ICS 33.050
CCS M 30

团 体 标 准

T/TAF 192—2023

基于数据沙箱的数据流通产品技术要求与测评方法

Technical requirements and testing methods for data circulation products based on data sandboxes

2023-11-24 发布 2023-11-24 实施

电信终端产业协会 发布

目　　次

前　言

本文件根据 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：百度在线网络技术（北京）有限公司、北京元宇宙文化有限公司、中国信息通信研究院、联想（北京）有限公司、郑州信大捷安信息技术股份有限公司、蚂蚁科技集团股份有限公司、北京京东世纪贸易有限公司。

本文件主要起草人：王霞、边元松、瞿晓楠、刘小丽、袁琦、郭建领、王欢、齐萱、王海棠、郭强、于欢、王国林、安媛媛、王昱龙、李汝鑫、林巍巍、刘献伦、康亮、林冠辰、李然。

引　言

伴随着物联网和移动互联网的落地应用，智慧城市、智慧金融、智慧医疗等应用领域相继兴起，以数据要素为生产力的万物互联时代已经到来。但随着数据安全法律法规的日趋严格与完善，企业在数据开放共享过程中面临着数据安全、合规应用等问题，如何能在保证数据安全的前提下推进数据要素的流通与应用受到了各界的广泛关注。针对这样的两难困境，数据沙箱技术在保护数据安全的前提下，为数据开放共享、促进数据价值挖掘提供了一个切实可行的解决方案。在大数据产业快速发展的牵引下，我国数据沙箱技术产品正在逐步成熟、应用场景快速扩充，其产业化也在快速进行。

数据沙箱技术是一种数据拥有方在保证原始私有数据不出数据方定义的私有边界的前提下，通过数据的所有权和使用权分离，从而帮助数据使用方完成某项机器学习任务的机器学习模式。基于数据沙箱的数据流通产品是提供给数据开放共享过程中各参与方使用，提供数据安全开放共享所需的计算和通信等功能，并满足机器学习任务需求的软件系统或软硬件一体化系统。

本文件聚焦于数据沙箱技术，期望为数据的安全开放共享构建一套行之有效的技术规范，从而有效助力行业的健康发展，推进产业进一步的落地应用。

基于数据沙箱的数据流通产品技术要求与测试方法

1 范围

本文件规定了基于数据沙箱的数据流通产品的技术要求和测试方法，主要包含系统管理能力、数据管理能力、计算能力、安全性、性能要求等。

本文件适用于基于数据沙箱的数据流通产品的研发、测试、评估和验收等。

2 规范性引用文件

下列文件中的内容通过本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 5271.8—2001 信息技术 词汇 第8部分:安全

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 35295—2017 信息技术 大数据 术语

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据沙箱 data sandbox

数据沙箱是一种通过构建完全隔离的调试环境和运行环境来分离数据所有权和使用权，从而确保数据安全的技术。

3.2

数据集 data set

数据记录汇聚的数据形式。

[来源：GB/T 35295—2017，2.1.46]

3.3

数据脱敏 data desensitization

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

[来源：GB/T 37988—2019，3.12]

3.4

样例数据 sample data

通过预定义的规则，将全量数据的部分条目抽取出来，能够体现出全量数据的分布情况的数据。

3.5

全量数据　full data

从数据源读取出的，经过数据转换为标准格式，内容未经过抽样或脱敏处理的数据。

3.6

调试环境　debug environment

通过隔离技术实现的，可防御内部的恶意攻击，单向访问隔离，用户之间相互隔离，对系统内部业务隔离，对数据集访问受限，仅可访问样例数据，用于工程代码撰写和调试的可视环境。

3.7

运行环境　run environment

通过隔离技术实现的用于工程代码撰写和调试的可视环境，具备单向访问隔离机制，可实现用户之间相互隔离，对系统内部业务隔离，内部数据集访问受限，可防御内部的恶意攻击。

3.8

工程代码　project code

使用者定义的用于表示业务逻辑的具有版本信息的程序代码，例如：数据处理，生成模型，或模型推理。

3.9

安全审计　security audit

对信息系统记录与活动的独立评审和考察，以测试系统控制的充分程度,确保对于既定安全策略和运行规程的符合性，发现安全违规并在控制、安全策略和过程三方面提出改进建议。

[来源：GB/T 25069—2022，3.24]

3.10

共享　share

信息控制者向其他控制者提供信息，且双方分别对信息拥有独立控制权的行为。

[来源：GB/T 35273—2020，3.13]

3.11

机器学习　machine learning

功能单元通过获取新知识或技能，或通过整理已有的知识或技能来改进其性能的过程。

[来源：GB/T 5271.31—2006，31.1.2]

3.12

端口　port

链接的端点。

注：在互联网协议的语境下,端口是传输控制协议(TCP)连接或用户数据报协议(UDP)消息的逻辑信道端点。基于TCP或UDP的应用协议,通常已分配默认端口号,如为超文本传输协议(HTTP)的端口号是80。

[来源：GB/T 25069—2022，3.130]

4　缩略语

下列缩略语适用于本文件。

ACC：准确度（Accuracy）
AUC：受试者工作特征曲线下的面积（Area Under Curve）
CSV：逗号分隔值(Comma-Separated Values)
JPG：联合图像专家组（Joint Photographic Experts Group）
KS：模型区分度评估值（Kolmogorov-Smirnov）
LOGO：商标（logotype）
MSE：均方误差（Mean Square Error）
SQL：结构化查询语言（Structured Query Language）
TXT：文本（text）

5 概述

数据沙箱技术是一种数据拥有方在保证原始私有数据不出数据方定义的私有边界的前提下，通过构造相互分离的调试环境和运行环境，实现数据不动代码动，从而帮助数据使用方完成某项机器学习任务的机器学习模式。

基于数据沙箱技术的数据流通产品是提供给数据开放共享过程中各参与方使用，提供数据安全开放共享所需的计算和通信等功能，并满足机器学习任务需求的软件系统或软硬件一体化系统。

基于数据沙箱技术的数据流通产品根据使用场景通常分为以下几种：

数据对内共享：企业或组织将数据安全开放给内部或跨团队的数据需求方进行调试、测试等作业，在保护原始数据不被触碰的前提下，实现数据价值的安全对内流通。

数据对外开放：企业或组织将数据安全开放给外部的数据需求方进行建模、分析等作业，在数据不出域的前提下，实现数据价值的挖掘。

基于数据沙箱技术的数据流通产品典型应用场景如下：

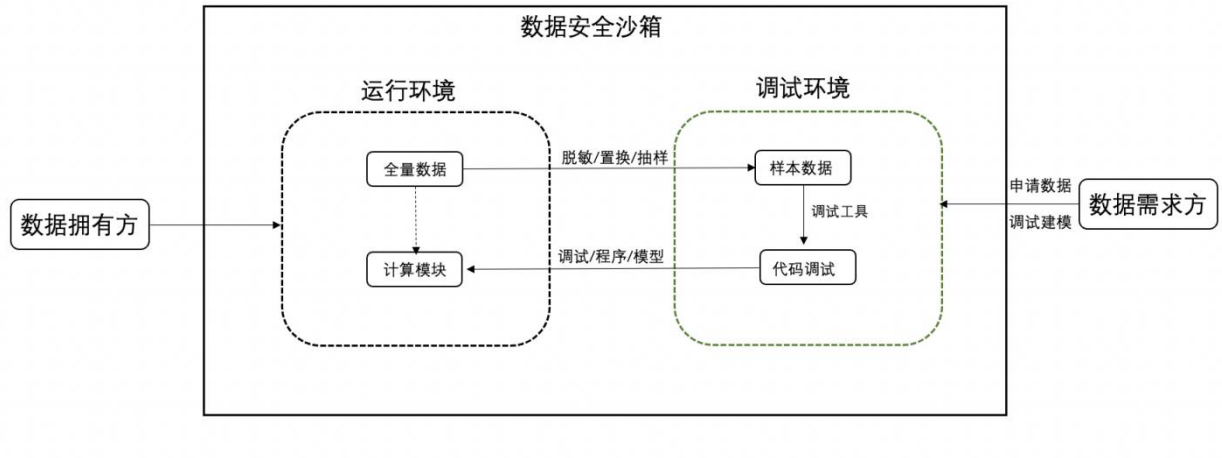

图 1　基于数据沙箱技术的数据流通产品典型应用场景

该应用场景主要包括调试环境、运行环境、数据拥有方、数据需求方 4 个部分。数据拥有方对全量数据进行抽样脱敏后生成样例数据，开放给数据需求方；数据需求方可在调试环境内进行代码的调试，调试完成后将代码推送至运行环境，在运行环境中基于全量数据运行代码，运行产生的结果经审批后可被数据需求方下载使用，以实现数据所有权和使用权的分离，保护原始数据不会被触碰。

6 技术要求

6.1 系统管理要求

6.1.1 集群管理

集群管理应符合以下要求：

a) 应支持对集群进行添加、编辑、启用、禁用、删除；
b) 应支持对集群计算环境规格、数据网关进行配置并进行连通性测试。

6.1.2 用户管理

用户管理应符合以下要求：

a) 应支持对用户及用户组进行添加、设置、启用、禁用、编辑、删除；
b) 应支持对用户及用户组进行批量导入、导出；
c) 应支持对用户及用户组设置访问控制策略。

6.1.3 资源管理

应支持对系统创建的调试环境或运行环境进行查看、搜索、删除。

6.1.4 日志管理

应支持对系统创建的运行任务的日志进行查看、搜索、审计。

6.1.5 模型管理

应支持对系统创建的所有模型进行查看、搜索、审计。

6.1.6 审计管理

应支持用户操作行为日志的查看、搜索、下载。

6.1.7 系统设置

系统设置应符合以下要求：

a) 应支持登录超时配置功能；
b) 应支持用户口令丢失找回功能；
c) 应支持消息类型通知方式可配置；
d) 应支持系统登录背景、LOGO 可配置。

6.2 数据管理要求

6.2.1 数据源管理

数据资源管理应符合以下要求：

a) 应支持对不同类型数据源，包括MySQL、Oracle、MariaDB、PostgreSQL、BOS进行添加、编辑、禁用、删除；
b) 应支持对数据源连通性进行检测；
c) 应支持根据数据源名称、主机IP、端口等多种条件进行数据源搜索。

6.2.2 脱敏标签管理

脱敏标签管理应符合以下要求：

a) 应支持内置常用数据，包括姓名、身份证号码、手机号、邮箱的脱敏识别规则和处理规则；
b) 应支持自定义敏感数据的识别规则并对其进行编辑、删除；
c) 应支持自定义敏感数据的处理规则并对其进行编辑、删除。

6.2.3 数据集添加

系统应能够支持对数据集进行添加，具体要求应符合以下内容：

a) 应支持数据集的添加、查看、编辑、删除；
b) 应支持多种数据集添加方式，文件方式包括CSV, TXT,JPG,数据库连接方式包括MySQL、Oracle、MariaDB、PostgreSQL、BOS。

6.2.4 数据处理

数据处理应符合以下要求：

a) 应支持对数据集基于自定义或内置的脱敏标签进行脱敏处理；
b) 应支持对数据集进行抽样，支持多种类型抽样方式，包括随机抽样、分层抽样、快速抽样；
c) 应支持对数据集执行数据抽样脱敏任务并预览处理效果、以及终止、删除任务；
d) 应支持查看抽样脱敏后产生的样例数据集的数据集名称、数据集描述、数据集字段类型、样例数据；
e) 对文本数据的处理性能应不低于:30GB/h,对图片数据的处理性能应不低于20GB/h；
f) 脱敏处理的准确率应不低于：60%。

6.2.5 数据集管理

数据集管理应符合以下要求：

a) 应支持数据集的查看、授权、发布、下架、编辑、删除；
b) 应支持根据数据集ID、数据集名称进行数据集的搜索；
c) 应可查看数据集的信息，包括：数据集名称、数据集大小、数据来源、数据集标签、数据量、查看次数、授权次数、下载次数。

6.2.6 申请审核管理

申请与审核管理应符合以下要求：

a） 应支持用户对上架的数据集进行查看、搜索和申请；
b） 应支持用户对在运行环境中执行任务所产生的计算结果进行申请和下载；
c） 应支持对用户提起的申请进行查看和审批；
d） 应支持对申请文件、代码、数据集进行审计。

6.3 计算要求

6.3.1 代码调试

建模代码调试应符合以下要求：

a） 应支持以 Python 为主的多种语言编程的调试环境；
b） 应支持对调试环境进行添加及删除；
c） 应支持常见的代码编译工具，包括：Web Shell、VSCode、Jupyter Notebook；
d） 应支持常见的机器学习框架，包括：TensorFlow、Pytorch、Pycharm；
e） 应具备调试环境与运行环境分离的技术架构；
f） 应支持在调试环境中调用抽样脱敏后的样例数据集并进行代码的调试。

6.3.2 全量任务

全量任务应符合以下要求：

a） 应支持基于全量数据在运行环境中运行代码；
b） 应支持任务的添加、查看、终止、删除；
c） 应支持对运行任务的状态、运行时长、创建时间、任务开始时间、任务日志、任务输出信息进行查看；
d） 应支持基于机器学习算法进行模型训练和预测，包括:回归模型、二分类模型、多分类模型。
e） 应支持查看包括KS、AUC、ACC、MSE在内的模型评估指标。

6.4 安全要求

6.4.1 数据流通安全

数据流通安全应符合以下要求：

a） 参与数据开放共享的数据方原始数据，在建模任务执行过程中不应以明文形式被带出安全域；
b） 需保护模型训练过程的中间结果、日志文件、模型预测产生的结果文件、模型训练结束后的评估数据等，防止越权访问；
c） 应保护系统使用人员的信息安全，保障信息不被泄露或窥探；
d） 建模任务的结果仅允许授权方获取，非授权方无法直接查看计算结果。

6.4.2 网络通信安全

宜采用安全的通信协议加密，无法通过抓包解析出原始数据。

6.4.3 系统稳定性

可为参与方之间提供稳定的网络传输、安全的计算执行，宜具备在网络抖动、硬件故障等异常情况下进行断点恢复的功能。

6.4.4 系统安全性

系统安全性应符合以下要求：

a) 应保护调试环境与运行环境相互隔离，保护在系统区域内的运行过程是不可以窥探、干扰、可审计的；

b) 应防止调试环境和运行环境间的跨域访问，防止不同用户间的任务相互影响或窥探。

7 测试方法

7.1 系统管理

7.1.1 集群管理

测试项目	集群管理
测试目的	系统具备对集群进行添加、编辑、启用、禁用、删除的功能，同时具备对集群计算环境规格、数据网关进行配置并进行连通性测试的功能。
预置条件	系统已部署完成。
测试步骤	1）使用有集群管理权限的账号登录系统操作界面； 2）添加新集群，查看是否成功添加； 3）配置集群基本信息、计算环境规格、数据网关，并测试连通性，查看是否连接成功； 4）编辑已存在集群的信息，查看是否成功编辑； 5）禁用已启用的集群，查看是否成功禁用； 6）启用已禁用的集群，查看是否成功启用； 7）删除已添加成功的集群，查看是否成功删除。
预期结果	1） 步骤 2 完成后，查看到新集群添加成功，集群列表显示新增的信息,包括：集群名称、创建时间、创建用户； 2） 步骤 3 完成后，查看到集群计算环境规格、数据网关已配置，查看到已完成连通性测试； 3） 步骤 4 完成后，查看到集群编辑成功，集群列表显示更新的信息，包括：集群名称、创建时间、创建用户； 4） 步骤 5 完成后，集群状态显示已禁用； 5） 步骤 6 完成后，集群状态显示启用中； 6） 步骤 7 完成后，查看到集群删除成功。
备注	必选

7.1.2 用户管理

测试项目	用户管理
测试目的	系统具备对用户账号的添加、设置、启用、禁用、编辑、删除功能，同时具备对用户及用户

	组的批量导入及导出功能、访问控制策略设置功能。
预置条件	系统已部署完成。
测试步骤	1） 使用有用户管理权限的账户登录系统操作界面； 2） 添加新用户账号，配置用户名称、用户邮箱、用户口令，设置访问控制策略，查看是否成功添加； 3） 使用新添加的用户账号及口令进行登录，查看是否成功登录； 4） 编辑用户，修改用户名称、用户邮箱，查看是否成功编辑； 5） 禁用用户，使用禁用的用户账号和口令登录系统，查看是否成功禁用； 6） 启用用户，使用启用的用户账号和口令登录系统，查看是否成功启用； 7） 删除已添加的用户账号，使用已删除的用户账号和口令登录系统，查看是否成功删除； 8） 批量导入用户，查看是否成功批量导入； 9） 导出所有用户信息，查看文件是否能批量导出； 10） 添加用户组，配置用户组名称、添加用户组成员，设置访问控制策略，查看是否成功添加； 11） 编辑用户组信息，修改用户组名称，查看是否成功编辑； 12） 禁用用户组，查看是否成功禁用； 13） 启用用户组，查看是否成功启用； 14） 删除已添加的用户组账号，查看是否成功删除； 15） 批量导入用户组，查看是否成功批量导入； 16） 导出所有用户组信息，查看文件是否能成功批量导出。
预期结果	1） 步骤 2 完成后，查看到用户添加成功、访问控制策略设置成功； 2） 步骤 3 完成后，查看到账号登录成功； 3） 步骤 4 完成后，查看到用户编辑成功； 4） 步骤 5 完成后，查看到用户已禁用； 5） 步骤 6 完成后，查看到用户已启用； 6） 步骤 7 完成后，查看到用户删除成功； 7） 步骤 8 完成后，查看到用户批量导入成功； 8） 步骤 9 完成后，查看到用户信息文件批量导出成功； 9） 步骤 10 完成后，查看到用户组添加成功、访问控制策略设置成功； 10） 步骤 11 完成后，查看到用户组编辑成功； 11） 步骤 12 完成后，查看到用户组已禁用； 12） 步骤 13 完成后，查看到用户组已启用； 13） 步骤 14 完成后，查看到用户组删除成功； 14） 步骤 15 完成后，查看到用户组批量导入成功； 15） 步骤 16 完成后，查看到用户组信文件批量导出成功。
备注	必选

7.1.3 资源管理

测试项目	资源管理
测试目的	系统具备对创建的调试环境或运行环境进行查看、搜索、删除的功能。
预置条件	1）系统已部署完成； 2）系统已添加集群；

	3）系统已创建调试环境。
测试步骤	1） 使用有资源管理权限的账户登录系统操作界面； 2） 查看调试环境列表，查看是否成功展示所有已存在调试环境信息，包括：环境名称、环境规格、创建时间、创建用户； 3） 根据列表展示字段搜索调试环境，查看是否成功返回搜索结果； 4） 删除已存在的调试环境，查看是否成功删除； 5） 查看运行环境列表，查看是否成功展示所有已存在运行环境信息，包括：环境名称、环境规格、创建时间、创建用户； 6） 根据列表展示字段搜索运行环境，查看是否成功返回搜索结果； 7） 删除已存在的运行环境，查看是否成功删除；
预期结果	1） 步骤 2 完成后，调试环境列表显示所有已存在调试环境信息，包括：环境名称、环境规格、创建时间、创建用户； 2） 步骤 3 完成后，可根据环境名称、环境规格、创建用户字段来搜索调试环境，可根据创建时间对调试环境进行排序后查看； 3） 步骤 4 完成后，查看到调试环境删除成功； 4） 步骤 5 完成后，运行环境列表显示所有已存在运行环境信息，包括：环境名称、环境规格、创建时间、创建用户； 5） 步骤 6 完成后，可根据环境名称、环境规格、创建用户字段来搜索运行环境，可根据创建时间对运行环境进行排序后查看； 6） 步骤 7 完成后，查看到运行环境删除成功。
备注	必选

7.1.4 日志管理

测试项目	日志管理
测试目的	系统具备对运行任务的日志进行查看、搜索、审计的功能。
预置条件	1）系统已部署完成； 2）系统已存在任务运行记录。
测试步骤	1） 使用有日志管理权限的账号登录系统操作界面； 2） 查看日志列表所有已运行任务的日志及其关联的任务信息，查看是否成功展示：日志名称、日志生成时间； 3） 按日志名称搜索日志，查看是否成功返回搜索结果； 4） 根据日志生成时间对日志进行排序，查看是否根据所选顺序进行展示； 5） 将列表展示的日志下载到本地，查看是否成功审计；
预期结果	1） 步骤 2 完成后，日志列表展示所有已运行任务的日志及其关联的任务信息，包括：日志名称、日志生成时间； 2） 步骤 3 完成后，日志列表返回匹配日志名称的日志信息； 3） 步骤 4 完成后，日志列表根据日志生成时间的倒序或顺序，展示日志信息； 4） 步骤 5 完成后，查看到日志下载成功，可对下载日志进行审计。
备注	必选

7.1.5 模型管理

测试项目	模型管理
测试目的	系统具备对创建的所有模型进行查看、搜索、审计的功能。
预置条件	1） 系统已部署完成； 2） 系统已有运行成功的模型。
测试步骤	1） 使用有模型管理权限的账号登录系统操作界面； 2） 查看模型列表是否成功展示所有模型及关联任务的信息，包括：模型大小、创建时间、工程名称； 3） 查看是否可成功展示模型代码详情； 4） 根据模型大小、工程名称搜索模型，查看是否成功返回搜索结果； 5） 根据创建时间对模型进行排序，查看是否根据所选顺序进行展示。
预期结果	1） 步骤 2 完成后，可对系统创建的所有模型审计； 2） 步骤 3 完成后，可查看模型代码的详情； 3） 步骤 4 完成后,模型列表成功返回搜索结果，包括匹配模型大小或名称的模型信息； 4） 步骤 5 完成后，模型列表根据创建时间的倒序或顺序，展示日志信息，系统具备对创建的所有模型进行审计的功能。
备注	必选

7.1.6 审计管理

测试项目	审计管理
测试目的	系统具备对用户操作行为日志的查看、搜索、下载功能。
预置条件	1）系统已部署完成； 2）系统已有用户在系统上进行了操作；
测试步骤	1） 使用有审计管理权限的账号登录系统操作界面； 2） 查看审计列表，查看是否成功展示所有用户的操作行为记录信息，包括：操作时间、操作用户、IP、行为分类、行为详情； 3） 按操作时间对用户操作日志进行排序，查看是否成功返回搜索结果； 4） 按操作用户搜索用户操作日志，查看是否成功返回搜索结果； 5） 按 IP 搜索用户操作日志，查看是否成功返回搜索结果； 6） 按行为分类搜索用户操作日志，查看是否成功返回搜索结果； 7） 将列表展示的日志下载到本地，打开日志文件，查看是否成功下载和查看；
预期结果	1） 步骤 2 完成后，可查看到审计列表显示所有用户的操作行为日志，包括：操作时间、操作用户、IP、行为分类、行为详情； 2） 步骤 3 完成后，成功返回搜索结果，审计列表根据操作时间的倒序或顺序，展示用户操作行为日志； 3） 步骤 4 完成后，成功返回搜索结果，审计列表返回匹配操作用户的操作行为日志； 4） 步骤 5 完成后，成功返回搜索结果，审计列表返回匹配操作用户 IP 的操作行为日志； 5） 步骤 6 完成后，成功返回搜索结果，审计列表返回匹配行为分类的操作行为日志； 6） 步骤 7 完成后，查看到用户操作日志下载成功，打开文件，可查看用户的操作行为日志，日志信息与审计列表展示的日志信息一致。
备注	必选

7.1.7 系统设置

测试项目	系统设置
测试目的	系统具备登录超时配置、用户口令找回配置、消息类型通知方式可配置、系统登录背景及页面 LOGO 可配置的功能。
预置条件	系统已部署完成。
测试步骤	1） 使用有系统设置权限的账号登录系统操作界面； 2） 开启登录超时配置，自定义超时时间，再次登录且无操作放置到满足超时时间，查看是否需重新登录； 3） 开启口令找回服务，在登录页输入账号名，查看是否可成功找回口令或重设口令； 4） 根据消息通知类型配置不同的通知方式，查看通知方式是否生效且符合配置； 5） 上传本地图片作为系统登录页背景，查看是否成功设置； 6） 上传本地图片作为系统 LOGO，查看是否成功设置。
预期结果	1） 步骤 2 完成后，查看到登录超时设置成功，再次登录且无操作放置到满足超时时间，自动退出当前账号，查看到当用户登录超时需重新登录； 2） 步骤 3 完成后，查看到口令找回服务开启成功，在登录页输入账号名，可通过邮箱验证方式完成口令重新设置，查看到设置成功请重新登录； 3） 步骤 4 完成后，查看到消息类型通知方式配置成功； 4） 步骤 5 完成后，查看到图片上传成功，刷新页面后，可查看系统登录页背景更新为已上传图片； 5） 步骤 6 完成后，查看到图片上传成功，刷新页面后，可查看系统 LOGO 更新为已上传图片。
备注	必选

7.2 数据管理

7.2.1 数据源管理

测试项目	数据源管理
测试目的	系统具备对不同类型数据源进行添加、编辑、禁用、删除及数据源连通性检测的功能，同时具备根据数据源名称、主机 IP、端口搜索数据源的功能。
预置条件	系统已部署完成。
测试步骤	1） 使用有数据源管理权限的账号登录系统操作界面； 2） 分别添加 MySQL、Oracle、MariaDB、PostgreSQL、BOS 类型的数据源，并配置数据源信息，测试连通性，查看是否添加成功，并测试成功； 3） 查看数据源列表，查看是否成功展示所有的数据源信息，包括：数据源名称、数据源类型、状态、创建时间、创建用户； 4） 编辑数据源信息，查看是否成功编辑； 5） 根据数据源名称或主机 IP 或端口搜索数据源，查看是否成功返回搜索结果； 6） 禁用已有的数据源，查看是否成功禁用； 7） 启用已有的数据源，查看是否成功启用； 8） 删除已添加的数据源，查看是否成功删除。
预期结果	1） 步骤 2 完成后，查看到 MySQL、Oracle、MariaDB、PostgreSQL、BOS 类型的数据源添加成功，各数据源测试连接成功；

	2） 步骤 3 完成后，查看到数据源列表所有已添加的数据源信息，包括：数据源名称、数据源类型、状态、创建时间、创建用户； 3） 步骤 4 完成后，查看到数据源编辑成功，数据源列表更新已编辑的数据源信息； 4） 步骤 5 完成后，成功返回搜索结果，数据源列表根据搜索的数据源名称或主机 IP 或端口，展示对应的数据源信息； 5） 步骤 6 完成后，查看到数据源禁用成功； 6） 步骤 7 完成后，查看到数据源启用成功； 7） 步骤 8 完成后，查看到数据源删除成功。
备注	必选

7.2.2 脱敏标签管理

测试项目	脱敏标签管理
测试目的	系统应内置常用脱敏标签以实现对姓名、身份证号码、手机号、邮箱的识别和处理，同时具备对脱敏识别规则和处理规则的添加、编辑、删除功能。
预置条件	系统已部署完成。
测试步骤	1） 使用有脱敏标签管理权限的账号登录系统操作界面； 2） 查看系统内置脱敏标签的识别规则和处理规则，查看是否可实现对姓名、身份证号码、手机号、邮箱的识别和处理； 3） 添加脱敏标签，配置脱敏标签信息，包括:标签名称、标签描述、识别规则、处理规则，查看是否成功添加； 4） 查看脱敏标签列表是否成功展示：标签名称、标签描述、识别规则、处理规则； 5） 编辑脱敏标签，查看是否成功编辑； 6） 根据标签名称或标签描述搜索脱敏标签，查看是否成功返回搜索结果； 7） 删除已添加的脱敏标签，查看是否成功删除。
预期结果	1） 步骤 2 完成后，脱敏标签列表展示内置的脱敏标签，识别规则覆盖姓名、身份证号码、手机号、邮箱，处理规则可对识别出的敏感字符进行遮掩； 2） 步骤 3 完成后，查看到脱敏标签添加成功； 3） 步骤 4 完成后，脱敏标签列表显示新增脱敏标签信息，包括:标签名称、标签描述、识别规则、处理规则； 4） 步骤 5 完成后，查看到脱敏标签编辑成功，脱敏标签列表显示编辑后的脱敏标签信息； 5） 步骤 6 完成后，成功返回搜索结果，脱敏标签列表返回符合标签名称或标签描述的脱敏标签； 6） 步骤 7 完成后，查看到脱敏标签删除成功。
备注	必选

7.2.3 数据集添加

测试项目	数据集添加
测试目的	系统具备对 MySQL、Oracle、MariaDB、PostgreSQL、BOS、CSV, TXT，JPG 类型的数据集进行添加、查看、编辑、删除功能。
预置条件	1）系统已部署完成；

	2）系统已完成对 MySQL、Oracle、MariaDB、PostgreSQL、BOS 数据源的接入。
测试步骤	1） 使用有数据集添加权限的账号登录系统操作界面； 2） 添加数据集，并分别从已接入的 MySQL、Oracle、MariaDB、PostgreSQL、BOS 数据源选择数据库表，配置数据集基本信息，包括：数据集名称、数据集说明，查看是否成功添加； 3） 添加数据集，并分别从本地上传 CSV、TXT、JPG 文件，配置数据集基本信息，包括：数据集名称、数据集说明，查看是否成功添加； 4） 查看已添加的数据集信息，查看是否成功展示数据集名称、数据集说明、创建时间、更新时间； 5） 编辑已添加的数据集，查看是否成功编辑； 6） 删除已添加的数据集，查看是否成功删除。
预期结果	1） 步骤 2 完成后，查看到 MySQL、Oracle、MariaDB、PostgreSQL、BOS 数据集添加成功； 2） 步骤 3 完成后，查看到从本地上传的 CSV、TXT、JPG 格式的数据集添加成功； 3） 步骤 4 完成后，可在列表页查看已添加的数据集信息，包括：数据集名称、数据集说明、创建时间； 4） 步骤 5 完成后，查看到数据集编辑成功，列表页更新编辑后的数据集信息； 5） 步骤 6 完成后，查看到数据集删除成功。
备注	必选

7.2.4 数据处理

测试项目	数据处理
测试目的	系统具备对数据集基于自定义或内置的脱敏标签进行脱敏处理的功能，具备包括随机抽样、分层抽样、快速抽样的数据集抽样功能，具备对处理任务进行执行、终止、预览处理任务效果、删除的功能，具备查看样例数据集信息的功能，对文本数据的处理性能应不低于:30GB/h，对图片数据的处理性能应不低于 20GB/h；脱敏处理的准确率应不低于：60%。
预置条件	1）系统已部署完成； 2）系统已成功添加文本数据集和图片数据集； 3）系统已成功添加脱敏标签。
测试步骤	1） 使用有数据处理权限的账号登录系统操作界面； 2） 添加数据处理任务，查看是否成功添加数据处理任务； 3） 配置抽样策略，可选择项包含随机抽样、分层抽样、快速抽样，查看是否成功配置抽样策略； 4） 配置脱敏标签，选择自定义脱敏标签或内置的脱敏标签，查看是否成功配置脱敏标签； 5） 执行数据处理任务，查看是否成功执行； 6） 预览数据处理结果，查看脱敏效果是否符合任务配置的脱敏标签； 7） 查看数据处理任务产生的样例数据集的信息，查看是否成功展示数据集名称、数据集描述、数据集字段类型、样例数据信息； 8） 终止数据处理任务，查看是否成功终止； 9） 构造数据处理任务及 30GB 的文本数据，查看是否可在 1 小时内执行完毕； 10）构造数据处理任务及 20GB 的图片数据，查看是否可在 1 小时内执行完毕； 11）构造 1000 条文本数据，并配置不少于 5 条脱敏标签，构造数据处理任务，查看脱敏效果，记录脱敏准确的数据条数；

	12）删除已添加的数据处理任务，查看是否删除成功。
预期结果	1） 步骤 2 完成后，查看到数据处理任务添加成功； 2） 步骤 3 完成后，查看到抽样策略配置成功； 3） 步骤 4 完成后，查看到脱敏标签配置成功； 4） 步骤 5 完成后，查看到数据处理任务执行成功，抽样成功、脱敏处理成功； 5） 步骤 6 完成后，预览到数据处理任务效果，抽样脱敏效果与数据处理任务配置的抽样策略、脱敏标签一致； 6） 步骤 7 完成后，数据处理任务产生的样例数据集的信息包括：数据集名称、数据集描述、数据集字段类型、样例数据； 7） 步骤 8 完成后，查看到数据处理任务终止成功； 8） 步骤 9 完成后，查看到系统在 1 小时内可完成对所有文本数据的处理，系统对文本数据的处理性能不低于:30GB/h； 9） 步骤 10 完成后，查看到系统在 1 小时内可完成对所有图片数据的处理，系统对图片数据的处理性能不低于 20GB/h； 10）步骤 11 完成后，记录了脱敏准确的数据条数，条数不少于 600 条，脱敏处理的准确率不低于 60%； 11）步骤 12 完成后，查看到数据处理任务删除成功。
备注	必选

7.2.5 数据集管理

测试项目	数据集管理
测试目的	系统具备数据集的查看、授权、发布、下架、编辑、删除功能，可根据数据集 ID、数据集名称进行数据集的搜索，可查看数据集的信息，包括：数据集被申请使用过的次数、被授权的次数、被下载的次数等。
预置条件	1）系统已部署完成； 2）系统已成功添加数据集并执行了数据处理任务。
测试步骤	1） 使用有数据集管理权限的账号登录系统操作界面； 2） 查看数据集列表查看所有通过数据处理任务生成的数据集信息，查看是否成功展示数据集名称、数据集大小、数据来源、数据集标签、数据量、查看次数、授权次数、下载次数等信息； 3） 授权数据集至某用户或用户组，查看是否成功授权； 4） 发布数据集，查看是否成功发布； 5） 下架数据集，查看是否成功下架； 6） 编辑数据集，查看是否成功编辑； 7） 根据数据集 ID 搜索数据集，查看是否成功返回搜索结果； 8） 根据数据集名称搜索数据集，查看是否成功返回搜索结果； 9） 删除数据集，查看是否成功删除。
预期结果	1） 步骤 2 完成后，数据集列表展示所有通过数据处理任务生成的数据集信息，包括：数据集名称、数据集大小、数据来源、数据集标签、数据量、查看次数、授权次数、下载次数； 2） 步骤 3 完成后，查看到数据集授权成功，登录该授权对象的账号，可查看到该数据集信息；

	3） 步骤 4 完成后，查看到数据集发布成功； 4） 步骤 5 完成后，查看到数据集下架成功； 5） 步骤 6 完成后，查看到编辑成功； 6） 步骤 7 完成后，成功返回搜索结果，数据集列表返回匹配数据集 ID 的数据集信息； 7） 步骤 8 完成后，成功返回搜索结果，数据集列表返回匹配数据集名称的数据集信息； 8） 步骤 9 完成后，查看到删除成功。
备注	必选

7.2.6 申请审核管理

测试项目	申请审核
测试目的	系统具备对已上架的数据集进行查看、搜索和申请的功能，具备对在运行环境中执行任务所产生的计算结果进行申请和下载的功能，具备对用户提起的申请进行查看和审批的功能，具备对申请文件、代码、数据集进行审计的功能。
预置条件	1）系统已部署完成； 2）系统已执行全量任务，且任务输出结果包含模型文件和计算结果文件。
测试步骤	1） 使用有申请权限的账号登录系统操作界面； 2） 查看已上架的数据集，根据数据集名称搜索数据集，查看是否返回匹配的数据集； 3） 申请数据集，查看是否成功申请； 4） 查看全量任务的输出，申请下载模型文件和计算结果文件，查看是否成功申请； 5） 使用有审核权限的账号登录系统操作界面； 6） 查看申请审核列表所展示的所有申请信息，查看是否成功展示申请名称、申请类型、申请时间、申请用户、申请明细等信息； 7） 查看申请明细信息是否成功展示申请人、申请时间、申请的数据集或文件的名称； 8） 查看模型代码详情、数据集详情、申请文件的详情，查看是否成功审计； 9） 执行通过申请操作，查看是否成功通过； 10）执行拒绝申请操作，查看是否成功拒绝。
预期结果	1） 步骤 2 完成后，查看到与数据集名称所匹配的数据集； 2） 步骤 3 完成后，查看到已上架的数据集申请提交成功； 3） 步骤 4 完成后，查看到下载模型文件和计算结果文件申请提交成功； 4） 步骤 6 完成后，申请审核列表展示所有申请信息，包括：申请名称、申请类型、申请时间、申请用户、申请明细； 5） 步骤 7 完成后，申请明细详情展示信息包括：申请人、申请时间、申请的数据集或文件的名称； 6） 步骤 8 完成后，查看到成功显示模型代码、数据集、申请文件的审计详情； 7） 步骤 9 完成后，查看到申请已通过； 8） 步骤 10 完成后，查看到申请已拒绝。
备注	必选

7.3 计算

7.3.1 代码调试

测试项目	代码调试
测试目的	系统具备以 Python 为主的多语言编程的调试环境，具备调试环境的添加和删除功能，并具备包括 Web Shell、VSCode、Jupyter Notebook 在内的代码编译工具，具备包括 TensorFlow、Pytorch、Pycharm 在内的机器学习框架，具备调试环境与运行环境分离的技术架构，支持在调试环境中调用样例数据集进行代码的调试。
预置条件	1）系统已部署完成； 2）系统已申请数据集。
测试步骤	1） 使用有代码调试权限的账号登录系统操作界面； 2） 添加调试环境，选择在调试环境中使用的代码编译工具，选项包括：Web Shell、VSCode、Jupyter Notebook，选择在调试环境中使用的机器学习框架，选项包括 TensorFlow、Pytorch、Pycharm，查看是否成功添加； 3） 进入调试环境，使用 Python 语言编写程序并执行，查看是否成功执行； 4） 进入调试环境，使用非 Python 语言编写程序并执行，查看是否成功执行； 5） 进入调试环境，调用已申请的样例数据集，编写程序并执行，查看是否成功调试代码； 6） 进入调试环境后，查看是否存在调试环境与运行环境未分离的情况； 7） 删除已添加的调试环境，查看是否成功删除。
预期结果	1） 步骤 2 完成后，查看到调试环境添加成功，且进入调试环境后，可查看所选择的代码编译工具界面，可查看到机器学习框架的版本； 2） 步骤 3 完成后，查看到使用 Python 语言编写程序执行成功； 3） 步骤 4 完成后，查看到使用非 Python 语言编写程序执行成功； 4） 步骤 5 完成后，查看到调用样例数据集进行的代码调试已完成； 5） 步骤 6 完成后，查看到不能以任何方式从调试环境跳转到运行环境，调试环境与运行环境在技术架构层面做到了分离； 6） 步骤 7 完成后，查看到调试环境删除成功。
备注	必选

7.3.2 全量任务

测试项目	全量任务
测试目的	系统具备运行环境执行全量任务的功能，具备任务的添加、查看、终止、删除功能，并具备任务详情查看的功能，包括：运行任务的状态、运行时长、创建时间、任务开始时间、任务日志、任务输出信息，支持回归模型、二分类模型、多分类模型的训练和预测，支持查看包括 KS、AUC、ACC、MSE 在内的模型评估指标。
预置条件	1） 系统已部署完成； 2） 系统已创建调试环境并完成了回归模型训练代码、预测代码的调试； 3） 系统已创建调试环境并完成了二分类模型训练代码、预测代码的调试； 4） 系统已创建调试环境并完成了多分类模型训练代码、预测代码的调试。
测试步骤	1） 使用有全量任务权限的账号登录系统操作界面； 2） 添加全量任务，查看是否成功添加； 3） 终止全量任务，查看是否成功终止； 4） 重新添加全量任务，查看任务运行详情信息是否成功展示：运行任务的状态、运行时长、创建时间、任务开始时间、任务日志、任务输出信息； 5） 提交回归模型训练及预测的全量任务，查看是否成功输出预测结果；

	6） 提交二分类模型训练及预测的全量任务，查看是否成功输出预测结果； 7） 提交多分类模型训练及预测的全量任务，查看是否成功输出预测结果； 8） 查看回归模型的评估指标，查看是否包含 MSE 值； 9） 查看二分类模型的评估指标，查看是否包含 KS 值和 AUC 值； 10）查看多分类模型的评估指标，查看是否包含 ACC 值； 11）删除全量任务，查看是否成功删除。
预期结果	1） 步骤 2 完成后，查看到全量任务添加成功； 2） 步骤 3 完成后，查看到全量任务终止成功； 3） 步骤 4 完成后，查看到全量任务添加成功，查看任务运行详情信息，包括：运行任务的状态、运行时长、创建时间、任务开始时间、任务日志、任务输出信息； 4） 步骤 5 完成后，可查看回归模型训练预测结果； 5） 步骤 6 完成后，可查看二分类模型训练预测结果； 6） 步骤 7 完成后，可查看多分类模型训练预测结果； 7） 步骤 8 完成后，可查看回归模型的评估指标包含 MSE 值的评估指标； 8） 步骤 9 完成后，可查看二分类模型的评估指标包含 KS 值、AUC 值的评估指标； 9） 步骤 10 完成后，可查看多分类模型的评估指标包含 ACC 值的评估指标； 10）步骤 11 完成后，查看到全量任务删除成功。
备注	必选

7.4 安全

7.4.1 数据隐私安全

测试项目	数据隐私安全
测试目的	系统应具备数据隐私安全保护能力，建模任务中不会将原始数据以明文形式被带出安全域，建模中间输出物不存在越权访问，建模结果仅允许授权方获取，系统采用的设计方案具备抗恶意攻击的能力，用户的信息不会被泄露。
预置条件	1） 系统已部署完成； 2） 系统已添加用户； 3） 系统已申请数据集； 4） 系统已创建调试环境、添加全量任务并完成执行。
测试步骤	1） 使用有代码调试和全量任务权限的账号登录系统操作界面； 2） 进入调试环境，查看是否可调用、下载未申请的数据集； 3） 查看全量任务详情，查看是否可查看其他非本人提交的任务信息，包括：任务日志、评估指标； 4） 查看全量任务输出信息，查看是否可不经申请直接下载模型预测产生的结果文件； 5） 听取技术人员对设计方案的安全性机制的描述。
预期结果	1） 步骤 2 完成后，不可调用未申请的数据集，不可下载未申请的数据集，建模任务中不会将原始数据以明文形式被带出安全域； 2） 步骤 3 完成后，仅可查看自己提交的任务信息，包括：任务日志、评估指标，建模中间输出物不存在越权访问； 3） 步骤 4 完成后，只可查看申请下载并通过审批了的结果文件，建模结果仅允许授权方获取；

	4） 步骤 5 完成后，系统安全设计方案应覆盖对使用系统的人员信息安全保护，且具备抗恶意攻击的能力。
备注	必选

7.4.2 网络通信安全

测试项目	网络通信安全
测试目的	系统计算节点网络交互宜采用安全的通信协议加密，无法通过抓包解析出原始数据。
预置条件	系统已部署完成。
测试步骤	1） 启动建模分析任务； 2） 扫描计算节点的网络端口，查看扫描结果是否有异常； 3） 监听参与数据建模分析任务的计算单元的网络通信，查看监听数据是否有异常； 4） 抓取相关的网络通信包，查看是否能解析出原始数据。
预期结果	1） 步骤 2 完成后，扫描结果显示，安全节点只监听配置的网络端口； 2） 步骤 3 完成后，监听数据显示，计算单元间有加密解密流程； 3） 抓取数据包经过加密，无法被解析出原始数据。
备注	可选

7.4.3 系统稳定性

测试项目	系统稳定性
测试目的	系统可为参与方之间提供稳定的网络传输、安全的计算执行，宜具备在网络抖动、硬件故障等异常情况下进行断点恢复的功能。
预置条件	1） 系统已部署完成； 2） 已添加全量任务并执行成功。
测试步骤	1） 使用有代码调试和全量任务权限的账号登录系统操作界面； 2） 执行全量任务，查看是否成功执行； 3） 模拟网络中断异常情况，查看全量任务是否成功完成； 4） 若全量任务失败，重新启动同一全量任务，查看全量任务是否成功完成； 5） 模拟硬件故障情况，查看全量任务是否成功完成； 6） 若全量任务失败，重新启动同一全量任务，查看全量任务是否成功完成。
预期结果	1） 步骤 2 完成后，查看到全量任务执行成功； 2） 步骤 3 完成后，短时间网络干扰下，能完成全量任务并输出计算结果，长时间网络干扰下，报错任务未完成且不输出错误计算结果； 3） 步骤 4 完成后，去除网络干扰下，全量任务能成功完成且输出计算结果，具备在网络抖动下进行断点恢复的功能。 4） 步骤 5 完成后，报错任务未完成且不输出错误计算结果； 5） 步骤 6 完成后，去除硬件故障干扰下，全量任务能成功完成且输出计算结果，具备在硬件故障下进行断点恢复的功能。
备注	可选

7.4.4 系统安全性

测试项目	系统安全性
测试目的	系统应具备调试环境与运行环境相互隔离的技术架构，保护在系统区域内的运行过程是不可以窥探、干扰、可审计的，且可防止调试环境和运行环境间的跨域访问，防止不同用户间的任务相互影响或窥探。
预置条件	1） 系统已部署完成； 2） 系统已添加全量任务并执行成功。
测试步骤	1） 使用有日志管理权限的账号登录系统操作界面； 2） 查看日志列表中所有已运行任务的日志及其关联的任务信息，查看是否成功展示：日志名称、日志生成时间、日志相关的全量任务； 3） 听取技术人员对于系统调试环境与运行环境隔离技术方案的介绍，判断是否满足不可以窥探、干扰的要求； 4） 听取技术人员对于防止不同用户间任务相互影响、窥探的机制的介绍，判断是否满足不可以相互影响或窥探的要求。
预期结果	1） 步骤 2 完成后，可查看日志列表所有已运行任务的日志及其关联的任务信息，包括：日志名称、日志生成时间、日志相关的全量任务； 2） 步骤 3 完成后，判断系统方案可实现调试环境与运行环境隔离，且在系统区域内的运行过程是不可以窥探、干扰的； 3） 步骤 4 完成后，判断系统方案可防止不同用户间任务相互影响、窥探。
备注	必选

电信终端产业协会团体标准

基于数据沙箱的数据流通产品技术与测评要求

T/TAF 192—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn