

# 山西省能源局 山西省公安厅

## 文件

晋能源信监发〔2021〕92号

---

## 山西省能源局 山西省公安厅 关于印发《煤炭企业网络安全等级保护工作 管理办法（试行）》的通知

各市能源局、市公安局：

为深入贯彻落实国家网络安全等级保护制度和关键信息基础设施安全保护制度，根据《中华人民共和国网络安全法》《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，省能源局会同省公安厅联合制定了《煤炭企业网络安全

等级保护工作管理办法（试行）》，现予以印发，请遵照执行。



# 煤炭企业网络安全等级保护工作管理办法

(试行)

## 第一章 总 则

**第一条** 为深入贯彻落实网络安全等级保护制度，规范全省煤炭企业网络基础设施、信息系统、智能化工业控制系统等网络在新技术、新应用情况下网络安全等级保护工作的有序开展，提高全省煤炭企业网络安全保障能力和水平，根据《中华人民共和国网络安全法》《信息安全等级保护管理办法》《网络安全等级保护基本要求》等法律法规、标准和规范，制定本办法。

**第二条** 山西省行政区域内的煤炭企业建设、运营、维护、使用的网络，开展网络安全等级保护工作及监督管理，适用本办法。

本办法所称煤炭企业，是指在山西省行政区域内依法批准的从事煤炭资源开采、洗选加工的企业，包括各煤炭企业的上级集团公司。

**第三条** 全省煤炭企业在网络建设和运营过程中，应当依照法律、行政法规和国家标准要求，实施分等级保护、分等级监管，坚持“分级保护、突出重点，常态监督、综合防护，同步建设、动态调整”的原则，落实网络安全保护管理制度和技术措施。

**第四条** 根据国家标准，各煤炭企业建设、运营、维护、使用

的网络，网络安全保护等级依次分为以下五级：

第一级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益；

第二级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全；

第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害；

第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害；

第五级，等级保护对象受到破坏后，会对国家安全造成特别严重危害。

## 第二章 工作职责

**第五条** 各级能源主管部门负责组织、协调、指导和监督煤炭企业依法开展网络安全等级保护工作，督促煤炭企业落实网络安全主体责任，监督检查煤炭企业网络安全等级保护制度落实情况；市级及以上能源主管部门负责对各煤炭企业网络安全等级保护定级对象及安全保护等级确定工作进行审核。

**第六条** 各级公安机关负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫。

**第七条** 煤炭企业是网络建设、运营、维护和使用的主体，应当依法履行下列安全保护义务，保障网络和信息安全：

（一）确定网络安全等级保护工作责任人，建立网络安全等级保护工作责任制，落实责任追究制度；

（二）建立安全管理和技术保护制度，建立人员管理、教育培训、系统安全建设、系统安全运维等制度；

（三）落实机房安全管理、设备和介质安全管理、网络安全管理等制度，制定操作规范和工作流程；

（四）落实身份识别、防范恶意代码感染传播、防范网络入侵攻击的管理和技术措施；

（五）落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，并按照规定留存 6 个月以上可追溯网络违法犯罪的相关网络日志；

（六）落实数据分类、重要数据备份和加密等措施；

（七）依法收集、使用、处理个人信息，并落实个人信息保护措施，防止个人信息泄露、损毁、篡改、窃取、丢失和滥用等；

（八）落实违法信息发现、阻断、消除等措施，落实防范违法信息大量传播、违法犯罪证据灭失等措施；

（九）落实联网备案和用户真实身份查验等责任；

(十) 对网络中发生的案(事)件,应当在24小时内向属地公安机关报告;泄露国家秘密的,应当同时向属地保密行政管理部门报告;

(十一) 法律、行政法规规定的其他网络安全保护义务。

**第八条** 第三级及以上网络运营的煤炭企业,除履行本办法第七条规定的网络安全保护义务外,还应履行下列安全保护义务:

(一) 确定网络安全管理机构,设立首席网络安全官,明确网络安全等级保护的工作职责,对网络变更、网络接入、运维和技术保障单位变更等事项建立逐级审批制度;

(二) 制定并落实网络安全总体规划和整体安全防护策略,制定安全建设方案,并经专业技术人员评审通过;

(三) 对网络安全管理负责人和关键岗位的人员进行安全背景审查,落实持证上岗制度;

(四) 对为煤炭企业提供网络设计、建设、运维和技术服务的机构和人员进行安全管理;

(五) 落实网络安全态势感知监测预警措施,建设网络安全防护管理平台,对网络运行状态、网络流量、用户行为、网络安全案(事)件等进行动态监测分析;

(六) 落实重要网络设备、通信链路、系统的冗余、备份和恢复措施;

(七) 建立网络安全等级测评制度,定期开展等级测评,并

将测评情况及安全整改措施、整改结果向公安机关和有关部门报告；

(八) 法律、行政法规规定的其他网络安全保护义务。

### 第三章 组织实施

**第九条** 网络建设、运营、维护、使用的煤炭企业应当按照《网络安全等级保护实施指南》具体实施等级保护工作。

**第十条** 煤炭企业已运营（运行）的网络，须根据国家规定确定安全保护等级，并组织专家开展定级评审；在专家出具评审意见后，确定安全保护等级为第二级及以上的网络，须在 30 日内报请主管部门审核后，并至设区的市级及以上公安机关办理备案手续。

**第十一条** 煤炭企业新建网络，须在网络规划设计阶段根据国家规定确定安全保护等级，并组织专家开展定级评审；在专家出具评审意见后，确定为安全保护等级第二级及以上的网络，须在安全保护等级确定后 5 个工作日内，报请主管部门审核，并在收到审核意见后，按照国家网络安全管理规范和技术标准进行建设；安全保护等级确定后 30 日内，须到设区的市级及以上公安机关办理备案手续。

**第十二条** 煤炭企业网络建设项目实行工程监理制，项目建设

单位应当按照信息系统工程监理有关规定，委托信息工程监理单位对项目建设进行工程监理。

**第十三条** 煤炭企业跨设区的市或者全省统一联网运行的网络，由省级能源主管部门统一拟定安全保护等级，统一组织定级评审。

**第十四条** 主管部门在收到煤炭企业提交的审核申请后，依法对定级情况和专家评审意见进行审核；对定级准确、评审意见符合等级保护要求的，应当在收到审核申请后 5 个工作日内出具《网络安全等级保护审核意见书》；对不符合等级保护要求的，应当在收到审核申请之日起 5 个工作日内通知企业予以改正；发现定级不准的，应当在收到审核申请之日起 5 个工作日内通知企业重新确定等级。

**第十五条** 公安机关在收到煤炭企业提交的备案申请后，依法对备案材料进行审核；对定级准确、备案材料符合等级保护要求的，应当在收到备案申请后 10 个工作日内颁发《网络安全等级保护备案证明》；对不符合等级保护要求的，应当在收到备案申请之日起 10 个工作日内通知企业予以纠正；发现定级不准的，应当在收到备案申请之日起 10 个工作日内通知企业重新审核确定等级。

**第十六条** 煤炭企业建设、运营、维护、使用网络的功能、服务范围、服务对象和处理的数据等发生重大变化时，应当依法变更网络的安全保护等级，重新确定网络安全保护等级后，须按照

本办法向能源主管部门和公安机关重新申请审核、备案。

因网络撤销或变更调整安全保护等级的，须当网络撤销或变更调整后 10 个工作日内向原受理审核的能源主管部门和受理备案的公安机关办理备案撤销或变更手续。

**第十七条** 煤炭企业新建的安全保护等级为第三级及以上的网络上线运行前，应当委托符合国家有关规定的第三方网络安全等级测评机构，按照网络安全等级保护有关标准规范进行等级测评，通过等级测评后方可投入运行；对云计算、移动互联、物联网、工业控制、大数据等新技术、新应用，测评过程中要在安全通用要求的基础上满足安全扩展要求。

**第十八条** 煤炭企业应当对其安全保护等级为第二级的网络每两年至少开展一次网络安全等级保护测评；对其安全保护等级为第三级的网络每年至少开展一次网络安全等级保护测评；对其安全保护等级为第四级的网络每半年至少开展一次网络安全等级保护测评；对其安全保护等级为第五级的网络应当依据特殊安全需求进行网络安全等级保护测评。对等级测评中发现的安全风险隐患，煤炭企业须制定整改方案、落实整改措施、消除风险隐患，并将开展网络安全等级测评的工作情况及测评结果向审核、备案的能源主管部门和公安机关报备。

**第十九条** 煤炭企业应当每年至少对本单位落实网络安全等级保护制度情况和网络安全状况开展一次自查，发现安全风险隐

患及时整改。

**第二十条** 第三方网络安全等级测评机构应当为煤炭企业提供安全、客观、公正的等级测评服务；应当与煤炭企业签署服务协议，并对测评人员进行安全保密教育，与其签订保密责任书，明确测评人员的安全保密义务和法律责任。

**第二十一条** 第三方网络安全等级测评机构等网络服务提供者应当保守服务过程中知悉的煤炭企业重要数据；不得非法使用或擅自发布、披露在提供服务中收集掌握的煤炭企业数据信息和系统漏洞、恶意代码、网络入侵攻击等网络安全信息。

**第二十二条** 网络服务提供者 of 煤炭企业提供网络建设、运行维护、安全监测、数据分析等网络服务，应当符合国家有关法律法规和技术标准的要求。

**第二十三条** 煤炭企业的生产控制系统与其他系统须做好边界划分和防护，且采用隔离手段进行隔离，禁止任何穿越边界的网络服务；实时控制和数据传输的生产控制系统须使用独立的网络设备组网，与其他系统采用物理隔离；生产控制系统涉及无线传输的，无线终端须进行唯一标识和鉴别，并采取加密传输的安全措施。

**第二十四条** 煤炭企业应当采购、使用符合国家法律法规和有关标准规范要求的网络产品和服务。

煤炭企业安全保护等级为第三级及以上网络，应当采用与其

安全保护等级相适应的网络产品和服务；对重要部位使用的网络产品，应当委托专业测评机构进行专项测试，根据测试结果选择符合要求的网络产品。

**第二十五条** 煤炭企业安全保护等级为第三级及以上的网络应当选择使用符合以下条件的信息安全产品：

（一）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；

（二）产品的核心技术、关键部件具有中国自主知识产权；

（三）产品研制、生产单位及其主要业务、技术人员无犯罪记录；

（四）产品研制、生产单位须声明没有故意留有或者设置漏洞、后门、木马等程序和功能；

（五）对国家安全、社会秩序、公共利益不构成危害；

（六）对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

**第二十六条** 煤炭企业安全保护等级为第三级及以上网络应当在境内实施技术维护，不得境外远程技术维护；因业务需要，确需进行境外远程技术维护的，应当进行网络安全评估，并采取风险管控措施；实施技术维护，应当记录并留存技术维护日志，并在公安机关检查时如实提供。

**第二十七条** 煤炭企业应当建立并落实重要数据和个人信息

安全保护制度；采取保护措施，保障数据和信息在收集、存储、传输、使用、提供、销毁过程中的安全；建立异地备份恢复等技术措施，保障重要数据的完整性、保密性和可用性。

**第二十八条** 煤炭企业应当按照国家有关规定，制定网络安全应急预案，定期开展网络安全应急演练。

煤炭企业处置网络安全事件时应当保护现场，记录并留存相关数据信息，并及时向能源主管部门和公安机关报告。

## 第四章 监督管理

**第二十九条** 县级以上能源主管部门监督指导煤炭企业依照网络安全等级保护制度和相关标准规范要求，落实网络安全管理和技术保护措施，开展网络定级备案、等级测评、安全建设整改、安全自查、网络安全防范、重大活动网络安全保护等工作。

**第三十条** 县级及以上公安机关对煤炭企业依照国家法律法规要求，落实网络安全等级保护制度，开展网络安全防范、网络安全事件应急处置、重大活动网络安全保护等工作，实行监督管理。

**第三十一条** 县级及以上能源主管部门和公安机关可依法对煤炭企业开展下列网络安全工作情况进行检查：

（一）网络安全管理制度、措施的落实情况，日常网络安全

防范工作情况；

（二）网络需求是否发生变化，原定保护等级是否准确；

（三）备案材料与运营使用单位、系统的符合情况，网络安全产品使用是否符合要求；

（四）网络安全等级测评情况，安全风险隐患整改情况；

（五）网络安全事件应急处置和恢复工作情况；

（六）重大活动网络安全保护工作落实情况；

（七）其他应当进行监督检查的事项。

**第三十二条** 国家对网络安全等级保护测评机构实行推荐目录管理，各煤炭企业应当委托符合国家有关规定的第三方网络安全等级测评机构开展等级测评工作。

**第三十三条** 省级能源主管部门和公安机关在履行网络安全等级保护监督管理职责中，发现煤炭企业网络存在较大安全风险隐患或者发生安全事件的，可以约谈煤炭企业的法定代表人、主要负责人。

**第三十四条** 各级能源主管部门和公安机关要加强对煤炭企业网络安全等级保护工作的监督检查，对检查中发现的问题要责令煤炭企业采取措施立即消除；不能立即消除的，应当依法责令其限期改正并给予警告；拒不改正或导致危害网络安全后果，构成犯罪的，依法予以处罚；构成犯罪的，依法追究刑事责任。

## 第五章 附 则

**第三十五条** 本办法下列用语的含义：

网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

信息系统，是指计算机或者其它信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、工业控制系统和采用移动互联技术的系统等。

网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

工业控制系统，是指包括多种工业生产中使用的控制系统，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）等控制系统。

智能煤矿，是指将人工智能、工业物联网、云计算、大数据、机器人、智能装备等与现代煤炭开发利用深度融合，形成全面感

知、实时互联、分析决策、自主学习、动态预测、协同控制的智能系统，实现煤矿开拓、采掘（剥）、运输、通风、安全保障、经营管理等过程的智能化运行。

**第三十六条** 本办法由山西省能源局和山西省公安厅负责解释，自发布之日起实施。

(信息公开形式：主动公开)

---

抄送：省应急厅。

---

山西省能源局

2021年3月1日印发

---