晋城市人民政府办公室文件

晋市政办〔2021〕43号

晋城市人民政府办公室
关于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实施意见

各县（市、区）人民政府、开发区管委会，市人民政府各委、办、局：

为贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《公安部 国家保密局 国家密码管理局 国务院信息化工作办公室关于印发〈信息安全等级保护管理办法〉的通知》（公通字〔2007〕43号）、《公安部关于印送〈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〉的函》（公网安〔2020〕1960号）要求，严格落实网络安全等级保护和关键信息基础设施安全保护制度，大力推进重要

网络系统运营、使用单位（以下简称网络运营者）网络安全等级保护定级备案、等级测评、建设整改等工作，切实保障关键信息基础设施、重要网络和数据安全，消除各类网络安全隐患，为经济社会发展创造和谐稳定的网络环境，结合我市工作实际，特制定本实施意见。

一、指导思想

以习近平总书记关于网络强国的重要思想为指引，按照党中央、国务院和省委、省政府，市委、市政府有关决策部署要求，坚持以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为基础，以保护关键信息基础设施、重要网络和数据安全为重点，全面加强网络安全设施建设、防范管理、监测预警、应急处置、侦查打击、情报信息等各项工作，为促进我市经济社会信息化安全有序发展提供坚实保障。

二、总体目标

网络安全等级保护定级备案、等级测评、安全建设和执法检查等基础工作全面开展。网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施得到有效落实。关键信息基础设施的数据安全、人员管理、应急处置等重点安全保护措施全面落实。网络安全监测预警、应急处置能力和综合防护能力明显提升，网络环境实现有效治理，基本建成党委领导、政府主导、部门负责、社会参与的“打防管控”一体化网络安全综合防控体系。

三、工作任务

（一）深入贯彻实施国家网络安全等级保护制度

1.全面推进网络定级备案工作。网络运营者要全面梳理本单位各类网络、系统，特别是云计算、物联网、新型互联网、大数据、智能制造等新技术应用的基本情况，依据《信息安全技术网络安全等级保护实施指南》《信息安全技术网络安全等级保护定级指南》等国家标准，在规划设计阶段确定网络的安全保护等级。对拟定为第二级（含）以上的网络，运营者应当组织专家评审，有行业主管部门的，应当在评审后报请主管部门核准；第二级（含）以上网络运营者应当在网络安全保护等级确定后10个工作日内到公安机关备案。因网络撤销或变更调整安全保护等级的，应当在10个工作日内向原备案公安机关办理备案撤销或变更手续。公安机关应当对网络运营者提交的备案材料进行审核，对定级准确、备案材料符合要求的，应在10个工作日内出具网络安全等级保护备案证明。

2.定期开展网络安全等级测评。网络运营者要依据《信息安全技术网络安全等级保护基本要求》等国家标准，委托符合国家有关规定的等级测评机构定期对已定级备案网络的安全性进行检测评估，查找可能存在的网络安全问题和隐患，并及时将等级测评报告提交公安机关和行业主管部门。第三级（含）以上网络的运营者应当每年开展一次网络安全等级测评，新建的第三级（含）以上网络应在通过等级测评后投入运行；鼓励第二级

网络的运营者每两年开展一次网络安全等级测评。在开展安全等级测评服务过程中，网络运营者要与等级测评机构签署安全保密协议，并对等级测评全过程进行监督管理。市公安局要按照公安部《网络安全等级保护测评机构管理办法》（公信安〔2018〕765号）要求，加强对等级测评机构在本行政辖区内测评活动的监督管理，建立测评人员背景审查和人员审核制度，确保等级测评过程客观、公正、安全，发现违规情形的，要及时报省、市网络安全等级保护工作领导小组办公室。

3.持续推进网络安全建设整改。网络运营者特别是电子政务类大数据中心、云平台、重要信息系统运营单位应在网络建设和运营过程中，同步规划、同步建设、同步使用有关网络安全保护措施，要在现有安全保护措施的基础上，结合等级测评发现的问题隐患，对照《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护安全设计技术要求》等国家标准，认真开展等级保护安全建设和整改加固工作，全面落实安全保护技术措施，建立完善网络安全管理制度。公安机关要针对测评结果中存在风险隐患的单位开展网络安全督导检查，确保相关网络运营者及时对网络安全风险隐患进行整改加固，切实提高网络安全防护能力。

4.加强供应链安全管理。网络运营者要加强网络关键人员的安全管理，第三级（含）以上网络运营者要对为其提供设计、建设、运维、技术服务的机构和人员加强管理，评估服务过程中可

能存在的安全风险，并采取相应的管控措施。网络运营者要加强网络运维管理，因业务需要确需通过互联网远程运维的，要进行评估论证，并采取相应的管控措施。网络运营者要采购、使用符合国家法律法规和有关标准规范要求的网络产品及服务，第三级（含）以上网络运营者应积极使用安全可信的网络产品及服务。市公安局要主导建立网络安全服务公司报备制度，对在我市开展系统研发、集成、运维业务的公司及技术人员进行背景审查，各级各部门要在开展相关信息化建设时，主动要求参与建设的网络安全服务公司到市公安局报备。

5. 落实密码安全防护要求。网络运营者要认真贯彻落实《中华人民共和国密码法》等有关法律法规规定和密码应用相关标准规范。第三级（含）以上网络运营者要正确、有效采用密码技术对网络系统进行保护，使用符合相关要求的密码产品和服务。第三级（含）以上网络运营者要在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

（二）加强关键信息基础设施安全保护

6. 关键信息基础设施的认定及职能分工。重要行业和领域的主管部门、监督管理部门（以下简称保护工作部门）要按照国家有关要求，根据本行业、本领域的关键信息基础设施认定规则，组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并向公安机关报告。在网信部门统筹协调下，公安、

国家安全、保密、密码管理等部门单位按照职责分工负责关键信息基础设施安全保护和监督管理工作；保护工作部门负责对本行业、本领域关键信息基础设施安全保护工作的组织领导，落实本行业、本领域网络安全指导监督责任；关键信息基础设施运营者要设置专门安全管理机构，组织开展关键信息基础设施安全保护工作，主要负责人对本单位关键信息基础设施安全保护负总责。

7.落实关键信息基础设施重点防护措施。关键信息基础设施运营者要依据网络安全等级保护标准，开展安全建设并进行等级测评，发现问题和风险隐患要及时整改；依据关键信息基础设施安全保护标准，加强安全保护和保障，并进行安全检测评估。要梳理网络资产，建立资产档案，强化核心岗位人员管理、整体防护、监测预警、应急处置、数据保护等重点保护措施，合理分区分域，收敛互联网暴露面，加强网络攻击威胁管控，强化纵深防御，积极利用新技术开展网络安全保护，构建以密码技术、可信计算、人工智能、大数据分析等为核心的网络安全保护体系，不断提升关键信息基础设施内生安全、主动免疫和主动防御能力。有条件的关键信息基础设施运营者要组建自己的安全服务机构，承担关键信息基础设施安全保护任务，鼓励通过迁移上云或购买安全服务等方式，提高网络安全专业化、集约化保障能力。

8.加强重要数据和个人信息保护。关键信息基础设施运营者要建立并落实重要数据和个人信息安全保护制度，加强数据安全风险评估，对关键信息基础设施中的重要网络和数据库进行容

灾备份，采取身份鉴别、访问控制、密码保护、安全审计、安全隔离、可信验证等关键技术措施，切实保护重要数据全生命周期安全。关键信息基础设施运营者在境内运营中收集和产生的个人信息和重要数据要在境内存储，因业务需要，确需向境外提供的，要遵守有关规定并进行安全评估。

9.强化核心岗位人员和产品服务的安全管理。关键信息基础设施运营者要对本单位专门安全管理机构的负责人和关键岗位人员进行安全背景审查，加强管理。要对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，采购安全可信的网络产品和服务，确保供应链安全。当采购产品和服务可能影响国家安全的，要按照国家有关规定通过安全审查。公安机关要依托网络安全服务机构的报备制度，加强对关键信息基础设施安全服务机构和人员的安全管理，为关键信息基础设施运营者开展安全保护工作提供支持。

（三）强化网络安全保护工作协作配合

10.实施网络安全立体化监测体系建设。各级各部门要全面加强网络安全监测，对关键信息基础设施、重要网络等开展实时监测，发现网络攻击和安全威胁，立即报告属地公安机关和有关部门，并采取有效措施处置；邀请第三方技术公司开展监测时，要提前向公安机关报备。网络运营者、关键信息基础设施运营者要根据系统承载业务重要性的不同，主动与公安机关对接，在单位互联网出口部署监测设备，将相关流量数据汇入公安机关网络

安全技术平台，开展实时监测、通报预警、应急处置、安全防护、指挥调度等工作。公安机关每年要组织技术力量对全市重点网络、重要系统和关键信息基础设施开展安全监测和应急处置工作，建立常态化、实战化的网络安全监测机制。

11.加强网络安全信息共享和通报预警。晋城市网络与信息安全通报中心要充分发挥职能作用，加强全市网络安全信息通报预警力量建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报预警和处置。网络运营者要建立网络安全监测预警机制，发现预警信息和网络安全事件，及时向备案公安机关报告。

12.完善网络安全应急处置机制。网络运营者要与公安机关密切配合，建立网络安全事件报告制度和应急处置机制。第三级（含）以上网络运营者和关键信息基础设施运营者要定期开展应急演练，有效处置网络安全事件，并针对应急演练中发现的突出问题和漏洞隐患，及时整改加固，完善保护措施。公安机关要每年针对全市重点网络、重要系统和关键信息基础设施组织开展网络攻防应急演练，全面检验各网络运营者和关键信息基础设施运营者的安全防护、监测预警和应急处置能力，并针对演练中发现的突出问题和漏洞隐患，及时督促整改加固，完善保护措施，不断提升安全保护能力和对抗能力。

13.强化网络安全隐患整改督办、事件处置和案件侦办。市公安局建立挂牌督办制度，针对网络运营者安全保护工作不力、

重大安全问题隐患久拖不改，或存在较大网络安全风险、发生重大网络安全案（事）件的，按照规定的权限和程序，会同保护工作部门挂牌督办，并加大监督检查和行政执法力度，依法依规进行行政处罚，同时保护工作部门要组织本行业、本领域开展整改整顿。网络运营者要按照有关要求采取措施，及时进行整改，消除重大风险隐患。电信业务经营者、网络服务提供者要配合公安机关对发生的重大网络安全威胁和事件开展调查处置，要为公安机关打击网络违法犯罪活动提供技术支持和协助；网络运营者在发现违法犯罪线索、重大网络安全威胁和事件时，要及时报告属地公安机关和有关部门并提供必要协助。

14.强化网络安全自查和监督检查。网络运营者要定期对网络安全保护状况、安全保护制度及技术措施的落实进行自查，对发现存在的安全问题要及时整改。公安机关要依法对网络运营者及各子系统运营者开展监督检查，重点检查《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国密码法》《中华人民共和国计算机信息系统安全保护条例》等法律法规落实情况；网络安全领导机构、专门管理部门、人员配备、管理制度、相关保障及网络安全责任制落实情况；网络安全监测、网络安全应急预案制定和演练情况；网络安全状况和重大事件报告、等级测评、风险评估、重大风险隐患和问题的处置及责任追究情况；重要数据和公民个人信息保护、新技术新应用的安全防护、信息技术应用创新以及公安机关通报重大案（事）件处置落

实情况；网络安全负责人和相关岗位人员教育培训、通报预警机制建设和工作开展情况等。

四、保障措施

（一）加强组织领导。各级各部门要高度重视网络安全等级保护和关键信息基础设施安全保护工作，将其列入重要议事日程，研究解决网络安全机构设置、人员配备、经费投入、安全保护措施建设等重大问题，明确本单位主要负责人是网络安全的第一责任人，主管网络安全的领导班子成员是直接责任人，成立网络安全专门机构，明确任务分工，抓好责任落实。

（二）加强经费保障。各级财政部门要做好网络安全保护经费保障工作，保障公安机关组织开展的网络攻防应急演练、技术检测所需费用；确保二级（含）以上网络、关键信息基础设施等开展等级测评、安全建设整改、教育培训等经费投入。

（三）加强宣传引导。各县（市、区）人民政府及有关部门要组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作；要充分发挥大众媒体在网络安全宣传中的作用，针对不同人群、不同对象开展形式多样的宣传，进一步提高网络安全意识和防范技能。

（四）加强考核评价。各级各部门要进一步建立健全网络安全考核评价制度，明确考核指标，组织开展考核。公安机关要每年组织对各县（市、区）、各市直相关单位推进网络安全工作情况进行考核评价，评选网络安全等级保护、关键信息基础设施安

全保护工作先进单位，并将结果报告市委、市政府，通报市委网信办，考核结果将运用于全市平安建设考核评价体系。

（五）加强责任落实。市公安局要持续加大对各级各部门职责履行和工作落实情况的督导检查力度，建立定期通报和约谈制度；对未按照要求开展网络安全等级保护测评和整改，发生重大网络安全案（事）件的，将依法依规追究部门单位、企业及相关领导和直接责任人的责任。

晋城市人民政府办公室

2021年11月22日

（此件公开发布）

抄送：市委各部门，市人大常委会办公室，市政协办公室，市法院，市检察院，各人民团体，各新闻单位。

市属各事业单位，驻市各单位，各大中型企业。

晋城市人民政府办公室　　2021年11月22日印发