ICS 03.060
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0250—2022

证券期货业数据安全管理与保护指引

Guidance for data security management and protection of securities and futures industry

2022-11-14 发布　　2022-11-14 实施

中国证券监督管理委员会　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。

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/TC 180/SC4）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：中国证券监督管理委员会、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、申万宏源证券有限公司、上海证券有限责任公司、深圳财富趋势科技股份有限公司、恒生电子股份有限公司、浙江邦盛科技有限公司、中国金融期货交易所技术公司、海通期货股份有限公司、北京梆梆安全科技有限公司。

本文件主要起草人：姚前、蒋东兴、周云晖、陆骋、周思宇、王晓、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，大部分证券期货业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。

本文件基于JR/T 0158—2018 《证券期货业数据分类分级指引》，采用其中根据数据泄露或损坏造成的影响将数据分为不同级别的数据分级方法，提供了各级数据在数据采集、数据展现、数据传输、数据处理、数据存储（包含数据备份与恢复、删除、销毁环节）过程中的数据管理和技术指引，供证券期货业机构参考。其中，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。

在本文件中，黑体字部分表示相较低一等级数据增加或增强的要求。

证券期货业数据安全管理与保护指引

1 范围

本文件描述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，以及各级数据关于数据采集、数据展现、数据传输、数据处理、数据存储的数据安全管理与保护的思路和方法。

本文件适用于证券期货业机构开展数据安全管理与保护工作的参考和指引。

注：证券期货业机构包括证券期货业市场核心机构（简称核心机构）、证券期货基金经营机构（简称经营机构）、证券期货信息技术服务机构（简称服务机构）、证券期货业市场监管机构（简称监管机构）

本文件不适用于涉及国家秘密的数据。

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 22080—2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 35273—2020 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—2020 《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》、GB/T 22080—2016 《信息技术 安全技术 信息安全管理体系 要求》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 data contact

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

数据控制者 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，并对其完整性、可用性和安全性负责的个人或机构。

3.3

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。

注：一个过程域中包含一个或多个相关活动。

[来源：GB/T 37988—2019，3.9]

3.4

数据采集 data acquisition

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

3.5

数据展现 data display

在直接呈现终端、应用程序终端等所有可以接触数据的呈现区域呈现数据的过程。

3.6

数据传输 data transmission

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的过程。

3.7

数据处理 data processing

信息系统和数据接触者对数据进行使用、加工或转移的过程。

3.8

数据存储 data storage

将数据以各种不同的形式保存、备份与恢复、删除、销毁的过程。

3.9

数据传输介质 transmission medium

在网络中传输数据信息的载体。

注：包含有线传输介质和无线传输介质。

3.10

信息基础设施 infrastructure

承载信息系统的实体电子设备、虚拟运行环境、共用的机房物理环境等基础设施。

3.11

可控区域 controlled area

在每个数据过程域中，数据控制者独立拥有直接承载数据的信息基础设施和其所承载信息系统的管理权或使用权的区域。

3.12

非可控区域 uncontrolled area

在每个数据过程域中，数据控制者非独立拥有直接承载数据的信息基础设施或其所承载信息系统的所有权或使用权的区域。

3.13

数据完整性 data integrity

保护数据正确和完整的特性。

[来源：GB/T 22080—2016，3.8]

3.14

数据可用性 data availability

根据授权实体的要求可访问和使用数据。

[来源：GB/T 22080—2016，3.2]

3.15

数据安全性 data security

以数据安全为中心，保护数据的可用、完整和机密的特性。

3.16

应用程序接口 application programming interface；API

预先定义的接口或软件系统不同组成部分衔接的约定。

4 基本原则

4.1 过程域

数据安全保护措施宜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

对不同安全等级的数据对象进行综合考量，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指引。

4.3 安全性

数据安全性包含管理安全性与技术安全性，从组织、制度、技术三个方面建立完备的数据安全保护措施，保护证券期货业机构的数据和客户信息安全，防范信息泄露。将授权机制、岗位职责与安全技术相结合，在整个数据流转过程中保护数据安全，不被泄露给非授权的对象。

4.4 可用性

数据在各个过程域中的各环节无缺失、损毁，保障数据的完整、可用。

4.5 适配性

对证券期货业机构的不同实际情况具备适配性，使各证券期货业机构可以参考本文件，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，保障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 总体指引

组织架构的规定旨在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。证券期货业机构宜明确数据安全管理的最高责任人，由管理层人员担任，负责领导协调数据安全部门开展工作，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。

数据安全工作涉及的部门包括数据安全管理部门、业务管理部门、合规风控部门、信息技术部门、内部审计部门。

5.2 数据安全管理部门

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：

a) 组织制定数据管理制度，根据数据分类分级原则明确各类数据的分类分级，对数据进行分类分级管理，规范不同分类分级数据的处理方式和处理人员；
b) 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；
c) 明确数据安全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，宜设立数据安全管理相关岗位，并定义各岗位的职责；
d) 明确数据使用的授权机制，明确数据使用的组织、证券期货业机构及人员的责任及义务。

5.3 合规风控部门

合规风控部门是数据安全合规和风险管理工作落实部门，其职责包括：

a) 负责数据安全管理合规和风险制度的编制；
b) 通过指导、规范、检查等手段，对数据安全管理措施和落实情况进行合规风控监管。

5.4 业务管理部门

业务管理部门是业务数据的控制者，其职责包括：

a) 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；
b) 制定本部门所辖范围内关于业务数据安全、合规监督管理等工作的管理要求，防范业务数据泄露。

5.5 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，其职责包括：

a) 负责按照数据安全的制度和技术标准实施数据安全技术保护措施，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、泄露、被篡改、被毁损；
b) 制定和落实针对数据直接接触者的安全技术防控要求；
c) 负责信息系统的数据安全评估、数据安全事件管理和应急响应等工作。

5.6 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。

6 制度指引

核心机构、经营机构、服务机构和监管机构宜建立主要的数据安全管理制度，内容包括：

a) 管理规定：
   1) 数据安全管理：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；
b) 管理细则：
   1） 权限管理：明确权限管理要求，明确访问权限、访问方式及申请流程；
   2) 介质管理：明确数据存放介质管理要求，保障存储介质可追踪、可核查。保障数据在介质中的存放周期、存放方式、访问权限的安全性；
   3) 场所管理：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；
   4) 数据安全防护：根据数据对本证券期货业机构的价值、所受安全威胁的程度，明确数据安全防护要求，并采取相应的数据安全防护措施，保障本证券期货业机构具备与自身适配的数据安全防护能力；
   5) 数据安全事件管理：明确数据安全事件管理机制，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，并依据《中华人民共和国网络安全法》等相关法规规定，形成相应的事件处置预案。同时，保障相关管理要求、处置预案的有效性，定期评估和修订；
   6) 数据安全应急管理：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要求和应急预案，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，保障应急管理措施的有效性；
   7) 数据安全审计：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要求，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，保障审计的有效性和时效性；
   8) 数据安全教育培训：明确数据安全教育培训机制，明确数据安全教育培训工作的计划、培训人员、培训内容及方法等事项。

7 安全管理指引

7.1 1级数据安全指引

7.1.1 数据采集

7.1.1.1 可控区域

7.1.1.1.1 管理指引

对第1级数据的数据采集工作在可控区域中的具体管理指引如下：

a) 宜明确该级数据的可采集范围；
b) 自动化访问采集流量不超过设定的阈值。

7.1.1.1.2 技术指引

对第1级数据的数据采集工作在可控区域中的具体技术指引如下：

a) 采集该级数据时，宜在数据中标明来源和采集时间，以提升数据的可追溯性；
b) 采取自动化手段访问采集数据的，宜有监控措施监控数据采集过程，保障采集数据的准确性、完整性和安全性。

7.1.1.2 非可控区域

7.1.1.2.1 管理指引

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指引如下：

a) 宜满足该级可控区域的管理指引；
b) 在非可控区域采集数据时，可跟踪和记录数据采集过程。

7.1.1.2.2 技术指引

宜满足该级可控区域的技术指引（见 7.1.1.1.2）。

7.1.2 数据展现

7.1.2.1 可控区域

7.1.2.1.1 管理指引

宜采取合理的技术措施保障数据展现的准确性。

7.1.2.1.2 技术指引

宜通过技术手段获取数据展现终端的操作系统信息。

7.1.2.2 非可控区域

7.1.2.2.1 管理指引

宜满足该级可控区域的管理指引（见 7.1.2.1.1）。

7.1.2.2.2 技术指引

宜满足该级可控区域的技术指引（见 7.1.2.1.2）。

7.1.3 数据传输

7.1.3.1 可控区域

7.1.3.1.1 技术指引

对第1级数据的数据传输工作在可控区域中的具体技术指引如下：

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，保障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；
d) 宜对大批量数据的一次性传输进行审批和关注；
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，保障能有效应对突发性数据传输要求；
g) 具备技术条件的情况下，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。

7.1.3.1.2 数据接触者指引

对第1级数据的数据传输工作在可控区域中的具体数据接触者指引如下：

a) 确保数据传输符合权限，不私自或越权传输数据；
b) 确保数据传输的时效性，准确、高效地完成数据传输；
c) 确保数据传输符合职责，不做数据传输之外的、针对所传输数据的、未经授权的事情。

7.1.3.2 非可控区域

7.1.3.2.1 管理指引

对第1级数据的数据传输工作在非可控区域中的具体管理指引如下：

a) 如需使用第三方的数据传输介质，证券期货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，保障数据传输介质的安全性与可用性；
b) 证券期货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；
c) 宜避免数据传输介质在证券期货业机构人员不在场的情况下出现在非可控区域。

7.1.3.2.2 技术指引

宜满足该级可控区域的技术指引（见 7.1.3.1.1）。

7.1.3.2.3 数据接触者指引

宜满足该级可控区域的数据接触者指引（见 7.1.3.1.2）。

7.1.4 数据处理

7.1.4.1 可控区域

7.1.4.1.1 管理指引

对第1级数据的数据处理工作在可控区域中的具体管理指引如下：

a) 明确数据接触者的责任；
b) 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。

7.1.4.1.2 技术指引

对第1级数据的数据处理工作在可控区域中的具体技术指引如下：

a) 宜支持针对数据接触者的用户识别和身份鉴别，保证数据接触者的唯一性；
b) 宜提供如下数据处理保护：
    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) 做好数据处理逻辑的完整性检查与判断。

7.1.4.2 非可控区域

7.1.4.2.1 管理指引

宜满足该级可控区域的管理指引（见 7.1.4.1.1）。

7.1.4.2.2 技术指引

宜满足该级可控区域的技术指引（见 7.1.4.1.2）。

7.1.4.2.3 数据接触者指引

若委托第三方机构进行数据处理，非可控区域的数据接触者宜获得证券期货业机构的专属授权，以“一事一授”为宜。

7.1.5 数据存储

7.1.5.1 可控区域

7.1.5.1.1 管理指引

对第1级数据的数据存储工作在可控区域中的具体管理指引如下：

a) 数据存储期限、位置依据《中华人民共和国网络安全法》等相关法规规定；
b) 宜明确管理人员、管理对象；
c) 如证券期货业机构发生兼并、重组、破产等情况，数据承接方承接数据安全责任和义务，并宜使用逐一传达（或公告）的方式通知个人信息主体。

7.1.5.1.2 技术指引

对第1级数据的数据存储工作在可控区域中的具体技术指引如下：

a) 安全控制：数据存储宜做好操作留痕，并形成检查或审计机制；
b) 存储安全：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，并做好数据存储信息系统的安全检查与防范。

7.1.5.1.3 数据接触者指引

数据接触者宜经授权后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 管理指引

宜满足该级可控区域的管理指引（见 7.1.5.1.1）。

7.1.5.2.2 技术指引

宜满足该级可控区域的技术指引（见 7.1.5.1.2）。

7.1.5.2.3 数据接触者指引

宜满足该级可控区域的数据接触者指引（见 7.1.5.1.3）。

7.2 2级数据安全指引

7.2.1 数据采集

7.2.1.1 可控区域

7.2.1.1.1 管理指引

对第2级数据的数据采集工作在可控区域中的具体管理指引如下：

a) 宜明确该级数据的可采集范围；
b) 自动化访问采集流量不超过设定的阈值。

7.2.1.1.2 技术指引

对第2级数据的数据采集工作在可控区域中的具体技术指引如下：

a) 采集该级数据时，宜在数据中标明来源和采集时间，以提升数据的可追溯性；
b) 采取自动化手段访问采集数据的，宜有监控措施监控数据采集过程，保障采集数据的准确性、完整性和不可篡改性。

7.2.1.1.3 数据接触者指引

宜根据该级数据分类的情况，对数据接触者进行权限限定。

7.2.1.2 非可控区域

7.2.1.2.1 管理指引

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指引如下：

a) 宜满足该级可控区域的管理指引（见 7.2.1.1.1）；
b) 在非可控区域采集数据时，可跟踪和记录数据采集过程。

7.2.1.2.2 技术指引

宜满足该级可控区域的技术指引（见7.2.1.1.2）。

7.2.1.2.3 数据接触者指引

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指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.2.1.1.3）；
b) 数据接触者在非可控区域进行离线采集时，宜经授权后复制、修改、使用数据；
c) 宜做好对采集人员的安全责任及意识培训，防止数据泄露。

7.2.2 数据展现

7.2.2.1 可控区域

7.2.2.1.1 管理指引

对第2级数据的数据展现工作在可控区域中的具体管理指引如下：

a) 该级数据展现终端可配合数据控制者的要求，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) 系统管理员宜不直接接触业务数据；
   2) 宜有权限管理岗位；
   3) 互斥岗位宜权限独立；
   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) 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) 通过认证方式授权的用户只能访问证券期货业机构授权的业务系统；
   2) 宜采取合理的技术措施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证券期货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) 宜采取合理的技术措施保障数据展现的准确性。

7.2.2.1.2 技术指引

对第2级数据的数据展现工作在可控区域中的具体技术指引如下：

a) 宜对数据展现对象采取权限控制，以记录或防止数据被不当获取和使用；
b) 宜通过技术手段获取数据展现终端的操作系统信息。

7.2.2.1.3 数据接触者指引

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指引如下：

a) 证券期货业机构人员对在工作过程中接触的数据，非经数据控制者同意或授权，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；
b) 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 管理指引

对第2级数据的数据展现工作在非可控区域中的具体管理指引如下：

a) 宜满足该级可控区域的管理指引（见 7.2.2.1.1）；
b) 该级数据在需要展现的情况下，宜有严格的身份识别与授权程序，保障数据展现符合权限规定；
c) 因监管机构要求提供、证券期货业机构内部研究、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，需要保障数据调阅凭证真实、可信并做好调阅留痕。

7.2.2.2.2 技术指引

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指引如下：

a) 宜满足该级可控区域的技术指引（见 7.2.2.1.2）；
b) 采用减少数据展现量、水印、身份识别前置等技术确保数据展现安全性。

7.2.2.2.3 数据接触者指引

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指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.2.2.1.3）；
b) 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，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，避免重要信息外泄；
c) 涉及聘用第三方服务机构及人员提供信息技术开发、业务咨询、合作等外包服务的，宜与第三方服务机构签署保密协议，明保障密义务，宜确保按照约定获取及传播机构数据。

7.2.3 数据传输

7.2.3.1 可控区域

7.2.3.1.1 管理指引

对第2级数据的数据传输工作在可控区域中的具体管理指引如下：

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，证券期货业机构宜根据自身情况，明确如下事项：

宜有针对数据传输的、独立的安全机制。

c) 在数据传输方式上，宜考虑如下事项：
   1) 由相关人员负责对数据传输方案进行安全风险管控；
   2) 明确核心业务数据传输安全评估机制，可从传输目的合理性、传输数据的范围和合规性、传输方式的安全性、传输后管理责任和约束措施等方面进行评估；
   3) 负责数据传输安全的人员宜具备对数据传输业务的理解能力,能够结合合规性要求给出适当的安全解决方案，宜具备数据接口调用的安全意识和安全知识；
   4) 由相关人员负责数据传输的安全风险控制和数据服务接口安全管理工作；
   5) 明确核心业务数据传输的安全制度和审核流程；
   6) 核心业务或系统宜定义数据接口安全策略。

7.2.3.1.2 技术指引

对第2级数据的数据传输工作在可控区域中的具体技术指引如下：

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，保障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；
d) 宜对大批量数据的一次性传输进行审批和关注；
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，保障能有效应对突发性数据传输要求；
g) 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；
h) 宜有协议接口和 API 接口监控和异常处置能力；
i) 具备技术条件的情况下，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；
j) 发布、共享、交易或向境外提供数据的，依据《中华人民共和国网络安全法》等相关法规规定。

7.2.3.1.3 数据接触者指引

对第2级数据的数据传输工作在可控区域中的具体数据接触者指引如下：

a) 确保数据传输符合权限，不私自或越权传输数据；
b) 确保数据传输的时效性，准确、高效地完成数据传输；
c) 确保数据传输符合职责，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) 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做好数据安全管理。

7.2.3.2 非可控区域

7.2.3.2.1 管理指引

对第2级数据的数据传输工作在非可控区域中的具体管理指引如下：

a) 对数据传输介质的指引：
   1) 如需使用第三方的数据传输介质,证券期货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，保障数据传输介质的安全性与可用性；
   2) 证券期货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证券期货业机构人员不在场的情况下出现在非可控区域。
b) 对数据传输形式的指引：
   1) 证券期货业机构宜对非可控区域的数据传输进行专项评估；
   2) 宜以非明文或不可读方式传输数据。

c) 在数据传输方式上，宜考虑如下事项：
   1) 明确数据传输的原则和安全规范，明确数据传输内容范围和数据传输的管控措施，及数据传输涉及证券期货业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、组件或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) 明确数据传输的审核制度，保障数据传输符合合规要求；
   4) 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 技术指引

对第2级数据的数据传输工作在非可控区域中的具体技术指引如下：

a) 宜满足该级可控区域的技术指引（见 7.2.3.1.2）；
b) 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；
c) 宜尽量以证券期货业机构可控的协议接口或 API 作为数据传输主要方式；
d) 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；
e) 宜确保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 数据接触者指引

宜满足该级可控区域的数据接触者指引（见 7.2.3.1.3）。

7.2.4 数据处理

7.2.4.1 可控区域

7.2.4.1.1 管理指引

对第2级数据的数据处理工作在可控区域中的具体管理指引如下：

a) 明确数据接触者的责任；
b) 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，保障最小使用权限原则，不可非法生成、擅自修改、泄露、丢失与破坏信息系统数据；
c) 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；
d) 数据处理逻辑宜符合业务要求，保障合规，进行充分测试并验证，保障数据的完整、可用，并做好防护措施，保障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；
e) 数据生成依据《中华人民共和国网络安全法》等相关法规规定；
f) 涉及数据的直接处理，宜采取双人或全程监控的方式，保障数据处理逻辑符合要求，数据处理结果符合预期；
g) 直接数据处理宜做好防护措施，保障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。

7.2.4.1.2 技术指引

对第2级数据的数据处理工作在可控区域中的具体技术指引如下：

a) 宜支持针对数据接触者的用户标识和用户鉴别，保证数据接触者的唯一性；
b) 宜提供如下数据处理保护：
   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） 宜做好数据处理逻辑的完整性检查与判断。

c） 数据处理权限控制：宜制定数据处理权限在不同粒度上的控制规则，未经授权的人员或信息系统不可执行数据处理，且不可处理授权以外的数据；
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，保障满足数据处理需求；
e） 在数据处理安全控制方面，宜考虑如下事项：
1） 数据处理逻辑宜符合业务要求，保障合规，并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，在约定时间范围内对每一次的数据处理做安全控制管控，对不符合预期的情况，预设数据处理逻辑；
3） 对于有关联关系的数据处理，宜保障处理逻辑的完整性；
4） 数据处理专用终端进行，操作流程可追溯；
5） 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；
6） 具有有效、覆盖数据全生命周期的数据安全保护措施。

7.2.4.1.3 数据接触者指引

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指引如下：

a） 数据处理前宜获得数据控制者的授权，并签订相应协议；
b） 宜遵循数据处理要求，仅在授权范围内进行数据处理，宜避免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 管理指引

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指引如下：

a） 宜满足该级可控区域的管理指引（见 7.2.4.1.1）；
b） 原则上，证券期货业机构宜在可控区域处理数据，如有特殊需求，证券期货业机构需要在非可控区域处理数据时，宜采取有效措施保障数据接触者、数据处理逻辑、数据使用范围和数据的安全。

7.2.4.2.2 技术指引

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指引如下：

a） 宜满足该级可控区域的技术指引（见 7.2.4.1.2）；
b） 宜做好数据处理逻辑的完整性检查与判断；
c） 宜尽量对数据处理逻辑进行唯一性标识；
d） 宜采取技术手段，如加密、变形、遮蔽、添加噪声等方式保障数据处理逻辑的安全；
e） 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；
f） 宜以不可读或非明文方式展示或保留数据处理的留痕信息。

7.2.4.2.3 数据接触者指引

宜满足该级可控区域的数据接触者指引（见7.2.4.1.3）。

7.2.5 数据存储

7.2.5.1 可控区域

7.2.5.1.1 管理指引

对第2级数据的数据存储工作在可控区域中的具体管理指引如下：

a) 数据存储期限、位置依据《中华人民共和国网络安全法》等相关法规规定；
b) 宜制定相应的数据存储管理要求和相关机制，包括管理人员、管理对象、职责范围，离线数据、备份数据的恢复策略和流程，数据删除和销毁机制等；
c) 如证券期货业机构发生兼并、重组、破产等情况，数据承接方承接数据安全责任和义务，并宜使用逐一传达（或公告）的方式通知个人信息主体；
d) 宜制订针对移动存储介质的管理要求，确保数据在移动存储环节的安全；
e) 宜制定数据删除和销毁的机制，针对数据内容进行有效地清除、净化机制，实现对数据的有效销毁。

7.2.5.1.2 技术指引

对第2级数据的数据存储工作在可控区域中的具体技术指引如下：

a) 对物理安全的指引：
   1) 宜采取技术手段对存储的数据进行防护，并建立数据存储区域的不间断监控机制和访问控制机制；
   2) 宜建立多数据备份存储区域，各数据备份存储区域之间的物理距离宜满足灾备要求。
b) 对安全控制的指引：
   1) 宜建立数据存储的权限控制机制，确保获得授权的数据接触者才能进行数据存储操作；
   2) 数据存储和数据处理的权限宜相互独立；
   3) 数据存储宜做好操作留痕，并形成检查或审计机制。
c) 对存储安全的指引：
   1) 数据存储宜获得数据控制者的授权；
   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，并做好数据存储信息系统的安全检查与防范；
   3) 宜制订相应的多备份存储区域数据同步方案，保障各备份存储区域数据的一致性和完整性，并确保每个存储区域的数据具备独立的可恢复性和可用性；
   4) 当需要销毁数据时，宜使用数据销毁工具对各类数据进行有效销毁，确保数据销毁的有效性。

7.2.5.1.3 数据接触者指引

对第2级数据的数据存储工作在可控区域中的具体数据接触者指引如下：

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) 数据接触者宜经授权后执行或变更数据存储要求；
c) 宜采用双人或全程监控的方式执行数据的存储操作。

7.2.5.2 非可控区域

7.2.5.2.1 管理指引

对第2级数据的数据存储工作在非可控区域中的具体管理指引如下：

a) 宜满足该级可控区域的管理指引（见 7.2.5.1.1）；
b) 除依据《中华人民共和国网络安全法》等相关法规规定外，原则上宜在可控区域存储数据。

7.2.5.2.2 技术指引

对第2级数据的数据存储工作在非可控区域中的具体技术指引如下：

a) 宜满足该级可控区域的技术指引（见 7.2.5.1.2）；
b) 宜以临时存储为主；
c) 除数据控制者授权外，存储的数据宜进行脱敏、加密处理；
d) 执行数据存储操作宜确保数据接触者处于独立的安全空间。

7.2.5.2.3 数据接触者指引

对第2级数据的数据存储工作在非可控区域中的具体数据接触者指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.2.5.1.3）；
b) 宜有数据存储授权，宜以“一事一议”为原则进行授权；
c) 除依据《中华人民共和国网络安全法》等相关法规规定外，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级数据安全指引

7.3.1 数据采集

7.3.1.1 可控区域

7.3.1.1.1 管理指引

对第3级数据的数据采集工作在可控区域中的具体管理指引如下：

a) 针对个人信息方面的指引：
   1) 宜制定并公开采集使用规则，数据控制者需得到个人信息主体的明示同意或默认授权后，方可按照规则采集和使用个人数据；
   2) 从其他途径获得个人信息，与直接采集个人信息负有同等的保护责任和义务；
   3) 不宜因个人信息主体拒绝或者撤销同意采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；
   4) 不宜依据个人信息主体是否授权采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。
b) 针对个人和机构信息的通用指引：
   1) 自动化访问采集流量不超过设定的阈值；
   2) 以经营为目的采集数据或个人敏感信息的，宜明确负责数据安全的最高责任人。

7.3.1.1.2 技术指引

对第3级数据的数据采集工作在可控区域中的具体技术指引如下：

a) 针对个人信息方面的指引：
   1) 收到有关个人信息查询、更正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、更正或注销账号；
   2) 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：
      (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) 经过脱敏处理；
      (4) 执法机关依法履行职责所必需。
   3) 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；

4) **向境外提供个人信息的，依据《中华人民共和国网络安全法》等相关法规规定执行。**

b) **针对个人和机构信息的通用指引：**

1) 采集该级数据时，宜在数据中标明来源和采集时间，以提升数据的可追溯性；

2) 采取自动化手段访问采集数据的，宜有监控措施监控数据采集过程，保障采集数据的准确性、完整性和不可篡改性。

7.3.1.1.3 数据接触者指引

宜根据该级数据分类的情况，对数据接触者进行权限限定。

7.3.1.2 非可控区域

7.3.1.2.1 管理指引

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指引如下：

a) 宜满足该级可控区域的管理指引（见 7.3.1.1.1）；

b) 在非可控区域采集数据时，可跟踪和记录数据采集过程。

7.3.1.2.2 技术指引

宜满足该级可控区域的技术指引（见 7.3.1.1.2）。

7.3.1.2.3 数据接触者指引

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指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.3.1.1.3）；

b) 数据接触者在非可控区域进行离线采集时，宜经授权后复制、修改、使用数据；

c) 宜做好对采集人员的安全责任及意识培训，防止数据泄露。

7.3.2 数据展现

7.3.2.1 可控区域

7.3.2.1.1 管理指引

对第3级数据的数据展现工作在可控区域中的具体管理指引如下：

a) 该级数据展现终端可配合数据控制者的要求，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，确保恰当的授权：

1) 系统管理员宜不直接接触业务数据；

2) 宜有权限管理岗位；

3) 互斥岗位宜权限独立；

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) **服务机构人员宜不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) 通过认证方式授权的用户只能访问证券期货业机构授权的业务系统；

2) 宜采取合理的技术措施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证券期货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) 宜采取合理的技术措施保障数据展现的准确性。

7.3.2.1.2 技术指引

对第3级数据的数据展现工作在可控区域中的具体技术指引如下：

a) **宜实施通信与接入管制，**依据《中华人民共和国网络安全法》等相关法规规定**并结合证券期货业机构实际情况，对数据的展现请求采取认证、权限控制、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；**

b) 宜通过技术手段获取数据展现终端的操作系统信息；

c) **宜对展现的数据进行标识，以唯一识别数据控制者身份；**

d) **宜根据证券期货业机构自身情况限定可展现数据的终端类型与展现方式；**

e) **宜采用数据校验，数据可追溯等机制保障展现数据的准确性。**

7.3.2.1.3 数据接触者指引

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指引如下：

a) 证券期货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；

b) 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；

c) **宜仅授权人员可直接查看未经脱敏处理的数据；**

d) **数据接触者宜识别并评估数据展现环境的安全性；**

e) **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，宜确保国家安全、经济运行、社会稳定和他人合法权益。**

7.3.2.2 非可控区域

7.3.2.2.1 管理指引

对第3级数据的数据展现工作在非可控区域中的具体管理指引如下：

a) 宜满足该级可控区域的管理指引（见 7.3.2.1.1）；

b) 数据安全等级为该级的数据，原则上宜在可控区域展现。确有需要展现的情况下，宜有严格的身份识别与授权程序，保障数据展现符合权限规定；

c) 因监管机构要求提供、证券期货业机构内部研究、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，需要保障数据调阅凭证真实、可信并做好调阅留痕；

d) **数据要尽可能地缩小接触者的范围，且只能提供只读操作；**

e) **严格限定数据接触者的相关权限，保障数据的安全性。**

7.3.2.2.2 技术指引

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指引如下：

a) 宜满足该级可控区域的技术指引（见 7.3.2.1.2）；

b) **数据展现终端（含软件、硬件）宜经过授权；**

c) **数据展现终端（含软件、硬件）宜对该级别数据做非持久性存储；**

d) **限制数据批量展示，防止数据被批量获取；**

e) 采用减少数据展现量、水印、身份识别前置等技术确保数据展现安全性。

7.3.2.2.3 数据接触者指引

对第3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指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.3.2.1.3）；
b) 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，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，避免重要信息外泄；
c) 涉及聘用第三方服务机构及人员提供信息技术开发、业务咨询、合作等外包服务的，宜与第三方服务机构签署保密协议，明确保密义务，宜确保按照约定获取及传播证券期货业机构数据。

7.3.3 数据传输

7.3.3.1 可控区域

7.3.3.1.1 管理指引

对第3级数据的数据传输工作在可控区域中的具体管理指引如下：

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，确保数据传输介质均有备份；
   5) 有统一、适用的数据传输介质报废制度。
b) 对数据传输形式的指引：
   1) 数据传输的内容宜尽量在传输过程中不直接可见或非明文可读；
   2) 宜有针对数据传输的、独立的安全机制；
   3) 数据的传输宜遵循“一事一议”的原则，申请授权。
c) 在数据传输方式上，宜考虑如下事项：
   1) 设立相关岗位和人员负责数据传输管理，提供相关原则和技术能力，并推广相关要求在相关业务的落地执行；
   2) 明确数据传输的原则和安全规范，明确数据传输内容范围和数据传输的管控措施，及数据传输涉及证券期货业机构或部门相关用户职责和权限；
   3) 明确数据提供者与传输数据使用者的数据安全责任和安全防护能力的相关要求；
   4) 明确数据传输审计规程和审计日志管理要求，明确审计记录要求，为数据传输安全事件的处置、应急响应和事后调查提供帮助；
   5) 使用外部的软件开发包、组件或源码前宜进行安全评估，获取的数据宜符合证券期货业机构的数据安全要求；
   6) 设立相关岗位和人员负责数据传输工作，并且对数据传输人员进行安全培训；
   7) 明确数据传输的审核制度，保障数据传输符合合规要求；
   8) 明确数据传输内容、适用范围及规范，数据传输者与使用者权利和义务；
   9) 定期审查传输的数据中是否含有非公开信息，并采取相关措施满足数据传输的合规性；
   10) 采取必要措施建立数据传输事件应急处理流程；
   11) 设立统一的岗位和人员负责数据接口安全管理，由该岗位人员负责制定整体的规则并推广相关流程的推行；
   12) 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，并明确数据接口安全要求，包括接口名称、接口参数等；

13） 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。

7.3.3.1.2 技术指引

对第3级数据的数据传输工作在可控区域中的具体技术指引如下：

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，保障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，确保数据在传输过程中不被分流；
d） 宜对大批量数据的一次性传输进行审批和关注；
e） 宜有协议接口和 API 接口监控和异常处置能力；
f） 宜充分评估数据传输能力，保障能有效应对突发性数据传输要求；
g） 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；
h） 具备技术条件的情况下，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；
i） 运用合适的加密技术和手段，保障数据在数据传输过程中的安全性；
j） 宜尽可能采用具有独立安全机制的数据传输介质；
k） 宜采取措施保障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；
l） 宜对传输数据及数据传输过程进行监控审计，传输的数据宜属于传输业务需求且没有超出数据传输使用授权范围；
m） 宜明确传输数据格式规范；
n） 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，同时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；
o） 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；
p） 证券期货业机构发布、共享、交易或向境外提供数据，依据《中华人民共和国网络安全法》等相关法规规定。

7.3.3.1.3 数据接触者指引

对第3级数据的数据传输工作在可控区域中的具体数据接触者指引如下：

a） 确保数据传输符合权限，不私自或越权传输数据；
b） 确保数据传输的时效性，准确、高效地完成数据传输；
c） 确保数据传输符合职责，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） 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做好数据安全管理；
e） 宜能够充分理解证券期货业机构的数据传输规程，并根据数据传输的业务执行相应的风险评估，从而提出实际的解决方案；
f） 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；
g） 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。

7.3.3.2 非可控区域

7.3.3.2.1 管理指引

对第3级数据的数据传输工作在非可控区域中的具体管理指引如下：

a） 对数据传输介质的指引：

1) 证券期货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，保障数据传输介质的安全性与可用性；
2) 证券期货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) 宜确保数据传输介质仅在证券期货业机构人员在场的情况下出现在非可控区域。

b) 对数据传输形式的指引：
1) 证券期货业机构宜对非可控区域的数据传输进行专项评估；
2) 宜以非明文或不可读方式传输数据。

c) 在数据传输方式上，宜考虑如下事项：
1) 明确数据传输的原则和安全规范，明确数据传输内容范围和数据传输的管控措施，及数据传输涉及证券期货业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、组件或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) 明确数据传输的审核制度，保障数据传输符合合规要求；
4) 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；
5) **定期评估数据传输机制、相关组件和传输通道的安全性；**
6) **针对数据传输明确安全传输细则和审核流程；**
7) **细化明确各类数据传输场景的审核流程，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 技术指引

对第3级数据的数据传输工作在非可控区域中的具体技术指引如下：

a) 宜满足该级可控区域的技术指引（见 7.3.3.1.2）；
b) 宜有针对数据传输的监控机制，确保数据在传输过程中不被不当获取或破坏；
c) 宜尽量以证券期货业机构可控的协议接口或 API 作为数据传输主要方式；
d) **直接提供数据实体的情况下，宜要对数据实体进行脱敏及保密处理；**
e) **宜保障数据按授权路径进行定向传输；**
f) 宜有协议接口和 API 接口监控和异常处置能力；
g) **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；**
h) **对于数据的批量传输，需采用有效的制度和工具控制数据批量传输的安全风险；**
i) **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 数据接触者指引

宜满足该级可控区域的数据接触者指引（见 7.3.3.1.3）。

7.3.4 数据处理

7.3.4.1 可控区域

7.3.4.1.1 管理指引

对第3级数据的数据处理工作在可控区域中的具体管理指引如下：

a) 可遵循“谁处理，谁负责”的原则，明确数据接触者的责任；
b) 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，保障最小使用权限原则，不可非法生成、擅自修改、泄露、丢失与破坏信息系统数据；

c） 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；
d） 数据处理逻辑宜符合业务要求，保障合规，进行充分测试并验证，保障数据的完整、可用。
e） 数据生成依据《中华人民共和国网络安全法》等相关法规规定；
f） 涉及数据的直接处理，宜采取双人或全程监控的方式，保障数据处理逻辑符合要求，数据处理逻辑符合预期；
g） 直接数据处理宜做好防护措施，保障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；
h） **宜及时评估数据处理结果，并进行相应的数据等级变更；**
i） **宜及时掌握数据等级分布情况；**
j） **宜建立信息系统性能容量评估机制。**

7.3.4.1.2 技术指引

对第3级数据的数据处理工作在可控区域中的具体技术指引如下：
a） 宜支持针对数据接触者的用户标识和用户鉴别，保证数据接触者的唯一性；
b） 宜提供符合该级的数据处理保护：
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） 宜做好数据处理逻辑的完整性检查与判断；
4） **做好处理原因的留痕并考虑数据处理的可恢复性。**
c） 数据处理权限控制：宜制定数据处理权限在不同粒度上的控制规则，未经授权的人员或信息系统不可执行数据处理，且不可处理授权以外的数据；
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，保障满足数据处理需求；
2） **证券期货业机构宜视自身情况做好数据处理能力的弹性管理，保障在需要的时候，能快速、及时地调整信息系统的数据处理能力。**
e） 在数据处理安全控制方面，宜考虑如下事项：
1） 数据处理逻辑宜符合业务要求，保障合规，且在投入生产使用前经过完整、严格的测试；
2） 直接数据处理，宜有复核或审核机制，在约定时间范围内对每一次的数据处理做安全控制管控，对不符合预期的情况，预设数据处理逻辑；
3） 对于有关联关系的数据处理，宜保障处理逻辑的完整性；
4） 数据处理专用终端进行，操作流程可追溯；
5） 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。
6） 具有有效、覆盖数据全生命周期的数据安全保护措施；
7） **需脱敏处理的数据，宜保障数据处理的不可逆性，可在保证数据安全的情况下，尽量提高数据有效性。**

7.3.4.1.3 数据接触者指引

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指引如下：
a） 数据接触者在数据处理前宜获得数据控制者的授权，并签订相应协议；
b） 数据接触者宜遵循数据处理要求，宜经授权后变更数据处理要求或进行数据处理；
c） **证券期货业机构宜对数据接触者进行权限限定，并限定数据接触者的数据处理工作区域，确保在恰当的区域处理适当类型或等级的数据；**

d) **数据接触者宜配合证券期货业机构的要求，提供自身特征信息。**

7.3.4.2 非可控区域

7.3.4.2.1 管理指引

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指引如下：

a) 宜满足该级可控区域的管理指引（见 7.3.4.1.1）；
b) 原则上，证券期货业机构宜在可控区域处理数据，如有特殊需求，证券期货业机构需要在非可控区域处理数据时，宜采取有效措施保障数据接触者、数据处理逻辑、数据使用范围和数据的安全。

7.3.4.2.2 技术指引

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指引如下：

a) 宜满足该级可控区域的管理指引（见 7.3.4.1.2）；
b) 宜做好数据处理逻辑的完整性检查与判断；
c) 宜尽量对数据处理逻辑进行唯一性标识；
d) 宜采取技术手段，如加密、变形、遮蔽、添加噪声等方式保障数据处理逻辑的安全；
e) 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；
f) 宜以不可读或非明文方式展示或保留数据处理的留痕信息；
g) **宜对数据添加数据水印，保障对可能泄露的数据进行溯源；**
h) **宜对数据进行隐私保护。**

7.3.4.2.3 数据接触者指引

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指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.3.4.1.3）；
b) **数据接触者宜配合证券期货业机构的要求，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 管理指引

对第3级数据的数据存储工作在可控区域中的具体管理指引如下：

a) 数据存储期限、位置依据《中华人民共和国网络安全法》等相关法规规定；
b) **宜建设完善的数据存储体系；**
c) 宜制定相应的数据存储管理要求和相关机制，包括管理人员、管理对象、职责范围，离线数据、备份数据的恢复策略和流程，数据删除和销毁机制等；
d) 宜制订针对移动存储介质的管理要求，确保数据在移动存储环节不会泄露；
e) 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证券期货业机构自身的要求被以合适的方式销毁；
f) **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；**
g) **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；**
h) 如证券期货业机构发生兼并、重组、破产等情况，数据承接方承接数据安全责任和义务，并宜使用逐一传达（或公告）的方式通知个人信息主体。

7.3.5.1.2 技术指引

对第3级数据的数据存储工作在可控区域中的具体技术指引如下：

a) 对物理安全的指引：
   1) 宜采取技术手段对存储的数据进行防护，并建立数据存储区域的不间断监控机制和访问控制机制；
   2) 宜建立多数据备份存储区域，各数据备份存储区域之间的物理距离宜满足灾备要求。
b) 对安全控制的指引：
   1) 宜建立数据存储的权限控制机制，确保获得授权的数据接触者才能进行数据存储操作；
   2) 数据存储和数据处理的权限宜相互独立；
   3) 数据存储宜做好操作留痕，并形成检查或审计机制。
c) 对存储安全的指引：
   1) 数据存储宜获得数据控制者的授权；
   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，并做好数据存储信息系统的安全检查与防范；
   3) 宜制订相应的多备份存储区域数据同步方案，保障各备份存储区域数据的一致性和完整性，并确保每个存储区域的数据具备独立的可恢复性和可用性；
   4) 当需要销毁数据时，宜使用数据销毁工具对各类数据进行有效销毁，确保数据销毁的有效性；
   5) **宜做好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露风险。**
b) **个人信息不宜超出采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 数据接触者指引

对第3级数据的数据存储工作在可控区域中的具体数据接触者指引如下：

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) 数据接触者宜经授权后执行或变更数据存储要求；
c) 宜采用双人或全程监控的方式执行数据的存储操作。

7.3.5.2 非可控区域

7.3.5.2.1 管理指引

对第3级数据的数据存储工作在非可控区域中的具体管理指引如下：

a) 宜满足该级可控区域的管理指引（见 7.3.5.1.1）；
b) 除依据《中华人民共和国网络安全法》等相关法规规定外，原则上宜在可控区域存储数据。

7.3.5.2.2 技术指引

对第3级数据的数据存储工作在非可控区域中的具体技术指引如下：

a) 宜满足该级可控区域的技术指引（见 7.3.5.1.2）；
b) 宜以临时存储为主；
c) 除数据控制者授权外，存储的数据宜进行脱敏、加密处理；
d) 执行数据存储操作宜确保数据接触者处于独立的安全空间；
e) **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 数据接触者指引

对第3级数据的数据存储工作在非可控区域中的具体数据接触者指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.3.5.1.3）；
b) 宜有数据存储授权，宜以“一事一议”为原则进行授权；
c) 除依据《中华人民共和国网络安全法》等相关法规规定外，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。

7.4 4级数据安全指引

7.4.1 数据采集

7.4.1.1 可控区域

7.4.1.1.1 管理指引

对第4级数据的数据采集工作在可控区域中的具体管理指引如下：

a) **针对个人信息方面的指引：**
   1) 数据采集宜制定并公开采集使用规则，数据控制者需得到个人信息主体的明示同意或默认授权后，方可按照规则采集和使用个人数据；
   2) 从其他途径获得个人信息，与直接采集个人信息负有同等的保护责任和义务；
   3) 不宜因个人信息主体拒绝或者撤销同意采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；
   4) 不宜依据个人信息主体是否授权采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。
b) **针对个人和机构信息的通用指引：**
   1) 自动化访问采集流量不超过设定的阈值；
   2) 以经营为目的采集数据或个人敏感信息的，宜明确负责数据安全的最高责任人。

7.4.1.1.2 技术指引

对第4级数据的数据采集工作在可控区域中的具体技术指引如下：

a) 针对个人信息方面的指引：
   1) 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；
   2) 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：
      (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) 经过脱敏处理；
      (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。
   3) 向境外提供个人信息的，依据《中华人民共和国网络安全法》等相关法规规定执行。
b) 针对个人和机构信息的通用指引：
   1) 采集该级数据时，宜在数据中标明来源和采集时间，以提升数据的可追溯性；
   2) 采取自动化手段访问采集数据的，宜有监控措施监控数据采集过程，保障采集数据的准确性、完整性和不可篡改性。

7.4.1.1.3 数据接触者指引

宜根据该级数据分类的情况，对数据接触者进行权限限定。

7.4.1.2 非可控区域

7.4.1.2.1 管理指引

该级数据不宜在非可控区域采集。

7.4.1.2.2 技术指引

该级数据不宜在非可控区域采集。

7.4.1.2.3 数据接触者指引

该级数据不宜在非可控区域采集。

7.4.2 数据展现

7.4.2.1 可控区域

7.4.2.1.1 管理指引

对第4级数据的数据展现工作在可控区域中的具体管理指引如下：

a) 该级数据展现终端可配合数据控制者的要求，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) 系统管理员宜不直接接触业务数据；
   2) 宜有权限管理岗位；
   3) 互斥岗位宜权限独立；
   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) 服务机构人员宜不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) 通过认证方式授权的用户只能访问证券期货业机构授权的业务系统；
   2) 宜采取合理的技术措施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证券期货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) 宜采取合理的技术措施保障数据展现的准确性。

7.4.2.1.2 技术指引

对第4级数据的数据展现工作在可控区域中的具体技术指引如下：

a) 宜实施通信与接入管制，依据《中华人民共和国网络安全法》等相关法规规定并结合证券期货业机构实际情况，对数据的展现请求采取认证、权限控制、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；
b) 宜通过技术手段获取数据展现终端的操作系统信息；
c) 宜对展现的数据进行标识，以唯一识别数据控制者身份；
d) 宜根据证券期货业机构自身情况限定可展现数据的终端类型与展现方式；
e) 宜采用数据校验，数据可追溯等机制保障展现数据的准确性。

7.4.2.1.3 数据接触者指引

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指引如下：

a) 证券期货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；
b) 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；
c) 宜避免除授权人员以外的其他人员直接查看未经脱敏处理的数据；
d) 数据接触者宜识别并评估数据展现环境的安全性；
e) 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，宜避免影响国家安全、经济运行、社会稳定和损害他人合法权益。

7.4.2.2 非可控区域

7.4.2.2.1 管理指引

对第4级数据的数据展现工作在非可控区域中的具体管理指引如下：

a) 宜满足该级可控区域的管理指引（见 7.4.2.1.1）；
b) 数据安全等级为该级的数据，原则上宜在可控区域展现。确有需要展现的情况下，宜有严格的身份识别与授权程序，保障数据展现符合权限规定；
c) 因监管机构要求提供、证券期货业机构内部研究、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，需要保障数据调阅凭证真实、可信并做好调阅留痕；
d) 数据要尽可能地缩小接触者的范围，且只能提供只读操作；
e) 严格限定数据接触者的相关权限，保障数据的安全性。

7.4.2.2.2 技术指引

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指引如下：

a) 宜满足该级可控区域的技术指引（见 7.4.2.1.2）；
b) 数据展现终端（含软件、硬件）宜经过授权或认证；
c) 数据展现终端（含软件、硬件）宜避免对该级别数据做持久性存储；
d) 限制数据批量展示，防止数据被批量获取；
e) 采用减少数据展现量、水印、身份识别前置等技术保障数据展现安全性。

7.4.2.2.3 数据接触者指引

对第4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指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.4.2.1.3）；
b) 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，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，避免重要信息外泄；

c） 涉及聘用第三方服务机构及人员构提供信息技术开发、业务咨询、合作等外包服务的，宜与第三方服务机构签署保密协议，明保障密义务，宜确保按照约定获取及传播证券期货业机构数据。

7.4.3 数据传输

7.4.3.1 可控区域

7.4.3.1.1 管理指引

对第4级数据的数据传输工作在可控区域中的具体管理指引如下：

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） 对数据传输形式的指引：
   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） 数据的传输宜遵循“一事一议”的原则，申请授权。

c） 在数据传输方式上，宜考虑如下事项：
   1） 设立相关岗位和人员负责数据传输管理，提供相关原则和技术能力，并推广相关要求在相关业务的落地执行；
   2） 明确数据传输的原则和安全规范，明确数据传输内容范围和数据传输的管控措施，及数据传输涉及证券期货业机构或部门相关用户职责和权限；
   3） 明确数据提供者与传输数据使用者的数据安全责任和安全防护能力的相关要求；
   4） 明确数据传输审计规程和审计日志管理要求，明确审计记录要求，为数据传输安全事件的处置、应急响应和事后调查提供帮助；
   5） 使用外部的软件开发包、组件或源码前宜进行安全评估，获取的数据宜符合证券期货业机构的数据安全要求；
   6） 设立相关岗位和人员负责数据传输工作，并且对数据传输人员进行安全培训；
   7） 明确数据传输的审核制度，保障数据传输符合合规要求；
   8） 明确数据传输内容、适用范围及规范，数据传输者与使用者权利和义务；
   9） 定期审查传输的数据中是否含有非公开信息，并采取相关措施满足数据传输的合规性；
   10） 采取必要措施建立数据传输事件应急处理流程；
   11） 设立统一的岗位和人员负责数据接口安全管理，由该岗位人员负责制定整体的规则并推广相关流程的推行；
   12） 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，并明确数据接口安全要求，包括接口名称、接口参数等；
   13） 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；
   14） 在证券期货业机构统一的数据传输原则基础上，针对主要的数据传输场景明确安全细则或审批流程；
   15） 定期评估数据传输机制、相关组件和传输通道的安全性；

16） 在传输数据时，对数据接收方的数据安全防护能力进行评估，明确各类数据传输场景的审核流程，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 技术指引

对第4级数据的数据传输工作在可控区域中的具体技术指引如下：

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，保障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；
d） 宜对大批量数据的一次性传输进行审批和关注；
e） 宜有协议接口和 API 接口监控和异常处置能力；
f） 宜充分评估数据传输能力，保障能有效应对突发性数据传输要求；
g） 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；
h） 具备技术条件的情况下，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；
i） 运用合适的加密技术和手段，保障数据在数据传输过程中的安全性；
j） 宜尽可能采用具有独立安全机制的数据传输介质；
k） 宜采取措施保障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；
l） 宜对传输数据及数据传输过程进行监控审计，传输的数据宜属于传输业务需求且没有超出数据传输使用授权范围；
m） 宜明确传输数据格式规范；
n） 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，同时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；
o） 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；
p） 证券期货业机构发布、共享、交易或向境外提供数据，依据《中华人民共和国网络安全法》等相关法规规定。

7.4.3.1.3 数据接触者指引

对第4级数据的数据传输工作在可控区域中的具体数据接触者指引如下：

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） 数据接触者对接入其平台的第三方应用，宜明确数据安全指引和责任，督促监督第三方应用运营者做好数据安全管理；
e） 宜能够充分理解证券期货业机构的数据传输规程，并根据数据传输的业务执行相应的风险评估，从而提出实际的解决方案；
f） 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指引建立相应的应急方案；
g） 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。

7.4.3.2 非可控区域

7.4.3.2.1 管理指引

对第4级数据的数据传输工作在非可控区域中的具体管理指引如下：

a） 对数据传输介质的指引：

1) 证券期货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，保障数据传输介质的安全性与可用性；
2) 证券期货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证券期货业机构人员不在场的情况下出现在非可控区域。

b) 对数据传输形式的指引：
1) 证券期货业机构宜对非可控区域的数据传输进行专项评估；
2) 宜以非明文或不可读方式传输数据。

c) 在数据传输方式上，宜考虑如下事项：
1) 明确数据传输的原则和安全规范，明确数据传输内容范围和数据传输的管控措施，及数据传输涉及证券期货业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、组件或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) 明确数据传输的审核制度，保障数据传输符合合规要求；
4) 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；
5) 定期评估数据传输机制、相关组件和传输通道的安全性；
6) 针对数据传输明确安全传输细则和审核流程；
7) 细化明确各类数据传输场景的审核流程，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 技术指引

对第4级数据的数据传输工作在非可控区域中的具体技术指引如下：

a) 宜满足该级可控区域的技术指引（见 7.4.3.1.2）；
b) 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；
c) 宜尽量以证券期货业机构可控的协议接口或 API 作为数据传输主要方式；
d) 直接提供数据实体的情况下，宜要对数据实体进行脱敏及保密处理；
e) 宜保障数据按授权路径进行定向传输；
f) 宜有协议接口和 API 接口监控和异常处置能力；
g) 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；
h) 对于数据的批量传输，需采用有效的制度和工具控制数据批量传输的安全风险；
i) 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 数据接触者指引

宜满足该级可控区域的数据接触者指引（见 7.4.3.1.3）。

7.4.4 数据处理

7.4.4.1 可控区域

7.4.4.1.1 管理指引

对第4级数据的数据处理工作在可控区域中的具体管理指引如下：

a) 可遵循“谁处理，谁负责”的原则，明确数据接触者的责任；

b) 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，保障最小使用权限原则宜按照 GB／T 37988-2019 的 9.3.2.3 执行，不可非法生成、擅自修改、泄露、丢失与破坏信息系统数据；
c) 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；
d) 数据处理逻辑宜符合业务要求，保障合规，进行充分测试并验证，保障数据的完整、可用；
e) 数据生成依据《中华人民共和国网络安全法》等相关法规规定；
f) 涉及数据的直接处理，宜采取双人或全程监控的方式，保障数据处理逻辑符合要求，数据处理逻辑符合预期；
g) 直接数据处理宜做好防护措施，保障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；
h) 宜及时评估数据处理结果，并进行相应的数据等级变更；
i) 宜依据 JR／T 0158-2018 及时掌握数据等级分布情况；
j) 宜建立信息系统性能容量评估机制。

7.4.4.1.2 技术指引

对第4级数据的数据处理工作在可控区域中的具体技术指引如下：

a) 宜支持针对数据接触者的用户标识和用户鉴别，保证数据接触者的唯一性；
b) 宜提供符合该级的数据处理保护：
   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) 做好数据处理逻辑的完整性检查与判断；
   4) 做好处理原因的留痕并考虑数据处理的可恢复性。
c) 数据处理权限控制：宜制定数据处理权限在不同粒度上的控制规则，未经授权的人员或信息系统不可执行数据处理，且不可处理授权以外的数据；
d) 数据处理能力指引：
   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，保障满足数据处理需求；
   2) 证券期货业机构宜视自身情况做好数据处理能力的弹性管理，保障在需要的时候，能快速、及时地调整信息系统的数据处理能力。
e) 在数据处理安全控制方面，宜考虑如下事项：
   1) 数据处理逻辑宜符合业务要求，保障合规，且在投入生产使用前经过完整、严格的测试；
   2) 直接数据处理，宜有复核或审核机制，在约定时间范围内对每一次的数据处理做安全控制管控，对不符合预期的情况，预设数据处理逻辑；
   3) 对于有关联关系的数据处理，宜保障处理逻辑的完整性；
   4) 数据处理专用终端进行，操作流程可追溯；
   5) 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；
   6) 具有有效、覆盖数据全生命周期的数据安全保护措施；
   7) 需脱敏处理的数据，宜保障数据处理的不可逆性，可在保证数据安全的情况下，尽量提高数据有效性。

7.4.4.1.3 数据接触者指引

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指引如下：

a) 数据接触者在数据处理前宜获得数据控制者的授权，并签订相应协议；

b) 数据接触者宜遵循数据处理要求，宜避免擅自变更数据处理要求或擅自进行数据处理；
c) 证券期货业机构宜对数据接触者进行权限限定，并限定数据接触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；
d) 数据接触者宜配合证券期货业机构的要求，提供自身特征信息。

7.4.4.2 非可控区域

7.4.4.2.1 管理指引

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指引如下：
a) 宜满足该级可控区域的管理指引（见 7.4.4.1.1）；
b) 原则上，证券期货业机构宜在可控区域处理数据，如有特殊需求，证券期货业机构需要在非可控区域处理数据时，宜采取有效措施保障数据接触者、数据处理逻辑、数据使用范围和数据的安全；
c) **数据处理宜遵守频率和数据量最小化原则；**
d) **数据直接处理宜通过加不可逆加密方式进行；**
e) **宜及时掌握数据等级分布情况。**

7.4.4.2.2 技术指引

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指引如下：
a) 宜满足该级可控区域的管理指引（见 7.4.4.1.2）；
b) 宜做好数据处理逻辑的完整性检查与判断；
c) 宜尽量对数据处理逻辑进行唯一性标识；
d) 宜采取技术手段，如加密、变形、遮蔽、添加噪声等方式保障数据处理逻辑的安全；
e) 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；
f) 宜以不可读或非明文方式展示或保留数据处理的留痕信息；
g) 宜对数据添加数据水印，保障对可能泄露的数据进行溯源；
h) 宜对数据进行隐私保护。

7.4.4.2.3 数据接触者指引

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指引如下：
a) 宜满足该级可控区域的数据接触者指引（见 7.4.4.1.3）；
b) 数据接触者宜配合证券期货业机构的要求，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 管理指引

对第4级数据的数据存储工作在可控区域中的具体管理指引如下：
a) 数据存储期限、位置依据《中华人民共和国网络安全法》等相关法规规定；
b) 宜建设完善的数据存储体系；
c) 宜制定相应的数据存储管理要求和相关机制，包括管理人员、管理对象、职责范围，离线数据、备份数据的恢复策略和流程，数据删除和销毁机制等；
d) 宜制定针对移动存储介质的管理要求，确保数据在移动存储环节的安全；

e) 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证券期货业机构自身的要求被以合适的方式销毁；
f) 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；
g) 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；
h) 如证券期货业机构发生兼并、重组、破产等情况，数据承接方承接数据安全责任和义务，并宜使用逐一传达（或公告）的方式通知个人信息主体。

7.4.5.1.2 技术指引

对第4级数据的数据存储工作在可控区域中的具体技术指引如下：

a) 对物理安全的指引：
   1) 宜采取技术手段对存储的数据进行防护，并建立数据存储区域的不间断监控机制和访问控制机制；
   2) 宜建立多数据备份存储区域，各数据备份存储区域之间的物理距离宜满足灾备要求。
b) 对安全控制的指引：
   1) 宜建立数据存储的权限控制机制，确保获得授权的数据接触者才能进行数据存储操作；
   2) 数据存储和数据处理的权限宜相互独立；
   3) 数据存储宜做好操作留痕，并形成检查或审计机制。
c) 对存储安全的指引：
   1) 数据存储宜获得数据控制者的授权；
   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，并做好数据存储信息系统的安全检查与防范；
   3) 宜制订相应的多备份存储区域数据同步方案，保障各备份存储区域数据的一致性和完整性，并确保每个存储区域的数据具备独立的可恢复性和可用性；
   4) 当需要销毁数据时，宜使用数据销毁工具对各类数据进行有效销毁，确保数据销毁的有效性；
   5) 宜做好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露风险。
d) 个人信息不宜超出采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的除外。

7.4.5.1.3 数据接触者指引

对第4级数据的数据存储工作在可控区域中的具体数据接触者指引如下：

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) 数据接触者宜经授权后执行或变更数据存储要求；
c) 宜采用双人或全程监控的方式执行数据的存储操作。

7.4.5.2 非可控区域

7.4.5.2.1 管理指引

对第4级数据的数据存储工作在非可控区域中的具体管理指引如下：

a) 宜满足该级可控区域的管理指引（见7.4.5.1.1）；
b) 除依据《中华人民共和国网络安全法》等相关法规规定外，原则上宜在可控区域存储数据。

7.4.5.2.2 技术指引

对第4级数据的数据存储工作在非可控区域中的具体技术指引如下：

a) 宜满足该级可控区域的技术指引（见 7.4.5.1.2）；
b) 宜以临时存储为主；
c) 除数据控制者授权外，存储的数据宜进行脱敏、加密处理；
d) 执行数据存储操作宜确保数据接触者处于独立的安全空间；
e) 数据存储介质宜具备独立的安全控制措施，**定期验证安全控制措施的有效性，**避免被任意访问。

7.4.5.2.3 数据接触者指引

对第4级数据的数据存储工作在非可控区域中的具体数据接触者指引如下：

a) 宜满足该级可控区域的数据接触者指引（见 7.4.5.1.3）；
b) 宜有数据存储授权，宜以“一事一议”为原则进行授权，**并定期对授权审核审计**；
c) 除依据《中华人民共和国网络安全法》等相关法规规定外，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。

参 考 文 献

[1] 中华人民共和国网络安全法[J]. 中华人民共和国全国人民代表大会常务委员会公报，2016(3):10-18.

[2] 中华人民共和国个人信息保护法[J]. 中华人民共和国全国人民代表大会常务委员会公报，2021(6):10-18.