TC260-PG-2024XA

网络安全标准实践指南

—学术科技服务平台数据安全要求

（征求意见稿 v1.0-202409）

全国网络安全标准化技术委员会秘书处

2024 年 9 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、国家工业信息安全发展研究中心等单位的技术支持。

摘　要

为规范学术科技服务平台数据处理活动，保障数据安全，促进学术科技数据依法合理有效利用，保护个人、组织合法权益，维护国家安全和社会公共利益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，制定本文件。

目　录

1 范围

本文件规定了学术科技服务平台数据安全保护要求，提出了学术科技服务平台运营者应履行的安全责任和义务。

本文件适用于规范学术科技服务平台运营者数据处理活动，也可为有关主管监管部门组织开展相关检查评估提供参考。

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 35273—2020 信息安全技术 个人信息安全规范

GB/T 43697—2024 数据安全技术 数据分类分级规则

GB/T AAAA—XXXX 数据安全技术 敏感个人信息处理安全要求

GB/T BBBB—YYYY 数据安全技术 数据安全保护要求

GB/T CCCC—ZZZZ 数据安全技术 数据安全风险评估方法

3 术语与定义

3.1

学术科技服务平台　academic and scientific service platform

面向社会公众提供学术科技数据的检索、访问、下载、分析、批量供给等服务的网络平台。

注：本文件的学术科技服务平台，主要是指面向社会公众提供学术科技数据的网络平台，不包括高校、科研院所、国家机关单位、自然人处理学术科技数据的情况。

3.2

学术科技数据　academic and scientific data

学术科技服务平台在提供产品和服务过程中收集、产生的数据等。

注：学术科技数据包括学术文献、研究数据、学者信息、科研机构信息、用户信息、用户行为日志等数据及相关元数据。

3.3

学术科技数据处理　academic and scientific data processing

学术科技数据的收集、存储、使用、加工、传输、提供、公开、删除等。

3.4

学术科技服务平台运营者　operator of academic and scientific service platform

学术科技服务平台的所有者、管理者和服务提供者。

3.5

公开学术科技数据　open academic and scientific data

已授权网络公开传播且无访问限制的学术科技数据。

注 1：已授权是指经作者授权，且通过作者所在单位、学术科技服务平台的学术科技成果公开审查的。

注 2：用户通过正常商业行为，注册学术科技服务平台、购买学术科技数据进行访问属于无访问限制。

3.6

非公开学术科技数据　Non-public academic and scientific data

未授权网络传播或具有访问限制的学术科技数据。

注：学术科技数据仅对部分群体开放或仅在部分单位内部使用，或者用户通过正常商业行为无法访问的，属于具有访问限制。

4　基本要求

学术科技服务平台运营者应建立安全、开放、高效的公开学术科技数据共享机制，促进学术科技交流，并遵守以下基本要求：

a)　应对所处理学术科技数据、个人信息的安全负责，加强数据保护，依法履行数据安全义务；

b)　应按照 GB/T 43697-2024《数据安全技术 数据分类分级规则》、GB/T BBBB—YYYY《数据安全技术 数据安全保护要求》中规定的要求，对掌握的学术科技数据进行分类分级保护，合理区分平台上的公开学术科技数据、非公开学

术科技数据;

c) 个人信息处理应遵守 GB/T 35273—2020《信息安全技术 个人信息安全规范》中规定的要求，敏感个人信息处理应遵守 GB/T AAAA—XXXX《数据安全技术 敏感个人信息处理安全要求》中规定的要求;

d) 针对非公开学术科技数据，应参照重要数据管理要求，实行重点保护。

5 数据处理安全要求

5.1 数据收集

学术科技服务平台运营者应采取合法、正当、必要和诚信的方式收集数据，遵守以下要求:

a) 收集非公开学术科技数据，应该充分告知作者处理目的、方式、范围等;

b) 收集个人信息，应依法取得个人同意，限于实现处理目的的最小范围，不得过度收集个人信息。

5.2 数据存储

学术科技服务平台运营者开展数据存储活动时，遵守以下要求:

a) 应将公开学术科技数据、非公开学术科技数据分开存储，在境内收集和产生的非公开学术科技数据应当存储在境内;

b) 存储非公开学术科技数据的，应采用访问控制、密码技术等措施进行安全保护。

5.3 数据使用与加工

学术科技服务平台运营者开展数据使用加工时，遵守以下要求:

a) 处理非公开学术科技数据，应仅用于收集时与作者约定的处理目的、方式、范围，不得用于其他用途，法律法规另有规定的除外;

b) 处理公开学术科技数据或已公开的个人信息，对相关机构、个人权益有重大影响的，应当取得相关机构、个人同意;

c) 从事网络出版活动应取得版权所有者的授权，涉及学位论文的，应当取得作者、作者导师和所属单位的单独授权。

5.4 数据传输

学术科技服务平台运营者应采用技术措施保护数据传输的完整性和保密性，防止数据篡改和泄露。

5.5 数据提供和公开

学术科技服务平台运营者开展数据提供和公开活动时，遵守以下要求:

a）公开学术科技数据包含作者敏感个人信息的，应进行脱敏处理;

b）公开学术科技数据时，确需公开项目信息的，宜仅公开项目类

型、项目编号；

c）公开学术科技数据时，涉及作者敏感学术称号，承担敏感科研项目信息等数据的，应按照国家有关规定或者有关部门的要求及时进行删除；

注：学术称号是在人才评审或项目实施过程中给予作出突出贡献人才的标识。

d）向第三方提供或者公开发布学术科技数据关联分析结果，涉及使用算法、模型等提供信息服务的应按照国家有关规定进行备案；

e）因业务等需要，确需向中华人民共和国境外提供在境内收集和产生的非公开学术科技数据的，应通过数据出境安全评估；

f）涉及个人信息出境的，应遵守国家有关规定要求，出境个人信息中不应涉及敏感单位的名称、地址、所承担项目等信息；

g）不应绕过学术科技服务平台通过线下方式向境外提供学术科技数据和平台上的个人信息。

5.6 数据删除

学术科技服务平台运营者开展数据删除活动时，遵守以下要求：

a) 应建立针对数据业务下线、账号注销、超出数据保存期限等情况下的数据删除管理制度，明确审批机制；

b) 建立数据删除安全策略和操作规程，明确删除对象、删除原因、删除流程、删除技术处置策略等；

c) 存储非公开学术科技数据和个人信息的介质进行报废处理时，可采用物理损毁等方式销毁介质，以确保数据和个人信息不能被恢复。

6 安全管理要求

6.1 组织管理

学术科技服务平台运营者遵循以下要求：

a) 注册用户超过1000万人或者处理重要数据的学术科技服务平台运营者应明确数据安全负责人和数据安全管理机构，数据安全负责人应当具备数据安全专业知识和相关管理工作经历，数据安全管理机构在人员、技术水平方面应具备数据安全风险防范能力；

b) 制定实施数据安全内部管理制度、操作规程和数据安全事件应急预案；

c) 定期组织开展数据安全风险监测、风险评估、应急演练、安全宣传教育培训等活动，及时处置数据安全风险和事件；

d) 制定实施数据安全相关投诉举报、处理制度，并接受、处理数据安全相关投诉与举报。

6.2 用户管理

学术科技服务平台运营者遵循以下要求：

a) 应建立个人、组织用户管理制度，对用户进行分类管理；

b) 应与用户签订协议，内容包括但不限于:

1) 要求用户不得擅自向第三方提供通过平台获取的学术科技数据;

2) 要求用户处理学术科技数据应当符合社会公德和伦理，遵守商业道德和职业道德，有利于促进经济社会、科学技术发展，增进人民福祉，不得危害国家安全、科技安全、公共利益。

6.3 内容管理

学术科技服务平台运营者遵循以下要求:

a) 建立信息发布传播管理规则和内容安全处置技术措施;

b) 针对平台上的信息推送、编辑、排序、选择、组织、制作等活动进行安全管理;

c) 及时发现、阻断法律、行政法规禁止发布或者传输的信息，并按照规定向有关主管部门报告。

6.4 应急响应

学术科技服务平台运营者遵循以下要求:

a) 发生数据安全事件时，应立即采取处置措施，按照规定及时告知用户并向有关主管部门报告;

b) 对发生的可能损害个人、组织合法权益的数据安全事件，应立即采取补救措施，并及时通知利害关系人。

6.5 安全审计

学术科技服务平台运营者遵循以下要求:

a) 明确数据安全审计责任部门，配备安全审计员，开展日常安全审计工作;

b) 结合数据处理场景明确审计策略，定期开展安全审计，对审计发现问题进行整改跟踪;

c) 对数据批量复制、下载、导出、修改、删除等操作行为进行审计;

d) 对网络运维管理活动、用户行为、网络异常行为、网络安全事件等进行审计，对数据收集、存储、使用、加工、传输、提供、公开、删除等全流程数据处理活动的数据处理、权限管理、人员操作等行为记录日志，日志留存期限不低于六个月。

6.6 安全评估

学术科技服务平台运营者遵循以下要求:

a) 明确数据安全评估工作的职能部门、职责及相关人员;

b) 制定数据安全评估制度，并明确评估的原则、方法、内容和结果，以及风险处置情况;

c) 注册用户超过1000万人或者处理重要数据的学术科技服务平台运营者,应按照GB/T CCCC—ZZZZ《数据安全技术 数据安全风险评估方法》中规定的要求，每年度对学术科技

数据、个人信息的处理活动开展风险评估，并形成年度风险评估报告。风险评估报告应当包括以下内容:

1) 运营者组织架构、实际控制人、受益人以及运营管理团队和核心成员等信息;
2) 运营者基本信息、数据安全管理机构信息、数据安全负责人姓名和联系方式等;
3) 处理学术科技数据、个人信息的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身;
4) 数据安全管理制度及实施情况，数据备份、加密、访问控制等安全防护措施及有效性;
5) 发现的数据安全风险，发生数据安全事件及处置情况;
6) 提供、委托处理、共同处理重要数据的风险评估情况;
7) 学术科技数据、个人信息出境情况，包括数据接收方名称、联系方式、出境数据的类型、数量及目的，出境数据的存储地点、存储期限、使用范围和方式等，或者被境外访问、下载情况等;
8) 法律法规规定的其他报告内容。

参 考 文 献

[1] 《中华人民共和国数据安全法》

[2] 《中华人民共和国个人信息保护法》

[3] 《中华人民共和国著作权法》

[4] 《网络数据安全管理条例（草案）》

[5] 《网络出版服务管理规定》

[6] 《科学数据管理办法》