河南省第十三届人民代表大会常务委员会
公　　告

第 92 号

《河南省网络安全条例》已经河南省第十三届人民代表大会常务委员会第三十六次会议于 2022 年 11 月 26 日审议通过，现予公布，自 2023 年 6 月 1 日起施行。

河南省人民代表大会常务委员会

2022 年 11 月 26 日

河南省网络安全条例

（2022 年 11 月 26 日河南省第十三届人民代表大会常务委员会第三十六次会议通过）

目　录

第一章　总　则

第一条　为了保障网络安全，维护国家安全和社会公共利益，保护自然人、法人和非法人组织的合法权益，促进经济社会高质量发展，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》《中华人民共和国个人信息保护法》等有关法

律、行政法规，结合本省实际，制定本条例。

第二条 本省行政区域内网络安全的建设、保障、监管，以及网络使用、网络数据处理等活动，适用本条例。

涉密网络及其数据的安全保护，按照国家法律、行政法规的规定执行。

第三条 网络安全工作应当贯彻总体国家安全观，坚持网络安全与信息化发展并重，遵循统筹规划、综合治理、科学发展、确保安全的原则。

第四条 县级以上人民政府应当将网络安全纳入国民经济和社会发展规划，加大对网络安全建设维护的投入，建立健全网络安全机构，加强网络安全执法队伍建设，完善网络安全工作综合协调机制，解决网络安全重大问题，提升网络安全保障能力。

第五条 县级以上网信部门是网络安全工作的主管部门，负责统筹协调网络安全工作和相关监督管理工作。

县级以上工业和信息化、公安、保密管理、密码管理部门和国家安全机关、省电信管理机构等，应当在各自职责范围内负责网络安全保护和监督管理工作。

第六条 网络相关行业组织应当按照章程，加强行业自律，指导会员落实国家网络安全制度，加强网络安全保护，促进行业健康发展。

第七条 网络运营者、网络数据处理者和个人信息处理者应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业

道德，诚实守信，履行网络安全保护义务，承担社会责任，接受政府和社会监督。

第八条 任何个人或者组织使用网络不得违反法律、法规，不得危害网络安全，不得利用网络危害国家安全和社会公共利益，不得利用网络扰乱经济秩序和社会秩序，不得利用网络侵害他人合法权益。

任何个人或者组织对危害网络安全的行为，有权投诉、举报。收到投诉、举报的部门应当及时处理。

第九条 国家机关、人民团体、企业事业单位、新闻媒体应当以社会主义核心价值观为导向，倡导健康文明的网络行为，引导全社会依法办网、文明上网、安全用网，提高网络安全防范意识，营造共同维护网络安全的良好环境。

第十条 县级以上人民政府应当对在网络安全工作中做出突出贡献的个人和组织，按照有关规定给予表彰和奖励。

第二章 网络安全建设

第十一条 县级以上网信部门应当会同有关部门，根据上级网络安全规划以及本行政区域国民经济和社会发展规划，编制网络安全规划，报同级网络安全和信息化委员会同意后实施，并报上一级网信部门备案。

第十二条 省人民政府标准化部门和省网信、行政审批政务

信息管理等部门应当根据各自职责，组织网络安全标准的宣传、推广和应用。

鼓励高等院校、科研机构、企业、行业组织等参与网络安全国家标准、行业标准的制定工作。

第十三条 县级以上人民政府应当安排网络安全专项资金，扶持重点网络安全技术产业和项目。

省人民政府设立的互联网产业发展基金，应当支持网络安全建设运营。

鼓励金融机构支持网络安全技术创新和产业发展。

第十四条 省人民政府及有关部门应当支持省实验室和省级以上工程技术研究中心、技术创新中心、重点实验室等，开展网络安全技术研究，加强网络安全平台建设。

鼓励和支持高等院校、科研机构、企业参与网络安全技术创新项目和网络安全平台建设。

第十五条 省人民政府应当支持网络安全技术的研发和应用，重点支持安全芯片设计制造、网络安全态势感知、网络安全自主防御等关键技术攻关；推动网络安全技术产品升级，支持新技术在网络安全领域的应用，推广安全可信的网络产品和服务。

省人民政府及有关部门应当支持网络安全相关企业、高等院校、科研机构协同开展关键技术攻关，引导网络安全产业集聚，推动网络安全技术应用与网络安全产业融合发展。

第十六条 省人民政府及有关部门应当指导支持高等院校、

职业学校开设网络安全相关专业、课程，建设国家一流网络安全学院；鼓励高等院校、科研机构与企业共建网络安全实训基地，加强人才交流。

县级以上人民政府及有关部门应当将网络安全高层次、高技能以及紧缺人才纳入人才体系，在住房、职称评定以及配偶就业、子女入学等方面提供支持。

第十七条 县级以上人民政府及有关部门应当组织开展经常性网络安全宣传教育活动，指导支持教育机构、大众传媒、行业组织、专业机构等做好网络安全宣传工作，提高全社会网络安全意识和防护能力。

国家机关、人民团体、企业事业单位应当建立健全网络安全培训制度。鼓励社会力量、网络安全企业开展网络安全培训。

县级以上人民政府教育部门、学校应当加强青少年网络安全教育，推进网络安全知识技能进校园、进课堂，增强青少年网络安全意识。

第十八条 省、设区的市人民政府应当推进网络安全社会化服务体系建设。

鼓励支持符合条件的企业、机构依法开展网络安全规划咨询、安全集成、安全认证、产品检测、风险评估、应急响应、容灾备份等网络安全服务。

第三章　网络安全保障

第十九条　县级以上网信、公安等有关部门应当指导督促网络运营者落实关键信息基础设施安全保护、网络安全等级保护、数据安全保护、个人信息保护、密码应用安全性评估、云计算服务安全评估、网络信息安全投诉举报等制度，落实相关国家标准的强制性要求，制定网络安全事件应急预案。

第二十条　本省对国家关键信息基础设施按照有关法律、行政法规，予以重点保护。

县级以上人民政府应当在网络安全等级保护制度的基础上，对本行政区域内未列入国家关键信息基础设施的重要信息系统加强保护。重要信息系统的范围和识别指南由省网信部门会同公安等部门制定。省人民政府行业主管部门负责制定本行业、本领域的重要信息系统认定规则，根据认定规则识别本行业、本领域的重要信息系统，通知网络运营者，并向省网信、公安部门报送识别结果。

第二十一条　网信部门应当统筹协调有关部门建立重要信息系统网络安全信息共享机制，会同行业主管部门检查、检测重要信息系统安全风险，对重要信息系统领域的网络安全事件应急处置与网络功能恢复等，提供技术支持和指导。

行业主管部门负责指导和监督本行业、本领域重要信息系统安全保护工作，建立健全网络安全监测预警机制和网络安全事件

应急预案，定期组织开展网络安全检查监测、应急演练。

第二十二条 重要信息系统建设应当确保具有支持业务稳定、持续运行的性能；网络安全技术措施应当与重要信息系统同步规划、同步设计、同步建设、同步验收、同步使用，确保网络安全、数据安全和信息安全。

第二十三条 重要信息系统运营者应当履行下列安全保护义务：

（一）建立健全网络安全管理制度，明确安全管理负责人；

（二）对重要信息系统设计、建设、运行、维护等服务实施安全管理；

（三）对重要信息系统和数据库采取容灾备份和加密等措施；

（四）编制网络安全事件应急预案，定期开展应急演练；

（五）法律、法规规定的其他义务。

重要信息系统运营者应当履行网络安全保护主体责任。运营者采购网络产品和服务，应当按照规定与提供者签订协议，明确提供者的技术支持、网络安全运行维护和安全保密责任，并对其履行监督责任。

第二十四条 省人民政府有关部门应当根据国家数据分类分级保护制度要求，对本行业、本领域的网络数据实行分类分级管理，确定本行业、本领域重要数据具体目录，对列入目录的网络数据进行重点保护。

省人民政府行业主管部门确定的重要数据具体目录应当报省

网信部门备案。省网信部门应当及时和公安、国家安全等有关部门共享备案信息。

第二十五条 网络数据处理者开展网络数据处理活动应当履行下列安全保护义务：

（一）制定管理制度和操作规程，合理确定网络数据处理的操作权限；

（二）采取安全技术措施和其他必要措施保障网络数据安全以及网络数据处理系统、存储环境等安全；

（三）加强风险监测，发现存在网络数据安全缺陷、漏洞时，应当立即采取补救措施；

（四）发生网络数据安全事件时，应当立即采取处置措施，及时告知利害关系人，并按照规定向设区的市级以上行业主管部门和网信、公安部门报告；

（五）法律、法规规定的其他义务。

第二十六条 网络运营者应当加强对用户发布信息内容的管理，建立健全用户注册、信息发布审核机制，发现法律、行政法规禁止发布或者传输的信息，应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向属地网信、公安等有关部门报告。

网络运营者应用算法推荐技术提供互联网信息服务，应当履行算法安全主体责任，不得利用算法推荐服务传播法律、行政法规禁止的信息，不得设置违反法律、行政法规或者违背公序良

俗、公平竞争的算法模型。

第二十七条 提供平台服务的网络运营者应当建立保障数据安全的平台规则和隐私保护制度，不得损害公平竞争，不得侵害用户合法权益。

第二十八条 任何个人或者组织应当对其使用网络的行为负责，在网络上发布信息应当遵守法律法规、社会公德和公序良俗，不得利用网络制作、发布、传播法律、行政法规禁止发布或者传输的信息。

第二十九条 利用网络收集、使用个人信息，应当遵循合法、正当、必要和诚信等原则，明示收集、使用信息的目的、方式和范围等事项，履行告知义务，并取得本人或者监护人同意；法律、行政法规另有规定的除外。

处理的个人信息应当为履行法定职责或者提供服务、产品所必需，不得过度收集个人信息；不得因个人不同意提供非必需的个人信息，拒绝提供服务或者产品。

第三十条 利用网络处理个人信息应当采取下列措施，确保个人信息处理活动符合法律、行政法规的规定：

（一）制定管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化、匿名化等安全技术措施；

（四）发生个人信息泄露、篡改、丢失的，应当立即采取补救措施，通知当事人，并向设区的市级以上行业主管部门和网

信、公安部门报告；

（五）法律、行政法规规定的其他措施。

第三十一条 任何个人或者组织不得非法侵入、干扰、攻击、破坏网络，不得实施窃取、泄露、篡改以及非法获取、公开、交易网络数据等危害网络安全的行为。

第四章 网络安全监管

第三十二条 县级以上网信部门和有关部门依法在各自职责范围内负责网络运行安全、网络数据安全、网络信息安全工作。

第三十三条 县级以上网信部门负责统筹协调本行政区域内网络安全保障体系建设、网络安全监测预警和应急处置工作；统筹协调关键信息基础设施和重要信息系统安全保护、网络数据和个人信息安全保护工作；依法组织开展网络运行安全、网络数据安全、网络信息安全的监督管理和执法工作。

县级以上网信部门根据需要，可以会同有关部门开展网络安全联合执法、案件督办等工作。

第三十四条 县级以上人民政府工业和信息化部门负责工业领域网络安全的监督管理工作。

无线电管理机构负责无线电干扰查处相关工作。

第三十五条 县级以上人民政府公安部门负责指导、监督、检查网络安全等级保护、关键信息基础设施安全保护和重要信息

系统保护工作；依法查处涉及网络安全的违法犯罪行为。

第三十六条 保密管理部门负责指导监督机关、单位网络保密工作；负责对涉密网络及关键信息基础设施运营者采购保密设备、产品和服务的保密监管；负责涉密信息系统的测评审查和风险评估等安全保密工作；负责对各类网络进行保密监测预警和保密检查；负责各类网络失泄密案件的查处及危害评估和密级鉴定。

第三十七条 密码管理部门会同有关部门查处网络信息系统密码失泄密事件和违法违规研制、使用密码行为；负责全省涉密网络密码规划管理；负责关键信息基础设施、重要信息系统密码应用推进和监督管理；负责管理全省商用密码应用安全性评估工作；会同有关部门建立密码安全监测预警、风险评估、信息通报、重大事项会商和分级响应等协作机制。

第三十八条 省、设区的市国家安全机关负责开展网络反间谍安全防范指导、检查及反间谍技术防范检查检测、处置等相关工作。

第三十九条 省电信管理机构负责指导督促电信企业和互联网企业落实网络与信息安全管理责任，依据职责权限组织开展电信网和互联网网络安全监督检查、监测预警、风险评估、威胁治理、信息通报、应急管理与处置等工作。

第四十条 县级以上行业主管部门指导监督本行业、本领域的网络安全保障工作，负责本行业、本领域的关键信息基础设施

和重要信息系统安全保护，承担本行业、本领域网络数据安全监管职责，依法定期开展网络安全检查，开展网络安全隐患排查，处置网络安全事件，并及时将情况通报同级网信部门。

第四十一条 各级国家机关应当按照属地管理和谁主管谁负责的原则，落实网络安全工作责任制，建立健全网络安全工作体系，提升网络安全保障能力，确保关键信息基础设施、重要信息系统、网络运行、网络数据和网络信息的安全可控。

第四十二条 网信、公安、国家安全及有关主管部门依法履行网络安全监管职责时，网络运营者、网络数据处理者、个人信息处理者应当予以配合。

第四十三条 县级以上网信部门应当按照网络安全监测预警和信息通报制度要求，统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

行业主管部门应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，与同级网信部门共享本行业、本领域的网络安全信息。

第四十四条 省、设区的市网信部门负责统筹协调本行政区域内网络安全事件应急处置工作，建立健全跨区域、跨部门、跨行业的联动处置机制。公安、电信管理等部门在职责范围内负责相关网络安全事件处置工作。能源、电信、交通等行业应当为网络安全事件应急处置与网络功能恢复提供重点保障和支持。

第四十五条 县级以上网信部门发现网络存在较大安全风险或者发生网络安全事件的，可以依法约谈相关网络运营者、网络数据处理者、个人信息处理者的法定代表人或者主要负责人。被约谈者应当按照有关要求及时消除网络安全风险、妥善处置网络安全事件，及时处置法律、行政法规禁止发布或者传输的信息。

第四十六条 省、设区的市网信部门应当建立健全网络安全投诉、举报制度，建立投诉举报平台，公开投诉举报电话，接受社会各界对危害网络安全行为的投诉举报。对属于本部门职权范围内的，应当在三十日内办结并答复；情况复杂的，经单位负责人同意可以延长三十日。对不属于本部门职权范围内的投诉举报，应当在三日内转有关部门办理。有关部门应当在上述时间内办结并答复投诉人、举报人，并向网信部门反馈办理结果。

网信部门及其他有关部门应当为投诉人、举报人保密，保护投诉人、举报人的合法权益。

第四十七条 省、设区的市人民政府应当将网络安全工作纳入高质量发展综合绩效考核体系，建立绩效考核指标，对下级人民政府进行网络安全工作考核。

第五章 法律责任

第四十八条 违反本条例规定的行为，法律、行政法规已有法律责任规定的，从其规定。

第四十九条 违反本条例第二十三条第一款规定，重要信息系统运营者未履行安全保护义务的，由县级以上网信、公安部门根据管理权限责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上十万元以下罚款，对直接负责的主管人员处一万元以上五万元以下罚款。

第五十条 违反本条例第二十九条第一款规定，利用网络收集、使用个人信息未依法履行告知义务，未依法取得本人或者监护人同意的，由县级以上网信部门责令改正，给予警告，没收违法所得，对违法收集、使用个人信息的应用程序，责令暂停提供服务；拒不改正的，责令终止提供服务，并处十万元以上一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重或者造成严重后果的，由省网信部门责令改正，没收违法所得，并处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以禁止其在五年内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第五十一条 违反本条例第三十条第一项至三项规定的，由县级以上网信部门责令改正；拒不改正的，处一万元以上五万元以下罚款。

违反本条例第三十条第四项规定，发生个人信息泄露、篡

改、丢失事件，未立即采取补救措施的，由县级以上网信部门责令改正，并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上五万元以下罚款；情节严重或者造成严重后果的，按照本条例第五十条第二款规定执行。未通知当事人并向设区的市级以上行业主管部门和网信、公安部门报告的，由县级以上网信部门责令改正；拒不改正的，处一万元以上五万元以下罚款。

第五十二条 国家机关及其工作人员有下列情形之一的，由其上级机关或者网信部门责令改正；对直接负责的主管人员和其他直接责任人员，按照管理权限依法给予处分；构成犯罪的，依法追究刑事责任：

（一）未按照要求受理投诉举报或者反馈办理结果的；

（二）未履行网络安全保护义务，发生较大以上网络安全事件的；

（三）收集与履行法定职责无关的个人信息的；

（四）将履行工作职责中获取的信息用于其他不当用途的。

第六章 附 则

第五十三条 本条例自 2023 年 6 月 1 日起施行。