中华人民共和国交通运输部令
2023年第20号

《铁路关键信息基础设施安全保护管理办法》已于2023年12月1日经第27次部务会议通过，现予公布，自2024年2月1日起施行。

部长（签名章）

2023年12月17日

铁路关键信息基础设施安全保护管理办法

第一章 总　则

第一条　为了保障铁路关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》等法律、行政法规，制定本办法。

第二条　铁路关键信息基础设施的安全保护和监督管理工作，适用本办法。

本办法所称铁路关键信息基础设施，是指在铁路领域，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益的重要网络设施、信息系统等。

第三条　国家铁路局是负责铁路领域关键信息基础设施安全保护工作的部门，在职责范围内负责全国铁路关键信息基础设施安全保护和监督管理工作。

地区铁路监督管理局按照国家铁路局要求，开展本辖区铁路关键信息基础设施的安全保护和监督管理工作。

第四条　铁路关键信息基础设施安全保护坚持强化和落实铁路关键信息基础设施运营者（以下简称运营者）主体责任，加强和规范保护工作部门监督管理，发挥社会各方面的作用，共同保护铁路关键信息基础设施安全。

第五条　任何个人和组织不得实施非法侵入、干扰、破

坏铁路关键信息基础设施的活动，不得危害铁路关键信息基础设施安全。

第二章　铁路关键信息基础设施认定

第六条　国家铁路局负责制定铁路关键信息基础设施认定规则，并报国务院公安部门备案，抄送国家网信部门。

制定认定规则应当主要考虑下列因素:

（一）网络设施、信息系统等对于铁路关键核心业务的重要程度;

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度;

（三）对其他行业和领域的关联性影响。

第七条　国家铁路局根据认定规则，负责组织认定铁路关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门，抄送国家网信部门。

第八条　铁路关键信息基础设施发生改建、扩建、运营者变更等较大变化，可能影响认定结果的，运营者应当及时将相关情况报告国家铁路局。国家铁路局自收到报告之日起3 个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门，抄送国家网信部门。

第三章　运营者责任和义务

第九条 铁路关键信息基础设施的网络安全保护等级应当不低于第三级。

运营者应当依照有关法律、行政法规的规定以及国家标准的强制性要求，在国家网络安全等级保护制度的基础上，突出保护重点，落实防护措施，加强全生命周期管理，保障铁路关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第十条 新建、改建、扩建铁路关键信息基础设施的，运营者应当做到安全防护措施与关键信息基础设施同步规划、同步建设、同步使用，并采取检测评估、安全演练等方式验证安全保护措施的有效性。

第十一条 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。

运营者的主要负责人对所运营的铁路关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

运营者应当为每个铁路关键信息基础设施明确安全管理责任人。

第十二条 运营者应当设置专门安全管理机构，保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

运营者应当对专门安全管理机构负责人和关键岗位人员进行安全背景审查。专门安全管理机构的负责人和关键岗

位人员的身份、安全背景等发生变化或者必要时，运营者应当根据情况重新进行安全背景审查。

第十三条 专门安全管理机构具体负责本单位的铁路关键信息基础设施安全保护工作，履行下列职责：

（一）建立健全网络安全管理、评价考核制度，拟订铁路关键信息基础设施安全保护计划；

（二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

（三）按照国家及铁路行业要求，制定本单位网络安全事件应急预案，定期开展应急演练，处置网络安全事件；

（四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

（五）组织网络安全教育、培训；

（六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

（七）对铁路关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

（八）按照规定报告网络安全事件和重要事项。

第十四条 运营者应当加强铁路关键信息基础设施供应链安全保护，优先采购安全可信的网络产品和服务。运营者采购网络产品和服务，应当预判该产品和服务投入使用后对国家安全的影响。可能影响国家安全的，应当按照国家有关规定申报网络安全审查。

第十五条 运营者应当加强数据安全保护，明确重要数

据和个人信息的保护措施，将在我国境内运营中收集和产生的个人信息和重要数据存储在境内。因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估。法律、行政法规另有规定的，依照其规定执行。

第十六条 运营者应当自行或者委托网络安全服务机构对铁路关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照国家铁路局要求报送情况。

第十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的铁路关键信息基础设施，运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估。

商用密码应用安全性评估应当与铁路关键信息基础设施安全检测和风险评估、网络安全等级测评制度相衔接，避免重复评估、测评。

第十八条 运营者应当加强全过程保密管理，采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第十九条 运营者应当制定本单位的监测预警和信息通报制度，加强对铁路关键信息基础设施监测，研判整体安全态势。

第二十条 铁路关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规

定向国家铁路局、公安机关报告，并立即启动本单位网络安全事件应急预案。

铁路关键信息基础设施发生特别重大网络安全事件或者发现特别重大网络安全威胁时，国家铁路局应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

第二十一条 运营者发生合并、分立、解散等情况，应当及时报告国家铁路局，并按照国家铁路局的要求对铁路关键信息基础设施进行处置，确保安全。

第四章 保障和监督

第二十二条 国家铁路局应当制定铁路关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

第二十三条 国家铁路局应当依托国家网络安全信息共享机制，组织建立铁路关键信息基础设施网络安全监测预警制度，及时掌握铁路关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

第二十四条 国家铁路局应当组织建立健全铁路关键信息基础设施网络安全事件应急预案体系，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

第二十五条 国家铁路局定期组织开展铁路关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全

隐患、完善安全措施。

检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

第二十六条 运营者对国家铁路局依法开展的网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的铁路关键信息基础设施网络安全检查工作应当予以配合。

第二十七条 国家铁路局、网络安全服务机构及其工作人员对于在铁路关键信息基础设施安全保护过程中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售、非法向他人提供或者进行其他违法活动。

第五章 法律责任

第二十八条 运营者违反本办法规定的，由国家铁路局依照《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》等法律、行政法规的规定予以处罚。

第二十九条 国家铁路局及其工作人员存在下列情形之一的，按照有关法律、行政法规的规定予以处分:

（一）未履行铁路关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的;

（二）在开展铁路关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生

产、销售单位的产品和服务的;

（三）将在铁路关键信息基础设施安全保护工作中获取的信息泄露、出售、非法向他人提供或者进行其他违法活动的。

第六章　附　则

第三十条　本办法自 2024 年 2 月 1 日起施行。