

证券期货业数据安全 管理与保护指引

JR/T 0250—2022

目 次

前言.....II

引言.....III

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 基本原则.....3

 4.1 过程域.....3

 4.2 实用性.....3

 4.3 安全性.....3

 4.4 可用性.....3

 4.5 适配性.....3

5 组织架构.....3

 5.1 总体指引.....3

 5.2 数据安全管理部门.....4

 5.3 合规风控部门.....4

 5.4 业务管理部门.....4

 5.5 信息技术部门.....4

 5.6 内部审计部门.....4

6 制度指引.....4

7 数据安全管理与保护指引.....5

 7.1 1级数据安全指引.....5

 7.2 2级数据安全指引.....8

 7.3 3级数据安全指引.....15

 7.4 4级数据安全指引.....24

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管理权或使用权的区域。

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、数据管理和数据存贮。

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) 数据安全管理制度：明确数据安全管理制度，明确数据安全管理工作组织架构、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。

7.1.2.1 非可控区域

7.1.2.1.1 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。

7.1.2.1.2 技术指引

宜满足该级可控区域的技术指引（见 7.1.3.1.1）。

7.1.2.1.3 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）。

7.1.3 数据处理

7.1.3.1 可控区域

7.1.3.1.1 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。

7.1.3.1.2 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。

7.1.3.2 非可控区域

7.1.3.2.1 管理指引

宜满足该级可控区域的管理指引（见 7.1.4.1.1）。

7.1.3.2.2 技术指引

宜满足该级可控区域的技术指引（见 7.1.4.1.2）。

7.1.3.2.3 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。

7.1.4 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》等相关法律法规规定；
- 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。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/467155056042006062>