ICS 03.060
CSS A 11

JR

中华人民共和国金融行业标准

XX/T XXXXX—XXXX

证券期货业数据安全管理与保护指引

The guidance of data management and protection

for securities and futures industry

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国证券监督管理委员会　　发布

目　　次

前　　言 2
引　　言 3
证券期货业数据安全管理与保护指引 4
1 范围 4
2 规范性引用文件 4
3 术语和定义 4
4 基本原则 6
4.1 过程域原则 6
4.2 实用性原则 6
4.3 安全性原则 6
4.4 可用性原则 6
4.5 适配性原则 6
5 组织架构 6
5.1 数据安全相关部门职责 7
5.2 数据安全管理部门的职责要求 7
5.3 数据安全管理岗位的要求 8
6 制度要求 8
7 工作要求 8
7.1 1 级数据安全要求 9
7.2 2 级数据安全要求 14
7.3 3 级数据安全要求 23
7.4 4 级数据安全要求 34

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范》的规定起草。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC180）归口。

本文件起草单位：中国证券监督管理委员会科技监管局、中国证券监督管理委员会信息中心、中证信息技术服务有限责任公司、海通证券股份有限公司、光大证券股份有限公司、富国基金管理有限公司、上海金仕达软件科技有限公司、防特网信息科技（北京）有限公司、申万宏源证券、上海证券、通达信、恒生电子、邦盛金融、中国金融期货交易所技术公司、海通期货、北京梆梆安全科技有限公司。

本文件主要起草人：姚前、刘铁斌、周云晖、李向东、沈云明、王洪涛、王东、杨超、刘嵩、杨纯、胡智慧、张丽君、杨硕、支晓峰、徐一丁、彭铭、卜婵敏、张颖博、朱少鹏、何铁军、赵智鹏、仇肇青、李强、赵千里、于守清、周雄伟、张千里、黄山、沈徐。

引　言

近年来，随着金融科技的发展，证券期货业积累了大量数据资产，如客户数据、交易数据、行情数据、资讯数据等。数据已成为证券期货业的重要资产和核心竞争力，充分发挥数据价值，用数据驱动创新，实现高质量发展，已成为行业共识。在数据应用得到不断发展的同时，数据安全问题也日益受到重视。

证券期货行业掌握的大量高敏感性、高重要性数据，需要施以适当的数据安全保障措施，来保障投资者权益及证券市场的公平性和稳定性。经证券期货业数据安全管理现状调研，大部分机构尚未建立健全的数据安全管理组织架构；技术手段未能全面覆盖数据生命周期。因此，为加强证券期货业数据安全管理水平，特制定本文件。

本文件作为一个推荐性标准，基于《证券期货业数据分类分级指引》，提供了数据采集、数据展示、数据传输、数据存储、数据存储过程中的数据管理要求和技术要求，供行业机构参考。

证券期货业数据安全管理与保护指引

1 范围

本文件规定了证券期货业数据安全管理与保护相关的术语和定义、基本原则、组织架构、制度要求，以及各级数据的数据采集、数据展现、数据传输、数据处理、数据存储的安全要求等内容。

本文件适用于行业机构，包括证券期货基金经营机构（以下简称市场经营机构）、证券期货信息技术服务机构（以下简称市场服务机构）的数据安全管理与保护工作的参考和指引。

注1：市场经营机构，是指经国务院证券监督管理机构和有关主管部门批准设立，并依法登记注册的证券公司、基金管理公司和期货公司等在证券市场上经营证券业务的金融机构。

注2：市场服务机构，是指经国务院证券监督管理机构和有关主管部门批准设立，并依法登记注册的投资咨询机构、财务顾问机构、资信评级机构、资产评估机构、会计师事务所、信息公司、科技公司等从事证券期货服务业务的机构。

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 35273-2017 信息安全技术个人信息安全规范

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

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

3 术语和定义

GB/T 35273-2017、GB/T 37988-2019、JR/T 0158-2018界定的以及下列术语和定义适用于本文件。

3.1

数据接触者

在数据采集、数据展现、数据传输、数据处理、数据存储过程中的参与者。

注：包括投资者、经营机构、服务机构、核心机构、监管机构等。

3.2

数据采集 data acquisition

从系统外部的其他系统、移动终端等渠道获取个人信息和其他外部数据，并输入到系统内部的过程。

3.3

数据展现 data display

数据在所有可以接触数据的直接呈现终端、应用程序终端和其他数据呈现区域呈现的过程。

3.4

数据传输 data transmission

数据传递的中间环节，指数据在系统内部、系统之间或人与人之间、人机之间的传送和交换。

3.5

数据处理 data processing

信息系统、数据管理人员执行的对数据的使用、加工或转移。

3.6

数据存储 data storage

将数据以各种不同的形式保存起来。

注：包含所有与数据保存相关的环节，主要分为四个方面：数据存储、备份与恢复、数据删除、数据销毁。

3.7

可控区域 controlled area

在每个数据过程域中，数据所有者独立拥有直接承载数据的基础设施的管理权或使用权，且独立拥有基础设施所承载信息系统的所有权或使用权的区域。

3.8

非可控区域 uncontrolled area

在每个数据过程域中，数据所有者非独立拥有直接承载数据的基础设施的管理权或使用权，或非独立拥有基础设施所承载信息系统的所有权或使用权的区域。

3.9

数据过程域 data process area

实现同一数据目标的相关数据活动的集合（参考GB／T 37988-2019）。

注：一个过程域中包含一个或多个相关活动。

示例：“元数据管理”这一过程域中，包含建立元数据管理规范、建立元数据访问控制策略、建立元数据技术工具等相关活动。

3.10

数据所有者 data controller

可以授权或拒绝访问某些数据、决定数据使用和数据处理目的和方式，并对其准确性、完整性和及时性负责的个人或机构。

3.11

基础设施 infrastructure

基础设施是指承载信息系统的服务器、通讯设备、存储设备等实体电子设备，不包括共用的机房物理环境以及基于基础设施采用虚拟化技术（包括云化技术、软件定义技术等）实现的虚拟服务器、云主机、云服务等虚拟运行环境。

3.12

数据分级 data grading

依据相关原则，结合数据的影响对象、影响范围、影响程度三要素确定数据的等级级别。

注：本文件采用《证券期货业数据分类分级指引》中的数据分级方法。本文件中所述“第X级基本要求”即为对应《证券期货业数据分类分级指引》中所定义的“第X级”数据分级。

4 基本原则

4.1 过程域原则

数据安全保护措施应覆盖数据全生命周期，本文件包含5个过程域：数据采集、数据展现、数据传输、数据处理和数据存储。

4.2 实用性原则

对不同安全等级数据对象的安全敏感度进行综合考量，基于数据安全等级的差异，制定相应的数据安全防护措施，并区分管理和技术的要求，本文件在行业内具备实用性的原则。

4.3 安全性原则

数据安全性包含管理安全性与技术安全性，从组织、技术、制度三个方面建立完备的数据安全保护措施，保护经营机构的经营数据和客户信息安全，防范信息泄露。将审批流程、岗位职责与安全技术相结合，在整个数据流转过程中，保障数据被安全和适当的使用，不被泄露给非授权的对象。

4.4 可用性原则

数据在采集、展现、传输、处理、存储等各环节无缺失、损毁，确保数据的完整、可用。

4.5 适配性原则

对不同行业机构的不同实际情况具备适配性，使各行业机构可以参考该文件，根据自身实际情况采取合适的方式将数据安全管理落实到具体的组织架构与岗位职责中，确保符合数据安全相关规范性文件或者流程的要求。

5 组织架构

5.1 数据安全相关部门职责

组织架构的规定旨在在组织内明确各项数据安全管理职责的责任划分，建立数据安全工作分工协作机制，并指定数据安全管理的主责部门（以下简称“数据安全管理部门”），为数据安全管理提供组织保障。

数据安全相关部门包括业务部门、数据运营部门、风险合规管理部门、信息技术部门、内部审计部门，各部门的数据安全工作职责为：

5.1.1 业务部门

业务部门是业务数据的所有者，其职责包括：根据数据分类分级原则对业务数据进行分级分类管理；根据统一权限管理策略，制定本部门的业务数据授权审批流程，合理进行数据的权限审批与使用，对业务账号与接入终端的合规使用进行日常管理；负责本部门所辖范围内的业务数据安全、合规监督管理等工作。

5.1.2 数据运营部门

数据运营部门是承载数据的信息系统的管理者，负责业务账号与接入终端的日常管理的相关技术支持；负责根据数据安全管理制度与技术标准建立并执行数据全生命周期的运营管理操作规程，并定期修订更新；负责制定信息系统的数据安全评估工作。如无独立的数据运营部门，其管理职责可由信息技术部门落实。

5.1.3 风险合规部门

风险合规部门是数据安全的管理者，负责数据安全管理制度与技术标准的编制（如数据分类分级标准、数据保护策略等）；通过指导、规范、审核、检查等手段，对数据安全管理措施和落实情况进行技术监管，确保有关标准规范有效贯彻施行，发现问题通知有关部门予以纠正，并组织、督促审计发现问题的整改工作。

5.1.4 信息技术部门

信息技术部门是数据安全保护措施的实施者，负责按照数据安全的制度和技术标准实施数据安全保护措施，包括但不限于数据加密、数据脱敏、认证授权、身份鉴别、访问控制和安全审计等，从技术手段上防止数据丢失、泄漏、被篡改、被毁损。

5.1.5 内部审计部门

内部审计部门是数据安全稽核工作落实部门，主要负责对数据安全管理情况和效果进行检查和评价，并督促整改，保障数据安全管理要求的有效落实。如无独立的内审部门，其管理职责可并入风险合规部门落实。

5.2 数据安全管理部门的职责要求

数据安全管理部门牵头负责数据安全管理工作，主要职责包括：

——组织制定数据管理制度，明确各类数据的安全等级，规范不同数据安全等级的处理方式和处理人员。

——明确本机构数据安全管理的最高责任人，宜由机构管理层人员担任。

——明确数据管理相关的管理岗位和职能，明确对数据的准确性、内容等要素进行核实或确认的部门或岗位，应设立安全主管、安全管理等岗位，并定义各岗位的职责。

——明确数据使用的授权机制，明确数据使用的组织、机构及人员的责任及义务。

5.3 数据安全管理岗位的要求

数据安全岗位宜包含数据安全主管、数据管理岗、介质管理岗、权限管理岗和保密管理岗，主要工作职责为：

——数据安全主管：数据安全管理的最高责任人

——数据管理岗：负责数据在整个流转过程中安全相关策略、制度的制定，并定期对机构的数据安全状态进行评估、审计和检查。组织并开展数据安全相关的培训工作。

——介质管理岗：对数据的存放介质和保存期等进行规范。确保介质存放在介质库或档案室等安全的环境中，并实行存储环境专人管理，实现对各类介质和备份数据的控制和保护。

——权限管理岗：采用权限分割、互相制约、最小化原则对人员权限进行管理，尤其对系统超级用户的权限加以限制，体现权限最小化原则。对于管理用户，严格做好权限交叉与互斥管理，由不同的管理用户来动态地控制系统的管理，实现互相制约。对于非管理用户，即普通用户，依据权限最小化原则，严格限制其权限范围，不允许进行授权以外的操作。

——保密管理岗：制订并落实数据保密措施，加强事前预防和保密意识教育，定期开展保密检查，查漏补缺，及时发现并解决与保密工作或措施相关的失密事件。

6 制度要求

组织应建立主要的数据安全管理制度，包括：

——数据安全管理制度：明确数据安全管理机制，明确数据安全管理工作的组织架构、组织形式、岗位职责、资源配置等事项。

——权限管理制度：明确权限管理制度体系，明确访问权限、访问方式及申请流程。

——介质管理制度：明确数据存放介质管理制度，实现存储介质可追踪、可核查。确保数据在介质中的存放周期、存放方式、访问权限的安全性。

——场所管理制度：明确数据展现、传输、处理及存储区域的管理，明确对相应场所的物理要求、访问要求、监控要求、维护要求、防护要求等。

——数据保密制度：明确数据保密的岗位职责，明确数据密级，对于涉密数据的访问制订相应的数据防护措施，对于接触敏感数据的人员和岗位制定相应的保密要求。

——数据安全防护制度：根据数据规模、所受安全威胁的程度，制订数据安全防护制度，并采取相应的数据安全防护措施，确保本机构具备与自身适配的数据安全防护能力。

——数据安全事件管理制度：制定数据安全事件的相关制度，就数据安全事件的发现、评估、上报、处置、跟踪、反馈等方面提出明确的流程和要求，并根据国家及行业相关的要求，形成相应的事件处置预案。同时，确保相关管理制度、处置预案的有效性，定期评估和修订。

——数据安全审计制度：明确数据安全内部审计责任与周期，形成数据安全内部审计制度，进行定期的数据安全专项审计，并就审计行为和结果进行记录和跟踪，确保审计的有效性和时效性。

——数据安全应急管理制度：评估分析数据安全工作存在的风险，制定相应数据安全应急管理制度和应急预案，定期开展数据安全应急预案演练，并基于演练结果持续优化应急预案，确保应急管理措施的有效性。

——其它数据安全相关制度：可根据自身实际情况制订的其它有助于保障数据安全的制度或规定。

7 工作要求

基于《JR/T 0158-2018 证券期货业数据分类分级指引》定义的数据安全等级，明确各级数据的安全保护措施，数据安全等级递进关系遵从分类分级指引中数据重要程度规定。各级工作要求中黑体为该级新增要求。

7.1 1级数据安全要求

7.1.1 数据采集

7.1.1.1 可控区域

7.1.1.1.1 管理要求

对第1级数据的数据采集工作在可控区域中的具体管理要求如下：

a) 宜明确该级数据的可采集范围。
b) 采取自动化手段访问收集网站数据的，宜有监控措施监控数据采集过程，保障数据采集的准确性、完整性和不可篡改性。
c) 自动化访问采集流量不超过网站日均流量的三分之一。
d) 兼并、重组、破产的，数据承接方宜承接数据安全责任和义务。没有数据承接方的，可对数据作删除处理。

7.1.1.1.2 技术要求

采集该级数据时，宜在数据中标明来源和收集时间，以提升数据的可追溯性。

7.1.1.1.3 数据接触者要求

对第1级数据的数据采集工作在可控区域中的具体数据接触者要求如下：

a) 数据接触者对接入其平台的第三方应用，宜明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。
b) 宜根据该级数据分类的情况，对数据接触者进行权限限定。

7.1.1.2 非可控区域

7.1.1.2.1 管理要求

对第1级数据的数据采集工作在非可控区域中的具体管理要求如下：

a) 数据采集宜在可控区域使用信息系统自动化进行采集，确保数据采集的安全性、不可篡改性。如有特殊需要，在非可控区域进行离线采集时，宜保证数据电子化过程中的安全性，加强对采集人员的安全责任及意识培训，防止数据泄露。
b) 在非可控区域采集数据时，不宜进行批量数据采集。可跟踪和记录数据采集过程，同时宜遵守可控区域的要求。

7.1.1.2.2 技术要求

对第1级数据的数据采集工作在非可控区域中的具体技术要求如下：

a) 宜满足可控区域的技术要求。
b) 对纸质载体采集的数据，宜采用类似 OCR 扫描的技术对数据进行自动识别、录入。

7.1.1.2.3 数据接触者要求

对第1级数据的数据采集工作在非可控区域中的具体数据接触者要求如下：

a) 宜满足该级可控区域的数据接触者要求
b) 数据接触者在非可控区域进行离线采集时，不能私自复制、修改、使用数据。

7.1.2 数据展现

7.1.2.1 可控区域

7.1.2.1.1 管理要求

对第1级数据的数据展现工作在可控区域中的具体管理要求如下：
a) 该级数据展现终端可配合数据所有者的要求，提供终端相关信息。
b) 该级数据不需要进行权限管理，可在互联网上向公众发布展示，可不设置认证、鉴权机制。
c) 该级数据可经互联网邮件方式向特定人群发送，可以由内部邮件方式向特定人群发送。
d) 该级数据允许截屏、拍照等方式拷贝。
e) 宜取合理的技术措施确保数据展现的准确性。当数据有误时，应及时更正。

7.1.2.1.2 技术要求

对第1级数据的数据展现工作在可控区域中的具体技术要求如下：
a) 宜通过技术手段获取数据展现终端的特征信息。
b) 宜对展现的数据进行标识，以唯一识别数据所有者身份。
c) 宜根据机构自身情况限定可展现数据的终端类型与展现方式。
d) 宜采用数据校验，数据可追溯等机制确保展现数据的准确性。

7.1.2.1.3 数据接触者要求

无。

7.1.2.2 非可控区域

7.1.2.2.1 管理要求

宜满足该级可控区域的管理要求

7.1.2.2.2 技术要求

对第1级数据的数据展现工作在非可控区域中的具体技术要求如下：
a) 数据展现终端（含软件、硬件）宜经过行业机构授权或认证。
b) 限制数据批量展示，采取反爬措施，防止数据被批量获取。

7.1.2.2.3 数据接触者要求

无。

7.1.3 数据传输

7.1.3.1 可控区域

7.1.3.1.1 管理要求

对第1级数据的数据传输工作在可控区域中的具体管理要求如下：
a) 宜制定相应的管理制度，明确如下事项：

1) 有专职人员保管重要的数据传输介质。
2) 有针对数据传输介质的定期安全性检查。
3) 有数据传输介质的使用申请流程及授权规定。
4) 有适用的数据传输介质选用标准，避免数据传输介质出现无备份状况。
5) 有统一、适用的数据传输介质报废制度。

b) 该级数据可经互联网、专线网或内部局域网传输，不需要加密。
c) 在数据交换方式上，需考虑如下事项：
1) 对数据共享方案进行安全风险管控。
2) 对数据发布的安全风险进行控制。
3) 核心业务或系统需定义数据接口安全策略。

7.1.3.1.2 技术要求

对第1级数据的数据传输工作在可控区域中的具体技术要求如下：

a) 进行数据传输之前，数据发送方与接收方之间应有身份合法性验证机制。
b) 宜采用一定的数据校验技术，确保数据经过传输后的完整性和一致性。
c) 宜采用数据传输监控机制，避免数据在传输过程中不被分流。
d) 宜避免大批量的数据被一次性传输。
e) 宜尽可能采用具有独立安全机制的数据传输介质。
f) 宜充分评估数据传输能力，确保能有效应对突发性数据传输要求。
g) 宜有协议接口和 API 接口监控和异常处置能力。
h) 全量数据传输和增量数据传输宜当采用相互独立的通道实施。

7.1.3.1.3 数据接触者要求

行业机构建立、健全数据管理规定，明确对数据传输人员的要求：

a) 遵守数据传输的权限要求，不私自或越权传输数据。
b) 遵守数据传输的时效性要求，准确、高效地完成数据传输。
c) 遵守数据传输职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。
a) 有义务配合做好所传输数据的保密工作。
a) 遵守数据传输的权限要求，不私自或越权传输数据。
b) 遵守数据传输的时效性要求，准确、高效地完成数据传输。
c) 遵守数据传输职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。
a) 有义务配合做好所传输数据的保密工作。

7.1.3.2 非可控区域

7.1.3.2.1 管理要求

非可控区域的数据传输必须经过行业机构的批准或授权，宜明确如下事项：

a) 对数据传输介质的要求：
1) 行业机构宜与所使用数据传输介质的所有者完成具有法律效力的责任与义务的约定，确保数据传输介质的安全性与可用性。
2) 行业机构自有数据传输介质在发生使用权转移时，双方需进行确认。
3) 宜避免数据传输介质在行业机构人员不在场的情况下出现在非可控区域。
b) 对数据传输形式的要求：对于第一级数据可以明文或可读方式传输数据。

7.1.3.2.2 技术要求

对第1级数据的数据传输工作在非可控区域中的具体技术要求如下：

a) 宜有针对数据传输的监控机制，避免数据在传输过程中被破坏。
b) 宜尽量以行业机构可控的协议接口或 API 作为数据传输主要方式。

7.1.3.2.3 数据接触者要求

对第1级数据的数据传输工作在非可控区域中的具体数据接触者要求如下：

a) 未经行业机构授权不得以任何方式擅自改变数据传输路径。
b) 未经行业机构授权不得以任何方式擅自损毁数据传输介质。
c) 未经行业机构授权不得擅自使用数据传输介质。

7.1.4 数据处理

7.1.4.1 可控区域

7.1.4.1.1 管理要求

对第1级数据的数据处理工作在可控区域中的具体管理要求如下：

a) 数据处理可遵循“谁处理，谁负责”的原则，明确数据处理者的责任。
b) 数据处理宜采取用户权限管理、数据权限管理等方式管理数据处理权限。
c) 未经授权，不可非法生成、擅自修改、泄漏、丢失与破坏信息系统数据。
d) 数据处理宜记录数据操作日志，并按文档保管要求统一管理。
e) 宜在测试环境和生产环境均实现数据的可恢复性

7.1.4.1.2 技术要求

对第1级数据的数据处理工作在可控区域中的具体技术要求如下：

a) 宜支持针对数据处理者的用户标识和用户鉴别，保证数据处理者的唯一性。
    1) 在登录或连接系统时，宜采用鉴别方式中“基于知道的”（如口令）、“基于拥有的”（如证书或令牌）、“基于个人特征的”（如指纹、眼纹等）等机制进行用户身份鉴别，以确保数据处理者的合法性。
    2) 数据处理者的身份鉴别方式宜有定期或不定期的安全评估，以确保其鉴别方式的安全。
    3) 宜采集数据接触者的特征信息，辅助进行身份鉴别。比如员工工号、终端识别码、身份认证类型、预留信息等。
b) 该级数据处理，宜提供如下处理保护：
    1) 操作日志留痕。
    2) 直接数据处理，宜做好监控和处理前备份工作。

7.1.4.1.3 数据接触者要求

对第1级数据的数据处理工作在可控区域中的具体数据接触者要求如下：

a) 数据接触者在数据处理前，宜获得行业机构的授权，并在授权范围内进行数据处理。
b) 数据接触者宜与行业机构签订相应的保密协议。

7.1.4.2 非可控区域

7.1.4.2.1 管理要求

原则上，行业机构宜避免在非可控区域处理生产数据。

7.1.4.2.2 技术要求

对第1级数据的数据处理工作在非可控区域中的具体技术要求如下：

a) 宜加强数据处理逻辑的完整性检查与判断。
b) 宜尽量对数据处理逻辑进行唯一性标识。

7.1.4.2.3 数据接触者要求

对第1级数据的数据处理工作在非可控区域中的具体数据接触者要求如下：

a) 非可控区域的数据处理者必须获得行业机构的专属授权，以“一事一授”为宜。
b) 数据接触者宜与行业机构签订相应的保密协议。

7.1.5 数据存储

7.1.5.1 可控区域

7.1.5.1.1 管理要求

1 级数据在可控区域应充分重视数据存储安全，具体管理要求如下：

a) 数据存储期限、位置宜满足法律法规及相关适用规定。
b) 宜制订相应的数据存储管理要求，明确管理人员、管理对象及职责范围。对申请流程、存储检查、介质安全、数据销毁（含介质）、存储密级、时限等做出规定。
c) 根据信息系统的重要性水平，性能容量评估结果，为不同信息系统选择相应的数据存储方案。
d) 该级数据可采用较低的备份频率和验证频率，采用简化的恢复策略和流程，对存储介质、存储区域无特别限制。
e) 宜区别对待临时数据存储与持久化数据存储。
f) 宜制订针对离线数据、备份数据的存储管理要求，确保它们的可恢复能力。
g) 宜制定数据删除和销毁机制，对于第一级数据，在防止数据泄露的前提下，可按照自定义的信息处理方法处置。

7.1.5.1.2 技术要求

1 级数据在可控区域数据存储的技术要求如下：

a) 物理安全
    1) 宜充分评估数据存储区域的安全级别并采取技术手段进行防护，包括数据存储区域的物理位置、防火、防雷、电力保障、电磁防护、防盗窃和防破坏等。
    2) 宜建立数据存储区域的不间断监控机制，确保及时发现并处置突发事件。
    3) 宜建立访问控制机制，确保获得授权的数据接触者访问数据存储区域和存储介质。
b) 安全控制
    1) 宜建立数据存储的权限控制机制，如用户权限矩阵、多因子身份识别等，确保获得授权的数据接触者才能进行数据存储操作。
    2) 该级数据，无需对数据存储权限的授权设立期限或次数限制。
    3) 宜避免数据存储者同时拥有数据处理的权限。
    4) 数据存储宜做好操作留痕，并形成检查或审计机制。
c) 存储安全
    1) 数据存储宜获得数据所有者的授权。

2) 该级数据，可制订简易的数据存储策略，对存储介质、存储区域可不做特别限制。
3) 宜通过多种技术手段定期或不定期地检查存储数据的可用性、安全性，如查询、抽样恢复、完整性检查等。
4) 宜加强信息系统的安全检查与防范，定期或不定期的对信息系统进行安全检查与加固，确保信息系统在安全补丁、漏洞修补、木马防范、病毒查杀、后门修复等方面及时得到更新，严防数据损毁、泄漏。
5) 宜对各类数据进行有效销毁，确保以不可逆的方式销毁数据及其副本内容。

7.1.5.1.3 数据接触者要求

1 级数据在可控区域数据存储的数据接触者要求如下：

a) 宜制订数据存储操作及数据存储介质的管理规定，明确接触者的资质及岗位要求。
b) 数据存储及存储介质管理人员宜为行业机构正式员工。针对其他人员执行数据存储相关工作的情况，行业机构宜与其及所属组织签订相应的工作合同。
c) 数据接触者不得擅自执行或变更数据存储要求。

7.1.5.2 非可控区域

7.1.5.2.1 管理要求

1 级数据在非可控区域应充分重视数据存储安全，具体管理要求如下：

a) 行业机构宜与数据存储区域所属的组织签订相关协议，明确约定责任与义务，确保该区域的安全。
b) 非可控区域的数据存储授权审批宜严于可控区域的数据存储授权审批。
c) 宜与数据存储实际执行者所属的组织签订工作合同，明确数据存储操作要求及保密责任。

7.1.5.2.2 技术要求

1 级数据在非可控区域数据存储的技术要求如下：

a) 宜以临时存储为主，存储期限宜以数据接触者在场为限。数据接触者为非人主体的情况下，可以数据接触者失活为限。
b) 除数据所有者授权外，宜避免以明文或可读方式存储数据。
c) 执行数据存储操作宜确保数据接触者处于相对独立的安全空间。

7.1.5.2.3 数据接触者要求

1 级数据在非可控区域数据存储的数据接触者要求如下：

a) 宜有特别的数据存储授权，宜以“一事一议”为原则进行授权。
b) 除监管及法律法规要求外，第三方人员不可在非可控区域执行数据存储操作或访问存储介质。

7.2 2 级数据安全要求

7.2.1 数据采集

7.2.1.1 可控区域

7.2.1.1.1 管理要求

对第2级数据的数据采集工作在可控区域中的具体管理要求如下：

a) 宜明确该级数据的可采集范围。

b) 采取自动化手段访问收集网站数据的，宜有监控措施监控数据采集过程，保障数据采集的准确性、完整性和不可篡改性。
c) 自动化访问采集流量不超过网站日均流量的三分之一。
d) 兼并、重组、破产的，数据承接方宜承接数据安全责任和义务。没有数据承接方的，可对数据作删除处理。

7.2.1.1.2 技术要求

对第2级数据的数据采集工作在可控区域中的具体技术要求如下：

a) 采集该级数据时，宜在数据中标明来源和收集时间，以提升数据的可追溯性。
b) **发布、共享、交易或向境外提供重要数据前，宜当评估可能带来的安全风险，并报经行业主管监管部门同意。**

7.2.1.1.3 数据接触者要求

对第2级数据的数据采集工作在可控区域中的具体数据接触者要求如下：

a) 数据接触者对接入其平台的第三方应用，宜明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。
b) 根据该级数据分类的情况，对数据接触者进行权限限定。

7.2.1.2 非可控区域

7.2.1.2.1 管理要求

对第2级数据的数据采集工作在非可控区域中的具体管理要求如下：

a) 数据采集宜在可控区域使用信息系统自动化进行采集，确保数据采集的安全性、不可篡改性。如有特殊需要，在非可控区域进行离线采集时，宜保证数据电子化过程中的安全性，加强对采集人员的安全责任及意识培训，防止数据泄露。
b) 在非可控区域采集数据时，不宜进行批量数据采集。可跟踪和记录数据采集过程，同时宜遵守可控区域的要求。

7.2.1.2.2 技术要求

对第2级数据的数据采集工作在非可控区域中的具体技术要求如下：

a) 宜满足可控区域的技术要求。
b) 对纸质载体采集的数据，宜采用类似 OCR 扫描的技术对数据进行自动识别、录入。

7.2.1.2.3 数据接触者要求

对第2级数据的数据采集工作在非可控区域中的具体数据接触者要求如下：

a) 宜满足该级可控区域的数据接触者要求
b) 数据接触者在非可控区域进行离线采集时，不得私自复制、修改、使用数据。

7.2.2 数据展现

7.2.2.1 可控区域

7.2.2.1.1 管理要求

对第2级数据的数据展现工作在可控区域中的具体管理要求如下：

a) 该级数据展现终端可配合数据所有者的要求，提供终端相关信息。
b) 该级数据展现可按照“必须知道”、“最小授权”和“最小功能” 原则进行权限管理。建立和完善岗位权限管理流程，避免不恰当的授权。
   1) 系统管理员宜该避免直接接触业务数据；
   2) 宜有专用的权限管理岗位；
   3) 互斥岗位要避免权限交叉；
   4) 业务信息的展现及使用均宜在业务开展及管理所需最小授权范围内使用；
   5) 禁止服务机构人员直接接触未经脱敏处理的原始数据；
   6) 按该级数据要求对数据接触者进行披露并保存访问记录。
c) 针对不同前端展现系统软件和终端硬件设备，建立和完善数据安全管理措施，以保证数据不被截取、泄露、盗取：
   1) 经营机构人员只能以公司授权的用户按公司规定的认证方式访问公司授权的业务系统；
   2) 尽量降低该级数据终端对外暴露的程度；
   3) 通过数据展现终端改变数据展现方式的操作或行为宜经过授权或审批；
   4) 可控区域的所有数据展现软件及设备宜由行业机构拥有完全独立的所有权、使用权、支配权，并拥有完全独立、自主的投放、更新及销毁权。
d) 宜取合理的技术措施确保数据展现的准确性。当数据有误时，宜及时更正。

7.2.2.1.2 技术要求

对第2级数据的数据展现工作在可控区域中的具体技术要求如下：

a) 数据展现宜采用区域化管理，区域与数据访问权限绑定。
b) 宜实施通信与接入管制，按照监管要求并结合行业机构实际情况，对数据的展现请求采取认证、留痕与监测等控制措施，以记录或防止数据被不当获取和使用。
c) 宜通过技术手段获取数据展现终端的特征信息。
d) 宜对展现的数据进行标识，以唯一识别数据所有者身份。
e) 宜根据机构自身情况限定可展现数据的终端类型与展现方式。
f) 宜采用数据校验，数据可追溯等机制确保展现数据的准确性。

7.2.2.1.3 数据接触者要求

对第2级数据的数据展现工作在可控区域中的具体数据接触者要求如下：

a) 行业机构人员对在工作过程中接触的数据，非因工作需要，在任职期间和离职或更换工作岗位后不可将其泄露给公司其他员工或任何第三方；人员离岗后需立即终止其所有数据访问权限，并需取回各种用于接触数据的身份识别证件、钥匙、徽章、密码等软硬件口令或设备。

7.2.2.2 非可控区域

7.2.2.2.1 管理要求

因非可控区域不确定性更高的特性，宜充分评估该级数据在非可控区域展现的必要性，针对不同前端展现系统软件和终端设备，建立和完善数据安全管理措施，以保证数据不被截取、泄露、盗取，具体要求如下：

a) 数据安全等级为该级的数据，有需要展现的情况下，宜有严格的身份识别与授权程序，确保数据展现符合权限规定。

b) 因监管部门要求提供、行业机构内部研究、行政或业务审批、追偿、检查审计、配合司法调查等调阅特定信息，需要确保数据调阅凭证真实、可信并做好调阅留痕。

7.2.2.2.2 技术要求

对第2级数据的数据展现工作在非可控区域中的具体技术要求如下：

a) 数据展现终端（含软件、硬件）宜经过行业机构授权或认证。
b) 限制数据批量展示，采取反爬措施，防止数据被批量获取。
c) 采用减少数据展现量、水印、身份识别前置等技术加强数据展现安全性。

7.2.2.2.3 数据接触者要求

对第2级数据的数据展现工作在非可控区域中的具体数据接触者要求如下：

a) 对数据接触者进行必要数据安全宣传和培训，强调对数据进行保护的必要性，避免敏感信息外泄；
b) 涉及聘用服务机构及人员为行业机构提供信息技术开发、业务咨询、合作等外包服务的，宜与外包方签署保密协议，明确保密义务，不得违反约定擅自获取及传播行业机构数据。

7.2.3 数据传输

7.2.3.1 可控区域

7.2.3.1.1 管理要求

对第2级数据的数据传输工作在可控区域中的具体管理要求如下：

a) 宜制定相应的管理制度，明确如下事项：
   1) 有专职人员保管重要的数据传输介质。
   2) 有针对数据传输介质的定期安全性检查。
   3) 有数据传输介质的使用申请流程及授权规定。
   4) 有适用的数据传输介质选用标准，避免数据传输介质出现无备份状况。
   5) 有统一、适用的数据传输介质报废制度。
b) 在数据传输的形式上，行业机构宜根据自身情况，明确如下事项：
   1) 数据传输的内容宜尽量避免在传输过程中直接可见或明文可读。
   2) 应有针对数据传输的、独立的安全机制。
c) 在数据交换方式上，需考虑如下事项（结合 GB/T 37988-2019 数据交换安全部分）：
   1) 宜由业务团队相关人员负责对数据共享方案进行安全风险管控。
   2) 宜明确核心业务数据共享安全评估机制,可从共享目的合理性、共享数据的范围和
   3) 合规性、共享方式的安全性、共享后管理责任和约束措施等方面进行评估。
   4) 负责数据共享安全的人员宜具备对数据共享业务的理解能力,能够结合合规性要求给出适当的安全解决方案。
   5) 宜由业务团队相关人员负责数据发布的安全风险控制。
   6) 宜明确核心业务数据公开发布的安全制度和审核流程。
   7) 负责数据发布安全工作的人员宜基本理解数据发布安全的制度要求。
   8) 宜由业务团队相关人员负责数据服务接口安全管理工作。
   9) 核心业务或系统宜定义数据接口安全策略。
   10) 负责数据接口安全工作的人员宜具备基本的数据接口调用的安全意识和安全知识。

7.2.3.1.2 技术要求

对第2级数据的数据传输工作在可控区域中的具体技术要求如下：

a) 进行数据传输之前，数据发送方与接收方之间宜有身份合法性验证机制。
b) 宜采用一定的数据校验技术，确保数据经过传输后的完整性和一致性。
c) 宜采用数据传输监控机制，避免数据在传输过程中不被分流。
d) 宜避免大批量的数据被一次性传输。
e) 宜尽可能采用具有独立安全机制的数据传输介质。
f) 宜采用技术工具实现对数据接口调用的身份鉴别和访问控制。
g) 宜有协议接口和 API 接口监控和异常处置能力。
h) 全量数据传输和增量数据传输宜当采用相互独立的通道实施。

7.2.3.1.3 数据接触者要求

行业机构建立、健全数据管理规定，明确对数据传输人员的要求：

a) 遵守数据传输的权限要求，不私自或越权传输数据。
b) 遵守数据传输的时效性要求，准确、高效地完成数据传输。
c) 遵守数据传输职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。
a) 有义务配合做好所传输数据的保密工作。

7.2.3.2 非可控区域

7.2.3.2.1 管理要求

非可控区域的数据传输必须经过行业机构的批准或授权，宜明确如下事项：

a) 对数据传输介质的要求：
   1) 行业机构宜与所使用数据传输介质的所有者完成具有法律效力的责任与义务的约定，确保数据传输介质的安全性与可用性。
   2) 行业机构自有数据传输介质在发生使用权转移时，双方宜进行确认。
   3) 宜避免数据传输介质在行业机构人员不在场的情况下出现在非可控区域。
b) **对数据传输形式的要求：**
   1） 行业机构宜对非可控区域的数据传输进行专项评估。
   2） 禁止以明文或可读方式传输数据。
c) **在数据交换方式上，宜考虑如下事项：**
   1) 宜明确数据共享的原则和安全规范,明确数据共享内容范围和数据共享的管控措施,及数据共享涉及机构或部门相关用户职责和权限。
   2) 使用外部的软件开发包/组件/源码前宜进行安全评估,获取的数据宜符合组织的数据安全要求。
   3) 宜明确数据公开发布的审核制度,严格审核数据发布合规要求。
   4) 宜明确数据接口安全控制策略,明确规定使用数据接口的安全限制和安全控制措施,如身份鉴别、访问控制、授权策略、签名、时间戳、安全协议等。

7.2.3.2.2 技术要求

非可控区域的数据传输，宜明确如下事项（结合GB/T 37988-2019数据交换安全部分）：

a) 宜有针对数据传输的监控机制，避免数据在传输过程中被不当获取或破坏。

b) 宜尽量以行业机构可控的协议接口或 API 作为数据传输主要方式。
c) 直接提供数据实体的情况下，必须要对数据实体进行异化及保密处理。
d) 宜采取措施确保个人信息在委托处理、共享、转让等对外提供场景的安全合规,如数据脱敏、数据加密、安全通道、共享交换区域等。
e) 宜对共享数据及数据共享过程进行监控审计,共享的数据宜属于共享业务需求且没有超出数据共享使用授权范围。
f) 宜具备对接口不安全输入参数进行限制或过滤能力,为接口提供异常处理能力。
g) 宜对跨安全域间的数据接口调用采用安全通道、加密传输、时间戳等安全措施。
h) 宜有协议接口和 API 接口监控和异常处置能力。
i) 宜加强在网络传输过程中数据的保密性、完整性、可用性、可控性，使用良好的加密机制、安全认证机制和访问控制策略。

7.2.3.2.3 数据接触者要求

行业机构建立、健全数据管理规定，明确对数据传输人员的要求：
a) 遵守数据传输的权限要求，不私自或越权传输数据。
b) 遵守数据传输的时效性要求，准确、高效地完成数据传输。
c) 遵守数据传输职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。
d) 有义务配合做好所传输数据的保密工作。

7.2.4 数据处理

7.2.4.1 可控区域

7.2.4.1.1 管理要求

对第2级数据的数据处理工作在可控区域中的具体管理要求如下：
a) 数据处理可遵循“谁处理，谁负责”的原则，明确数据处理者的责任。
b) 数据处理宜采取用户权限管理、数据权限管理等方式管理数据处理权限。
c) 未经授权，不可非法生成、擅自修改、泄漏、丢失与破坏信息系统数据。
d) 数据处理宜记录数据操作日志，并按文档保管要求统一管理。
e) 宜在测试环境和生产环境均实现数据的可恢复性
f) 信息系统宜采取用户权限管理、数据权限管理等途径，对数据处理进行控制，确保有数据处理权限的人员或系统才能处理数据。
g) 数据处理逻辑宜符合业务要求，确保合规，进行充分测试并验证，确保数据的完整、可用。
h) 数据生成宜符合监管及法律法规的要求。
i) 涉及敏感数据的直接处理，宜采取双人或全程监控的方式，确保数据处理逻辑符合要求，数据处理结果符合预期。
j) 直接数据处理宜做好防护措施，确保数据处理失败或不符合预期的情况下，能恢复处理之前的数据状态。
k) 宜确保系统测试、业务测试等非生产要求导致的数据处理在完成相关任务后，数据状态能恢复到处理之前。

7.2.4.1.2 技术要求

对第2级数据的数据处理工作在可控区域中的具体技术要求如下：
a) 宜支持针对数据处理者的用户标识和用户鉴别，保证数据处理者的唯一性。

1) 在登录或连接系统时，宜采用鉴别方式中“基于知道的”（如口令）、“基于拥有的”（如证书或令牌）、“基于个人特征的”（如指纹、眼纹等）等机制进行用户身份鉴别，以确保数据处理者的合法性。
2) 数据处理者的身份鉴别方式宜有定期或不定期的安全评估，以确保其鉴别方式的安全。
3) 宜采集数据接触者的特征信息，辅助进行身份鉴别。比如员工工号、终端识别码、身份认证类型、预留信息等。

b) 针对该级数据，宜提供如下处理保护：
1) 操作日志留痕。
2) 直接数据处理，宜做好监控和处理前备份工作。

c) **数据处理权限控制：**
1) **不可处理授权以外的数据。**
2) **未经授权的人员或信息系统不可执行数据处理。**
3) **宜制订数据处理权限在不同粒度上的控制规则，如区域级、人员级、系统级、用户级、文件级、库级、表级、字段级、语句级等。**

d) **数据处理能力要求：可根据信息系统重要性水平、性能容量评估情况，制定数据处理能力测试，确保满足数据处理需求。**

e) **数据处理安全控制：**
1) **数据处理逻辑宜符合业务要求，并通过合规部门确认。**
2) **数据处理宜在投入生产环境前经过充分测试。**
3) **直接数据处理，宜有复核或审核机制。**
4) **数据处理时必须在约定时间范围内对每一次的数据处理做边界管控，对符合预期及不符合预期的情况，预设数据处理逻辑。**
5) **对于有关联关系的数据处理，宜确保处理逻辑的完整性。**
6) **数据处理专用终端进行，操作流程可追溯。**
7) **对于数据处理终端缓存的数据进行删除，以保证数据处理过程中涉及的数据不会被恢复。**

7.2.4.1.3 数据接触者要求

对第2级数据的数据处理工作在可控区域中的具体数据接触者要求如下：

a) 数据接触者在数据处理前，宜获得行业机构的授权，并在授权范围内进行数据处理。
b) 数据接触者宜与行业机构签订相应的保密协议。
c) **数据处理者宜遵循数据处理要求，不得擅自变更数据处理要求或擅自进行数据处理。**

7.2.4.2 非可控区域

7.2.4.2.1 管理要求

对第2级数据的数据处理工作在非可控区域中的具体管理要求如下：

a) 原则上，行业机构宜避免在非可控区域处理生产数据。
b) **如有特殊需求，行业机构需要在非可控区域处理数据时，宜采取有效措施确保数据处理者、数据处理逻辑、数据使用范围和数据的安全。**
c) **非可控区域的数据处理授权审批宜严于可控区域的数据处理授权审批。**

7.2.4.2.2 技术要求

对第2级数据的数据处理工作在非可控区域中的具体技术要求如下：

a) 宜加强数据处理逻辑的完整性检查与判断。
b) 宜尽量对数据处理逻辑进行唯一性标识。
c) **宜采取技术手段，如加密、变形、遮蔽、添加噪声等方式确保数据处理逻辑的安全。**
d) **宜采取技术手段，对数据处理的规模设定阈值进行监控，对于异常情况具备安全管控手段。**
e) **宜避免以可读或明文方式展示或保留数据处理的留痕信息。**

7.2.4.2.3 数据接触者要求

对第2级数据的数据处理工作在非可控区域中的具体数据接触者要求如下：

a) 非可控区域的数据处理者必须获得行业机构的专属授权，以“一事一授”为宜。
b) 数据接触者宜与行业机构签订相应的保密协议。
c) **数据处理者宜遵循数据处理要求，不得擅自变更数据处理要求或擅自进行数据处理。**

7.2.5 数据存储

7.2.5.1 可控区域

7.2.5.1.1 管理要求

2 级数据在可控区域应充分重视数据存储安全，具体管理要求如下：

a) 数据存储期限、位置宜满足法律法规及相关适用规定。
b) 宜制订相应的数据存储管理要求，明确管理人员、管理对象及职责范围。对申请流程、存储检查、介质安全、数据销毁（含介质）、存储密级、时限等做出规定。
c) 根据信息系统的重要性水平，性能容量评估结果，为不同信息系统选择相应的数据存储方案。
d) 宜区别对待临时数据存储与持久化数据存储。
e) 宜制订针对离线数据、备份数据的存储管理要求，确保它们的可恢复能力。
f) **宜视自身数据分类分级情况，充分利用多中心容灾能力，建设完善的数据存储体系，如可用性、备份类型、备份频率、存储介质、存储区域等。**
g) **宜制订针对移动存储介质的管理要求，避免敏感数据在移动存储环节泄漏。**
h) **宜制定数据删除和销毁的机制，针对数据内容进行有效的清除、净化机制，实现对数据的有效销毁，防止因存储介质上数据内容的恶意恢复而导致的数据泄漏风险（参照 GB/T 37988-2019）。**

7.2.5.1.2 技术要求

2 级数据在可控区域数据存储的技术要求如下：

a) 物理安全
   1) 宜充分评估数据存储区域的安全级别并采取技术手段进行防护，包括数据存储区域的物理位置、防火、防雷、电力保障、电磁防护、防盗窃和防破坏等。
   2) 宜建立数据存储区域的不间断监控机制，确保及时发现并处置突发事件。
   3) 宜建立访问控制机制，确保获得授权的数据接触者访问数据存储区域和存储介质。
   4) **宜建立多数据存储区域，各数据存储区域之间的物理距离宜满足灾备要求。**
b) 安全控制
   1) 宜建立数据存储的权限控制机制，如用户权限矩阵、多因子身份识别等，确保获得授权的数据接触者才能进行数据存储操作。
   2) 宜避免数据存储者同时拥有数据处理的权限。
   3) 数据存储宜做好操作留痕，并形成检查或审计机制。
   4) **针对该级别的数据，可考虑对其数据存储权限的授权设立期限或次数限制。**

c) 存储数据的安全

1) 数据存储宜获得数据所有者的授权。

2) 宜通过多种技术手段定期或不定期地检查存储数据的可用性、安全性，如查询、抽样恢复、完整性检查等。

3) 宜加强信息系统的安全检查与防范，定期或不定期的对信息系统进行安全检查与加固，确保信息系统在安全补丁、漏洞修补、木马防范、病毒查杀、后门修复等方面及时得到更新，严防数据损毁、泄漏。

4) **宜采用数据同步技术，保障各数据存储区域数据的一致性。瞬时的数据同步可以是增量同步，但在一定时间内，宜保证多个数据存储区域数据的一致性和完整性。**

5) **宜充分评估信息系统对于数据安全的要求，制订相应的多存储区域数据同步方案。数据同步可以是实时，也可以是定时的**

6) **多存储区域存储数据的情况下，宜确保每个存储区域的数据具备独立的可恢复性和可用性。**

7) **宜根据自身数据分类分级的情况，针对不同类别、不同等级的数据，制订相应的数据存储策略。**

8) **宜避免以明文或可读方式存储敏感数据。**

9) **宜使用数据销毁工具对各类数据销毁（参照 GB/T 37988-2019），包括但不限于网络存储数据、针对闪存、硬盘、磁带、光盘等数据的有效销毁，确保以不可逆的方式销毁数据及其副本内容，从而保证数据销毁的有效性。**

7.2.5.1.3 数据接触者要求

2 级数据在可控区域数据存储的数据接触者要求如下：

a) 宜制订数据存储操作及数据存储介质的管理规定，明确接触者的资质及岗位要求。

b) 数据存储及存储介质管理人员宜为行业机构正式员工。针对其他人员执行数据存储相关工作的情况，行业机构宜与其及所属组织签订相应的工作合同。

c) 数据接触者不得擅自执行或变更数据存储要求。

d) **宜避免单人执行敏感数据的存储操作。**

7.2.5.2 非可控区域

7.2.5.2.1 管理要求

2 级数据在非可控区域应充分重视数据存储安全，具体管理要求如下：

a) 行业机构宜与数据存储区域所属的组织签订相关协议，明确约定责任与义务，确保该区域的安全。

b) 非可控区域的数据存储授权审批宜严于可控区域的数据存储授权审批。

c) 宜与数据存储实际执行者所属的组织签订工作合同，明确数据存储操作要求及保密责任。

d) **除监管及法律法规要求外，严禁在非可控区域以任何方式存储敏感数据。**

7.2.5.2.2 技术要求

2 级数据在非可控区域数据存储的技术要求如下：

a) 宜以临时存储为主，存储期限宜以数据接触者在场为限。数据接触者为非人主体的情况下，应以数据接触者失活为限。

b) 除数据所有者授权外，宜避免以明文或可读方式存储数据。

c） 执行数据存储操作宜确保数据接触者处于相对独立的安全空间。
d） 除监管及法律法规要求外，非可控区域存储的数据宜进行脱敏处理。
e） 除监管及法律法规要求外，数据存储介质宜具备独立的安全控制措施，避免被任意访问。

7.2.5.2.3 数据接触者要求

2 级数据在非可控区域数据存储的数据接触者要求如下：
a） 宜有特别的数据存储授权，宜以“一事一议”为原则进行授权。
b） 除监管及法律法规要求外，第三方人员不可在非可控区域执行数据存储操作或访问存储介质。

7.3 3 级数据安全要求

7.3.1 数据采集

7.3.1.1 可控区域

7.3.1.1.1 管理要求

对第3级数据的数据采集工作在可控区域中的具体管理要求如下：
A、针对个人信息方面的要求
a） 数据采集宜制定并公开收集使用规则，个人信息当主体同意征集后，方可按照规则收集和使用个人数据（依据 JR/T 0171-2020 7.1.1 c 以及 GB/T 35273-2017 5.3 a）。
b） 因业务需要，需扩大个人信息使用范围的，宜征得个人信息主体同意。
c） 从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务。
d） 不宜因个人信息主体拒绝或者撤销同意收集核心功能服务所需以外的其他信息,而拒绝提供核心业务功能服务。
e） 不宜依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为，包括服务质量、价格差异等。
f） 采集14周岁以下未成年人个人信息的,宜当征得其监护人同意(依据 GB/T 35273-2017 5.5 c)。
B、其他要求
a） 采取自动化手段访问收集网站数据，自动化访问收集流量不可超过网站日均流量三分之一。
b） 以经营为目的收集重要数据或个人敏感信息的，宜明确数据安全责任人。数据安全责任人由具有相关管理工作经历和数据安全专业知识的人员担任，参与有关数据活动的重要决策，直接向网络运营者的主要负责人报告工作。
c） 网络运营者兼并、重组、破产的，数据承接方宜承接数据安全责任和义务。没有数据承接方的，宜对数据作删除处理。
d） 发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，行业机构宜：
1） 立即采取补救措施。
2） 及时以电话、短信、邮件或信函等方式告知个人信息主体。
3） 并按要求向行业主管监管部门报告。

7.3.1.1.2 技术要求

对第3级数据的数据采集工作在可控区域中的具体技术要求如下：
A、针对个人信息方面的要求

a) 收到有关个人信息查询、更正、删除以及用户注销账号请求时，宜在合理时间和代价范围内予以查询、更正、删除或注销账号。
b) 向他人提供个人信息前，宜评估可能带来的安全风险，并征得个人信息主体同意。下列情况除外（依据 JR/T 0171-2020 7.1.1 d 以及 GB/T 35273-2017 8.5）：
   1) 从合法公开渠道采集且不明显违背个人信息主体意愿；
   2) 个人信息主体主动公开；
   3) 经过匿名化处理；
   4) 执法机关依法履行职责所必需；
   5) 维护国家安全、社会公共利益、个人信息主体生命安全所必需。
c) 向境外提供个人信息按有关规定（依据 GB/T 35273-2017 8.7 c）执行。

B、其他要求

a) 利用用户数据和算法推送新闻信息、商业广告等（以下简称“定向推送”），宜以明显方式标明“定推”字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。
b) 利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等信息，应以明显方式标明“合成”字样；不得以谋取利益或损害他人利益为目的自动合成信息。
c) 应采取措施督促提醒用户对自己的网络行为负责、加强自律，对于用户通过社交网络转发他人制作的信息，应自动标注信息制作者在该社交网络上的账户或不可更改的用户标识。
d) 网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意。

7.3.1.1.3 数据接触者要求

对第3级数据的数据采集工作在可控区域中的具体数据接触者要求如下：

a) 数据接触者对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。
b) 根据该级数据分类的情况，对数据接触者进行权限限定。
c) 数据接触者分析利用所掌握的数据资源，发布市场预测、统计信息、个人和企业信用等信息，不得影响国家安全、经济运行、社会稳定，不得损害他人合法权益。

7.3.1.2 非可控区域

7.3.1.2.1 管理要求

对第3级数据的数据采集工作在可非控区域中的具体管理要求如下：

a) 数据采集宜在可控区域使用信息系统自动化进行采集，确保数据采集的安全性、不可篡改性。如有特殊需要，在非可控区域进行离线采集时，宜保证数据电子化过程中的安全性，加强对采集人员的安全责任及意识培训，防止数据泄露。
b) 在非可控区域采集数据时，不宜进行批量数据采集。可跟踪和记录数据采集过程，同时宜遵守可控区域的要求。

7.3.1.2.2 技术要求

对第3级数据的数据采集工作在非可控区域中的具体技术要求如下：

a) 宜满足可控区域的技术要求。
b) 对纸质载体采集的数据，宜采用类似 OCR 扫描的技术对数据进行自动识别、录入。

7.3.1.2.3 数据接触者要求

对第3级数据的数据采集工作在非可控区域中的具体数据接触者要求如下：

a) 宜满足该级可控区域的数据接触者要求
b) 数据接触者在非可控区域进行离线采集时，不得私自复制、修改、使用数据。

7.3.2 数据展现

7.3.2.1 可控区域

7.3.2.1.1 管理要求

对第3级数据的数据展现工作在可控区域中的具体管理要求如下：

a) 该级数据展现终端可配合数据所有者的要求，提供终端相关信息。
b) 该级数据展现宜按照“必须知道”、“最小授权”和“最小功能” 原则进行权限管理。建立和完善岗位权限管理流程，避免不恰当的授权。
    1) 系统管理员宜避免直接接触业务数据；
    2) 宜有专用的权限管理岗位；
    3) 互斥岗位要避免权限交叉；
    4) 业务信息的展现及使用均宜在业务开展及管理所需最小授权范围内使用；
    5) 禁止服务机构人员直接接触未经脱敏处理的原始数据；
    6) 按该级数据要求对数据接触者进行披露并保存访问记录。
c) 针对不同前端展现系统软件和终端硬件设备，建立和完善数据安全管理措施，以保证数据不被截取、泄露、盗取：
    1) 经营机构人员只能以公司授权的用户按公司规定的认证方式访问公司授权的业务系统；
    2) 尽量降低该级数据终端对外暴露的程度；
    3) 通过数据展现终端改变数据展现方式的操作或行为宜经过授权或审批；
    4) 可控区域的所有数据展现软件及设备宜由行业机构拥有完全独立的所有权、使用权、支配权，并拥有完全独立、自主的投放、更新及销毁权。
d) 宜取合理的技术措施确保数据展现的准确性。当数据有误时，宜及时更正。

7.3.2.1.2 技术要求

对第3级数据的数据展现工作在可控区域中的具体技术要求如下：

a) 数据展现宜采用区域化管理，区域与数据访问权限绑定。
b) 宜实施通信与接入管制，按照监管要求并结合行业机构实际情况，对数据的展现请求采取认证、留痕与监测等控制措施，以记录或防止数据被不当获取和使用。
c) 宜通过技术手段获取数据展现终端的特征信息。
d) 宜对展现的数据进行标识，以唯一识别数据所有者身份。
e) 宜根据机构自身情况限定可展现数据的终端类型与展现方式。
f) 宜采用数据校验，数据可追溯等机制确保展现数据的准确性。

7.3.2.1.3 数据接触者要求

对第3级数据的数据展现工作在可控区域中的具体数据接触者要求如下：

a) 行业机构人员对在工作过程中接触的数据，非因工作需要，在任职期间和离职或更换工作岗位后不可将其泄露给公司其他员工或任何第三方；人员离岗后宜立即终止其所有数据访问权限，并宜取回各种用于接触数据的身份识别证件、钥匙、徽章、密码等软硬件口令或设备。
b) **行业机构宜禁止除授权人员以外的其他人员直接查看未经脱敏处理的敏感数据。**
c) **对于该级数据的使用者，使用数据时，宜符合该级数据使用规定。**
d) **数据接触者宜自觉识别并评估数据展现环境的安全性，避免在危险的环境中展现该级数据。**

7.3.2.2 非可控区域

7.3.2.2.1 管理要求

因非可控区域不确定性更高的特性，宜充分评估该级数据在非可控区域展现的必要性，针对不同前端展现系统软件和终端设备，建立和完善数据安全管理措施，以保证数据不被截取、泄露、盗取，具体要求如下：

a) 数据安全等级为该级的数据，原则上宜避免在非可控区域展现。确有需要展现的情况下，宜有严格的身份识别与授权程序，确保数据展现符合权限规定。
b) 因监管部门要求提供、行业机构内部研究、行政或业务审批、追偿、检查审计、配合司法调查等调阅特定信息，需要确保数据调阅凭证真实、可信并做好调阅留痕。
c) **敏感数据要尽可能地缩小接触者的范围，且只能提供只读操作。**

7.3.2.2.2 技术要求

对第3级数据的数据展现工作在非可控区域中的具体技术要求如下：

a) 数据展现终端（含软件、硬件）必须经过行业机构授权或认证；
b) **数据展现终端（含软件、硬件）不得保存敏感信息。**
c) 限制数据批量展示，采取反爬措施，防止数据被批量获取
d) 采用一些更加安全的数据展现方式，如减少数据展现量、敏感信息屏蔽、水印、身份识别前置等技术；

7.3.2.2.3 数据接触者要求

宜为数据接触者建立正确的安全意识，提高数据接触者的安全意识和数据保护意识，严格限定数据接触者的相关权限，保障数据的安全性，具体要求如下：

a) 对数据接触者进行必要数据安全宣传和培训，强调对数据进行保护的必要性，避免敏感信息外泄；
b) 涉及聘用服务机构及人员为行业机构提供信息技术开发、业务咨询、合作等外包服务的，宜与外包方签署保密协议，明确保密义务，不得违反约定擅自获取及传播行业机构数据。

7.3.3 数据传输

7.3.3.1 可控区域

7.3.3.1.1 管理要求

3级数据在可控区域内进行传输，宜参考如下管理要求（结合GB/T 37988-2019数据交换安全部分）：

a) 宜制定相应的管理制度，明确如下事项：
   1) 有专职人员保管重要的数据传输介质。
   2) 有针对数据传输介质的定期安全性检查。

3) 有数据传输介质的使用申请流程及授权规定。
4) 有适用的数据传输介质选用标准，避免数据传输介质出现无备份状况。
5) 有统一、适用的数据传输介质报废制度。

b) 传输形式：
1) 数据传输的内容宜尽量避免在传输过程中直接可见或明文可读。
2) 宜有针对数据传输的、独立的安全机制。
3) 敏感数据的传输宜遵循“一事一议”的原则，申请授权。

c) 在数据交换方式上，宜考虑如下事项：
1) 组织宜设立了统一的数据共享交换安全管理的岗位和人员,负责相关原则和技术能力的提供,并推广相关要求在相关业务的落地执行。
2) 宜明确数据共享的原则和安全规范,明确数据共享内容范围和数据共享的管控措施,及数据共享涉及机构或部门相关用户职责和权限。
3) 宜明确数据提供者与共享数据使用者的数据安全责任和安全防护能力。
4) 宜明确数据共享审计规程和审计日志管理要求,明确审计记录要求,为数据共享安全事件的处置、应急响应和事后调查提供帮助。
5) 使用外部的软件开发包/组件/源码前宜进行安全评估,获取的数据宜符合组织的数据安全要求。
6) 组织宜设立相关岗位人员,负责组织的数据公开发布信息,并且对数据发布人员进行安全培训。
7) 宜明确数据公开发布的审核制度,严格审核数据发布合规要求。
8) 宜明确数据公开内容、适用范围及规范,发布者与使用者权利和义务。
9) 宜定期审查公开发布的数据中是否含有非公开信息,并采取相关措施满足数据发布的合规性。
10) 宜采取必要措施建立数据公开事件应急处理流程。
11) 组织宜设立统一负责数据接口安全管理的岗位和人员,由该岗位人员负责制定整体
12) 的规则并推广相关流程的推行。
13) 宜明确数据接口安全控制策略,明确规定使用数据接口的安全限制和安全控制措施,如身份鉴别、访问控制、授权策略、签名、时间戳、安全协议等。
14) 宜明确数据接口安全要求,包括接口名称、接口参数等。
15) 宜与数据接口调用方签署了合作协议,明确数据的使用目的、供应方式、保密约定、数据安全责任等。
16) 负责数据接口安全工作的人员宜充分理解数据接口调用业务的使用场景,具备充分的数据接口调用的安全意识、技术能力和风险控制能力。

7.3.3.1.2 技术要求

3级数据在可控区域内进行传输，宜参考如下技术要求（结合GB/T 37988-2019数据交换安全部分）：

a) 进行数据传输之前，数据发送方与接收方之间宜有身份合法性验证机制。
b) 宜采用一定的数据校验技术，确保数据经过传输后的完整性和一致性。
c) 宜有针对数据传输的监控机制，避免数据在传输过程中不被分流。宜避免大批量的数据被一次性传输。
d) 宜有协议接口和 API 接口监控和异常处置能力。
e) 全量数据传输和增量数据传输宜采用相互独立的通道实施。

f) 运用合适的保密技术，确保敏感数据在数据传输过程中的保密性。
g) 宜尽可能采用具有独立安全机制的数据传输介质。
h) 宜采取措施确保个人信息在委托处理、共享、转让等对外提供场景的安全合规,如数据脱敏、数据加密、安全通道、共享交换区域等。
i) 宜对共享数据及数据共享过程进行监控审计,共享的数据宜属于共享业务需求且没有超出数据共享使用授权范围。
j) 宜明确共享数据格式规范,如提供机器可读的格式规范。
k) 宜建立数据发布系统,实现公开数据登记、用户注册等发布数据和发布组件的验证机制。
l) 宜具备对接口不安全输入参数进行限制或过滤能力,为接口提供异常处理能力。
m) 宜具备数据接口访问的审计能力,并能为数据安全审计提供可配置的数据服务接口。
n) 宜对跨安全域间的数据接口调用采用安全通道、加密传输、时间戳等安全措施。

7.3.3.1.3 数据接触者要求

行业机构建立、健全数据管理规定，明确对数据传输人员的要求（结合GB/T 37988-2019数据交换安全部分）：

a) 遵守数据传输的权限要求，不私自或越权传输数据。
b) 遵守数据传输的时效性要求，准确、高效地完成数据传输。
c) 遵守数据传输职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。
d) 有义务配合做好所传输数据的保密工作。
e) 负责数据共享该项工作的人员宜能够充分理解组织的数据共享规程,并根据数据共享的业务执行相应的风险评估,从而提出实际的解决方案.
f) 负责数据发布安全管理工作的人员宜充分理解数据安全发布的制度和流程,通过了岗位能力评估,并能够根据实际发布要求建立相应的应急方案。

7.3.3.2 非可控区域

7.3.3.2.1 管理要求

非可控区域的数据传输必须经过行业机构的批准或授权，宜明确如下事项（结合GB/T 37988-2019数据交换安全部分）：

a) 对数据传输介质的要求：
   1) 行业机构宜与所使用数据传输介质的所有者完成具有法律效力的责任与义务的约定，确保数据传输介质的安全性与可用性。
   2) 行业机构自有数据传输介质在发生使用权转移时，双方宜进行确认。
   3) 宜避免数据传输介质在行业机构人员不在场的情况下出现在非可控区域。
b) 对数据传输形式的要求：
   1) 行业机构宜对非可控区域的数据传输进行专项评估。
   2) 禁止以明文或可读方式传输数据。
c) 在数据交换方式上，宜考虑如下事项：
   1) 宜定期评估数据共享机制、相关组件和共享通道的安全性。
   2) 组织宜针对关键的数据资源发布明确了安全发布细则和审核流程。
   3) 组织宜细化明确各类数据发布场景的审核流程,从审核的有效性和审核的效率层面充分考虑流程节点的制定。

7.3.3.2.2 技术要求

非可控区域的数据传输，宜明确如下事项（结合GB/T 37988-2019数据交换安全部分）：

a) 宜有针对数据传输的监控机制，避免数据在传输过程中被不当获取或破坏。
b) 宜尽量以行业机构可控的协议接口或 API 作为数据传输主要方式。
c) 直接提供数据实体的情况下，必须要对数据实体进行异化及保密处理。
d) 宜确保敏感数据按授权路径进行定向传输。
e) 宜有协议接口和 API 接口监控和异常处置能力。
f) **对于有风险的数据传输行为，技术系统宜有阻断传输的功能。**
g) **对于数据的批量传输，因为涉及数据量较大，相关安全风险和安全危害也会被乘倍放大，需要采用有效的制度和工具控制数据批量传输的安全风险。**
h) **宜建立数据接口安全监控措施,以对接口调用进行必要的自动监控和处理。**

7.3.3.2.3 数据接触者要求

行业机构建立、健全数据管理规定，明确对数据传输人员的要求：
a) 遵守数据传输的权限要求，不私自或越权传输数据。
b) 遵守数据传输的时效性要求，准确、高效地完成数据传输。
c) 遵守数据传输职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。
d) 有义务配合做好所传输数据的保密工作。

7.3.4 数据处理

7.3.4.1 可控区域

7.3.4.1.1 管理要求

对第3级数据的数据处理工作在可控区域中的具体管理要求如下：
a) 数据处理可遵循“谁处理，谁负责”的原则，明确数据处理者的责任。
b) 数据处理宜采取用户权限管理、数据权限管理等方式管理数据处理权限。
c) 未经授权，不可非法生成、擅自修改、泄漏、丢失与破坏信息系统数据。
d) 数据处理宜记录数据操作日志，并按文档保管要求统一管理。
e) 宜在测试环境和生产环境均实现数据的可恢复性
f) 信息系统宜采取用户权限管理、数据权限管理等途径，对数据处理进行控制，确保有数据处理权限的人员或系统才能处理数据。
g) 数据处理逻辑宜符合业务要求，确保合规，进行充分测试并验证，确保数据的完整、可用。
h) 数据生成宜符合监管及法律法规的要求。
i) 涉及敏感数据的直接处理，宜采取双人或全程监控的方式，确保数据处理逻辑符合要求，数据处理结果符合预期。
j) 直接数据处理宜做好防护措施，确保数据处理失败或不符合预期的情况下，能恢复处理之前的数据状态。
k) 宜确保系统测试、业务测试等非生产要求导致的数据处理在完成相关任务后，数据状态能恢复到处理之前。
l) **宜及时评估数据处理结果的数据等级变更。**
m) **宜及时掌握数据等级分布情况（按照 JR／T 0158-2018 的 8 执行）。**

7.3.4.1.2 技术要求

对第3级数据的数据处理工作在可控区域中的具体技术要求如下：

a) 宜支持针对数据处理者的用户标识和用户鉴别，保证数据处理者的唯一性。
   1) 在登录或连接系统时，宜采用鉴别方式中“基于知道的”（如口令）、“基于拥有的”（如证书或令牌）、“基于个人特征的”（如指纹、眼纹等）等机制进行用户身份鉴别，以确保数据处理者的合法性。
   2) 数据处理者的身份鉴别方式宜有定期或不定期的安全评估，以确保其鉴别方式的安全。
   3) 宜采集数据接触者的特征信息，辅助进行身份鉴别。比如员工工号、终端识别码、身份认证类型、预留信息等。
b) 针对该级数据，宜提供符合该级的处理保护：
   1) 操作日志留痕。
   2) 直接数据处理，宜做好监控和处理前备份工作。
   3) **对敏感数据的处理，宜做好处理前、处理后及处理原因的留痕。针对敏感数据的处理，宜考虑数据处理的可恢复性。**
c) 数据处理权限控制：
   1) **严禁擅自处理授权以外的数据。**
   2) **严禁未经授权的人员或信息系统执行数据处理。**
   3) **宜制订数据处理权限在不同粒度上的控制规则，如区域级、人员级、系统级、用户级、文件级、库级、表级、字段级、语句级等。**
d) 数据处理能力要求：
   1) 可根据信息系统重要性水平、性能容量评估情况，制定数据处理能力测试，确保满足数据处理需求。
   2) **数据处理能力的建设宜以行业机构自身对于信息系统性能容量评估结论为依据。**
   3) **数据处理能力可视信息系统的地位而有所区别，比如备用信息系统。**
   4) **行业机构宜视自身情况做好数据处理能力的弹性管理，确保在需要的时候，能快速、及时地调整信息系统的数据处理能力。**
   5)
e) 数据处理安全控制：
   1) 数据处理宜在投入生产环境前经过充分测试。
   2) 直接数据处理，宜有复核或审核机制。
   3) 数据处理时必须在约定时间范围内对每一次的数据处理做边界管控，对符合预期及不符合预期的情况，预设数据处理逻辑。
   4) 对于有关联关系的数据处理，宜确保处理逻辑的完整性。
   5) 数据处理专用终端进行，操作流程可追溯。
   6) 对于数据处理终端缓存的数据进行删除，以保证数据处理过程中涉及的数据不会被恢复。
   7) **数据处理逻辑必须符合业务要求，确保合规，且在投入生产使用前经过完整、严格的测试。**
   8) **脱敏性质的数据处理，宜确保数据处理的不可逆性，可在保证敏感数据安全的情况下，尽量提高数据有效性和一致性。**

7.3.4.1.3 数据接触者要求

对第3级数据的数据处理工作在可控区域中的具体数据接触者要求如下：

a) 数据接触者在数据处理前，宜获得行业机构的授权，并在授权范围内进行数据处理。

b) 数据接触者宜与行业机构签订相应的保密协议。
c) 数据处理者宜遵循数据处理要求，不得擅自变更数据处理要求或擅自进行数据处理。
d) **行业机构宜根据该级数据分类的情况，对数据处理者进行权限限定。**
e) **行业机构宜根据自身对数据分类分级的情况，限定数据处理者的数据处理工作区域，避免在不恰当的区域处理不当类型或不当等级的数据。**
f) **数据接触者宜配合行业机构的要求，提供自身特征信息。**

7.3.4.2 非可控区域

7.3.4.2.1 管理要求

对第3级数据的数据处理工作在非可控区域中的具体管理要求如下：
a) 原则上，行业机构宜避免在非可控区域处理生产数据。
b) 如有特殊需求，行业机构需要在非可控区域处理数据时，宜采取有效措施确保数据处理者、数据处理逻辑、数据使用范围和数据的安全。
c) 非可控区域的数据处理授权审批宜严于可控区域的数据处理授权审批。

7.3.4.2.2 技术要求

对第3级数据的数据处理工作在非可控区域中的具体技术要求如下：
a) 宜加强数据处理逻辑的完整性检查与判断。
b) 宜尽量对数据处理逻辑进行唯一性标识。
c) 宜采取技术手段，如加密、变形、遮蔽、添加噪声等方式确保数据处理逻辑的安全。
d) 宜采取技术手段，对数据处理的规模设定阈值进行监控，对于异常情况具备安全管控手段。
e) 宜避免以可读或明文方式展示或保留数据处理的留痕信息。
f) **宜对敏感数据添加数据水印，确保对可能泄露的数据进行溯源。**
g) **宜对敏感数据进行隐私保护。**

7.3.4.2.3 数据接触者要求

对第3级数据的数据处理工作在非可控区域中的具体数据接触者要求如下：
a) 非可控区域的数据处理者必须获得行业机构的专属授权，以“一事一授”为宜。
b) 数据接触者宜与行业机构签订相应的保密协议。
c) 数据处理者宜遵循数据处理要求，不得擅自变更数据处理要求或擅自进行数据处理。
d) **数据接触者宜配合行业机构的要求，提供自身特征信息。**

7.3.5 数据存储

7.3.5.1 可控区域

7.3.5.1.1 管理要求

3 级数据在可控区域应充分重视数据存储安全，具体管理要求如下：
a) 数据存储期限宜满足行业监管要求，比如对于敏感数据、业务变更数据、交易记录等数据的保存宜不低于 20 年。
b) 宜制订相应的数据存储管理要求，明确管理人员、管理对象及职责范围。对申请流程、存储检查、介质安全、数据销毁（含介质）、存储密级、时限等做出规定。

c) 宜视自身数据分类分级情况，充分利用多中心容灾能力，建设完善的数据存储体系，如可用性、备份类型、备份频率、存储介质、存储区域等。
d) 宜区别对待临时数据存储与持久化数据存储。
e) 宜制订针对离线数据、备份数据的存储管理要求，确保它们的可恢复能力。
f) 宜制订针对移动存储介质的管理要求，避免敏感数据在移动存储环节泄漏。
g) 数据存储位置宜满足法律法规及行业监管要求。
h) **宜视信息系统数据处理情况的不同，而选择相应的数据存储方案，以满足不同的数据处理需求，如吞吐量、响应时间等。**
i) **数据存储能力的建设宜以行业机构自身对于信息系统性能容量评估结论为依据，在确保够用的同时，还要具备良好的弹性调整空间，以应对突发的数据存储需求。**
j) **宜制定数据销毁机制，确保该级数据及其承载介质以符合行业或机构自身的要求被以合适的方式销毁。**
k) **宜制定数据删除机制，在批量删除时保证双岗复核等必要的监督管理操作。**
l) **宜制定数据销毁指引，明确销毁方式和销毁要求，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制，从而实现对数据的有效销毁（参照 GB/T 37988-2019）。**

7.3.5.1.2 技术要求

3 级数据在可控区域数据存储的技术要求如下：

a) 物理安全
   1) 宜充分评估数据存储区域的安全级别并采取技术手段进行防护，包括数据存储区域的物理位置、防火、防雷、电力保障、电磁防护、防盗窃和防破坏等。
   2) 宜建立多数据存储区域，各数据存储区域之间的物理距离宜满足灾备要求。
   3) 宜建立数据存储区域的不间断监控机制，确保及时发现并处置突发事件。
   4) 宜建立访问控制机制，确保获得授权的数据接触者访问数据存储区域和存储介质。
b) 安全控制
   1) 宜建立数据存储的权限控制机制，如用户权限矩阵、多因子身份识别等，确保获得授权的数据接触者才能进行数据存储操作。
   2) 针对不同级别的数据，可考虑对其数据存储权限的授权设立期限或次数限制。
   3) 宜避免数据存储者同时拥有数据处理的权限。
   4) 数据存储宜做好操作留痕，并形成检查或审计机制。
c) 存储数据的安全
   1) 无论是临时存储，还是持久存储，数据存储都必须获得数据所有者的授权。
   2) 宜采用数据同步技术，保障各数据存储区域数据的一致性。瞬时的数据同步可以是增量同步，但在一定时间内，宜保证多个数据存储区域数据的一致性和完整性。
   3) 宜充分评估信息系统对于数据安全的要求，制订相应的多存储区域数据同步方案。数据同步可以是实时，也可以是定时的。
   4) 多存储区域存储数据的情况下，宜确保每个存储区域的数据具备独立的可恢复性和可用性。
   5) 宜根据自身数据分类分级的情况，针对不同类别、不同等级的数据，制订相应的数据存储策略。敏感数据宜至少有两个不同的存储区域且至少要使用两种不同类型的存储介质进行存储。
   6)

7） 宜通过多种技术手段定期或不定期地检查存储数据的可用性、安全性，如查询、抽样恢复、完整性检查等。

8） 宜避免以明文或可读方式存储敏感数据。

9） 宜加强信息系统的安全检查与防范，定期或不定期的对信息系统进行安全检查与加固，确保信息系统在安全补丁、漏洞修补、木马防范、病毒查杀、后门修复等方面及时得到更新，严防数据损毁、泄漏。

10） 宜加强对数据删除的检查和验证，对数据内容进行清除，防止因对存储介质上数据内容的恶意恢复而导致的数据泄漏风险。

11） 宜使用数据和介质销毁工具对各类数据和介质销毁（参照 GB/T 37988-2019），包括但不限于网络存储数据、针对闪存、硬盘、磁带、光盘等数据的有效销毁，确保以不可逆的方式销毁数据及其副本内容，从而保证数据销毁的有效性。

d） **个人信息不宜超出收集使用规则中的保存期限，用户注销账号后宜当及时删除其个人信息，经过处理无法关联到特定个人且不能复原（以下称匿名化处理）的除外。**

7.3.5.1.3 数据接触者要求

3 级数据在可控区域数据存储的数据接触者要求如下：

a） 宜制订数据存储操作及数据存储介质的管理规定，明确接触者的资质及岗位要求。

b） 数据存储及存储介质管理人员宜为行业机构正式员工。针对其他人员执行数据存储相关工作的情况，行业机构宜与其及所属组织签订相应的工作合同。

c） 数据接触者不得擅自执行或变更数据存储要求。

d） 宜避免单人执行敏感数据的存储操作。

7.3.5.2 非可控区域

7.3.5.2.1 管理要求

3 级数据在非可控区域应充分重视数据存储安全，具体管理要求如下：

a） 行业机构宜与数据存储区域所属的组织签订相关协议，明确约定责任与义务，确保该区域的安全。

b） 非可控区域的数据存储授权审批宜严于可控区域的数据存储授权审批。

c） 宜与数据存储实际执行者所属的组织签订工作合同，明确数据存储操作要求及保密责任。

d） 除监管及法律法规要求外，严禁在非可控区域以任何方式存储敏感数据。

7.3.5.2.2 技术要求

3 级数据在非可控区域数据存储的技术要求如下：

a） 宜以临时存储为主，存储期限宜以数据接触者在场为限。数据接触者为非人主体的情况下，宜以数据接触者失活为限。

b） 除数据所有者授权外，宜避免以明文或可读方式存储数据。

c） 执行数据存储操作宜确保数据接触者处于相对独立的安全空间。

d） 除监管及法律法规要求外，非可控区域存储的数据宜进行脱敏处理。

e） 除监管及法律法规要求外，数据存储介质宜具备独立的安全控制措施，避免被任意访问。

7.3.5.2.3 数据接触者要求

3 级数据在非可控区域数据存储的数据接触者要求如下：

a) 宜有特别的数据存储授权，宜以“一事一议”为原则进行授权。
b) 除监管及法律法规要求外，禁止第三方人员在非可控区域执行数据存储操作或访问存储介质。

7.4 4级数据安全要求

7.4.1 数据采集

7.4.1.1 可控区域

7.4.1.1.1 管理要求

对第4级数据的数据采集工作在可控区域中的具体管理要求如下：

A、针对个人信息类数据的要求

a) 数据采集宜制定并公开收集使用规则，个人信息当主体同意征集后，方可按照规则收集和使用个人数据（依据 JR/T 0171-2020 7.1.1 c 以及 GB/T 35273-2017 5.3 a）。
b) 因业务需要，需扩大个人信息使用范围的，宜当征得个人信息主体同意。
c) 从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务。
d) 不宜因个人信息主体拒绝或者撤销同意收集核心功能服务所需以外的其他信息，而拒绝提供核心业务功能服务。
e) 不宜依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为，包括服务质量、价格差异等。
f) 采集14周岁以下未成年人个人信息的，宜当征得其监护人同意（依据 GB/T 35273-2017 5.5 c）。

B、其他数据的要求

a) 采取自动化手段访问收集网站数据，自动化访问收集流量不可超过网站日均流量三分之一。
b) 以经营为目的收集重要数据或个人敏感信息的，宜当明确数据安全责任人。数据安全责任人由具有相关管理工作经历和数据安全专业知识的人员担任，参与有关数据活动的重要决策，直接向网络运营者的主要负责人报告工作。
c) 网络运营者兼并、重组、破产的，数据承接方宜承接数据安全责任和义务。没有数据承接方的，宜对数据作删除处理。
d) 发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，行业机构宜：
    1) 立即采取补救措施。
    2) 及时以电话、短信、邮件或信函等方式告知个人信息主体。
    3) 并按要求向行业主管监管部门报告。

7.4.1.1.2 技术要求

对第4级数据的数据采集工作在可控区域中的具体技术要求如下：

A、针对个人信息类数据的要求

a) 收到有关个人信息查询、更正、删除以及用户注销账号请求时，宜在合理时间和代价范围内予以查询、更正、删除或注销账号。
b) 向他人提供个人信息前，宜评估可能带来的安全风险，并征得个人信息主体同意。下列情况除外（依据 JR/T 0171-2020 7.1.1 d 以及 GB/T 35273-2017 8.5）：
    1) 从合法公开渠道采集且不明显违背个人信息主体意愿；
    2) 个人信息主体主动公开；
    3) 经过匿名化处理；

4) 执法机关依法履行职责所必需；
5) 维护国家安全、社会公共利益、个人信息主体生命安全所必需。

c) 向境外提供个人信息按有关规定（依据 GB/T 35273-2017 8.7 c）执行。

B、其他数据的要求

a) 利用用户数据和算法推送新闻信息、商业广告等（以下简称“定向推送”），宜以明显方式标明“定推”字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，宜停止推送，并删除已经收集的设备识别码等用户数据和个人信息。
b) 利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等信息，宜以明显方式标明“合成”字样；不得以谋取利益或损害他人利益为目的自动合成信息。
c) 宜采取措施督促提醒用户对自己的网络行为负责、加强自律，对于用户通过社交网络转发他人制作的信息，宜自动标注信息制作者在该社交网络上的账户或不可更改的用户标识。
d) 网络运营者发布、共享、交易或向境外提供重要数据前，宜评估可能带来的安全风险，并报经行业主管监管部门同意。

7.4.1.1.3 数据接触者要求

对第4级数据的数据采集工作在可控区域中的具体数据接触者要求如下：

a) 数据接触者分析利用所掌握的数据资源，发布市场预测、统计信息、个人和企业信用等信息，不得影响国家安全、经济运行、社会稳定，不得损害他人合法权益。
b) 数据接触者对接入其平台的第三方应用，宜明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。
c) 根据该级数据分类的情况，对数据接触者进行权限限定。

7.4.1.2 非可控区域

7.4.1.2.1 管理要求

对第4级数据的数据采集工作在非可控区域中的具体管理要求如下：

a) 数据采集宜在可控区域使用信息系统自动化进行采集，确保数据采集的安全性、不可篡改性。如有特殊需要，在非可控区域进行离线采集时，宜保证数据电子化过程中的安全性，加强对采集人员的安全责任及意识培训，防止数据泄露。
b) 在非可控区域采集数据时，不宜进行批量数据采集。可跟踪和记录数据采集过程，同时宜遵守可控区域的要求。

7.4.1.2.2 技术要求

对第4级数据的数据采集工作在非可控区域中的具体技术要求如下：

a) 宜满足可控区域的技术要求。
b) 对纸质载体采集的数据，宜采用类似 OCR 扫描的技术对数据进行自动识别、录入。

7.4.1.2.3 数据接触者要求

对第4级数据的数据采集工作在非可控区域中的具体数据接触者要求如下：

a) 宜满足该级可控区域的数据接触者要求
b) 数据接触者在非可控区域进行离线采集时，不得私自复制、修改、使用数据。

7.4.2 数据展现

7.4.2.1 可控区域

7.4.2.1.1 管理要求

对第4级数据的数据展现工作在可控区域中的具体管理要求如下：

a) 该级数据展现终端可配合数据所有者的要求，提供终端相关信息。
b) 该级数据展现宜按照“必须知道”、“最小授权”和“最小功能” 原则进行权限管理。建立和完善岗位权限管理流程，避免不恰当的授权。
   1) 系统管理员宜避免直接接触业务数据；
   2) 宜有专用的权限管理岗位；
   3) 互斥岗位要避免权限交叉；
   4) 业务信息的展现及使用均宜在业务开展及管理所需最小授权范围内使用；
   5) 禁止服务机构人员直接接触未经脱敏处理的原始数据；
   6) 按该级数据要求对数据接触者进行披露并保存访问记录。
c) 针对不同前端展现系统软件和终端硬件设备，建立和完善数据安全管理措施，以保证数据不被截取、泄露、盗取：
   1) 经营机构人员只能以公司授权的用户按公司规定的认证方式访问公司授权的业务系统；
   2) 尽量降低高安全级别终端对外暴露的程度；
   3) 通过数据展现终端改变数据展现方式的操作或行为宜经过授权或审批；
   4) 可控区域的所有数据展现软件及设备宜由行业机构拥有完全独立的所有权、使用权、支配权，并拥有完全独立、自主的投放、更新及销毁权。
d) **宜根据各个部门和岗位的职责明确授权审批部门及批准人，对重要资源的访问等关键活动进行审批，重要审批授权记录宜留档备查。**
e) 宜取合理的技术措施确保数据展现的准确性。当数据有误时，宜及时更正。

7.4.2.1.2 技术要求

对第4级数据的数据展现工作在可控区域中的具体技术要求如下：

a) 数据展现宜采用区域化管理，区域与数据访问权限绑定。
b) 宜实施通信与接入管制，按照监管要求并结合行业机构实际情况，对数据的展现请求采取认证、留痕与监测等控制措施，以记录或防止数据被不当获取和使用。
c) 宜通过技术手段获取数据展现终端的特征信息。
d) 宜对展现的数据进行标识，以唯一识别数据所有者身份。
e) 宜根据机构自身情况限定可展现数据的终端类型与展现方式。
f) 宜采用数据校验，数据可追溯等机制确保展现数据的准确性。

7.4.2.1.3 数据接触者要求

对第4级数据的数据展现工作在可控区域中的具体数据接触者要求如下：

a) 行业机构人员对在工作过程中接触的数据，非因工作需要，在任职期间和离职或更换工作岗位后不得将其泄露给公司其他员工或任何第三方；人员离岗后宜立即终止其所有数据访问权限，并宜取回各种用于接触数据的身份识别证件、钥匙、徽章、密码等软硬件口令或设备。
b) 行业机构宜禁止除授权人员以外的其他人员直接查看未经脱敏处理的敏感数据。
c) 数据接触者宜自觉识别并评估数据展现环境的安全性，避免在危险的环境中展现该级数据。

7.4.2.2 非可控区域

7.4.2.2.1 管理要求

因非可控区域不确定性更高的特性，宜充分评估该级数据在非可控区域展现的必要性，针对不同前端展现系统软件和终端设备，建立和完善数据安全管理措施，以保证数据不被截取、泄露、盗取，具体要求如下：

a) 数据安全等级为该级的数据，原则上宜避免在非可控区域展现。确有需要展现的情况下，宜有严格的身份识别与授权程序，确保数据展现符合权限规定。
b) 因监管部门要求提供、行业机构内部研究、行政或业务审批、追偿、检查审计、配合司法调查等调阅特定信息，需要确保数据调阅凭证真实、可信并做好调阅留痕。
c) 敏感数据要尽可能地缩小接触者的范围，且只能提供只读操作。

7.4.2.2.2 技术要求

对第4级数据的数据展现工作在非可控区域中的具体技术要求如下：

a) 数据展现终端（含软件、硬件）必须经过行业机构授权或认证。
b) 数据展现终端（含软件、硬件）不得保存敏感信息。
c) 限制数据批量展示，采取反爬措施，防止数据被批量获取。
d) 采用一些更加安全的数据展现方式，如减少数据展现量、敏感信息屏蔽、水印、身份识别前置等技术。

7.4.2.2.3 数据接触者要求

宜为数据接触者建立正确的安全意识，提高数据接触者的安全意识和数据保护意识，严格限定数据接触者的相关权限，保障数据的安全性，具体要求如下：

a) 对数据接触者进行数据安全宣传和培训，强调对数据进行保护的必要性，避免敏感信息外泄。
b) 涉及聘用服务机构及人员为行业机构提供信息技术开发、业务咨询、合作等外包服务的，宜与外包方签署保密协议，明确保密义务，不得违反约定擅自获取及传播行业机构数据。

7.4.3 数据传输

7.4.3.1 可控区域

7.4.3.1.1 管理要求

4级数据在可控区域内进行传输，宜参考如下管理要求（结合GB/T 37988-2019数据交换安全部分）

a) 针对传输介质，行业机构宜制定相应的管理制度，明确如下事项：
   1) 宜有专职人员保管重要的数据传输介质。
   2) 宜有针对数据传输介质的定期安全性检查。
   3) 宜有数据传输介质的使用申请流程及授权规定。
   4) 宜有适用的数据传输介质选用标准，避免数据传输介质出现无备份状况。
   5) 宜有统一、适用的数据传输介质报废规定。
b) 在数据传输的形式上，行业机构宜根据自身情况，明确如下事项：
   1) 数据传输的内容宜尽量避免在传输过程中直接可见或明文可读。
   2) 宜有针对数据传输的、独立的安全机制。
   3) 敏感数据的传输宜遵循“一事一议”的原则，申请授权。
c) **在数据交换方式上，宜考虑如下事项：**

1) 宜在组织统一的数据共享原则基础上,针对主要的数据共享场景明确了安全细则或审批流程,如对境外机构的数据共享安全细则、对政府机构的数据共享安全细则等。
2) 宜定期评估数据共享机制、相关组件和共享通道的安全性。
3) 宜在共享数据时,对数据接收方的数据安全防护能力进行评估。
4) 组织宜针对关键的数据资源发布明确了安全发布细则和审核流程。
5) 组织宜细化明确各类数据发布场景的审核流程,从审核的有效性和审核的效率层面充分考虑流程节点的制定。

7.4.3.1.2 技术要求

4级数据在可控区域内进行传输，宜参考如下技术要求（结合GB/T 37988-2019数据交换安全部分）

a) 进行数据传输之前，数据发送方与接收方之间宜有身份合法性验证机制。
b) 运用合适的保密技术，确保敏感数据在数据传输过程中的保密性。
c) 宜采用一定的数据校验技术，确保数据经过传输后的完整性和一致性。
d) 宜有针对数据传输的监控机制，避免数据在传输过程中不被分流。宜避免大批量的数据被一次性传输。
e) 宜尽可能采用具有独立安全机制的数据传输介质。
f) 行业机构宜充分评估数据传输能力，确保能有效宜对突发性数据传输要求。
g) 宜建立组织统一的数据共享交换系统,提示数据共享交换的安全风险并进行在线审核。
h) 宜配置数据共享机制或服务组件，明确数据共享最低安全防护要求。
i) 组织宜建立统一的数据发布系统,提示数据发布安全风险并进行在线审核。
j) 宜建立数据接口安全监控措施,以对接口调用进行必要的自动监控和处理。
k) 宜有协议接口和 API 接口监控和异常处置能力。
l) 全量数据传输和增量数据传输宜当采用相互独立的通道实施。

7.4.3.1.3 数据接触者要求

行业机构建立、健全数据管理规定，明确对数据传输人员的要求（结合GB/T 37988-2019数据交换安全部分）：

a) 遵守数据传输的权限要求，不私自或越权传输数据。
b) 遵守数据传输的时效性要求，准确、高效地完成数据传输。
c) 遵守数据传输职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。
d) 有义务配合做好所传输数据的保密工作。
e) 负责数据共享该项工作的人员宜能够充分理解组织的数据共享规程,并根据数据共享的业务执行相应的风险评估,从而提出实际的解决方案.
f) 负责数据发布安全管理工作的人员宜充分理解数据安全发布的制度和流程,通过了岗位能力评估,并能够根据实际发布要求建立相应的应急方案。

7.4.3.2 非可控区域

7.4.3.2.1 管理要求

非可控区域的数据传输必须经过行业机构的批准或授权，宜明确如下事项（结合GB/T 37988-2019数据交换安全部分）：

a) 对数据传输介质的要求：

1) 行业机构宜与所使用数据传输介质的所有者完成具有法律效力的责任与义务的约定，确保数据传输介质的安全性与可用性。
2) 行业机构自有数据传输介质在发生使用权转移时，双方宜进行确认。
3) 宜避免数据传输介质在行业机构人员不在场的情况下出现在非可控区域。

b) 对数据传输形式的要求：
1) 行业机构宜对非可控区域的数据传输进行专项评估。
2) 禁止以明文或可读方式传输数据。

c) 在数据交换方式上，宜考虑如下事项：
1) 宜定期评估数据共享机制、相关组件和共享通道的安全性。
2) 组织宜针对关键的数据资源发布明确了安全发布细则和审核流程。
3) 组织宜细化明确各类数据发布场景的审核流程,从审核的有效性和审核的效率层面充分考虑流程节点的制定。

7.4.3.2.2 技术要求

非可控区域的数据传输，宜明确如下事项（结合GB/T 37988-2019数据交换安全部分）

a) 宜有针对数据传输的监控机制，避免数据在传输过程中被不当获取或破坏。
b) 宜尽量以行业机构可控的协议接口或 API 作为数据传输主要方式。
c) 直接提供数据实体的情况下，必须要对数据实体进行异化及保密处理。
d) 宜确保敏感数据按授权路径进行定向传输。
e) 宜有协议接口和 API 接口监控和异常处置能力。
f) 对于有风险的数据传输行为，技术系统宜有阻断传输的功能。
g) 对于数据的批量传输，因为涉及数据量较大，相关安全风险和安全危害也会被乘倍放大，需要采用有效的制度和工具控制数据批量传输的安全风险。
h) 宜建立数据接口安全监控措施,以对接口调用进行必要的自动监控和处理。

7.4.3.2.3 数据接触者要求

行业机构建立、健全数据管理规定，明确对数据传输人员的要求：

a) 遵守数据传输的权限要求，不私自或越权传输数据。
b) 遵守数据传输的时效性要求，准确、高效地完成数据传输。
c) 遵守数据传输职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。
d) 有义务配合做好所传输数据的保密工作。

7.4.4 数据处理

7.4.4.1 可控区域

7.4.4.1.1 管理要求

对第4级数据的数据处理工作在可控区域中的具体管理要求如下：

a) 数据处理可遵循“谁处理，谁负责”的原则，明确数据处理者的责任。
b) 数据处理宜采取用户权限管理、数据权限管理等方式管理数据处理权限。
c) 未经授权，不可非法生成、擅自修改、泄漏、丢失与破坏信息系统数据。
d) 数据处理宜记录数据操作日志，并按文档保管要求统一管理。
e) 宜在测试环境和生产环境均实现数据的可恢复性

f) 信息系统宜采取用户权限管理、数据权限管理等途径，对数据处理进行控制，确保有数据处理权限的人员或系统才能处理数据。
g) 数据处理逻辑宜符合业务要求，确保合规，进行充分测试并验证，确保数据的完整、可用。
h) 数据生成宜符合监管及法律法规的要求。
i) 涉及敏感数据的直接处理，宜采取双人或全程监控的方式，确保数据处理逻辑符合要求，数据处理结果符合预期。
j) 直接数据处理宜做好防护措施，确保数据处理失败或不符合预期的情况下，能恢复处理之前的数据状态。
k) 宜确保系统测试、业务测试等非生产要求导致的数据处理在完成相关任务后，数据状态能恢复到处理之前。
l) 宜及时评估数据处理结果的数据等级变更。
m) 宜及时掌握数据等级分布情况（按照 JR／T 0158-2018 的 8 执行）。
n) **数据权限管理宜遵循最小使用权限原则（按照 GB／T 37988-2019 的 9.3.2.3 执行）。**

7.4.4.1.2 技术要求

对第4级数据的数据处理工作在可控区域中的具体技术要求如下：

a) 宜支持针对数据处理者的用户标识和用户鉴别，保证数据处理者的唯一性。
   1) 在登录或连接系统时，宜采用鉴别方式中“基于知道的”（如口令）、“基于拥有的”（如证书或令牌）、“基于个人特征的”（如指纹、眼纹等）等机制进行用户身份鉴别，以确保数据处理者的合法性。
   2) 数据处理者的身份鉴别方式宜有定期或不定期的安全评估，以确保其鉴别方式的安全。
   3) 宜采集数据接触者的特征信息，辅助进行身份鉴别。比如员工工号、终端识别码、身份认证类型、预留信息等。
b) 针对该级数据，宜提供符合该级的处理保护：
   1) 操作日志留痕。
   2) 直接数据处理，宜做好监控和处理前备份工作。
   3) 对敏感数据的处理，宜做好处理前、处理后及处理原因的留痕。针对敏感数据的处理，宜考虑数据处理的可恢复性。
c) 数据处理权限控制：
   1) 严禁擅自处理授权以外的数据。
   2) 严禁未经授权的人员或信息系统执行数据处理。
   3) 宜制订数据处理权限在不同粒度上的控制规则，如区域级、人员级、系统级、用户级、文件级、库级、表级、字段级、语句级等。
d) 数据处理能力要求：
   1) 可根据信息系统重要性水平、性能容量评估情况，制定数据处理能力测试，确保满足数据处理需求。
   2) 数据处理能力的建设宜以行业机构自身对于信息系统性能容量评估结论为依据。
   3) 数据处理能力可视信息系统的地位而有所区别，比如备用信息系统。
   4) 行业机构宜视自身情况做好数据处理能力的弹性管理，确保在需要的时候，能快速、及时地调整信息系统的数据处理能力。
e) 数据处理安全控制：
   1) 数据处理宜在投入生产环境前经过充分测试。
   2) 直接数据处理，宜有复核或审核机制。

3) 数据处理时必须在约定时间范围内对每一次的数据处理做边界管控，对符合预期及不符合预期的情况，预设数据处理逻辑。
4) 对于有关联关系的数据处理，宜确保处理逻辑的完整性。
5) 数据处理专用终端进行，操作流程可追溯。
6) 对于数据处理终端缓存的数据进行删除，以保证数据处理过程中涉及的数据不会被恢复。
7) 数据处理逻辑必须符合业务要求，确保合规，且在投入生产使用前经过完整、严格的测试。
8) 脱敏性质的数据处理，宜确保数据处理的不可逆性，可在保证敏感数据安全的情况下，尽量提高数据有效性和一致性。
9) **能对该级数据流动做好审计工作，具备风险排查能力，快速处置数据的篡改和泄漏等风险。**
10) **具有有效、覆盖数据全生命周期的数据安全保护措施。**

7.4.4.1.3 数据接触者要求

对第4级数据的数据处理工作在可控区域中的具体数据接触者要求如下：
a) 数据接触者在数据处理前，宜该获得行业机构的授权，并在授权范围内进行数据处理。
b) 数据接触者宜与行业机构签订相应的保密协议。
c) 数据处理者宜遵循数据处理要求，不得擅自变更数据处理要求或擅自进行数据处理。
d) 行业机构宜根据该级数据分类的情况，对数据处理者进行权限限定。
e) 行业机构宜根据自身对数据分类分级的情况，限定数据处理者的数据处理工作区域，避免在不恰当的区域处理不当类型或不当等级的数据。
f) 数据接触者宜配合行业机构的要求，提供自身特征信息。

7.4.4.2 非可控区域

7.4.4.2.1 管理要求

对第4级数据的数据处理工作在非可控区域中的具体管理要求如下：
a) 原则上，行业机构宜避免在非可控区域处理生产数据。
b) 如有特殊需求，行业机构需要在非可控区域处理数据时，宜采取有效措施确保数据处理者、数据处理逻辑、数据使用范围和数据的安全。
c) 非可控区域的数据处理授权审批宜严于可控区域的数据处理授权审批。
a) 数据处理必须遵守频率和数据量最小化原则
b) 数据直接处理，必须通过加不可逆加密方式进行。
c) 宜及时掌握数据等级分布情况。

7.4.4.2.2 技术要求

对第4级数据的数据处理工作在非可控区域中的具体技术要求如下：
a) 宜加强数据处理逻辑的完整性检查与判断。
b) 宜尽量对数据处理逻辑进行唯一性标识。
c) 宜采取技术手段，如加密、变形、遮蔽、添加噪声等方式确保数据处理逻辑的安全。
d) 宜采取技术手段，对数据处理的规模设定阈值进行监控，对于异常情况具备安全管控手段。
e) 宜避免以可读或明文方式展示或保留数据处理的留痕信息。
f) **宜对敏感数据添加数据水印，确保对可能泄露的数据进行溯源。**
g) **宜对敏感数据进行隐私保护。**
a) **宜对敏感数据进行不可逆的加密保护。**

7.4.4.2.3 数据接触者要求

对第4级数据的数据处理工作在非可控区域中的具体数据接触者要求如下：

a) 非可控区域的数据处理者必须获得行业机构的专属授权，以“一事一授”为宜。
b) 数据接触者宜与行业机构签订相应的保密协议。
c) 数据处理者宜遵循数据处理要求，不得擅自变更数据处理要求或擅自进行数据处理。
d) 数据接触者宜配合行业机构的要求，提供自身特征信息。

7.4.5 数据存储

7.4.5.1 可控区域

7.4.5.1.1 管理要求

4 级数据在可控区域应充分重视数据存储安全，具体管理要求如下：

a) 数据存储期限宜满足行业监管要求，比如对于敏感数据、业务变更数据、交易记录等数据的保存宜不低于 20 年。
b) 宜制订相应的数据存储管理要求，明确管理人员、管理对象及职责范围。对申请流程、存储检查、介质安全、数据销毁（含介质）、存储密级、时限等做出规定。
c) 宜视信息系统数据处理情况的不同，而选择相应的数据存储方案，以满足不同的数据处理需求，如吞吐量、响应时间等。
d) 宜视自身数据分类分级情况，充分利用多中心容灾能力，建设完善的数据存储体系，如可用性、备份类型、备份频率、存储介质、存储区域等。
e) 数据存储能力的建设宜以行业机构自身对于信息系统性能容量评估结论为依据，在确保够用的同时，还要具备良好的弹性调整空间，以应对突发的数据存储需求。
f) 宜区别对待临时数据存储与持久化数据存储。
g) 宜制订针对离线数据、备份数据的存储管理要求，确保它们的可恢复能力。
h) 宜制订针对移动存储介质的管理要求，避免敏感数据在移动存储环节泄漏。
i) 宜制定数据销毁机制，确保该级数据及其承载介质以符合行业或机构自身的要求被以合适的方式销毁。
j) 宜制定数据删除机制，在数据删除时保证有必要的审批和双岗复核等监督管理机制。
k) 宜制定数据销毁指引，明确销毁方式和销毁要求设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制，从而实现对数据的有效销毁，建立数据销毁效果评定机制，对数据销毁有效性进行评定（参照 GB/T 37988-2019）。
l) 数据存储位置宜满足法律法规及行业监管要求。

7.4.5.1.2 技术要求

4 级数据在可控区域数据存储的技术要求如下：

a) 物理安全
    1) 宜充分评估数据存储区域的安全级别并采取技术手段进行防护，包括数据存储区域的物理位置、防火、防雷、电力保障、电磁防护、防盗窃和防破坏等。
    2) 宜建立多数据存储区域，各数据存储区域之间的物理距离宜满足灾备要求。
    3) 宜建立数据存储区域的不间断监控机制，确保及时发现并处置突发事件。
    4) 宜建立访问控制机制，确保获得授权的数据接触者访问数据存储区域和存储介质。
b) 安全控制

1） 宜建立数据存储的权限控制机制，如用户权限矩阵、多因子身份识别等，确保获得授权的数据接触者才能进行数据存储操作。
2） 针对不同级别的数据，可考虑对其数据存储权限的授权设立期限或次数限制。
3） 宜避免数据存储者同时拥有数据处理的权限。
4） 数据存储宜做好操作留痕，并形成检查或审计机制。

c） 存储数据的安全
1） 无论是临时存储，还是持久存储，数据存储都必须获得数据所有者的授权。
2） 宜采用数据同步技术，保障各数据存储区域数据的一致性。瞬时的数据同步可以是增量同步，但在一定时间内，宜保证多个数据存储区域数据的一致性和完整性。
3） 宜充分评估信息系统对于数据安全的要求，制订相应的多存储区域数据同步方案。数据同步可以是实时，也可以是定时的。
4） 多存储区域存储数据的情况下，宜确保每个存储区域的数据具备独立的可恢复性和可用性。
5） 宜根据自身数据分类分级的情况，针对不同类别、不同等级的数据，制订相应的数据存储策略。敏感数据宜至少有两个不同的存储区域且至少要使用两种不同类型的存储介质进行存储。
6） 宜通过多种技术手段定期或不定期地检查存储数据的可用性、安全性，如查询、抽样恢复、完整性检查等。
7） 宜避免以明文或可读方式存储敏感数据。
8） 宜加强信息系统的安全检查与防范，定期或不定期的对信息系统进行安全检查与加固，确保信息系统在安全补丁、漏洞修补、木马防范、病毒查杀、后门修复等方面及时得到更新，严防数据损毁、泄漏。
9） 宜加强对数据删除的检查和验证，对数据内容进行清除，防止因对存储介质上数据内容的恶意恢复而导致的数据泄漏风险。
10） 宜使用统一的数据和介质销毁工具对各类数据和介质销毁（参照 GB/T 37988-2019），包括但不限于网络存储数据、针对闪存、硬盘、磁带、光盘等数据的有效销毁，确保以不可逆的方式销毁数据及其副本内容，从而保证数据销毁的有效性。
11） 使用国家权威机构认证的机构或设备对存储介质设备进行物理销毁或联系国家认定资质的销毁服务提供商执行存储介质的销毁工作，以保证介质销毁效果。

7.4.5.1.3 数据接触者要求

4 级数据在可控区域数据存储的数据接触者要求如下：

a） 宜制订数据存储操作及数据存储介质的管理规定，明确接触者的资质及岗位要求。
b） 数据存储及存储介质管理人员宜为行业机构正式员工。针对其他人员执行数据存储相关工作的情况，行业机构宜与其及所属组织签订相应的工作合同。
c） 数据接触者不得擅自执行或变更数据存储要求。
d） 宜避免单人执行敏感数据的存储操作。

7.4.5.2 非可控区域

7.4.5.2.1 管理要求

4 级数据在非可控区域应充分重视数据存储安全，具体管理要求如下：

a) 行业机构宜与数据存储区域所属的组织签订相关协议，明确约定责任与义务，确保该区域的安全。
b) 非可控区域的数据存储授权审批宜严于可控区域的数据存储授权审批。
c) 宜与数据存储实际执行者所属的组织签订工作合同，明确数据存储操作要求及保密责任。
d) 除监管及法律法规要求外，严禁在非可控区域以任何方式存储敏感数据。

7.4.5.2.2 技术要求

4 级数据在非可控区域数据存储的技术要求如下：

a) 宜以临时存储为主，存储期限宜以数据接触者在场为限。数据接触者为非人主体的情况下，宜以数据接触者失活为限。
b) 除数据所有者授权外，宜避免以明文或可读方式存储数据。
c) 执行数据存储操作宜确保数据接触者处于相对独立的安全空间。
d) 除监管及法律法规要求外，非可控区域存储的数据宜进行脱敏处理。
e) 除监管及法律法规要求外，数据存储介质宜具备独立的安全控制措施，避免被任意访问。

7.4.5.2.3 数据接触者要求

4 级数据在非可控区域数据存储的数据接触者要求如下：

a) 应有特别的数据存储授权，宜以“一事一议”为原则进行授权。
b) 除监管及法律法规要求外，禁止第三方人员在非可控区域执行数据存储操作或访问存储介质。