

重庆市经济和信息化委员会等六部门 关于印发重庆市工业信息安全管理实施 办法（试行）的通知

渝经信规范〔2021〕1号

各区县（自治县）人民政府，市政府有关部门，有关单位：

为贯彻落实《中华人民共和国网络安全法》、《加强工业互联网安全工作的指导意见》（工信部联网安〔2019〕168号），建立健全工业信息安全工作机制，加强工业信息安全指导、监督和管理工作的，我们制定了《重庆市工业信息安全管理实施办法（试行）》，经市政府同意，现印发给你们，请认真贯彻实施。

重庆市经济和信息化委员会

中共重庆市委网络安全和
信息化委员会办公室

重庆市公安局

重庆市应急管理局

重庆市通信管理局

重庆市密码管理局

2021年2月8日

（此件公开发布）

重庆市工业信息安全管理实施办法（试行）

第一章 总 则

第一条 为加强全市工业信息安全保障和应急管理工作，落实企业工业信息安全主体责任，加快构建工业信息安全保障和应急体系，建立健全工业信息安全工作机制，提高应对工业信息安全事件的组织协调和应急处置能力，依据《中华人民共和国网络安全法》《中华人民共和国突发事件应对法》《中华人民共和国密码法》《国务院关于深化制造业与互联网融合发展的指导意见》《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》，以及工业和信息化部等十部门《加强工业互联网安全工作的指导意见》、工业和信息化部《工业控制系统信息安全事件应急管理工作指南》等法规政策，制定本办法。

第二条 本办法适用于全市工业信息安全有关的政府职能部门以及主体企业实施的工业信息安全管理相关工作。主体企业包括工业企业、生产性服务企业、工业互联网平台企业、工业互联网基础设施运营企业，以及水、电、气等生产企业。

第三条 工业信息安全事件是指由于人为、软硬件缺陷或故



重庆市经济和信息化委员会规范性文件

障、自然灾害等原因，对工业信息安全保护对象造成或者可能造成严重危害，影响正常工业生产的事件。

第四条 工业信息安全保护对象主要包括工业控制系统、工业互联网平台和工业互联网基础设施。其中，直接或间接连接互联网外网和对国计民生、经济发展有重大影响的，经市经济信息委会同相关部门评估，作为重要工业信息安全保护对象。

第五条 本办法所称工业控制系统包括主体企业的生产数字化设备、软件控制系统和信息管理系统，工业互联网平台包括提供第三方服务的工业互联网平台和主体企业的平台，工业互联网基础设施包括工业互联网标识解析节点、主体企业的数据中心和超算中心等。

第六条 坚持政府指导、企业主体，坚持预防为主、平战结合，坚持快速反应、科学处置，充分发挥各方力量，共同做好工控安全事件的预防和处置工作。

第二章 工作职责

第七条 市经济信息委、市通信管理局根据各自安全管理职责，负责贯彻落实工业和信息化部、市委、市政府关于工业信息安全的工作部署，指导全市工业信息安全管理，建立工业信



重庆市经济和信息化委员会规范性文件

息安全风险监测、态势研判、预警通报、应急管理、安全检查等工作体系，定期组织开展全市工业信息安全检查工作。按照工业和信息化部统一部署，依托重庆市工业互联网安全态势感知平台，市经济信息委牵头会同市通信管理局，支持建设重庆市工业信息安全发展中心。

第八条 区县经济信息主管部门负责本地区工业信息安全管理，建立本地区重要工业信息安全保护对象台账，并对相应主体企业进行监督管理，适时组织开展本地区工业信息安全检查工作。

第九条 主体企业负有本单位工业信息安全的主体责任，应结合实际做好本单位工业信息安全防护，建立健全工业信息安全责任制，负责本单位工业信息安全保障和应急管理工作，落实人、财、物保障。主体企业负责依法落实网络安全等级保护制度，开展定级备案、等级测评、商用密码应用安全性评估和安全建设整改等工作。

第三章 工作机制

第十条 市经济信息委会同相关部门组织开展工业信息安全保护对象的重要性评估工作，形成重要工业信息安全保护对象



重庆市经济和信息化委员会规范性文件

清单，实施差异化管理机制，并指导区县经济信息主管部门做好工业信息安全管理 and 主体企业分级分类管理。

第十一条 市经济信息委负责推进工业信息安全技术支撑队伍建设，培育发展一批本地工业信息安全技术支撑机构（以下简称“技术支撑机构”），加强工业信息安全市场化服务供给，构建工业信息安全事件应急处置的技术支撑预备力量。

第十二条 建立涵盖市委网信办、市经济信息委、市公安局、区县网信主管部门、区县经济信息主管部门、区县公安主管部门、技术支撑机构、主体企业的工业信息安全联络员机制，明确工业信息安全的工作负责人和应急联络员。

第十三条 市委网信办、市经济信息委、市公安局指导技术支撑机构、主体企业等建立工业信息安全应急值守机制，必要时实行领导带班、专人值守工作制度，做好工业信息安全保护对象的安全风险、威胁和事件信息日常监测和报告工作。应急响应状态下，可实行“7×24”小时值守工作制度，加强安全监测、信息收集与研判、应急处置等工作。

第四章 监测预警

第十四条 重庆市工业互联网安全态势感知平台将重要工



业信息安全保护对象纳入日常线上监测范围，在互联网外网上开展安全风险监测、探测扫描、威胁分析等工作，并加强与市网络与信息安全信息通报中心的数据对接，实现信息数据共享。主体企业应对本单位重要工业信息安全保护对象进行重点防护和监测，结合实际定期开展检查、维护。

第十五条 针对中央网信办、工业和信息化部、公安部发布的可能影响我市工业信息安全保护对象的重大漏洞、威胁和风险隐患的情况，市委网信办、市经济信息委、市公安局、市通信管理局及时向有关区县网信主管部门、区县经济信息主管部门、区县公安主管部门和主体企业进行预警通报。

第十六条 主体企业应对市委网信办、市经济信息委、市公安局、市通信管理局和区县网信主管部门、区县经济信息主管部门、区县公安主管部门预警通报的情况和问题高度重视，及时自查、整改，必要时采取应急处置措施。

第五章 重保时期安全保障

第十七条 在国家和重庆市重要活动、会议等重保时期，市经济信息委指导区县经济信息主管部门、主体企业做好工业信息安全事件预防和应急管理工作，并配合工业和信息化部、市委、



市政府的统一部署。

第十八条 在国家和重庆市重要活动、会议等重保时期，区县经济信息主管部门、主体企业应加强重要工业信息安全保护对象的安全监测、预警和风险研判，对可能造成重大影响的风险和事件信息应第一时间上报。必要时，实行 24 小时零报告制度，重点单位、重要部位实施 24 小时值守，保持通信联络畅通。主体企业应加强对重要工业信息安全保护对象的防护和巡查，原则上不在重保时期对重要工业信息安全保护对象进行调整或升级。

第六章 应急处置

第十九条 市经济信息委牵头制定《重庆市工业信息安全事件应急预案》，建立市、区县、主体企业三级工业信息安全事件应急响应机制，明确工业信息安全事件分级处置细则。主体企业应制定本单位的工业信息安全事件应急预案。

第二十条 对于可能发生或已经发生的工业信息安全事件，主体企业应立即开展先期处置，并按照职责和规定权限启动相关应急预案，采取科学有效方法及时处置，控制事态发展，力争将损失降到最低，尽快恢复受损工业信息安全保护对象的正常运行。



第二十一条 对于发生的工业信息安全事件或重大风险隐患、异常安全威胁等，主体企业应逐级上报区县经济信息主管部门、区县网信主管部门、区县公安主管部门、市经济信息委、市委网信办、市公安局等相关部门，并积极配合研判和应急处置，不得瞒报、谎报。对因瞒报、谎报，造成严重后果的，依法进行处理。

第二十二条 工业信息安全事件的应急处置结束后，相关主体企业要尽快消除事件影响，恢复正常生产，进一步加强安全防护，做好事件分析总结。

第七章 保障措施

第二十三条 市经济信息委、区县经济信息主管部门、主体企业应结合实际，组织开展应急演练。

第二十四条 市经济信息委牵头建立重庆市工业信息安全专家组，为工业信息安全保障和应急工作提供技术咨询和决策支持。区县经济信息主管部门可结合实际组建本地区工业信息安全专家组，充分发挥专家作用，做好本地区工业信息安全保障和应急工作。

第二十五条 加强对工业信息安全事件应急装备和工具的



储备，及时调整、升级软硬件工具，利用信息化手段建立应急物资调度和保障机制，不断增强应急技术支撑能力。

第二十六条 加强工业信息安全政策资金保障，优化现有政策，支持工业信息安全技术支撑机构建设、专家队伍建设、基础平台建设、技术研发、应急演练、物资保障等。支持主体企业利用新一代信息技术，加强企业的工业信息安全建设，提升安全防护能力。

第八章 附则

第二十七条 涉及国家秘密、个人隐私与商业秘密的工业信息安全保护对象的安全管理，按照有关法律法规执行。

第二十八条 本办法自发布之日起三十日后施行。