加新的字段属性并根据配置生成字段名称，然后将伪列数据插入到对应的字段属性中。

D.4.5　水印溯源

水印溯源技术是指通过泄露数据中包含的水印数据识别其数据特征，并最终解析出水印信息的技

术。一般包括识别水印类型、解析水印信息、回溯分发内容，水印溯源技术实现方法见图 D.4。

a) 识别水印类型：指通过对泄露数据分析，判断其中哪些字段为植入的水印信息的字段。

b) 解析水印信息：通过对植入水印字段的解析，从中获取到水印代码内容。

c) 回溯分发内容：指通过解析出的水印代码，查询映射码表，并获取分发者、被分发者、分发时间、用途的关键信息的步骤。

图D.4　水印溯源技术实现方法

D.5　数据水印应用分类

D.5.1　静态水印

静态水印指类似通过静态脱敏的机制，在一次性的完成大批量数据的水印添加处理。静态水印通常会在将生产环境中的数据交付至开发、测试或者外发环境时使用，在外发数据的同时，植入水印信息。

静态水印技术可和静态脱敏技术结合使用。一方面降低外发数据的敏感性并且保证数据可用性，另一方面植入水印信息，确保数据一旦泄露，可进行追溯。

D.5.2　动态水印

动态水印指在数据的访问过程中，动态的在数据的查询访问请求返回的结果集中植入水印的方式。动态水印通常会在数据访问、数据实时交换、数据动态分发过程中使用，在实时交付访问者所需数据的同时，植入水印信息。

D.6　数据水印应用场景

数据水印常见应用场景分类及其描述见下表。

表　数据水印常见应用场景分类及其描述

序号	场景分类	使用场景	场景描述	动态水印	静态水印
1	技术	开发测试应用场景	金融行业所开发使用的业务系统中存在大量的客户敏感信息，如姓名、年龄、手机号码、银行卡号码、地址、工作信息等，在系统建设前期，往往需要使用上述信息进行开发测试，即使使用数据脱敏技术去除了		✓

序号	场景分类	使用场景	场景描述	动态水印	静态水印
	场 景		敏感信息，仍然需要使用水印技术向外发的数据中植入水印，标明分发者、分发目标、数据用途等。 在此场景中适合使用静态水印中的伪行水印技术，既能保证添加水印，又不会对数据结构有所影响从而干扰开发测试正常进行。		
2		数据分享应用场景	数据分享应用场景在一些特定需求下，部分隐私数据需要提供给其他机构或企业，需要使用水印技术向外发的数据中植入水印，标明分发者、分发目标、数据用途等。在此场景中适合使用静态水印中的伪列水印技术。		✓
3		数据科学研究应用场景	数据科学研究应用场景，其主要目的是通过数据进行研究，因此需要保留数据本身的一些特征。此场景中适合使用静态水印中的伪列水印技术，增加的部分列信息不会包含研究应用所用到的真实数据列，不会干扰研究结果。		✓
4		生产应用场景	生产场景主要指各类业务场景，当涉及访问敏感数据时，需要对获取到的数据植入水印信息，这种场景适合动态水印机制。	✓	
5		数据交换应用场景	数据交换场景主要是通过 API 接口方式向特定平台提供数据，这类场景适用动态水印机制。	✓	

参 考 文 献

[1] GB/T 4754—2017 国民经济行业分类

[2] GB/T 5271.1—2000 信息技术 词汇 第1部分：基本术语

[3] GB/T 37092—2018 密码模块安全检测要求

[4] GB/T 37939—2019 信息安全技术 网络存储安全技术要求

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

[6] GM/Z 0001—2013 密码术语

[7] GM/T 0002—2012 SM4分组密码算法

[8] JR/T 0149—2016 中国金融移动支付 支付标记化技术规范

[9] JR/T 0167—2018 云计算技术金融应用规范 安全技术要求

[10] ISO/IEC 20889:2018 Information technology-Security techniques-Privacy enhancing data deidentification terminology and classification of techniques

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

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

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