

ICS 35.240.01
I6440

团 体 标 准

T/WHCSA 003—2024

制造业数据安全中的数据分类分级 方法指南

Guide to data classification and grading methods in data security management of
manufacturing industry

2024-11-26 发布

2025-1-1 实施

武汉市网络安全协会 发布

目 次

前 言	III
引 言	IV
1 范围	5
2 规范性引用文件	5
2.1 制造业数据	5
2.2 安全管理	5
2.3 数据分类	5
2.4 数据分级	5
3 基本原则	5
3.1 科学实用原则	5
3.2 稳定可扩展原则	5
3.3 边界清晰原则	5
3.4 就高从严原则	6
3.5 动态更新原则	6
4 综述	6
4.1 数据特征	6
4.2 分类结构	6
4.3 分类规则	6
4.4 分级要素	6
4.5 分级规则	6
4.6 级别变更	7
5 数据分类分级流程	7
5.1 建立组织保障	7
5.2 建立制度流程	7
5.3 全面梳理数据资产	7
5.4 对数据资产分类	7
5.5 对数据资产分级	7
5.6 选择分类分级工具	8
5.7 建立数据分类分级标识	8
5.8 整理数据分类分级清单	8
5.9 数据安全防护	8
6 数据分类分级方法	8
6.1 数据分类	8
6.2 数据分级	8
附 录 A （资料性附录） 制造业数据分类示例	9
附 录 B （资料性附录） 制造业数据分级示例	10
附 录 C （资料性附录） 制造业数据分类分级示例	11
参 考 文 献	13

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。

本文件由武汉市网络安全协会提出。

本文件由武汉市网络安全协会归口。

本文件起草单位：武汉市网络安全协会、智网安云（武汉）信息技术有限公司、华中师范大学、湖北大学、中国电信股份有限公司武汉分公司、中国通信建设第三工程局有限公司、武汉三江航天网络通信有限公司、武汉数智云科技有限公司、武汉虹信技术服务有限责任公司、武汉烽火创新谷管理有限公司、武汉微创光电股份有限公司

本文件主要起草人：刘悦恒、梁忠辉、覃兵、曹高辉、黄辰、雷显开、乔奇、张玉萍、严媛、陈乐曦、方波、祝林、王清宇、荣金慧、费玉婷、赵桥、贺珊、张峰、邢亚平、陈佳阳。

引 言

在当今数字化时代，制造业数据的安全管理至关重要。随着制造业的数字化转型和数据量的不断增长，数据分类分级成为保障数据安全的关键环节。本指南旨在为制造业企业提供一套科学、实用的数据分类分级方法，帮助企业更好地管理和保护其数据资产。通过明确数据分类分级的原则、流程和方法，本指南将有助于企业提高数据安全水平，降低数据安全风险，确保制造业数据的安全、可靠和有效利用。同时，本指南也将为相关行业标准的制定和完善提供参考，推动制造业数据安全管理的规范化和标准化发展。

制造业数据安全中的数据分类分级方法指南

1 范围

本文件确立了标准化文件的结构及其起草的总体原则和要求，并规定了文件名称、层次、要素的编写和表述规则以及文件的编排格式。

本文件适用于制造企业在进行数据安全中对数据进行分类分级。

注：在不引起混淆的情况下，本文件中的“标准化文件”简称为“文件”。

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 43697-2024 数据安全技术 数据分类分级规则

GB/T 42128-2022 智能制造 工业数据 分类原则

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 38667—2020 信息技术 大数据数据分类指南

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

T/CCSA 278-2019 工业互联网平台 制造企业数据质量治理技术要求

工业领域重要数据和核心数据识别规则（草案）

2.1 制造业数据

制造类企业所有生产活动和服务所产生的，以一定形式记录、保存的文件、资料、图表和数据等各类信息的可再解释的形式化表示，以适用于通信、解释或处理。

2.2 安全管理

对各类风险和威胁进行识别、评估和控制的过程。

2.3 数据分类

根据制造业数据的属性或特征，将其按照一定的原则和方法进行区分和归类，并建立起一定的分类体系和排列顺序的过程。

2.4 数据分级

指按照一定的分级原则对制造业数据进行安全级别划定。

3 基本原则

3.1 科学实用原则

从便于数据管理和使用的角度，科学选择常见、稳定的属性或特征作为数据分类的依据，并结合实际需要对数据进行细化分类。

3.2 稳定可扩展原则

总体上应具有概括性和包容性，能够实现各种数据的分类，以及满足将来可能出现的数据类型。

3.3 边界清晰原则

数据分级的主要目的是为了数据安全，各个数据级别应做到边界清晰标准。

3.4 就高从严原则

当多个因素可能影响数据分级时，按照可能造成的最高影响对象和影响程度确定数据级别。

3.5 动态更新原则

根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分类分级、重要数据目录等进行定期审核更新。

4 综述

数据分类分级是指将数据建立起一种的分类体系和分级排列顺序，以便更好地管理和使用组织数据的过程。包括数据特征、分类结构、分类规则、分级要素、分级规则、级别变更。

4.1 数据特征

数据特征包括：

- a) 数据对象内容
- b) 数据产生来源
- c) 数据业务场景
- d) 数据保护要求

4.2 分类结构

按照数据分类要素，将数据分为三个层级，形成由一级类目、二级类目、三级类目构成的分类结构。一级类目以用户数据、业务数据、管理进行分类，共分为三类，二级类目和三级类目以数据对象内容、数据具体业务、数据分发范围、数据的敏感性、数据的保密性、数据的重要性为主要分类要素。数据分类结构见附录A。一级类目应维持不变，二级类目和三级类目可按需扩展。

4.3 分类规则

数据分类的通用规则包括：

- a) 数据分类时以主要业务特征为基准；
- b) 数据分类要有利于管理效率的提高；
- c) 同一主题的数据应隶属同一类。

4.4 分级要素

数据安全级别的判定基于对分级要素的评估。数据分级要素包括影响对象和影响程度。

4.5 分级规则

- a) 对公共利益或者个人、组织合法权益造成的影响；
- b) 对个人和企业、生产生活区域、对企业经营、行业发展、技术进步和产业生态等造成的影响；

c) 恢复数据或消除负面影响所需付出的代价；

d) 对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等重点领域国家安全造成的影响。

按照“国家安全”、“社会秩序和公共利益”、“个人、法人和其它组织合法权益”的顺序，从高确定影响程度；

4.6 级别变更

数据分级完成后，出现下列情形之一时，对相关数据的级别进行变更。

a) 数据内容发生变化，导致原有数据的分级级别不适用变化后的数据。

b) 因国家或行业主管部门要求变化，导致原定的数据级别不再适用。

c) 需要对数据级别进行变更的其他情形。

5 数据分类分级流程

5.1 建立组织保障

设立数据安全第一责任人，由第一责任人统筹整个数据安全治理及建设工作。

其次，设立领导层、监督层、管理层、执行层，四个层级之间相互协作，共同建设数据安全。

数据安全委员会成员通常由企业高级管理层、业务部门负责人、IT部门负责人、法务合规部门负责人等组成。

领导层：数据安全第一负责人（数据安全委员会主席）

监督层：数据安全监督员

管理层：数据资产管理委员

执行层：各委员及其部门其他成员

5.2 建立制度流程

制定数据分类分级制度流程文件，明确分类标准、分级标准、保密措施等。

5.3 全面梳理数据资产

按照组织范围、业务范围、系统范围依次梳理数据资产。

组织范围：盘点要覆盖哪些组织和部门，例如：集团本部、集团+分子公司等。

业务范围：盘点哪些业务的数据，例如：生产业务、采购业务、营销业务、财务业务、人力资源业务等。

系统范围：盘点哪些应用系统的数据，例如：ERP系统、MES系统、SCM系统、CRM系统、HR系统等。

基于不同的数据来源，根据不同的划分策略，数据资产梳理的内容：

5.4 对数据资产分类

根据业务运营和自身管理特点，按照树形结构，建立数据资源分类目录表。按照一级类别-二级子类别-三级子类别来进行组织，最多不超过三级。

5.5 对数据资产分级

根据重要程度和敏感程度，确定安全等级。

5.6 选择分类分级工具

分类分级工具需要具备的功能

- a) 数据资产扫描:对组织机构内网的数据库、大数据平台、文件系统、WEB业务系统、数据接口等数据资产进行智能化探测、数据资产梳理、敏感数据识别定位、数据分类分级,并形成数据资产清单和多维度可视化地图。
- b) 敏感数据自动发现:能够从海量数据中快速发现敏感数据,定位敏感数据存储与分布,统计敏感数据量,可以通过敏感数据自动发现能力,对数据库中的字段信息进行扫描,发现个人敏感数据信息、企业敏感信息。
- c) 数据分类分级管理:支持自定义的分类分级策略,除了通用行业内置策略外,支持精细化自定义配置。分级和分类配置是对资产等级的定义,分为用户自定义和系统内置两类,对资产进行分类分级时所使用的分类信息就来源于此。分类配置需要关联具体的分级信息,每一类数据对应不同的安全等级。
- d) 分类分级结果导出:用户可以通过图形报表的形式直观的展示资产地图,对数据分类分级结果的批量及部分导出,导出项包含并不限于任务名称、数据源名称、主机、数据库名、表名、字段名、匹配结果、敏感信息等。支持通过API接口将分类分级后的结果同步给其他设备。

5.7 建立数据分类分级标识

人工与技术手段结合,进行数据分类分级标识。

5.8 整理数据分类分级清单

输出数据分类分级清单,清单内容和形式。

5.9 数据安全防护

- a) 数据备份与恢复:数据备份是指将重要的数据复制到其他存储媒体或位置,以防止数据丢失或损坏。
- b) 访问控制:访问控制是通过身份验证、授权和权限管理等手段,限制对数据的访问和操作。
- c) 加密:加密是一种将数据转化为密文的过程,以保护数据的机密性。
- d) 安全策略和规范:安全策略和规范是指为组织或个人制定的一系列安全措施和准则,用于指导和规范数据安全的实施和管理。
- e) 安全审计和监控:安全审计和监控是指对数据的访问和操作进行监视和审查,以检测和预防潜在的安全威胁。
- f) 漏洞管理和修复:漏洞管理和修复是指对系统和应用程序进行漏洞扫描和修补,以防止潜在的安全漏洞被攻击者利用。
- g) 员工培训和教育:员工培训和教育是指向组织内部的员工提供有关数据安全的培训和教育,使其了解数据安全性的重要性和相关的最佳实践。
- h) 物理安全措施:物理安全措施是指采取措施保护存储数据的设备和设施,防止非法访问和物理破坏。
- i) 灾难恢复和业务连续性计划:灾难恢复和业务连续性计划是指为组织制定的一系列措施和计划,以应对灾难事件并确保业务的持续运行。

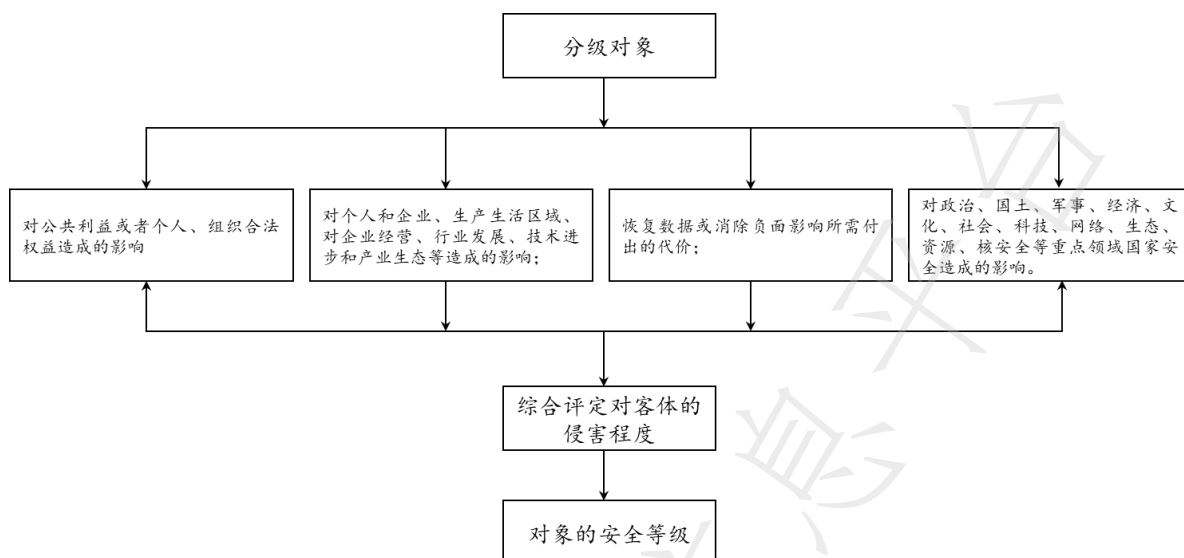
6 数据分类分级方法

6.1 数据分类

具体分类详见附录A。

6.2 数据分级

数据分级流程如下图所示:



具体分级详见附录B。

附录 A (资料性附录) 制造业数据分类示例

根据制造企业业务运营管理和数据安全特点,将企业数据分为用户数据、业务数据和管理数据三类,表A. 1、A. 2、A. 3分别给出了这三类数据的详细分类示例。

a) 用户数据分类

组织在开展业务服务过程中从个人用户或组织用户收集的数据,以及在业务服务过程中产生的归属于用户的数据。

b) 业务数据分类

业务数据分类可根据各部门业务具体情况,对业务数据进行细化分类。

c) 管理数据分类

管理数据分类可根据各部门实际管理情况,对管理数据进行细化分类。

A.1 用户数据分类示例

数据类别	类别定义	示例
用户数据	组织在开展业务服务过程中从个人用户或组织用户收集的数据，以及在业务服务过程中产生的归属于用户的数据	如个人用户信息（即个人信息）、组织用户信息（如组织基本信息、组织账号信息、组织信用信息等）

A.2 业务数据分类示例

数据类别	类别定义	示例
业务数据	组织在业务生产过程中收集和产生的非用户类数据	参考业务所属的行业数据分类分级，结合自身业务特点进行细分，如产品数据、合同协议等

A.3 管理数据分类示例

数据类别	类别定义	示例
管理数据	组织在机构经营管理过程中收集和产生的数据	如经营战略、财务数据、并购及融资信息等

附录 B (资料性附录) 制造业数据分级示例

根据数据对象的重要程度，将制造企业数据分为五个安全级别，其中核心数据对应5级，重要数据对应4级，一般数据对应级别1-3。示例见表B.1。

B.1 数据分级示例

重要程度	数据定级	说明	影响程度
核心	5级	1. 可能导致国家安全受到严重威胁，严重影响国家政权稳固、民族团结、领土完整。2. 可能导致严重危害社会秩序和公共利益，引发广泛的群体事件，或者导致经济利益和市场秩序遭到严重破坏等情况。3. 可能导致个人生命安全和财产安全无法保障、法人和组织遭受全局性或战略性破坏。	特别严重损害
重要	4级	1. 可能导致危及国家安全的重大事件，发生危害国家利益或造成重大损失的情况。2. 可能导致严重影响组织正常运行，或者影响重要/关键业务无法正常开展的情况。可能导致危害社会秩序和公共利益的事件，引发一定范围的群体事件，或者导致经济利益和市场秩序遭到破坏等情况。3. 可能导致个人、法人和组织面临重大信息安全风险、侵犯个人隐私等严重侵权的事件。	严重损害

一般	3级	1. 可能对国家安全造成一定影响或潜在影响。2. 可能导致影响组织正常运行, 或者影响个人、法人和组织部分业务无法正常开展的情况。对公共利益和社会秩序在一定范围内造成影响。3. 可能导致一定规模的个人、法人和组织信息泄漏、滥用等安全风险, 对个人、法人和组织权益可能造成一定影响。	一般损害
	2级	1. 可能导致干扰组织正常运行, 个人、法人和组织部分业务临时性中断等情况。对公共利益和社会秩序造成微弱影响。2. 可能导致个人、法人和组织经济利益、声誉等轻微受损, 或对合法权益造成部分或潜在影响	轻微损害
	1级	1. 信息公开对国家安全、社会秩序和公共利益、个人、法人和组织合法权益无任何损害。	无损害

附 录 C
(资料性附录)
制造业数据分类分级示例

根据数据对象的分类和分级维度, 对各个安全级别包含的数据子类示例见表C. 1。。

C. 1 数据分级示例

一级类别	二级子类别	三级子类别	数据分级参考
用户数据	个人信息数据	个人基本信息	一般个人基本信息
		个人敏感信息	重要个人敏感信息
	组织信息数据	组织基本信息	一般组织基本信息
			重要组织基本信息
		组织账号信息	一般组织账号信息
			重要组织账号信息
业务数据	研发数据	研发设计图纸文档	核心研发设计图纸
			重要研发设计图纸
			一般研发设计图纸
		产品模型文件	核心产品模型文件
			重要产品模型文件
			一般产品模型文件
	生产数据	开发测试代码	核心开发测试代码
			重要开发测试代码
			一般开发测试代码
		生产监控数据	核心生产监控数据
			重要生产监控数据
			一般生产监控数据
		工业控制信息	核心工业控制信息
			重要工业控制信息
			一般工业控制信息

		工况状态	核心工况状态
			重要工况状态
			一般工况状态
		工艺参数	核心工艺参数
			重要工艺参数
			一般工艺参数
		系统日志	核心系统日志
			重要系统日志
			一般系统日志
	运维数据	供应链数据	核心供应链数据
			重要供应链数据
			一般供应链数据
		物流数据	重要物流数据
			一般物流数据
		产品售后运维服务数据	重要产品售后运维服务数据
			一般产品售后运维服务数据
			核心外部交换数据
	外部数据	外部交换数据	重要外部交换数据
			一般外部交换数据
管理数据	管理域数据	规划与制度规范文件	重要规划与制度规范文件
			一般规划与制度规范文件
		固定资产信息	重要固定资产信息
			一般固定资产信息
		财务数据（合同、财政收支）	重要财务数据
			一般财务数据
		人力与客户信息	重要人力与客户信息
			一般人力与客户信息
		资源管理与业务统计数据（订单、仓储、排产）	核心资源管理与业务统计数据
			重要资源管理与业务统计数据
			一般资源管理与业务统计数据

参 考 文 献

- [1]GB/T 43697-2024 数据安全技术 数据分类分级规则
- [2]GB_T 42128-2022 智能制造 工业数据 分类原则
- [3]GB/T 35273—2020 信息安全技术个人信息安全规范
- [4]GB/T 38667—2020 信息技术大数据数据分类指南
- [5]GB/T 36073-2018 数据管理能力成熟度评估模型
- [6]GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
- [7]T/CCSA 278-2019 工业互联网平台 制造企业数据质量治理技术要求
- [8]工业领域重要数据和核心数据识别规则（草案）