ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

NY

中 华 人 民 共 和 国 农 业 行 业 标 准

NY/T XXXXX—XXXX

农业农村大数据平台 数据安全管理指南

Data security management guide of agricultural and rural big data platform

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

2024-10-8

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国农业农村部　　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。

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。

本文件由农业农村部市场与信息化司提出。

本文件由农业农村部数据标准化技术委员会归口。

本文件起草单位：农业农村部大数据发展中心，航天信息股份有限公司，绿盟科技集团股份有限公司，安恒信息技术股份有限公司。

本文件主要起草人：XX，XX……

农业农村大数据平台 数据安全管理指南

1 范围

本文件提出了农业农村大数据平台数据安全管理要求、数据安全技术防护要求和数据安全运行管理要求。

本文件适用于农业农村大数据平台建设和使用过程数据安全管理参考使用。

本文件不适用于涉及国家秘密的数据，涉及国家秘密的数据按照有关规定管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。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 37973-2019 《信息安全技术 大数据安全管理指南》

NY/T 4261-2022 《农业大数据安全管理指南》

GB/T 43697-2024 《数据安全技术 数据分类分级规则》

3 术语和定义

GB/T 5271.1-2000 《信息技术 词汇 第1部分：基本术语》、GB/T 35295-2017 《信息技术 大数据 术语》界定的以及下列术语和定义适用于本文件。

3.1

农业农村数据 agricultural and rural data

在涉农生产、经营、管理、服务过程中，制作或获取并以电子形式记录、保存的农业农村资源、主体、产品相关信息，也包括原始数据经统计、关联、挖掘或聚合等加工活动产生的衍生数据。

3.2

农业农村大数据平台 agricultural and rural big data platform

农业农村领域实现各类数据的采集、管理、分析和服务的大数据系统。

3.3

核心数据 core data

农业农村领域中，关系国家安全、国民经济命脉、重要民生、重大公共利益等的数据。

3.4

重要数据 important data

农业农村领域中，一旦遭受篡改、破坏、泄露，或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

注：一般不包括企业信息和个人信息，但该信息达到一定规模或精度后形成的衍生数据，如其遭到篡改、破坏、泄露，或者非法获取、非法利用，可能危害国家安全、公共利益，也应满足重要数据保护要求。

3.5

一般数据 common data

农业农村领域中，除核心数据、重要数据以外的数据。

3.6

敏感数据 sensitive data

农业农村领域中，泄露后可能会给社会或个人带来严重危害的数据。包括个人隐私数据和企业或社会机构不适合公布的数据等。

3.7

数据脱敏 data desensitization

通过模糊化等方法对原始数据进行处理以屏蔽敏感信息的数据保护方法。

3.8

数据治理 data governance

对数据资产管理行使权力和控制的活动集合，包括制定数据标准、提升数据质量、清理脏数据、去重等。

4 数据安全管理要求

4.1 策略与规程

a）应明确数据管理的范围和内容；
b）应建立完善的数据安全管理制度体系和流程；
c）应根据分类分级结果，针对不同安全等级的数据采取不同的安全保护措施；
d）对大数据平台的使用人员应进行身份鉴别和访问控制。

4.2 组织与角色

a）大数据平台责任主体为农业农村大数据平台建设部门或单位；
b）大数据平台使用角色分为政务、公众和运维三类人员。

5 数据安全技术防护

5.1 数据采集

5.1.1 数据源

a）应制定数据采集操作规程，明确数据采集的数据源、目的，规范数据采集渠道及其采集数据格式、采集流程和采集方式，并定期评估数据采集规程的合规性；

b）应采取技术和管理措施，使数据采集相关工具在获得授权后才能采集数据；宜具备对采集数据的异常行为进行检测告警能力；

c）应采用密码技术保证采集数据的真实性和完整性；
d）应采用必要的技术防范措施避免数据源的泄露；
e）应跟踪和记录数据采集操作过程，具备针对过程的追溯能力。

5.1.2 采集安全

f）应对采集终端进行安全认证，保证采集数据的真实性和可靠性；

g）应使用安全通信协议保证采集数据的机密性和完整性；

h）数据更新过程应保持数据一致性。

5.2 数据治理

5.2.1 分类分级

a）平台数据按照GB/T 43697-2024的要求进行分类；

b）平台数据按照安全级别分为核心数据、重要数据和一般数据。

5.2.2 数据清洗

c）应制定数据变换、转换、去重、纠错等数据清洗操作规范，明确数据清洗操作的要求、规范和方法，使数据清洗操作前后数据间的映射关系不变；

d）应采取技术手段和管理措施对所获取或清洗操作生成的数据进行保护，包括但不限于衍生数据以及操作日志等；

e）应记录数据清洗操作行为，在数据清洗完成后对产生的中间或临时数据进行安全删除。

5.2.3 数据标识

f）应依据数据分类分级要求建立数据识别和标记的操作规程；

g）应采用技术措施对收集的数据进行识别，并依据数据分类分级策略对收集数据的安全属性进行标记；

h）应定期对数据识别和标记的效果，影响范围等数据安全风险进行评估，宜通过工具对数据的标识、审核及标记结果使用过程进行管理，实现数据识别和标记变更的可追溯。

5.3 数据管理

5.3.1 数据资源目录

a）应对不同安全级别的数据进行授权管理；

b）应采用较强强度的密码技术保护核心数据和重要数据。

5.3.2 数据脱敏

c）应根据合规性要求和业务需要定义和识别敏感数据；

d）应根据数据使用场景需要，对敏感数据采用静态或动态方式进行脱敏处理；

e）应对脱敏过程进行监控审计，对敏感数据源、敏感数据类型、脱敏任务进行统计。

5.4 计算分析

a）应对接入大数据平台的第三方组件进行安全性评估；

b）应对模型训练数据进行单独管理、安全存储，应对训练得到的模型和模型参数等进行加密存储。

5.5 数据共享交换

a）应明确数据共享交换的内容和范围；

b）应明确数据共享的审核审批流程，为不同安全等级的数据制定不同的审批流程；

c）可使用隐私计算技术进行核心重要数据的共享交换；

d）可使用区块链技术进行数据确权、数据追溯和安全审计。

5.6 一张图

a）使用的敏感数据应进行脱敏处理；

b）可视化展示需使用数字水印技术，并可采用打印控制、剪切板控制、拷屏/截屏控制以及内存窃取控制等多种防泄密保护措施。

5.7 技术支撑

a）支持对用户的统一身份认证和权限管理；

b）数据资源和数据集的管理，应对用户进行身份鉴别和授权管理。

5.8 服务门户

a）应对使用的敏感数据进行脱敏处理。

5.9 数据存储

5.9.1 数据加密

a）应采用符合国家标准的加密算法来保护数据的机密性。应基于数据分类分级的结果，明确不同数据的加密要求，针对不同类型、不同级别的数据选择满足的数据加密算法，实现对在数据库、文件系统和存储介质上的数据加密存储；

b）应确保密钥的生成、存储、传输、秘钥更新和销毁过程安全可靠，并定期更换密钥；

c）应采用符合国家标准的较高强度的密码技术对核心数据和重要数据进行保护，采取必要的技术或者管控措施进行安全防控和访问控制措施，如采用数据库防火墙、数据脱敏、数据防泄漏、数据水印等技术。

d）宜采用符合国家相关标准规定的密码技术对一般数据进行保护，并根据业务需求采用必要的技术或者管控措施进行安全防控和访问控制措施，如采用数据库防火墙、数据脱敏、数据防泄漏、数据水印等多种组合技术能力。

e）对数据加密过程进行监控和审计，根据审计结果及时调整和优化加密策略，确保加密措施的有效性和合规性。

5.9.2 数据防泄漏

f）采用身份认证和权限控制管理，确保只有经过授权的人员才能访问数据。对于核心数据和重要数据，可实施多因素认证等增强措施；

g）根据数据分类分级结果，实施精细化访问控制管理。针对存储核心数据和重要数据的数据库自动发现、实时监控，发现异常访问行为并即时阻断；

h）在数据开放和共享过程中，对涉及核心数据和重要数据进行匿名化处理，降低数据再识别风险；

i）对存储在数据库、文件系统和存储介质上的数据，应采用基于深度内容识别技术，防止数据在存储过程中被未经授权地访问、泄露或篡改等；

j）建立有效的数据的访问和操作的监控和审计机制，实时检测异常行为和潜在的数据泄漏风险，及时发现和应对潜在的数据泄漏风险；

k）建立数据泄漏应急响应预案，及时、有效处置数据泄漏事件。

5.9.3 数据存储安全

l）应保障数据存储环境的物理和网络安全，采取必要的措施防止设备被毁坏或数据被非法访问；

m）建立用户权限控制机制，采取必要的技术或者管控措施进行安全防护；

n）建立数据存储安全审计能力，审计业务办理和数据查询等操作行为，为数据审计和追溯提供依据；

o）建立存储数据异常告警机制，及时了解数据的异常情况。

5.10 数据备份

5.10.1 备份策略

a）应根据数据的重要性、敏感性和业务关键性，确定备份策略。备份策略包括对象、时间、方式、介质、模式、优先级等。

5.10.2 备份方式

b）应根据数据特点和业务需要，采用全量备份、增量备份或差量备份方式。

5.10.3 备份频率

c）应根据数据的更新频率和业务需要，确定备份频率；

d）对于高频更新的数据，应设定较高的备份频率。

5.10.4 备份介质和位置

e）应选择合规、安全、可靠、可扩展的存储介质进行数据备份；

f）应存储在独立的物理位置或远程服务器上，具备容灾能力。

5.10.5 备份执行

g）应按照备份策略执行备份；

h）应记录备份过程的详细日志。

5.10.6 备份验证

i）应定期对备份数据进行验证，确保其完整性和可用性；

j）验证过程应包括数据可读性、可恢复性和备份过程中是否存在错误的检查。

5.10.7 恢复计划

k）应制定详细的备份恢复计划，包括恢复步骤、所需时间、恢复后的验证等；

l）恢复计划应覆盖不同级别数据灾难的应对场景。

5.10.8 恢复执行

m）应按照恢复计划执行恢复操作；

n）应记录恢复过程的详细日志。

5.10.9 恢复演练

o）应定期组织恢复演练，验证恢复计划的可行性和有效性；

p）应注意数据的保护和恢复操作的合规性。

6 数据安全运行管理

6.1 风险管理

6.1.1 风险预案

a）应明确风险管理的对象和范围，明确风险管理人员的角色和责任，明确风险管理对象的安全要求；

b）风险预案应符合国家应急响应有关政策要求，内容应包含总则、角色及职责、预防和预警机制、响应分级、处置流程、保障措施等。

6.1.2 风险评估

c）应制定风险评估计划，选择风险评估方法和工具，制定风险评估实施方案。风险评估计划和实施方案应得到风险管理人员的批准；

d）应对确立的风险管理对象所面临的风险进行识别，列出风险清单和脆弱性清单。风险识别方式可包括文档审查、人员访谈、使用评估工具等；

e）应对识别出的风险分析其发生的可能性，以及造成的损失和危害性。

6.1.3 风险处置

f）依据风险评估的结果，采取适当的安全措施更改风险，降低风险发生的几率，以及造成的损失和危害；

g）风险处置的方式包括风险规避、风险转移、风险消除和风险接受；

h）风险处置后应由风险管理人员对处置效果进行评价，对残余风险编制持续改进方案。

6.2 监测预警

6.2.1 数据监测

a）可采用主被动、手动添加、外部同步等方式对数据资产进行监测识别，包括API、数据库、文件数据等资产信息；

b）对流转中的数据进行监控，发现并测绘出核心数据、重要数据、一般数据的流转链路视图；

c）应采用技术手段监测数据安全威胁，包括攻击和异常行为识别、数据泄露监测等；

d）应采用技术手段，对监测数据进行深度分析和挖掘，发现潜在的安全威胁和异常行为，形成数据安全策略。

6.2.2 预警通报

e）建立有效预警机制，当监测到异常行为或潜在风险时，能够迅速触发预警；

f）根据风险的严重程度和紧急程度，设定不同的预警级别，对风险及时响应和处理；

g）预警信息应准确、快速地传达给相关责任人和部门，及时采取应对措施；

h）建立预警反馈机制，对预警信息的处理情况进行跟踪和评估，完善预警机制。

6.3 应急处理

6.3.1 应急预案

a）应根据数据安全事件的类型和级别，制定针对性的数据安全事件应急预案，明确应急策略、响应流程、处置措施和相关责任人；

b）应按照应急预案，定期组织开展数据安全事件应急演练活动。

6.3.2 应急处置

c）发生数据安全事件时，应立即启动数据安全事件应急预案，组织专业团队进行快速响应和处置；

d）应急处置过程中，应确保核心数据和重要数据的安全，防止数据泄露或损坏。

6.3.3 溯源分析

e）应对数据安全事件进行溯源分析，查明事件原因；

f）分析过程中，应收集并分析相关日志、监控记录等数据，找出安全漏洞和隐患。

6.3.4 事件报告

g）发生数据安全事件后，应及时、准确向上级主管部门进行报告，包括事件发生原因、处置过程、处置结果和改进措施。

6.4 数据安全审计

a）应建立数据全生命周期操作行为的日志，对异常行为进行识别、分析并及时督促整改，日志保存期限一般不少于6个月；

b）应实现对数据库的访问行为建立基线，对超出基线的操作可自动识别，对数据库风险操作行为进行审计和告警。