

# 工业互联网企业网络安全分类分级指南（试行）

（征求意见稿）

为加强工业互联网安全保障工作，提高工业互联网企业网络安全防范能力和水平，进一步明确和落实企业网络安全主体责任，加快构建工业互联网安全保障体系，促进工业互联网高质量发展，护航制造强国和网络强国战略实施，依据《加强工业互联网安全工作的指导意见》要求，制定本指南。

## 一、范围和原则

### （一）适用范围

工业和信息化部主管行业范围内的工业互联网企业的网络安全管理，适用本指南。

依据企业属性，工业互联网企业主要包括三类：

1. 应用工业互联网的工业企业（简称“联网工业企业”），主要涉及原材料工业、装备工业、消费品工业和电子信息制造业等行业；

2. 工业互联网平台企业（简称“平台企业”，主要指对外提供工业互联网平台等互联网信息服务的企业）；

3. 工业互联网基础设施运营企业，主要包括基础电信运营企业和标识解析系统建设运营机构。

本指南对联网工业企业网络安全分级进行规范。工业互联网平台企业和基础设施运营企业按照《通信网络安全防护

管理办法》的分级方式进行规范。

## **(二) 基本原则**

**企业分级与行业网络安全影响程度相关联。**以《国民经济行业分类》(GB/T 4754-2017)为基准细化联网工业企业行业类别，明确各相关行业网络安全影响程度，将企业所属行业网络安全影响程度作为企业分级评定的关键参考因素。

**行业指导与地方监管相结合。**工业和信息化部对主管行业领域的工业互联网企业网络安全工作开展指导管理。地方主管部门对本行政区域工业互联网企业的网络安全工作开展指导监管。

**企业自评与属地核查相结合。**工业互联网企业根据分级评定细则开展自评，地方主管部门对企业自评结果进行核查和确认。

## **二、企业分级**

### **(一) 联网工业企业分级**

联网工业企业分级主要考虑企业所属行业网络安全影响程度、企业规模、企业应用工业互联网的程度、企业发生网络安全事件的影响程度等要素。其中所属行业网络安全影响程度由低到高分别划分为一类、二类和三类（见附件1）。

企业分级采用计分方式进行，满分为100分：

评分大于等于80分的，为三级企业；

评分大于等于 60 分的，且小于 80 分的，为二级企业；  
评分小于 60 分的，为一级企业。

属于三类行业的规模以上联网工业企业原则上为三级。

## **（二）多重属性企业的分级**

对于同时具有联网工业企业、平台企业、工业互联网基础设施运营企业中两种以上属性的企业，按照其业务活动涉及的不同属性分别定级。

## **三、级别评定**

### **（一）制定评定规则**

工业和信息化部选择重点行业或区域开展分类分级试点，细化联网工业企业分级评定参考规则（见附件 2），形成评定规则。

### **（二）企业自评**

依托工业互联网企业网络安全分类分级管理服务平台，联网工业企业在线填报问卷，形成自评报告。

### **（三）核查确认**

地方主管部门可自行或组织第三方专业服务机构对企业提交的自评报告真实性、完整性进行核查，发现信息不真实、不完整的，通知企业予以补正后进行确认。

### **（四）级别变更**

当联网工业企业网络安全风险程度发生重大变化时，应

主动重新定级。

#### **四、安全管理**

省、市、县各级工业和信息化主管部门指导本行政区域内联网工业企业网络安全工作，省级通信管理局对本行政区域内平台企业、标识解析系统建设运营机构进行网络安全监督管理。地方工信和通信主管部门加强对三级工业互联网企业的安全监管。

##### **(一) 组织管理**

1. 三级工业互联网企业应当建立健全网络安全责任制，设置专门网络安全机构和安全管理负责人，组织制定和实施网络安全防护和培训计划，加强网络安全考核，确保安全投入；

2. 二级工业互联网企业应当明确专门的网络安全管理负责人，逐步建立健全并落实网络安全责任制，组织制定和实施网络安全防护和培训计划。

##### **(二) 安全防护**

1. 三级工业互联网企业应当根据工业互联网网络安全管理和技术防护系列标准规范要求，采取相应的技术防护措施；建设完善企业级工业互联网安全监测平台，并接入省级以上工业互联网安全监测平台。省级以上工业互联网安全监测平台定期向三级企业通报安全风险。

2. 二级工业互联网企业应当根据工业互联网网络安全管理和技术防护系列标准规范要求，采取相应的技术防护措施；积极建设企业级工业互联网安全监测平台，并与省级工业互联网安全监测平台对接。

### **(三) 风险评估**

1. 三级工业互联网企业应当至少每年进行一次网络安全风险评估与审计。

2. 二级工业互联网企业应当至少每两年进行一次网络安全风险评估与审计。

### **(四) 应急管理**

工业互联网企业应当制定切实可行的应急预案，建立应急响应机制，定期开展应急演练，采取必要措施消除安全隐患。发现重大网络安全风险和安全事件应当及时上报。

附件: 1. 联网工业企业所属行业网络安全分类指导目录

2. 联网工业企业分级评定参考规则

## 附件 1

### 联网工业企业所属行业网络安全分类指导目录

序号	行业名称	行业门类及代码
<b>一、三类行业</b>		
1	钢铁	31 黑色金属冶炼和压延加工业
2	有色	32 有色金属冶炼和压延加工业
3	石化化工	25 石油、煤炭及其他燃料加工业 26 化学原料和化学制品制造业（除日用化学品制造）
4	轨道交通装备	371 铁路运输设备制造 372 城市轨道交通设备制造
5	船舶及海洋工程装备	373 船舶及相关装置制造
6	航空航天装备	374 航空、航天器及设备制造
<b>二、二类行业</b>		
7	建材	30 非金属矿物制品业（除玻璃制品制造、陶瓷制品制造）
8	废弃资源回收加工	42 废弃资源综合利用业
9	机械	33 金属制品业（除金属制日用品制造） 34 通用设备制造业 35 专用设备制造业 38 电气机械和器材制造业（除电池制造、家用电力器具制造、非电力家用器具制造、照明器具制造） 40 仪器仪表制造业 43 金属制品、机械和设备修理业
10	汽车	36 汽车制造业
11	其他运输设备	375 摩托车制造 377 助动车制造 378 非公路休闲车及零配件制造

序号	行业名称	行业门类及代码
		379 潜水救捞及其他未列明运输设备制造
12	医药	27 医药制造业
13	电子设备制造	39 计算机、通信及其他电子设备制造业
<b>三、一类行业</b>		
14	轻工	16 烟草制品业 19 皮革、毛皮、羽毛及其制品和制鞋业 20 木材加工和木、竹、藤、棕、草制品业 21 家具制造业 22 造纸和纸制品业 23 印刷和记录媒介复制业 24 文教、工美、体育和娱乐用品制造业 29 橡胶和塑料制品业 268 日用化学产品制造 305 玻璃制品制造 307 陶瓷制品制造 338 金属制日用品制造 376 自行车和残疾人座车制造 384 电池制造 385 家用电力器具制造 386 非电力家用器具制造 387 照明灯具制造 411 日用杂品制造
15	纺织	17 纺织业 18 纺织服装、服饰业 28 化学纤维制造业
16	食品	13 农副食品加工 14 食品制造业 15 酒、饮料和精制茶制造业

## 附件 2

### 联网工业企业分级评定参考规则

序号	一级指标	评定要素	
1	企业所在行业网络安全影响程度（40分）	根据企业所在行业网络安全风险程度，包括纳入安全生产许可的行业，先期开展安全生产标准化工作的行业等因素，以及行业网络安全对我国政治、经济、社会等的影响程度，将企业所在行业分为三类行业、二类行业和一类行业（附件 1）	
2	企业规模（10分）	根据从业人员数量、营业收入、资产总额等将企业分为大型企业、中型企业、小微企业	
3	企业应用工业互联网的程度（30分）	根据企业信息化和工业化融合程度、互联互通、综合集成、数据分析利用四方面，综合判定企业应用工业互联网的程度为高、中、低三个等级	<b>企业两化融合程度：</b> 根据两化融合评估规范，分为起步建设阶段、单项覆盖阶段、集成提升阶段和创新突破阶段
			<b>互联互通程度：</b> 根据智能设备联网、信息网络设施建设、生产资源连接程度判定
			<b>综合集成程度：</b> 根据企业与产业链上下游横向集成、企业内部纵向集成，以及贯穿整个价值链的端到端集成程度判定
			<b>数据分析利用程度：</b> 根据运营智能决策、产品生命周期优化、生产智能管理、供应链优化、网络化协同、能耗与安全管理优化、服务化延伸程度判定
4	企业一旦发生网络安全事件的影响程度（20分）	企业根据自身情况，判定一旦发生重大网络安全事件后，关键数据、重要敏感信息和国家秘密信息丢失或被窃取、篡改、假冒的程度，以及对国家安全、社会秩序、经济建设和公众利益构成威胁的程度，分为一般影响、较大影响、重大影响和特别重大影响	