工业数据分类分级指南（试行）

第一章 总则

第一条 为贯彻《促进大数据发展行动纲要》《大数据产业发展规划（2016-2020 年）》有关要求，更好推动《数据管理能力成熟度评估模型》（GB/T 36073-2018）贯标和《工业控制系统信息安全防护指南》落实，指导企业提升工业数据管理能力，促进工业数据的使用、流动与共享，释放数据潜在价值，赋能制造业高质量发展，制定本指南。

第二条 本指南所指工业数据是工业领域产品和服务全生命周期产生和应用的数据，包括但不限于工业企业在研发设计、生产制造、经营管理、运维服务等环节中生成和使用的数据，以及工业互联网平台企业（以下简称平台企业）在设备接入、平台运行、工业 APP 应用等过程中生成和使用的数据。

第三条 本指南适用于工业和信息化主管部门、工业企业、平台企业等开展工业数据分类分级工作。涉及国家秘密信息的工业数据，应遵守保密法律法规的规定，不适用本指南。

第四条 工业数据分类分级以提升企业数据管理能力为目标，坚持问题导向、目标导向和结果导向相结合，企业主体、行业指导和属地监管相结合，分类标识、逐类定级和分级管理相结合。

第二章 数据分类

第五条 工业企业结合生产制造模式、平台企业结合服务运营模式，分析梳理业务流程和系统设备，考虑行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行分类梳理和标识，形成企业工业数据分类清单。

第六条 工业企业工业数据分类维度包括但不限于研发数据域（研发设计数据、开发测试数据等）、生产数据域（控制信息、工况状态、工艺参数、系统日志等）、运维数据域（物流数据、产品售后服务数据等）、管理数据域（系统设备资产信息、客户与产品信息、产品供应链数据、业务统计数据等）、外部数据域（与其他主体共享的数据等）。

第七条 平台企业工业数据分类维度包括但不限于平台运营数据域（物联采集数据、知识库模型库数据、研发数据等）和企业管理数据域（客户数据、业务合作数据、人事财务数据等）。

第三章 数据分级

第八条 根据不同类别工业数据遭篡改、破坏、泄露或非法利用后，可能对工业生产、经济效益等带来的潜在影响，将工业数据分为一级、二级、三级等 3 个级别。

第九条 潜在影响符合下列条件之一的数据为三级数据：

（一）易引发特别重大生产安全事故或突发环境事件，或造成直接经济损失特别巨大；

（二）对国民经济、行业发展、公众利益、社会秩序乃至国家安全造成严重影响。

第十条 潜在影响符合下列条件之一的数据为二级数据：
（一）易引发较大或重大生产安全事故或突发环境事件，给企业造成较大负面影响，或直接经济损失较大；
（二）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或影响持续时间长，或可导致大量供应商、客户资源被非法获取或大量个人信息泄露；
（三）恢复工业数据或消除负面影响所需付出的代价较大。

第十一条 潜在影响符合下列条件之一的数据为一级数据：
（一）对工业控制系统及设备、工业互联网平台等的正常生产运行影响较小；
（二）给企业造成负面影响较小，或直接经济损失较小；
（三）受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短；
（四）恢复工业数据或消除负面影响所需付出的代价较小。

第四章　分级管理

第十二条 工业和信息化部负责制定工业数据分类分级制度规范，指导、协调开展工业数据分类分级工作。各地工业和信息化主管部门负责指导和推动辖区内工业数据分类分级工作。有关行业、领域主管部门可参考本指南，指导和推动本行业、本领域工业数据分类分级工作。

第十三条 工业企业、平台企业等企业承担工业数据管理的主体责任，要建立健全相关管理制度，实施工业数据分类分级管理并开展年度复查，并在企业系统、业务等发生重大变更时应及时更新分类分级结果。有条件的企业可结合实际设立数据管理机构，配备专职人员。

第十四条 企业应按照《工业控制系统信息安全防护指南》等要求，结合工业数据分级情况，做好防护工作。
企业针对三级数据采取的防护措施，应能抵御来自国家级敌对组织的大规模恶意攻击；针对二级数据采取的防护措施，应能抵御大规模、较强恶意攻击；针对一级数据采取的防护措施，应能抵御一般恶意攻击。

第十五条 鼓励企业在做好数据管理的前提下适当共享一、二级数据，充分释放工业数据的潜在价值。二级数据只对确需获取该级数据的授权机构及相关人员开放。三级数据原则上不共享，确需共享的应严格控制知悉范围。

第十六条 工业数据遭篡改、破坏、泄露或非法利用时，企业应根据事先制定的应急预案立即进行应急处置。涉及三级数据时，还应将事件及时上报数据所在地的省级工业和信息化主管部门，并于应急工作结束后 30 日内补充上报事件处置情况。