附件

工业互联网安全分类分级管理办法

（公开征求意见稿）

第一章　总　则

第一条 【目的依据】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，维护国家安全和发展利益，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》等法律法规及国家有关规定，制定本办法。

第二条 【适用范围】在中华人民共和国境内开展工业互联网安全分类分级管理工作的，应当遵守相关法律、行政法规和本办法的要求。

第三条 【职责分工】工业和信息化部统筹指导开展工业互联网安全分类分级管理工作，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主管行业领域。

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门（以下简称地方工业和信息化主管部门），各省、自治区、直辖市及计划单列市通信管理局（以下简称地方通信管理局）开展本行政区域内工业互联网安全

分类分级管理。地方工业和信息化主管部门主要负责指导本行政区域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。地方通信管理局主要负责开展本行政区域内平台企业、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。

地方工业和信息化主管部门、地方通信管理局统称地方主管部门。

第四条 【工作原则】工业互联网安全分类分级管理工作遵循统筹指导、分类施策、分级防护、突出重点的原则，指导企业提升安全防护能力。

第二章　企业分类分级

第五条 【企业分类】工业互联网安全分类分级管理以工业互联网企业为对象，企业类型主要包括以下三类:

（一）应用工业互联网的工业企业（以下简称联网工业企业），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（以下简称平台企业），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（以下简称标识解析企业），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。

第六条 【自主定级】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低分为三级、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。

第七条 【定级核查】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（以下简称分类分级管理平台）开展信息登记，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。地方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，应当通知企业在二十个工作日内予以补正。

第八条 【分级防护】工业互联网企业应当按照联网工业企业、平台企业、标识解析企业、数据等相关安全防护标准规范，根据企业类型、自身级别落实相适应的安全要求，

采取管理、技术等措施，提升相关设备、控制、网络、平台、数据等的安全防护能力。

第九条 【符合性评测】工业互联网企业应当按照工业互联网安全评测相关标准规范，自行或委托第三方评测机构，定期开展标准符合性评测，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。

第十条 【安全整改】工业互联网企业对不符合分类分级防护相关标准规范要求的，应当及时制定整改计划，落实整改措施。

第三章　网络安全管理

第十一条 【管理制度】工业和信息化部建立健全工业互联网安全分类分级管理制度体系，组织制定评估评测、信息通报、应急预案等相关制度，以及分类分级、安全管理、安全服务等相关标准，建立完善安全检查、监测预警、应急处置、成效评价等工作机制。

地方主管部门应当建立健全属地工业互联网安全分类分级管理制度机制，将工业互联网安全纳入重点工作任务，督促企业落实网络安全主体责任，强化重点企业指导管理，定期向工业和信息化部报送工业互联网安全管理工作情况。地方工业和信息化主管部门、通信管理局加强工作协同，共同做好工业互联网安全工作。

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，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。企业应当配合工业和信息化部、地方主管部门的监督管理。

第十二条 【监测预警和信息通报】工业和信息化部建立健全工业互联网安全监测预警和信息通报机制，建设国家级安全态势感知与风险预警手段，组织开展安全风险监测、预警和通报，加强威胁信息共享。

地方主管部门建立属地工业互联网安全监测预警机制，建设地方工业互联网安全技术平台，组织开展本行政区域内安全风险监测，及时向相关企业通报安全风险隐患，指导企业及时整改。

工业互联网企业应当根据自身级别，建设网络安全风险监测手段，有效发现网络安全风险隐患并及时处置。三级工业互联网企业按照有关标准，加强企业平台与国家、地方平台之间的协同联动。

第十三条 【应急处置和演练】工业和信息化部建立健全工业互联网安全应急处置制度机制，组织协调工业互联网重大及以上网络安全事件应急处置，开展工业互联网安全演练。

地方主管部门建立属地工业互联网安全应急处置制度，组织开展工业互联网安全演练，做好本行政区域内工业互联网安全事件应急处置工作，发现重大及以上安全事件，及时上报工业和信息化部。

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，应当立即向地方主管部门报告。

第十四条 【检查评估】工业和信息化部建立健全工业互联网安全检查评估机制，定期组织开展对工业互联网企业的安全检查评估。

地方工业和信息化主管部门开展本行政区域内联网工业企业的安全评估，地方通信管理局开展本行政区域内平台企业、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。地方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工业和信息化部、地方主管部门的网络安全检查评估。

第四章 支持与保障

第十五条 【地方保障】地方主管部门要加大人员投入和经费支持力度，加强工业互联网安全工作相关考核激励，建设工业互联网安全资源池，壮大属地安全支撑服务力量。

第十六条 【宣贯培训】地方主管部门要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。加强工业互联网安全人才培养力度，鼓励行业企业、联盟协会、研究机构等开展工业互联网安全人才培训和岗位能力评价，支持举办工业互联网安全相关赛事活动。

第十七条 【安全服务】工业和信息化部鼓励、支持具备相关专业能力的第三方机构、网络安全企业等依据相关标准，开展工业互联网安全检测评估、安全咨询、安全运维、人员培训等安全服务，推动工业互联网安全服务认证，规范安全服务要求，提高安全服务质量。

第十八条 【关键设备】工业和信息化部指导联网工业企业识别重要工业控制系统，推动将分布式控制系统（DCS）等纳入网络关键设备目录，支持开展工业控制系统和设备安全检测。

第十九条 【技术应用】工业和信息化部支持地方主管部门以及行业企业、研究机构、高等学校等，通过专项项目、试点示范等方式，加大工业互联网安全技术研发和成果转化应用，选树分类分级防护典型案例，推广工业互联网安全产品和服务。

第五章 附则

第二十条 【法律责任】工业互联网企业违反本办法规定，不履行网络和数据安全保护义务的，存在较大安全风险

或者发生安全事件的，工业和信息化部、地方主管部门可以按照《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。

第二十一条 【施行日期】本办法自2023年　月　日起施行。