ICS 33.180.10
CCS M33

T/JSIC

江苏省通信学会团体标准

T/JSIC 022-2023

数据安全管理平台功能要求

Functional Requirements for Data Security Management Platform

2023-11-28 发布　　2023-12-01 实施

江苏省通信学会　发 布

全国团体标准信息平台

江苏省通信学会团体标准公告

2023 年 第 2 号 （总第 13 号）

江苏省通信学会和江苏省邮电标准化技术委员会于 2023 年联合立项编制《数据安全管理平台功能要求》。经主编单位（南京中新赛克科技有限责任公司）和参编单位（江苏中新赛克工业互联网安全技术创新中心有限公司、江苏省科学技术情报研究所、江苏省未来网络创新研究院、江苏绿盟安全科技有限公司）联合起草编制，学会和标委会已组织专家组完成该项团体标准征求意见稿、送审稿、报批稿的技术审查工作，现批准《数据安全管理平台功能要求》为江苏省通信学会团体标准，编号为：T/JSIC 022-2023，自 2023 年 12 月 1 日起开始实施。现予公告。

江苏省通信学会

江苏省邮电标准化技术委员会

2023 年 11 月 28 日

全国团体标准信息平台

前　言

本文件按照国家标准 GB/T 1.1-2020《标准化工作导则标准化工作导则 第一部分：标准化文件的结构和起草规则》《江苏省通信学会团体标准管理办法》（苏通学[2022] 33 号）、《江苏省通信学会团体标准制定程序》（苏通学[2022] 35 号）及《江苏省通信学会知识产权管理制度》（苏通学[2022] 36 号）进行起草。

本文件主要规范数据安全管理平台类产品的功能要求、性能要求和安全保障要求，共 7 章，适用于数据安全管理平台的设计、开发与测试，本文件所指数据安全管理平台不包括数据防泄漏等用于数据自身安全防护的工具类系统或平台。

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。

本文件由江苏省通信学会和江苏省邮电标准化技术委员会负责归口管理，南京中新赛克科技有限责任公司负责具体内容的解释。

本标准主编单位：南京中新赛克科技有限责任公司

本标准参编单位：江苏中新赛克工业互联网安全技术创新中心有限公司
江苏省科学技术情报研究所
江苏省未来网络创新研究院
江苏绿盟安全科技有限公司

本标准主要起草人员：顾欢欢　糜靖峰　王明意　王　飞
王玉斐　田利荣　张广兴　徐传婷

本标准主要审查人员：孙知信　戴　源　章　澎　朱同先
王小鹏　钟秋爽　孔肖菡

目　次

1 范 围

本文件规定了数据安全管理平台在数据安全功能、自身安全功能、性能及安全保障等方面的要求。

本文件适用于数据安全管理平台的设计、开发与测试。

全国团体标准信息平台

2 规范性引用文件

下列文件中的内容通过文中的规范化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 42250-2022 《信息安全技术 网络安全专用产品安全技术要求》

GB/T 18336.3-2015 《信息技术 安全技术 信息技术安全评估准则 第 3 部分：安全保障组件》

GB/T 25069-2022 《信息安全技术 术语》

GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

GB/T 39786 《信息安全技术 信息系统密码应用基本要求》

GB/T 37092 《信息安全技术 密码模块安全要求》

GB/T 25000.51-2016 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》

GB/T 38634.2《系统与软件工程 软件测试 第 2 部分：测试过程》

GB/T 38634.4-2020《系统与软件工程 软件测试 第 4 部分：测试技术》

GB/T 38667 《信息技术 大数据 数据分类指南》

GB/T 42775 《证券期货业数据安全风险防控 数据分类分级指引》

GB/T 42128 《智能制造 工业数据 分类原则》

GB/T 38674-2020 《信息安全技术 应用软件安全编程指南》

YD/T 3813 《基础电信企业数据分类分级方法》

YD/T 4244 《电信网和互联网数据分类分级技术要求与测试方法》

YD/T 4251 《电信运营商大数据安全管控分类分级技术要求》

YD/T 4243 《电信网和互联网数据资产识别与梳理技术实施指南》

YD/T 4241 《电信网和互联网数据安全评估技术实施指南》

YD/T 4221 《电信大数据平台敏感数据识别实施指南》

YD/T 3956 《电信网和互联网数据安全评估规范》

YD/T 3801 《电信网和互联网数据安全风险评估实施方法》

YD/T 3867 《基础电信企业重要数据识别指南》

NIST SP 800-63-3 《Digital Identity Guidelines（数字身份准则）》

TC260-PG-20212A 《网络安全标准实践指南-网络数据分类分级指引》

TC260-PG-20231A 《网络安全标准实践指南-网络数据安全风险评估实施指引》

3 术语和定义

GB 42250-2022、GB/T 18336.3-2015、GB/T 25069-2022、GB/T 30279-2020、GB/T 22239-2019、GB/T 28448-2019 界定的以及下列术语和定义适用于本文件。

3.1 数据安全管理平台 data security management platform

具有数据分类分级、敏感数据发现、数据资产安全管理、数据安全风险评估、数据安全态势感知等功能的平台，不包括数据防泄露等用于数据自身安全防护的工具或平台。

3.2 数据安全管理平台提供者 data security management platform provider

数据安全管理平台（3.1）产品的研发者、生产者或维护服务提供者。

3.3 数据安全态势感知 data security situation awareness

在数据分类分级的基础上，通过监测发现敏感数据，管理数据资产，并综合其他网络安全态势等信息，分析和处理数据安全事件、相关网络行为及用户行为等因素，掌握数据安全状态，预测数据安全趋势，并进行展示和监测预警的活动。

3.4 敏感数据 sensitive data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成严重危害，或者对公共利益造成一般危害，但不会危害国家安全的数据。

3.5 产品供应链 products supply chain

是指为满足数据安全管理平台产品的设计、研发、交付与运维等过程中的供应关系，通过资源和过程将需方、供方相互链接的网链结构，可用于将相关产品和服务提供给数据安全管理平台提供者（3.2）。

3.6 用户信息 user information

个人、法人或者其他组织在安装、使用数据安全管理平台过程中产生、收集、存储、传输、处理的电子方式记录的信息，包括网络流量信息、用户数据信息、安全状态信息、安全配置数据、运行过程日志等信息，也包括个人信息。

3.7 安全漏洞 security vulnerability

数据安全管理平台在需求分析、设计、实现、配置、测试、生产、运行、维护等过程中，无意或有意产生的、有可能被利用的缺陷或薄弱点。

3.8 系统 system

数据安全管理平台作为一个完整的整体，执行 3.1 中所描述的功能，由相关作用或相互依赖关系联合起来的子系统组成，作为一个整体而发挥其作用。

3.9 子系统 subsystem

数据安全管理平台中的二级或下级系统，具有相对独立的功能。

4 缩略语

API	Application Programming Interface	应用编程接口
FTP	File Transfer Protocol	文件传输协议
FTPS	FTP-over-SSL	在安全套接层使用的文件传输协议
HTTP	Hyper Text Transfer Protocol	超文本传输协议
HTTPS	Hyper Text Transfer Protocol Secure	安全超文本传输协议
SFTP	Secure File Transfer Protocol	安全文件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳
SSL	Secure Sockets Layer	安全套接层
Syslog	System log	系统日志

5 功能要求

5.1 总体功能框架

数据安全管理平台包括图 5.1 中的数据分类分级、敏感数据发现、数据资产安全管理、数据安全风险评估、数据安全态势感知等功能，可根据需求实现一种或几种功能。

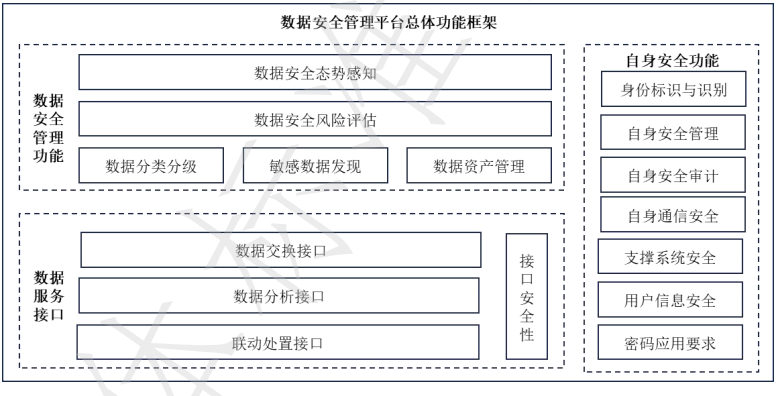

图 5.1 数据安全管理平台总体功能框架

5.2 数据安全管理功能要求

5.2.1 数据分类分级

平台的数据分类分级功能包括但不限于：

1.应遵循合法合规、界限明确、就高从严、注重时效和自主性原则，根据用户和行业需求、业务场景，满足国家和行业标准中给出的数据分类分级方法。

2.应支持对数据分类分级规则进行配置，准确标识数据类别和级别。

3.宜内置数据分类分级模板库，快速匹配不同的用户需求和业务场景。

5.2.2 敏感数据发现

平台的敏感数据发现功能包括但不限于：

1. 应根据用户和行业需求、业务场景，满足国家和行业标准给出的敏感数据识别要求。

2.应支持被动接收前端数据源发送的敏感数据，支持手动导入前端数据源的敏感数据。

3.应支持主动发起获取前端数据源的敏感数据，对数据库、文件系统等数据源进行字段级别、内容级别的深度扫描，支持结构化、半结构化和非结构化数据源，支持对扫描频率进行设置。

4.应根据应用场景支持两种或两种以上的采集协议进行敏感数据发现和采集，采集协议包括但不限于 Syslog、FTP/FTPS、SFTP、HTTP/HTTPS、SSH、SNMP 等。

5.应支持基于预置的敏感数据字典库对扫描到的数据进行匹配，识别敏感数据并梳理敏感数据在数据库、文件系统中的分布情况，支持根据应用场景自定义敏感数据字典库。

6.应支持展示平台管理的涉敏数据库及其数据库表、涉敏文件系统及其文件列表、敏感数据分布和类别等信息。

7.宜支持对网络流量的异常监测，通过内置的异常行为

告警规则和用户自定义规则，对异常流量数据进行告警、展示。

8.宜支持数据流转行为监测，对敏感指令、疑似暴力破解、特权账号使用、账号多 IP 使用等风险行为实时识别并告警。

5.2.3 数据资产管理

平台的数据资产管理功能包括但不限于：

1.应根据用户和行业需求、业务场景，满足国家和行业标准给出的数据资产识别和管理要求。

2.应支持通过人工添加、主动探测发现、被动识别等技术手段对目标数据库、文件系统、业务系统等数据源授权添加到平台中进行统一管理。

3.应支持建立数据资产画像。

4.应支持数据资产列表功能，全量统计当前系统中已探测到的数据库及其库表、字段信息，包括该字段的分类分级结果、敏感等级、归属的业务系统等信息。

5.宜实现数据资产地图，展示当前已经授权的数据库、文件系统、业务系统等数据源的分布以及数据分类分级、敏感数据发现等任务的进展情况。

6.宜支持结合内外部的分析能力预测潜在的数据资产风险。

5.2.4 数据安全风险评估

平台的数据安全风险评估功能包括但不限于：

1. 应根据用户和行业需求、业务场景，满足国家和行业标准给出的数据安全风险评估实施要求。

2.应提供数据安全风险核查功能，支持将 API 接口风险、弱口令、不合规配置、资产漏洞等核查结果以*.et、*.xls、*.xlsx等文件格式导入平台。

3.应支持结合数据类型、数据位置、数据重要程度、数据资产脆弱性、威胁信息等分析数据资产风险，评估数据资产风险等级。

4.应支持重要数据处理者对其数据处理活动开展风险评估。

5.可内置数据安全风险评估工具，支持评估准备、信息调研、风险识别、综合分析、评估总结等数据安全风险评估实施各阶段工作：

1）评估准备阶段工作包括确定评估目标、确定评估范围、组建评估团队、开展前期准备、制定评估方案等。

2）信息调研阶段工作包括数据处理者调研、业务和信息系统调研、数据资产调研、数据处理活动调研、安全措施调研等。

3）风险识别阶段工作包括数据安全管理、数据处理活动、数据安全技术、个人信息处理等的风险识别。

4）综合分析阶段工作包括梳理问题清单、数据安全风险分析与评价、提出整改建议。

5）评估总结阶段工作包括风险评估报告、安全风险处置

等。

5.2.5 数据安全态势感知

平台的数据安全态势感知功能包括但不限于：

1.应支持对数据的整体安全状况用分值或等级等方式进行评估和展示，例如以数据安全生命周期管理为主线，通过多维度量化指标，精准描述数据安全的实时风险和整体状况。

2.应支持对不同行业、不同区域、不同业务单元或不同数据资产等的局部数据安全状况采用分值或等级等方式进行评估和展示。

3.应支持对不同时间段的整体数据安全状况进行评估和展示。

4.应支持采用多种视图展示整体数据安全态势，展示视图至少包括以下中的两种：雷达图、地理信息图、关联关系图、威胁路径图、趋势图、同/环比图等。

5.应支持分角色展示，针对不同角色用户展示不同内容。

6.应支持展示整体数据安全状况的变化趋势，如分值或等级的变化等。

7.应支持根据应用场景和数据安全业务场景进行不同类型专题数据安全态势的评估和展示，如数据分类分级态势、敏感数据态势、数据资产态势、脆弱性态势、流量态势、攻击态势、异常行为态势、安全事件态势等。

8.应支持利用海量数据分析引擎及模型实现对数据风险的主动发现、精准定位、智能研判、快速处置、严格审计，

完成对数据安全保护工作的闭环处置流程。

9.应支持基于时间或其他数据字段对态势相关数据进行组合查询，支持对查询结果根据字段进行排序。

10.应支持根据数据分析、数据安全态势评估的结果生成统计报表并导出，支持基于指定时间段生成统计报表或生成周期性报表，支持自定义设置统计视图和报表模板，采用多种视图生成统计报表。

11.应支持根据数据分析结果生成整体数据安全状况分析报告并导出，支持根据数据分析结果生成不同区域、不同业务单元等的局部数据安全状况分析报告并导出，支持根据数据分析结果提供对策或修复建议，支持基于指定时间段产生分析报告或生成周期性分析报告，支持自定义设置分析报告的模板。

5.3 自身安全要求

5.3.1 身份标识和鉴别

平台的身份标识与鉴别安全要求包括但不限于：

1.应对用户身份进行标识和鉴别，身份标识具有唯一性。

2.应对用户身份鉴别信息进行安全保护，保障用户鉴别信息存储和传输过程中的保密性。

3.应具有登录失败处理功能，配置并启动结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

4.应具有登录超时处理功能，当登录连接超时自动退出。

5.鉴别机制应具有抗重放攻击的能力。

6.应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

7.当平台中存在默认口令时，应提示用户对默认口令进行修改，以减少用户身份被冒用的风险。

5.3.2 自身安全管理

平台的自身管理要求包括但不限于：

1.应区分管理员角色，划分为系统管理员、安全管理员和审计管理员，三类管理员角色权限能相互制约。系统管理员主要负责平台的日常运行维护工作，包括平台的安装、配置、升级、维护、运行管理，平台用户增加或删除，平台数据备份、运行日志审查和运行情况监控，应急条件下的安全恢复。安全管理员负责平台的安全管理工作，包括平台用户权限的授予与撤销，用户操作行为的安全设计，平台安全事件的审计、分析和处理，应急条件下的安全恢复。审计管理员主要负责对系统管理员和安全管理员的操作行为进行审计跟踪、分析和监督检查，及时发现违规行为。

2.应为授权系统管理员提供策略管理的功能，支持策略的集中管理和自定义设置，包括数据分类分级策略、敏感数据发现策略、监测策略和预警规则等。

3.应为授权系统管理员提供管理数据处理规则的功能，包括新增、删除、修改、查询、启用、停用数据处理规则等。

4.应为授权系统管理员提供数据分类分级模板库、数据分类分级规则库、敏感数据字典库、数据分析模型的管理，包括新增、删除、修改数据分析模型等。

5.应为授权系统管理员提供资产管理的功能，支持对采用人工添加、主动探测发现、被动识别等技术手段获取的资产信息进行管理。

6.应为授权安全管理员提供数据安全事件管理的功能，包括建立并动态维护数据安全事件库，对数据安全事件进行分类和分级等。

7.应建立威胁信息库，为授权安全管理员提供威胁信息管理的功能，支持对不同来源的威胁信息进行汇聚并及时更新。

8.应向授权安全管理员提供设置、查询和修改各种安全策略的功能。

9.应向授权审计管理员提供管理审计日志的功能。

10.应支持更新自身系统的能力，包括对软件系统的升级以及各种特征库、策略库的升级，保障升级安全，避免得到错误的、伪造的升级包和补丁程序。

11.应支持通过 Syslog 协议向日志服务器同步日志等信息。

12.应支持与外部时间服务器进行时间同步。

13.应提供安全策略有效性检查功能，如安全策略匹配情况检测等。

5.3.3 自身安全审计

平台的安全审计要求包括但不限于：

1.应对用户账户的登录和注销、系统启动、配置变更、增加/删除/修改管理员、保存/删除审计日志等操作行为进行监测、记录。

2.应对平台及其组件的运行状态进行监测，对异常状态进行告警，并记录日志。

3.日志记录应包括如下内容：事件发生的日期和时间，事件的类型，事件主体，事件操作结果。

4.应将日志存储于非易失性存储介质中，日志保存时间不少于六个月。

5.应仅允许授权审计管理员访问日志，对日志进行保护，防止受到未预期的删除、修改、覆盖和丢失。

5.3.4 自身通信安全

1.应采用校验技术或密码技术保证远程管理时的所有网络通信数据在传输过程中的完整性。

2.应采用密码技术保证远程管理时的所有网络通信数据在传输过程中的保密性。

3.应限定进行远程管理的 IP、MAC 地址。

4.应分离管理接口与业务接口。

5.3.5 支撑系统安全

平台的支撑系统安全要求包括但不限于：

1.不应提供多余的组件或网络服务。

2.重启不应导致安全策略和日志信息丢失。

3.不应包含已公开的中风险及以上漏洞。

注：漏洞风险等级参照 GB/T 30279 《信息安全技术 网络安全漏洞分类分级指南》中给出的网络安全漏洞分级方法。

5.3.6 用户信息安全

1.应仅收集实现功能所必需的用户信息。

2.应明示收集用户信息的目的、方式、范围、种类、存储位置和处理方式。

3.应建立和执行用户信息管理制度和流程，在设计、生产、升级等各阶段保障用户信息的安全，不超范围使用用户信息。

4.应在涉及个人信息处理时提供相关授权功能，在获得授权后方能处理个人信息。个人信息处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。授权功能包括但不限于个人信息收集前的授权同意、个人信息收集的授权撤回等。

5.应对收集到个人信息进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

6.应在未获得或撤回个人信息收集授权的情况下提供与个人信息无关的安全功能。

7.应在涉及个人信息传输和存储过程中，采用校验技术或密码技术保障个人信息的保密性和完整性。

8.应在涉及个人信息存储时提供对超出保存期限个人信息的处理功能，处理方式应与用户授权的处理方式一致，如采取删除或匿名化处理措施。

5.3.7 密码应用要求

1.应采用密码技术对登录用户进行身份鉴别，保证平台用户身份的真实性。

2.应采用密码技术保证平台重要数据在传输和存储过程中的机密性。

3.宜采用密码技术保证平台的访问控制信息的完整性。

4.宜采用密码技术保证平台重要信息资源安全标记的完整性。

5.宜采用密码技术保证平台重要数据在传输和存储过程中的完整性。

6.以上（5.3.7-1 至 5.3.7-5）如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。

7.以上（5.3.7-1 至 5.3.7-5）采用的密码产品或模块，应达到 GB/T 37092《信息安全技术 密码模块安全要求》中的二级及以上安全要求。

5.3.8 部署与运行环境安全

平台部署运行环境中的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运

维管理应满足 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中第 8.1 节规定的网络安全等级保护三级要求。

5.4 数据服务接口

5.4.1 数据交换接口

1.应支持与不同前端数据源、内部不同模块及其他外部系统通过接口进行数据交换，数据交换包括但不限于数据采集、共享、级联交换。

2.应支持不同类型、字段和格式的数据交换内容，其中类型包括日志、告警信息、威胁信息、数据资产信息、用户信息、脆弱性信息、数据安全事件等，字段和格式应基于类型进行定义。

5.4.2 数据分析接口

1.宜支持为内部不同模块及其他外部系统通过接口进行数据分析。

2.宜支持基于数据分析接口实现算术计算、逻辑关系计算、关联计算等分析能力。

5.4.3 联动处置接口

1.宜支持为内部不同模块及其他外部系统通过接口进行联动处置。

2.宜支持通过接口进行防护策略的更新、扫描策略的下发等操作。

5.4.4 接口安全性

应具有相应的数据服务接口安全保障机制，保证数据在传输过程中的可用性、完整性和保密性。

6 性能要求

6.1 通用要求

1.平台应支持市场上主流的数据库和数据库组件。

2.平台应符合 GB/T 25000.51-2016《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》中第 5.3 节，关于功能性、性能效率、兼容性、易用性、可靠性、信息安全性、维护性、可移植性的规定。

6.2 数据扫描要求

6.2.1 结构化数据

1.结构化数据资产发现扫描速率应不低于每分钟 20000 字段。

2.结构化数据分类分级扫描速率应不低于每分钟 500 字段（每字段数据抽样不超过 1000 行），支持并发任务数量不低于 10 个。

3.结构化敏感数据扫描速率应不低于每分钟 100 字段（每字段 10000 行数据），支持并发任务数量不低于 10 个。

6.2.2 非结构化数据

非结构化数据源扫描速率应不低于每小时 20GB。

7 安全保障要求

7.1 总体安全保障框架

数据安全管理平台安全保障应考虑供应链安全，贯穿需求分析、设计与开发、生产与交付、运行维护服务等全生命周期各阶段，并加强指导性文档、配置管理、用户信息保护、测试等环节的管理。

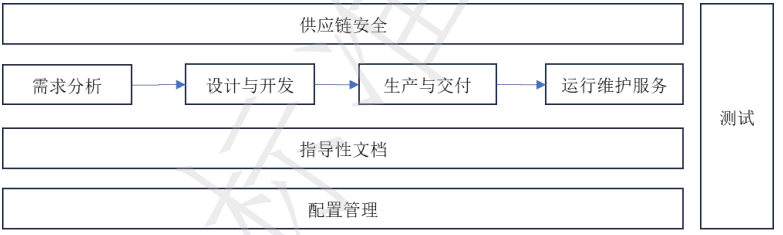

图 7.1 数据安全管理平台总体安全保障框架

7.2 供应链安全

平台提供者应满足以下安全保障要求：

1.制定供应商选择、评定和日常管理的程序，对供应商的开发环境、规范和人员、开发工具、安全测试和安全验证机制等提出管理要求，以确保其提供的关键部件满足安全要求，并保存对供应商选择、评价和日常管理的记录。

2.建立供应链各环节核心要素的追溯能力，保障核心要

素供应文档，核心要素包括核心技术知识产权、工具及部件等。核心技术知识产权如源代码、软硬件设计图等；工具如开发软件、编译软件、测试软件、测试仪表、管理软件、拷机软件等；部件如硬件机箱、操作系统等。

3.持续对供应链各环节相关人员开展安全意识和技能培训。

7.3 需求分析

平台提供者应实施以下与需求分析相关的管理：

1.根据法律法规的要求、标准约束和客户需求等形成业务需求说明书和自身安全需求说明书。

2.基于平台的部署和运行环境，以及自身安全需求说明书开展前期的风险评估，形成风险评估报告。

3.制定整体的数据安全管理策略和平台自身安全策略。

4.组织对业务需求说明书、自身安全需求说明书、风险评估报告、数据安全管理策略和自身安全策略进行评审。

5.分析确定数据安全管理平台功能性、性能效率、兼容性、易用性、可靠性、信息安全性、维护性、可移植性等方面的质量目标。

7.4 设计与开发

7.4.1 功能规范

平台提供者应提供完备的功能规范说明，并对功能规范说明进行评审，功能规范说明应满足以下要求：

1.根据平台类型清晰描述 5.2、5.3、5.4 定义的平台功能。

2.标识和描述平台所有功能接口的目的、使用方法及相关参数。

3.描述功能实施过程中，与功能接口相关的所有行为。

4.描述可能由功能接口的调用而引起的所有直接错误消息。

7.4.2 平台设计

平台提供者应对平台进行设计，提供平台设计文档，并对设计文档进行评审，平台设计文档应满足以下要求：

1.通过子系统描述平台结构，标识和描述平台功能的所有子系统，并描述子系统间的相互作用。

2.提供子系统和功能接口间的对应关系。

3.通过实现模块描述功能，标识和描述实现模块的目的、相关接口及返回值等，并描述实现模块间的相互作用及调用的接口。

4.提供实现模块和子系统间的对应关系。

7.4.3 开发实现

1.平台提供者应根据设计文档开发平台，编程实现过程应遵循 GB/T 38674-2020 《信息安全技术 应用软件安全编程指南》中关于安全功能实现、代码实现安全、资源使用安全、环境安全的要求，严禁在产品中设置恶意程序、隐蔽接口或未明示功能模块等。

2.平台提供者应提供软件代码、数据表单等开发实现文

档，应注释和详细描述平台功能的具体实现，描述代码实现与平台设计间的对应关系。

7.5 测试

7.5.1 测试覆盖

平台提供者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

1.表明测试文档中所标识的测试与功能规范中所描述的平台的功能间的对应性。

2.表明上述对应性是完备的，并证实功能规范中的所有功能接口都进行了测试。

7.5.2 测试深度

平台提供者应提供测试深度的分析，测试深度分析描述应满足以下要求：

1.证实测试文档中的测试与平台设计中的功能子系统和实现模块之间的一致性。

2.证实平台设计中的所有功能子系统、实现模块都已经进行过测试。

7.5.3 功能测试

1.平台提供者应对平台功能进行测试，测试设计和实现过程中使用的测试设计技术满足 GB/T 38634.4-2020《系统与软件工程 软件测试 第 4 部分：测试技术》第 5 章中关于测试设计技术和第 6 章中关于测试覆盖率测量的要求。

2.功能测试过程应进行组织级过程控制，对静态和动态

测试过程进行管理，满足 GB/T 38634.2-2020《系统与软件工程 软件测试 第 2 部分：测试过程》中第 5 章中关于组织级测试过程、第 7 章中关于测试管理过程和第 8 章中关于动态测试过程的要求。

3. 平台提供者应提供功能测试文档集，测试文档集应符合 GB/T 25000.51-2016《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》中第 6 章，关于测试计划、测试说明和测试结果的要求。

7. 5. 4　性能测试

1.平台提供者应对平台性能进行测试，测试设计和实现过程中使用的测试设计技术满足 GB/T 38634.4-2020《系统与软件工程 软件测试 第 4 部分：测试技术》第 5 章中关于测试设计技术和第 6 章中测试覆盖率测量的要求，性能测试包括但不限于以下平台质量属性指标：

1）平台功能性的完备性、正确性、适合性等指标。

2）平台性能效率的时间特性、资源利用性、容量等指标。

3）平台易用性的可辨识性、易学性、易操作性、用户差错防御性、用户界面舒适性、易访问性等指标。

4）平台可靠性的成熟性、可用性、容错性、易恢复性等指标。

5）平台信息安全性的保密性、完整性、抗抵赖性、可核查性、真实性等指标。

6）平台维护性的模块化、可重用性、易分析性、易修改性、易测试性等指标。

7）平台兼容性的共存性、互操作性等指标。

8）平台可移植性的适应性、易安装性、易替换性等指标。

9）平台与有关的标准、约定和法规以及类似规定的遵从程度。

2. 性能测试过程应进行组织级过程控制，对静态和动态测试过程进行管理，满足 GB/T 38634.2-2020《系统与软件工程 软件测试 第 2 部分：测试过程》中第 5 章中关于组织级测试过程、第 7 章中关于测试管理过程和第 8 章中关于动态测试过程的要求。

3. 平台提供者应提供性能测试文档集，测试文档集应符合 GB/T 25000.51-2016《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》中第 6 章，关于测试计划、测试说明和测试结果的要求。

7. 5. 5　独立测试

平台提供者应提供一组与其自测平台功能和性能时使用的同等资源，以用于平台功能和性能的抽样测试。

7. 5. 6　第三方测试

应通过具有法定资质的第三方检验检测机构出具的平台质量检测报告。

7.6 指导性文档

7.6.1 操作手册

平台提供者应提供明确和合理的操作用户指南，对每一种用户角色的描述应满足以下要求：

1.描述用户能访问的功能和特权，包含适当的警示信息。

2.描述平台功能及接口的用户操作方法，包括配置参数的安全值等。

3.标识和描述平台运行的所有可能状态，包括操作导致的失败或者操作性错误。

4.描述实现平台安全目的必须执行的安全策略。

7.6.2 准备程序

平台提供者应提供平台及其准备程序，准备程序描述应满足以下要求：

1.描述与开发者交付程序相一致的安全接收所交付平台必需的所有步骤。

2.描述部署安装平台及其运行环境必需的所有步骤。

7.7 配置管理

7.7.1 配置管理能力

平台提供者的配置管理能力应满足以下要求：

1.为平台的不同版本提供唯一的标识。

2.使用配置管理系统对组成平台的所有配置项进行维护，并进行唯一标识。

3.提供配置管理文档，配置管理文档描述用于唯一标识

配置项的方法。

4.配置管理系统提供自动方式来支持平台的生成，通过自动化措施确保配置项仅接受授权变更。

5.配置管理文档包括一个配置管理计划，描述用来接受修改过的或新建的作为平台组成部分的配置项的程序。配置管理计划描述如何使用配置管理系统，开发者实施的配置管理与配置管理计划相一致。

7.7.2 配置管理范围

平台提供者应提供平台配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

1.平台、安全保障要求的评估证据和平台的组成部分。

2.实现表示、安全缺陷报告及其解决状态。

7.8 生产与交付

平台提供者应满足以下安全保障要求：

1.提供开发安全文档。开发安全文档应描述在平台的开发环境中，为保护平台设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

2.明确定义用于开发平台的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

3.建立和执行规范的平台完整性检测流程，采取措施防范自制或采购的组件被篡改、伪造等风险。

4.建立内部交付和外部交付的控制程序，确保平台在交

付过程中不被破坏或篡改。

5.向用户明示包含在平台中的所有功能模块、外部接口和私有协议，告知用户平台中预置的所有账户和默认口令。

6.使用一定的交付程序交付平台，并将交付过程文档化。在给用户方交付平台的各版本时，交付文档应描述为维护安全所必需的所有程序。

7.9 运行维护服务

平台提供者应满足以下安全保障要求：

1.在法律法规规定或与用户约定的期限内，为平台提供持续的安全维护，不单方面中断或终止安全维护。

2.保护用户对软件（包含固件）安装和升级等的知情权和选择权，安装和升级软件时明示用户并获得用户同意。

3.建立和执行针对平台安全缺陷、漏洞的应急响应机制和流程，对发现的平台安全缺陷和漏洞采取修复或替代方案等补救措施，及时告知用户安全风险和可用的补救措施，并向有关主管部门报告。

4.根据运行维护服务协议和用户需求，提供对平台软件及其运行环境的调查研究和分析评价服务，提出平台的运行报告或建议。

5.根据运行维护服务协议和用户需求，提供平台运行的监控指标体系设计、平台运行监控、问题分析等服务。

6.根据运行维护服务协议，对平台及其运行环境的服务

请求或故障申报提供即时运行维护，以保障平台的正常运行。

7.根据运行维护服务协议和用户需求，对平台的功能和性能进行调优，并满足新的需求，包括功能改进、性能优化改进、适应性改进、预防性改进等。

本文件用词说明

1.为便于执行本文件条文时区别对待，对要求严格程度不同的用词说明如下：

1）表示很严格，非这样做不可的用词：正面词采用“必须”，反面词采用“严禁”；

2）表示严格，在正常情况均应这样做的用词：正面词采用“应”，反面词采用“不应”或“不得”；

3）表示允许稍有选择，在条件许可时首先应这样做的用词：正面词采用“宜”，反面词采用“不宜”；

4）表示有选择，在一定条件下可以这样做的用词，采用“可”。

2.条文中指明应按其他有关标准执行的写法为“应按……执行”或“应符合……的规定”。

江苏省通信学会团体标准

数据安全管理平台功能要求

Functional Requirements for Data Security Management Platform

T/JSIC 022-2023

条 文 说 明

条文说明

1 范围

随着《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》等法律的深入实施，数据成为战略资产，数据安全提升到国家战略。《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》（工信部网安[2022] 182 号）明确提出要加强数据安全重点标准供给，鼓励制定数据安全产品技术要求等标准制定。数据安全管理产品标准化是提升数据安全管理产品质量的必要手段。

本文件进一步规范数据安全管理平台类产品的功能技术要求，规范平台数据安全功能、自身安全功能以及产品全生命周期安全保障要求，有助于提升数据安全管理平台产品质量，全面提升数据安全保障效能。

本文件所指数据安全管理平台不包括数据防泄漏等用于数据自身安全防护的工具类系统或平台。

5 功能要求

5.2.1 数据分类分级

数据安全管理平台应根据用户需求、业务场景和相关行业要求，满足国家和行业标准中给出的数据分类分级方法，例如：

GB/T 38667 《信息技术 大数据 数据分类指南》

GB/T 42775 《证券期货业数据安全风险防控 数据分类分级指引》

GB/T 42128 《智能制造 工业数据 分类原则》

YD/T 3813 《基础电信企业数据分类分级方法》

YD/T 4244 《电信网和互联网数据分类分级技术要求与测试方法》

YD/T 4251 《电信运营商大数据安全管控分类分级技术要求》

TC260-PG-20212A 《网络安全标准实践指南-网络数据分类分级指引》

其中，TC260-PG-20212A 中给出了数据类别和级别参考示例，分别如表 5.2.1-1、表 5.2.1-2 所示。

表 5.2.1-1 数据主体视角的数据分类参考示例

数据分类	类别定义	示例
公共数据	公共管理和服务机构在依法履行公共管理和服务职责过程中收集、产生的数据，及其他组织和个人在提供公共服务中收集、产生的涉及公共利益的数据	如政务数据，及提供供水、供电、供热、公共交通、养老、教育、医疗健康、邮政等公共服务中涉及公共利益的数据等
个人信息	以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种	如个人身份信息、个人生物识别信息、个人财产信息、个人通信信息、

	信息，不包括匿名化处理后的信息	个人位置信息、个人健康生理信息等
法人数据	组织在生产经营和内部管理过程中，收集和产生的数据	如业务数据、经营管理数据、系统运行和安全数据等

表 5.2.1-2 数据分级规则参考示例

数据分级	传播范围	级别定义
公开级（1 级）	公开级数据具有公共传播属性，可对外公开发布、转发传播，但也需考虑公开的数据量和级别，避免由于类别较多或者数量过大被用于关联分析	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成轻微危害，但不会危害国家安全、公共利益
内部级（2 级）	内部级数据通常在组织内部、关联方共享和使用，相关方授权后可向组织外部共享	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成一般危害，或者对公共利益造成轻微危害，但不会危害国家安全
敏感级（3 级）	敏感级数据仅能由授权的内部机构或人员访问，如果要将数据共	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成严重危害，或者对公共利益

数据分级	传播范围	级别定义
	享到外部，需要满足相关条件并获得相关方的授权	造成一般危害，但不会危害国家安全
重要级（4 级）	重要级数据按照批准的授权列表严格管理，仅能在受控范围内经过严格审批、评估后才可共享或传播	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成特别严重危害，或者对公共利益造成严重危害，或者对国家安全造成轻微或一般危害
核心级（5 级）	核心级数据禁止对外共享或传播	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对国家安全造成严重或特别严重危害，或对公共利益造成特别严重危害

5.2.2 敏感数据发现

数据安全管理平台应根据用户需求、业务场景和相关行业要求，满足国家和行业标准中给出的敏感数据识别要求，例如：

YD/T 4221 《电信大数据平台敏感数据识别实施指南》

YD/T 3867 《基础电信企业重要数据识别指南》

5.2.3 数据资产管理

数据安全管理平台应根据用户需求、业务场景和相关行业要求，满足国家和行业标准中给出的数据资产识别和管理

要求，例如：

YD/T 4243 《电信网和互联网数据资产识别与梳理技术实施指南》

5.2.4 数据安全风险评估

数据安全管理平台应根据用户需求、业务场景和相关行业要求，满足国家和行业标准中给出的数据安全风险评估实施要求，例如：

YD/T 4241 《电信网和互联网数据安全评估技术实施指南》

YD/T 3956 《电信网和互联网数据安全评估规范》

YD/T 3801 《电信网和互联网数据安全风险评估实施方法》

TC260-PG-20231A 《网络安全标准实践指南-网络数据安全风险评估实施指引》

5.3.5 支撑系统安全

数据安全管理平台所依赖的基础支撑系统，可以从以下几种方法保障其安全性：

1.查看产品文档，并验证产品的支撑系统是否进行了必要的裁剪，是否不提供多余的组件或网络服务。

2.重启产品，验证安全策略和日志信息是否不丢失。

3.对产品进行安全性测试，验证是否不含已公开的中、高风险安全漏洞。

5.3.7 密码相关要求

依据《中华人民共和国密码法》《商用密码条例》，数据安全产品使用商用密码提升自身安全性，所以用的密码算法、密码协议、密钥管理机制等商用密码技术符合国家法律法规和相关国家标准要求。

6 性能要求

6.1 通用要求

数据安全管理平台应支持市场上主流的数据库和数据库组件，随着我国信息技术应用创新的深入推进，国产数据库系统的应用越来越多，数据安全管理平台需要支持国外及国产主流数据库系统，以适应更多的应用场景。包括但不限于：Oracle、SQLServer、MySQL、MiariaDB、PostgreSQL、GreenPlum、informix、clickhouse、DB2、GaussDB、MongoDB、ES、HBase、Hive、武汉达梦、南大通用、人大金仓。

GB/T 25000.51-2016 确立了就绪可用软件产品（RUSP）的质量要求、文档集要求和 RUSP 的符合性评价细则，旨在帮助各方进行 RUSP 需求制定、测试、标准符合性评价及认证等活动。数据安全管理平台具有较大的业务相关性和应用定制属性，总体上可依据 GB/T 25000.51-2016，结合具体应用场景和需求，对性能效率、兼容性、易用性、可靠性、维护性、可移植性等质量属性进行定义和测试。

7 安全保障要求

7.2 供应链安全

国家层面高度重视软件供应链安全问题，不断建立健全

法律法规、标准制度。为应对国内外软件供应链安全威胁，近年来我国先后颁布的《中华人民共和国网络安全法》《网络安全审查办法》《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》《关键信息基础设施安全保护条例》等政策法规强调加强软件供应链的安全保障。2018 年，我国出台了供应链安全管理国家标准《信息安全技术 ICT 供应链安全风险管理指南》(GB/T 36637-2018)，从产品全生命周期的角度开展风险分析及管理，以实现供应链的完整性、保密性、可用性和可控性安全目标。

7.4.6 第三方测试

第三方测试机构一般应具有 CANS、CMA 授权资质，且相关标准在认可范围之内，如 GB/T 25000.51-2016、GB 42250-2022。