

云南省通信管理局 云南省工业和信息化厅 文件

云通信局联发〔2025〕6号

云南省通信管理局 云南省工业和信息化厅 关于印发《云南省工业互联网安全分类分级 管理办法实施细则》的通知

各州（市）工业和信息化主管部门，各有关企业：

根据《工业互联网安全分类分级管理办法》（工信部网安〔2024〕68号）要求，为进一步加强云南省工业互联网安全分类分级管理工作，落实企业网络安全主体责任，提升工业互联网安全防护水平，护航新型工业化高质量发展，现将《云南省工业互联网安全分类分级管理办法实施细则》印发给你们，请认真抓好落实。

(此页无正文)



抄送：工业和信息化部网络安全管理局，中共云南省委网信办，云南省公安厅。

云南省通信管理局办公室

2025年3月12日印发

云南省工业互联网安全分类分级管理办法 实施细则

第一章 总则

第一条 目的和依据

为加强工业互联网安全分类分级管理，落实企业网络安全主体责任，提升工业互联网安全防护水平，促进工业互联网深度融合应用，护航新型工业化高质量发展，维护国家安全和利益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规及《工业互联网安全分类分级管理办法》的规定，制定本细则。

第二条 适用范围

工业和信息化部主管行业范围内在云南省经营的工业互联网企业适用本办法。

依据企业属性，工业互联网企业主要包括三类：

（一）应用工业互联网的工业企业（以下称联网工业企业），主要是指将新一代信息通信技术与工业系统深度融合，推动开展数字化研发、智能化制造、网络化协同、个性化定制、服务化延伸等的工业企业。

（二）工业互联网平台企业（以下称平台企业），主要是

指面向制造业数字化、网络化、智能化需求，基于云平台等方式对外提供工业大数据、工业 APP 等资源和公共服务的企业。

（三）工业互联网标识解析企业（以下称标识解析企业），主要是指工业互联网标识解析根节点运行机构、国家顶级节点运行机构、标识注册服务机构、递归节点运行机构等提供工业互联网标识服务的机构。

本细则所称设备、系统指的是公共互联网上监测发现的工业互联网企业的设备及系统。

第三条 职责分工

云南省工业和信息化厅主要负责指导省内联网工业企业的安全分类分级管理，同步加强工业控制系统网络安全防护。

云南省通信管理局主要负责开展省内平台企业、标识解析企业的安全分类分级管理，并在公共互联网上对联网设备、系统等进行安全监测。

各州（市）工业和信息化主管部门负责本行政区域内工业互联网企业网络安全事件的监督管理。

云南省工业和信息化厅、云南省通信管理局统称为主管部门。

第二章 企业分类分级

第四条 定级

工业互联网企业应当按照工业互联网安全定级相关标准规

范，结合企业规模、业务范围、应用工业互联网的程度、运营重要系统的程度、掌握重要数据的程度、对行业发展和产业链供应链安全的重要程度以及发生网络安全事件的影响后果等要素，开展自主定级。工业互联网企业级别由高到底分为三级、二级、一级。

当企业定级要素发生较大变化，可能影响企业定级结果时，企业应当在发生变化的三个月内重新定级。同时具有联网工业企业、平台企业、标识解析企业中两种及以上属性的企业，应当按照不同类型分别定级。

第五条 信息登记

完成自主定级的工业互联网企业通过全国工业互联网安全分类分级管理平台或与其对接的省级有关平台开展信息登记（以下简称分类分级管理平台），登记内容包括但不限于企业名称、企业类型、企业级别、联系方式、网络安全负责人等相关情况。

第六条 信息核查

主管部门通过分类分级管理平台，对企业提交登记的材料，在三十个工作日内开展核查，对材料内容不齐全、定级不准确的，通知企业在二十个工作日内予以补正。

第七条 符合性评测

工业互联网企业应当按照法律法规和相关标准，自行或委托第三方评测机构，定期开展符合性评测，三级工业互联网企业每年至少开展一次评测，二级工业互联网企业每两年至少开展一

次评测。一级工业互联网企业可参照二级企业相关要求开展评测。

第三章 网络安全管理及风险处置

第八条 企业网络安全责任

工业互联网企业承担本企业网络安全主体责任，企业主要负责人为本企业网络安全第一责任人，要建立健全企业内部网络安全管理制度，主动开展自主定级、安全建设、风险评估、安全整改和应急保障等工作，落实安全防护标准，有效应对网络安全风险，保障本企业工业互联网安全。积极将网络安全纳入企业发展规划和工作考核，加大网络安全投入，加强网络安全防护能力建设，有效防范化解网络安全风险。企业应当积极配合主管部门的监督管理。

第九条 重点企业

主管部门按照工业互联网企业级别，结合企业规模、业务范围、运营重要系统的程度等要素，制定云南省工业互联网网络安全风险防控重点企业名录，对名录内企业实施重点管理。重点企业要建立网络安全应急处置机制。建立网络安全监测预警和通报机制。三级工业互联网企业建设企业级工业互联网安全监测平台，鼓励二级工业互联网企业积极建设企业级工业互联网安全监测平台，鼓励基础电信企业、安全企业、安全评测机构等依托专业技术优势，提供安全服务，条件成熟后并接入我省相关监测管

理平台。

第十条 建立网络安全监测机制

监测处置工作参照《云南省公共互联网网络与数据安全威胁监测处置工作机制》进行。

（一）监测。主管部门建立健全工业互联网安全监测预警制度，建立安全评估评测机构队伍，按照职责分工对省内联网工业设备、系统等开展网络安全威胁监测、预警。工业互联网企业自行开展监测工作，对监测发现的公共互联网网络安全威胁，及时报送相关主管部门。

（二）威胁研判。主管部门组织技术支撑单位、信息通信行业网络安全应急保障专家队伍等专业机构对监测或收集到的威胁信息进行综合分析、验证、研判并提出处置意见。

（三）风险隐患通报。主管部门根据研判结果通知涉及的企业进行防范处置，出现重大问题、突发事件时，主管部门通报有关行业主管部门，按照既定规则联动处置。

（四）处置反馈。州（市）工业和信息化主管部门指导监督属地工业互联网企业，按通报要求于规定时限内完成整改，并将整改情况按通知渠道进行反馈。主管部门组织检查整改情况，实现闭环处置。

（五）未完成整改的情况处置。若工业互联网企业在规定时限内未完成整改或整改不到位的，主管部门将依照相关法律法规进行处理。

第十一条 应急处置

主管部门定期组织开展工业互联网安全演练，做好工业互联网安全事件应急处置工作。

工业互联网企业应当制定网络安全事件应急预案，定期开展安全演练，检验安全防护和应急处置能力。企业在网络安全事件发生后，立即启动应急预案，采取相应补救措施。发生一般及以上安全事件的，应当立即向主管部门报告。

第十二条 安全检查

云南省工业和信息化厅开展联网工业企业的安全评估，云南省通信管理局开展平台企业、标识解析企业的安全检查，对发现的网络安全风险隐患，指导企业加强安全整改。主管部门每年面向三级工业互联网企业开展安全检查评估，定期面向二级、一级工业互联网企业开展安全检查评估。

工业互联网企业应当配合主管部门开展网络安全检查评估。

第四章 支持与保障

第十三条 政策宣贯

主管部门加强工业互联网安全政策标准宣贯，充分利用大会、论坛等方式，提升工业互联网安全意识和能力，加强工业互联网人才培养力度，举办工业互联网安全相关赛事活动。

第十四条 政策支持

工业互联网企业要加强相关工作的执行落实，云南省工业和信息化厅结合企业相关工作的开展情况在评优评先、试点示范、考核检查等方面进行应用。云南省通信管理局发挥信息通信行业网络安全优势，加大对工业互联网企业网络安全定级、威胁监测处置，人才培养、创新示范试点项目申报的支持保障。

第十五条 总结会商

主管部门每年至少 1 次召开全体会议，分析总结当前工作，研究部署下一阶段工作任务。

第五章 附则

第十六条 处理依据

工业互联网企业不履行网络与数据安全保护义务的，主管部门按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规予以处理。

第十七条 施行日期

本细则自印发之日起施行。

