ICS 35.040
CCS L 80

NY

中华人民共和国农业行业标准

NY/T 4261—2022

农业大数据安全管理指南

Agricultural big data security management guide

2022-11-11 发布　　2023-03-01 实施

中华人民共和国农业农村部 发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　农业大数据安全管理原则 …… 2
4.1　合规性原则 …… 2
4.2　重要数据保护优先原则 …… 2
4.3　安全可靠原则 …… 2
4.4　可审计可追溯原则 …… 2
4.5　任务明确原则 …… 2
4.6　授权管理原则 …… 2
5　农业大数据安全管理角色与任务 …… 2
5.1　农业大数据安全管理者 …… 2
5.2　农业大数据安全执行者 …… 3
5.3　农业大数据安全监督者 …… 3
6　农业大数据通用安全管理 …… 3
6.1　概述 …… 3
6.2　策略与规程 …… 3
6.3　组织和人员管理 …… 4
6.4　用户角色管理 …… 4
6.5　用户授权 …… 4
6.6　鉴别与访问控制 …… 4
6.7　密钥管理 …… 5
6.8　日志审计 …… 5
6.9　数据溯源 …… 5
6.10　数据供应链安全管理 …… 5
6.11　数据安全事件应急 …… 5
7　农业大数据安全分类分级 …… 5
7.1　概述 …… 5
7.2　数据安全分类 …… 6
7.3　数据安全分级 …… 6
7.4　数据分类分级流程 …… 7
7.5　分类分级变更 …… 7
8　农业大数据活动安全的管控措施 …… 7
8.1　数据采集安全 …… 7
8.2　数据传输安全 …… 8
8.3　数据存储安全 …… 8
8.4　数据处理安全 …… 8
8.5　数据交换安全 …… 9

8.6 数据销毁安全 …… 9
附录 A(规范性) 农业大数据安全分级判断准则表 …… 10
附录 B(规范性) 农业大数据安全分类分级流程图 …… 12

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农业信息化标准化技术委员会归口。

本文件起草单位：北京邮电大学、中国电子技术标准化研究院。

本文件主要起草人：苏放、杨舒、姚宇星、李海东、刘朝苹、胡影。

引　言

农业大数据工作是大数据理念、技术和方法在农业领域的应用与实践。我国农业大数据经过多年建设，已积累了可观的农业数据资源，涉及自然资源、生产、管理、经营和服务等方面。然而数据的集中化和新技术的出现，使农业大数据建设面临新的安全风险和挑战，农业组织需要进一步加强针对农业大数据的安全指导。

为支撑农业组织建立农业大数据安全管理机制，促进农业大数据有效保护并实现安全风险可控，需要实现农业大数据安全管理指引。本文件用于指导农业组织做好农业大数据的安全管理工作，推动其在依据相关法律法规和标准规范、满足农业大数据相关方数据保护要求的前提下，制定有效的安全管理原则、策略和规程，保障农业大数据安全、合理地使用。

农业大数据安全管理指南

1 范围

本文件提出了农业大数据安全管理原则、农业大数据安全管理角色与任务、农业大数据通用安全管理、农业大数据安全分类分级和农业大数据活动安全的管控措施。

本文件适用于农业组织进行农业大数据安全管理，也可供第三方评估机构在进行农业大数据安全评估时参考使用。

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 17901.1 信息技术 安全技术 密钥管理 第1部分：框架

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 25062 信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范

GB/T 25069 信息安全技术 术语

GB/T 31508 信息安全技术 公钥基础设施 数字证书策略分类分级规范

GB/T 37973 信息安全技术 大数据安全管理指南

3 术语和定义

GB/T 25069、GB/T 31508 和 GB/T 37973 界定的以及下列术语和定义适用于本文件。

3.1

农业组织 agricultural organization

由作用不同的个体为实施共同的农业目标而建立的社会结构或团体。

注：农业组织包括各级政府农业农村主管部门及其事业单位，以及学会协会、涉农企业、社会团体和农业生产经营组织等。

3.2

农业大数据 agricultural big data

融合农业地域性、季节性、多样性、周期性等自身特征后产生的数据集合，具有来源广泛、类型多样、结构复杂、数量巨大、存在潜在价值的特点。

3.3

农业大数据活动 big data activity

农业组织（3.1）针对农业大数据（3.2）开展的一组特定任务的集合。

[来源：GB/T 37973，3.5，有修改]

注：主要包括数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等。

3.4

证书信任链 certificate chain

起始于根证书，终止于终端用户数字证书，由一系列数字证书组成，用于用户证书验证的可信任的有序证书序列。

[来源：GB/T 31508，3.16，有修改]

3.5

安全管理角色 security management role

在农业组织(3.1)中,承担数据信息安全管理、执行、监督等任务的部门或岗位的统称。

3.6

初始值　initial value

在农业大数据安全分类分级中,设定的数据分级固定值。

3.7

核心数据　core data

农业领域中,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。

3.8

重要数据　important data

农业领域中,一旦遭到篡改、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。

3.9

一般数据　common data

农业领域中,除核心数据、重要数据以外的数据。

3.10

用户　user

对农业大数据(3.2)的数据资源进行访问、操作的主体。

3.11

用户权限　user privilege

用户(3.10)可访问、操作农业大数据(3.2)的范围和程度。

3.12

用户角色　user role

用户(3.10)在农业大数据活动(3.3)中的一个工作职能。

注:被授予角色的用户具有相应的用户权限和责任。

4　农业大数据安全管理原则

4.1　合规性原则

符合我国法律法规和标准规范中对数据的保护规定,并持续跟进有关法律法规和标准规范。

4.2　重要数据保护优先原则

对涉及国家安全的农业大数据进行重点防护。

4.3　安全可靠原则

重视安全措施的有效性、数据来源的可靠性,重视数据的保密性、完整性、可用性和时效性。

4.4　可审计可追溯原则

可对农业大数据活动中各操作信息进行审计,并可追溯到相关的组织及人员。

4.5　任务明确原则

明确农业大数据安全管理角色和农业大数据全生存周期中与数据安全相关的其他角色的任务。

4.6　授权管理原则

若未获得授权,不得采集、发布有明确规定的敏感信息。在满足农业活动需求的基础上,授予最小操作权限,采集和处理具有最少数据类型和最小数据量的数据。

5　农业大数据安全管理角色与任务

5.1　农业大数据安全管理者

农业大数据安全管理者是对农业组织大数据安全负责的个人、部门或农业组织。主要负责数据安全相关领域和环节的数据安全建设规划、数据安全制度制定、数据安全保障决策，组织落实业务部门数据安全相关的工作。具体任务包括但不限于：

a) 划分农业大数据安全管理角色，并明确每个角色的相关任务；
b) 按照相关法律法规政策要求，制定农业大数据安全基本要求，根据部分数据的特殊性，给出针对性的安全要求，并根据相关法律法规政策做出必要的调整；
c) 确定数据安全分类分级的指导性初始值，制定数据分类分级的安全指南；
d) 明确数据访问控制策略，包括访问控制审批流程、角色划分、操作审计等；
e) 制定本组织对外提供数据的安全管理要求；
f) 建立农业大数据安全事件应急机制。

5.2 农业大数据安全执行者

农业大数据安全执行者是执行农业组织中数据安全相关工作的个人、部门或农业组织。主要负责数据安全相关领域和环节工作的执行，执行数据安全相关细则，落实各项安全措施，具体开展各项工作。具体任务包括但不限于：

a) 根据农业大数据安全管理者制定的相关规划和要求开展具体实施工作；
b) 结合农业大数据的实际应用情况，对数据安全分类分级指南进行细化和拓展，制定明确的数据分类分级清单；
c) 根据访问控制策略，负责授予权限的工作，为具体人员分配访问和操作权限；
d) 配合农业大数据安全管理者处置安全事件。

5.3 农业大数据安全监督者

农业大数据安全监督者是负责农业大数据安全监督管理工作的个人、部门或农业组织。主要负责农业大数据操作人员行为的检查、安全审计、安全风险评估等。具体任务包括但不限于：

a) 配合国家或行业部门进行数据安全审计检查；
b) 定期进行数据操作行为的安全检查，包括日志、操作流程等；
c) 定期在农业组织开展数据安全审计工作，形成审计报告；
d) 定期对农业大数据开展风险评估，并向有关主管部门报送风险评估报告。

6 农业大数据通用安全管理

6.1 概述

农业大数据通用安全管理以策略与规程、组织和人员管理、角色管理为基础，并结合用户授权、鉴别与访问控制、密钥管理、日志审计、数据溯源、数据供应链安全管理、数据安全事件应急，支撑农业大数据业务的开展。同时，可采用证书信任链建立农业组织之间安全的信任关系，满足跨部门、跨层级、跨区域的农业数据资源应用。在权限认证时，证书信任链可确定认证路径；在用户授权和密钥管理时，用户数字证书可提供权限信息和密钥信息；在日志审计时，证书信任链可鉴别数据活动者的合法性；在数据溯源时，证书信任链可提供追溯路径。

6.2 策略与规程

农业大数据安全策略与规程要考虑覆盖数据全生存周期的安全风险，内容包括但不限于：

a) 自上而下梳理农业大数据的安全需求，制定符合农业大数据安全管理的安全策略，明确安全方针、安全目标和安全原则；
b) 按照 GB/T 25056 的规定建设数字证书认证系统，制定数字证书认证服务、密钥管理服务、密码服务、数据服务等安全管理规范；
c) 制定数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等数据活动安全管理细则、合同要求及审核机制；
d) 根据农业组织及其所在领域的实际情况，制定基于角色划分的防护指南，试点先行，分步推进；

e) 对农业大数据安全管理策略和规程进行体系化的评估，制订提升农业大数据整体安全管理能力的计划。

6.2 组织和人员管理

6.3.1 组织管理

在农业大数据安全管理者的指导下，组织管理的内容包括但不限于：

a) 建立从决策层到基层的农业大数据安全管理组织架构；

b) 建立农业大数据安全管理组织机构，明确农业大数据安全岗位及其任务；

c) 建立农业大数据安全管理的分级管理制度，落实农业大数据的安全责任；

d) 建立监督管理职能部门，对农业大数据和用户操作行为进行安全监督管理。

6.3.2 人员管理

在组织中，人力资源管理是数据安全工作的重要环节，其中人员管理的内容包括但不限于：

a) 制定农业大数据人力资源安全策略，明确不同岗位人员在数据全生存周期各阶段的安全管控措施；

b) 制定农业大数据安全岗位人员招聘、录用、上岗、调岗、离岗、培训、考核、选拔等人员安全管理制度；

c) 建立岗位人员安全责任奖惩管理制度，对违反农业大数据安全操作规定而造成损失的人员给予相应惩戒处理，并记录相关违规信息；

d) 定期组织开展岗位人员教育培训，加强岗位人员的数据安全保护意识，提高安全管理的业务水平；

e) 涉密人员离岗离职依法依规实行脱密期管理。

6.4 用户角色管理

农业大数据安全管理者和执行者对于用户角色管理的内容包括但不限于：

a) 明确用户角色和用户权限的关系，建立用户角色划分及用户授权规范；

b) 根据现有的农业大数据系统架构建立分层分级的用户角色体系、统筹可拓展的农业大数据用户角色管理机制。

6.5 用户授权

农业大数据安全执行者对于用户授权的措施，包括但不限于：

a) 建立权限管理系统，支持应用接入，管理用户权限，通过数字证书的发放授予用户权限；

b) 用户数字证书需要上一级证书进行数字签名，构建证书信任链，保障数据合法访问和责任追溯；

c) 在农业大数据安全管理安全策略的集中统筹下，农业组织根据数据安全应用需求，可自主进行角色权限划分和授权，制定分级保护规范；

d) 用户权限粒度遵循授权管理原则，用户获取的权限是满足所需的最小权限；

e) 根据数据应用规则和用户安全评估，分配用户角色，签发数字证书，赋予用户对应的权限；

f) 同一个数字证书不宜签发给不同的用户，同一个用户可以拥有多个不同的数字证书；

g) 支持分散式、集中式及两者相互结合的多种授权管理机制；

h) 及时终止或变更离岗和转岗用户的数字证书，保证用户数字证书的合法性与安全性。

6.6 鉴别与访问控制

a) 农业大数据安全执行者对于鉴别与访问控制的措施，包括但不限于：

b) 参考 GB/T 25062 中基于角色的访问控制模型，建立用户身份鉴别管理系统，支持应用接入，实现对用户访问数据资源的身份鉴别与访问控制；

c) 采用用户数字证书中所包含角色对应的权限，对用户身份进行鉴别，实现身份鉴别与访问控制的联动控制，并保存用户访问操作记录；

d) 定期审核用户数字证书，及时删除或停用多余的、过期的用户数字证书；

e) 对超出权限限制的访问操作，设置告警机制。

6.7 密钥管理

密钥管理涵盖从密钥的产生到销毁的各个方面，主要包括密钥管理体制、密钥管理协议和密钥的产生、分配、更换和注入等方面。农业大数据安全执行者对于密钥管理的措施，包括但不限于：

a) 按照 GB/T 17901.1 的要求使用和管理有关密码技术和设施，并按要求生成、存取、更新、备份和销毁密钥；

b) 具备密钥集成管理的能力，并满足密钥管理互操作性等有关标准规范；

c) 具备密文数据透明处理能力。

6.8 日志审计

农业大数据涉及日志包括用户操作日志、运维操作日志、系统软件日志等。农业大数据安全监督者宜对日志开展数据安全专项审计。日志审计包括但不限于：

a) 审计日志包括事件类型、事件时间、事件主体、事件客体、事件成功/失败、事件详细信息等字段；

b) 确保审计日志不被未授权的访问、复制、修改和删除；

c) 审计日志需要定期进行备份，保证审计日志不丢失；

d) 提供对审计日志的导出和清空功能；

e) 日志留存不少于 6 个月。

6.9 数据溯源

农业大数据安全监督者需要配合农业大数据安全管理者和执行者的工作，对数据进行追溯，措施包括但不限于：

a) 针对采集、传输、存储、处理、交换和销毁等数据活动，分别对用户行为、证书信任链、角色管理策略等进行记录，制定分级的安全事件记录体系；

b) 记录并存储农业大数据活动中出现的安全事项，及时上报相关管理部门，并通过溯源技术，基于证书信任链，追踪到数据源头、应用源头及相关责任人。

6.10 数据供应链安全管理

农业大数据安全管理者建立数据供应链安全管理机制，防范数据上下游供应过程中存在的安全风险。管理措施包括但不限于：

a) 制定数据供应链安全管理规范，定义数据供应链的安全目标、原则、范围和内容，明确数据供应链的责任部门和人员，明确数据供应链上下游的责任和义务及组织部门的审核流程；

b) 设立负责数据供应链安全管理岗位和人员，由专职人员制订数据供应链安全管理要求和解决方案；

c) 通过业务培训，提高数据供应过程中工作人员的安全防范意识和能力，推进数据供应链安全管理解决方案的落实。

6.11 数据安全事件应急

农业大数据安全管理者建立数据安全事件应急机制，对各类数据安全事件进行及时响应和处置。需考虑的应急机制包括但不限于：

a) 制定数据安全事件应急工作指南，定义数据安全事件类型，明确不同类别事件的处置流程和方法；

b) 设立负责数据安全事件应急的岗位和人员；

c) 明确数据安全事件应急预案，定期开展应急演练；

d) 安全事件应急机制和应急预案随着组织实施情况不断调整、更新和完善。

7 农业大数据安全分类分级

7.1 概述

数据分类是把具有某种共同属性或特征的数据归并在一起，数据分级是对分类后的数据进行定级。为了便于农业大数据安全管理，宜先从安全管理的视角对农业大数据进行分类，然后对安全分类结果进行

安全等级划分，并实施不同的安全防护。

7.2 数据安全分类

7.2.1 安全分类对象

农业组织对数据进行安全分类时，依据应用场景和需要，可采用如下粒度确定安全分类对象：

a) 对数据目录中的数据项进行分类；

b) 对数据项集合进行整体分类；

c) 既对数据项集合整体进行分类，同时又对其中的数据项进行分类。

7.2.2 安全分类要素

数据分类从安全管理的视角，考虑数据安全性遭到破坏后可能造成的影响（如可能造成的危害、损失或潜在风险等）进行分类。考虑的安全分类要素包括但不限于：

a) 影响对象：农业大数据安全性遭到破坏后，受到危害影响的对象。一般地，影响对象包括国家安全、公共利益、企业合法权益和个人合法权益。

b) 影响范围：农业大数据安全性遭到破坏后，所造成的危害影响规模。一般地，影响范围可根据规模大小分为小范围、大范围和超大范围。

c) 影响程度：农业大数据安全性遭到破坏后，所造成的危害影响大小。一般地，影响程度可根据危害大小划分为特别严重损害、严重损害、一般损害和轻微损害。

7.2.3 安全影响评估

安全影响评估是对农业大数据安全遭受破坏后所造成的影响进行评估，宜综合考虑数据内容、数据规模、数据来源和业务特点等因素，评估结果是数据安全分类的依据。数据安全影响评估包括但不限于：

a) 安全性评估：通过评估农业大数据遭到不当披露所造成的影响，以及农业组织继续使用这些数据可能产生的影响，确定其影响对象、影响范围和影响程度；

b) 完整性评估：通过评估农业大数据遭受修改或损毁所造成的影响，以及农业组织继续使用这些数据可能产生的影响，确定其影响对象、影响范围和影响程度；

c) 可用性评估：通过评估农业大数据及其经处理后形成的各类数据出现访问或使用中断所造成的影响，以及农业组织无法正常使用这些数据可能产生的影响，确定其影响对象、影响范围和影响程度。

7.2.4 安全分类规则

农业大数据分类宜遵守的规则包括但不限于：

a) 农业组织可参照相应标准、规范和历史数据分类案例，根据数据应用需求，自主对数据进行安全分类；

b) 农业大数据安全分类宜考虑数据内容、数据规模、数据来源和业务特点等，场景导向，内容兼顾；

c) 不同农业大数据在安全要求上各有侧重，宜根据具体情况，以其所侧重的安全需求和相应评估结果，作为数据在不同要素上分类的依据；

d) 当数据的安全性、完整性和可用性要求基本一致时，宜以安全性评估结果作为主要分类依据。

7.3 数据安全分级

7.3.1 安全定级规则

农业大数据安全分级宜遵守的规则包括但不限于：

a) 农业组织可根据自身行业领域的数据安全管理需求，如业务属性、地域特点等，参照 7.3.2 中给出的指导性分级初始值自主确定数据定级，但不宜将数据的安全级别由高改为低；

b) 综合考虑数据安全分类中影响对象、影响范围和影响程度，遵循就高不就低原则；

c) 农业大数据安全定级宜采用专家研判和部门评审等方法，以保证分级分类的准确性、科学性和合规性。

7.3.2 分级描述

依据安全级别从高到低，将指导性数据安全分级初始值划分为五级、四级、三级、二级、一级，具体分级

判断准则见附录A。安全级别越高，数据要求的安全保护力度越大。其中，一级、二级、三级属于一般数据，四级属于重要数据，五级属于核心数据。

a） 五级数据判断准则：

1） 对国家安全造成严重影响或者特别严重影响，影响范围超大；

2） 对公共利益造成严重影响，影响范围超大；

3） 对公共利益造成特别严重影响，影响范围超大或者大。

b） 四级数据判断准则：

1） 对国家安全造成轻微影响或者一般影响，影响范围超大；

2） 对公共利益造成一般影响，影响范围超大；

3） 对公共利益造成严重影响，影响范围大；

4） 对企业合法权益造成严重影响或者特别严重影响，影响范围超大；

5） 对个人合法权益造成特别严重影响，影响范围超大。

c） 三级数据判断准则：

1） 对公共利益造成轻微影响，影响范围超大；

2） 对公共利益造成一般影响，影响范围大；

3） 对企业合法权益或者个人合法权益造成一般影响，影响范围超大；

4） 对企业合法权益造成严重影响或者特别严重影响，影响范围小或者大；

5） 对个人合法权益造成严重影响，影响范围大或者超大；

6） 对个人合法权益造成特别严重影响，影响范围小或者大。

d） 二级数据判断准则：

1） 对公共利益造成轻微影响，影响范围大；

2） 对企业合法权益或者个人合法权益造成轻微影响，影响范围超大；

3） 对企业合法权益或者个人合法权益造成一般影响，影响范围大或者小；

4） 对个人合法权益造成严重影响，影响范围小。

e） 一级数据判断准则：

对企业合法权益或者个人合法权益造成轻微影响，影响范围大或者小。

7.4 数据分类分级流程

数据安全分类分级流程如下：

a） 确定分类对象；

b） 确定分类要素；

c） 安全影响评估；

d） 综合考虑数据安全影响评估的结果，识别关键分类要素，进行初始分类；

e） 依照定级规则，对分类结果进行初始分级；

f） 专家研判和部门评审；

g） 分类分级结果审批。

分类分级流程图可参见附录B。

7.5 分类分级变更

如需变更农业大数据分类分级，可参照7.4中的分类分级流程进行变更。需变更的情形包括但不限于：

a） 因国家法律法规或农业组织对数据分类分级的要求发生变更，原有的分类分级不再适用；

b） 数据内容发生变化，如增加、减少、改变等情况，导致原有的分类分级不再适用；

c） 数据内容不变，但因数据的应用场景、处理方式等发生变化，导致原有的分类分级不再适用。

8 农业大数据活动安全的管控措施

8.1 数据采集安全

数据采集是农业组织进行数据获取的行为，获取途径包括田间观测、实验室化验、照相摄像、用户提交

报告、线下获取、系统运维与日志数据采集等方式。农业大数据采集过程安全管控措施包括但不限于：

a) 依据数据安全分类分级，对不同类别级别的数据制定并实施不同的安全采集策略和采集过程的安全防护措施；
b) 遵循数据最小化原则，只采集满足业务所需的最少数据；
c) 定义采集数据目的和用途，明确农业大数据的采集源、采集范围、采集频率，不搜集无关数据；
d) 设置统一的数据采集策略（例如采集周期、采集方式、采集内容等）进行采集行为限制，保证数据采集行为的一致性；
e) 制定采集数据的清洗、转换、加载等操作规范，明确操作方法、手段和流程，并做好采集数据的备份工作，避免操作过程中出现数据遗漏、丢失等问题；
f) 制定采集数据的质量保障规则，明确数据质量保障的策略、规程和要求，包括数据格式要求、数据完整性要求、数据源质量评价标准等；
g) 对采集行为进行日志记录和安全审计，并对超规模、超范围采集等异常行为设置监控及告警机制；
h) 不应采集个人敏感信息，如个人明确表明允许采集个人信息，也应尊重被采集人处理个人隐私的权利。

8.2 数据传输安全

数据传输是数据在农业组织不同系统之间、用户与系统之间的数据流动。例如，农田中传感器采集到的数据通过网络传输到数据中心。农业大数据传输过程安全管控措施包括但不限于：

a) 依据数据安全分类分级，明确数据安全传输的场景，建立相应的数据传输安全策略与规程；
b) 建立传输安全策略与规程的变更审核与监控机制；
c) 建设高可用性的网络，保证数据传输过程的稳定性；
d) 采取必要的措施保障传输通道、传输节点和传输数据的安全；
e) 建立传输数据完整性检测和数据恢复控制措施。

8.3 数据存储安全

数据存储是农业大数据在大数据系统进行储存的活动，包括结构化数据存储、非结构化数据存储及半结构化数据存储。例如，水稻当月进出口数量的结构化数据存储、农田遥感影像的非结构化数据存储。农业大数据存储过程安全管控措施包括但不限于：

a) 依据数据安全分类分级，对不同类别、不同级别的数据采用差异化安全存储，如针对不同类别、不同级别的数据选择适合的数据加密算法对数据加密存储；
b) 针对不同的存储媒体建立相应的格式化规程，并对租用第三方数据存储平台的资质能力和经营风险等进行安全评估；
c) 建立大数据平台审核管理要求，确保大数据平台的安全可靠性；
d) 对数据进行模糊化、关联识别等动态/静态脱敏措施；
e) 制定数据存储相关的安全规则和管理控制机制，采用必要的技术或管控措施进行安全防控和访问控制措施；
f) 建设数据存储安全审计能力，审计存储数据的操作行为；
g) 建立数据容灾备份及恢复机制，包括数据副本的更新频率、保存期限、数据时间版本控制等；
h) 制订数据容灾应急方案，若发生数据丢失或破坏，可及时地恢复数据；
i) 建立存储数据异常告警机制，及时了解存储数据的异常情况。

8.4 数据处理安全

数据处理是通过格式转换、脱敏处理、数据分析、数据可视化等一系列活动的组合，从农业大数据中提炼有价值的信息的操作。例如，根据原始的农产品批发价格数据生成“农产品批发价格200指数”。农业大数据处理过程安全管控措施包括但不限于：

a) 依据数据安全分类分级，划分操作的风险级别，明确高危操作，并制定高危操作阻断的安全策略；
b) 依据相关法律法规要求建立数据使用正当性原则，明确数据使用和分析的目的和范围；
c) 建立数据处理正当性的责任制度，保证数据在声明的目的和范围内进行分析处理和使用；

d） 对数据的处理提供细粒度的访问控制措施，限制数据处理过程中可访问的数据范围和处理目的，保护数据在处理过程中不被任何与处理目的无关的个人、组织和机构获取；

e） 建立数据脱敏规范，明确数据脱敏的使用场景、脱敏流程、脱敏规则、脱敏方法和使用限制等；

f） 对脱敏操作后的数据做适当标记，和原始数据能轻易区分开；

g） 建立数据分析的安全规范，明确数据分析的数据源、数据分析需求和分析逻辑的合规性；

h） 明确数据处理系统开发、上线、运维安全控制措施；

i） 对生产、测试等不同环境进行资源隔离；

j） 建立数据处理的监控审计机制，定期对数据处理操作行为进行审计，对数据分析行为进行监控告警；

k） 对数据分析结果的风险进行合规性评估，避免分析结果输出中包含可恢复的敏感数据。

8.5 数据交换安全

数据交换是在农业组织内部角色、外部实体或公众等之间传递原始数据、处理的数据等不同形式数据的活动。例如，农业农村部数据平台上每月猪肉批发价格需要通过农业农村部和地方的数据交换获取到。农业大数据交换过程安全管控措施包括但不限于：

a） 依据数据安全分类分级，对不同类别、级别的数据制定和实施不同的交换策略和交换过程的安全防护措施；

b） 建立明确的数据开放和共享场景，确保不超出共享数据的使用权限和使用范围；

c） 确认开放和共享的数据内容，确保数据内容满足业务场景需求的最小范围；

d） 提供有效的数据共享访问控制机制，明确不同机构或部门、不同身份与目的的用户权限，能提供的共享数据范围、周期、数量等；

e） 对共享数据的使用者提出明确的数据安全防护要求，在共享数据前需对使用者进行数据安全风险评估；

f） 建立数据共享审批流程，明确共享数据内容、交接方式及应用范围等，未经组织机构正式审批，不得向他人或外部组织机构泄露、出售或者非法提供组织机构内部数据；

g） 建立数据公开发布的审批制度，明确数据公开的内容及范围；

h） 在数据公布之前，对拟公布数据的敏感性进行评估，根据评估结果对需要公布的敏感信息进行脱敏操作；

i） 明确数据接口安全控制策略，明确规定使用数据接口的安全限制和安全控制措施；

j） 明确数据接口安全要求，包括接口名称、接口参数等；

k） 与数据接口调用方签署合作协议，明确数据的使用目的、供应方式、保密约定、数据安全责任等；

l） 审计数据交换过程，确保审计记录为安全事件的处置、应急响应和事后调查提供帮助。

8.6 数据销毁安全

数据销毁是农业组织删除数据及其副本的操作，如果数据来自于外部实体的数据流，则断开与数据流的连接。例如，对退服的存储服务器、磁盘阵列进行消磁或物理销毁等。农业大数据销毁过程安全管控措施包括但不限于：

a） 依据数据安全分类分级，建立数据销毁的审批和管理制度，明确数据销毁场景、销毁对象、销毁方式和销毁要求，并对销毁过程和销毁中的参与者进行记录控制；

b） 对超出数据留存期限的数据，进行删除或者匿名化处理，对留存期限有明确规定的，按相关规定执行；

c） 对数据进行销毁时，保证已删除的敏感数据不可被还原，并进行效果验证；

d） 对存储媒体进行销毁时，采用消磁、物理破坏等方式进行；

e） 当数据销毁可能会影响执法机构调查取证时，采取适当的存储和屏蔽措施；

f） 对存在多个副本的数据进行销毁时，确保数据的多个副本被使用相同的方式处理；

g） 在数据合作结束后，要求数据共享使用者按照共享前的约定进行数据销毁。

附 录 A
（规范性）
农业大数据安全分级判断准则表

根据数据安全性遭到破坏后的影响对象、影响范围、影响程度与安全等级的关系，制定农业大数据安全分级判断准则，见表 A.1。其中，安全等级中的‘—’符号表示某种影响对象、影响范围、影响程度的组合情况不存在，如国家安全影响范围不存在影响范围小或者大的情况。

表 A.1 农业大数据安全分级判断准则

影响对象	影响范围	影响程度	安全等级
国家安全	小	轻微	—
		一般	—
		严重	—
		特别严重	—
	大	轻微	—
		一般	—
		严重	—
		特别严重	—
	超大	轻微	四级
		一般	四级
		严重	五级
		特别严重	五级
公共利益	小	轻微	—
		一般	—
		严重	—
		特别严重	—
	大	轻微	二级
		一般	三级
		严重	四级
		特别严重	五级
	超大	轻微	三级
		一般	四级
		严重	五级
		特别严重	五级
企业合法权益	小	轻微	一级
		一般	二级
		严重	三级
		特别严重	三级
	大	轻微	一级
		一般	二级
		严重	三级
		特别严重	三级
	超大	轻微	二级
		一般	三级
		严重	四级
		特别严重	四级

表 A.1（续）

影响对象	影响范围	影响程度	安全等级
个人合法权益	小	轻微	一级
		一般	二级
		严重	二级
		特别严重	三级
	大	轻微	一级
		一般	二级
		严重	三级
		特别严重	三级
	超大	轻微	二级
		一般	三级
		严重	三级
		特别严重	四级

附　录　B
（规范性）
农业大数据安全分类分级流程图

农业大数据安全分类分级流程，见图 B.1。

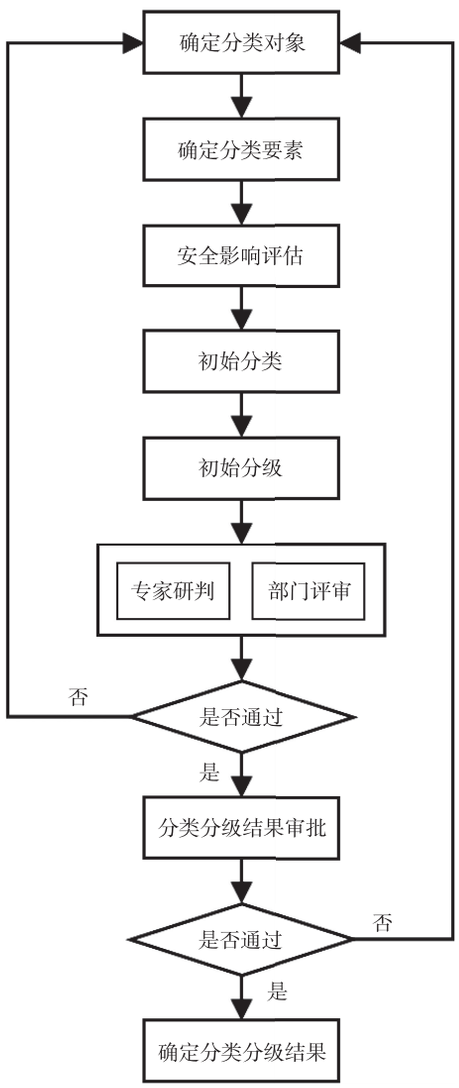

图 B.1　农业大数据安全分类分级流程