河南省数据局文件

豫数〔2026〕11号

河南省数据局
关于印发《非涉密政务信息系统安全防护建设审核指南》的通知

省直有关部门，各省辖市、济源示范区、航空港区行政审批和政务信息管理机构，省政务大数据中心：

为规范非涉密政务信息系统建设方案安全防护部分的设计和评审工作，提高安全防护设计的合规性、科学性和有效性，现将《非涉密政务信息系统安全防护建设审核指南》印发你们，请抓好贯彻落实。

河南省数据局

2026年8月11日

非涉密政务信息系统安全防护建设审核指南

第一章　总　　则

第一条　为规范非涉密政务信息系统建设方案安全防护部分的设计和评审工作，提高安全防护设计的合规性、科学性和有效性，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》《互联网政务应用安全管理规定》等法律法规及有关规定，结合工作实际，制定本指南。

第二条　本指南适用于河南省新建和升级改造的非涉密政务信息系统项目建设方案（以下简称建设方案）安全防护部分的统筹管理。涉及工作秘密的政务信息系统，依据相关规定执行。

第三条　政务部门在组织编制建设方案时，应当将安全防护作为重要组成部分，统筹谋划并贯穿方案编制全过程，全面筑牢安全防线，保障网络和数据安全。

第四条　本指南所称政务信息系统，是指由政务部门建设、运行和使用的，用于直接支撑政务部门业务应用的各类信息系统。

本指南所称各级政务部门，是指各级党委、人大、政府、政协、监委、法院、检察院及其所属部门，以及法律、法规授权具

有管理公共事务职能的事业单位和社会组织。

第二章　安全防护能力

第五条　建设方案应当明确系统的网络安全保护等级，制定网络安全等级保护定级、备案、建设、测评和整改等工作的实施计划。

第六条　建设方案应当包含单独的商用密码应用方案，或者相对独立的商用密码保护相关内容，并依据《信息安全技术信息系统密码应用设计指南》，包括但不限于：

（一）分析系统现状，明确需要密码保护的信息资源和所涉及的范围，确定系统的密码安全需求。

（二）参照系统网络安全等级保护定级标准，根据《信息安全技术信息系统密码应用基本要求》，进行密码应用设计，包括计算平台密码应用方案设计、密码支撑平台方案设计和业务应用的密码应用方案设计，并从系统的管理制度、人员管理、建设运行和应急处置四个方面提出密码应用管理要求。

（三）商用密码应用方案或者包含商用密码应用相关设计的建设方案应当通过商用密码应用安全性评估。

第七条　建设方案应当准确界定防护对象的安全边界，全面、清晰地阐述安全防护技术措施现状及安全防护需求。

第八条　建设方案应当包含网络安全体系设计内容，细化明确网络架构规划、安全防护部署、云安全资源复用等具体设计内

容，包括但不限于：

（一）科学规划整体网络拓扑架构，合理划分边界防护区、安全运维区、核心业务区等安全分区，逐项明确各分区的访问控制、隔离防护、权限管理等差异化安全防护策略。

（二）根据系统既定网络安全保护等级，配套规划适配的安全防护措施，列明基础防火墙、入侵检测系统、漏洞扫描、主机杀毒、日志审计、Web 应用防火墙、抗 DDoS 设备和数据库审计等安全软硬件清单，明确各类设备及系统的核心参数、配置数量、部署区域及接入部署方式。

（三）部署在省政务云的系统，应当优先采用政务云提供的基础安全防护能力，无需罗列政务云平台底层硬件的具体参数及部署位置，仅需在方案中明确依托的云安全资源清单、防护能力范围及配套落地安全策略。

第九条 建设方案应当包含数据安全防护内容，细化明确数据分类分级、加密防护、脱敏管控、数据备份、故障恢复等安全设计内容，包括但不限于：

（一）明确数据分类分级设计，制定数据分类分级划分标准及管理细则，列明核心数据、重要数据、一般数据目录清单，涉及重要数据处理的，应当单独制定数据安全风险评估实施计划，涉及核心数据处理的，按照国家有关规定执行。

（二）明确分级数据加密防护设计，制定差异化加密实施方案，列明各类数据对应的加密场景、加密安全强度与技术实现方

式，对身份证号、生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹、不满十四周岁未成年人的个人信息及其他敏感个人信息，明确存储、传输环节全量加密技术措施。

（三）明确全场景数据脱敏防护设计，制定数据脱敏实施规范，列明脱敏对象清单、分级脱敏规则、采用的脱敏算法及适用业务场景，对业务数据库、数据交互接口、前端展示页面、离线导出文件、系统操作日志等全部数据载体，逐一明确敏感个人信息、核心业务数据脱敏处置措施。

（四）明确数据备份安全设计，制定数据备份策略，列明备份类型、执行周期、数据最低保存期限、本地及异地存储部署方式，明确全量备份、增量备份执行安排。

（五）明确数据恢复安全设计，制定数据恢复策略，列明恢复操作流程、责任分工、校验标准，明确定期数据恢复演练的频次与内容，确保发生数据丢失、损毁等异常情况时能够快速、完整地完成数据恢复。

第十条 建设方案应当包含身份认证与访问安全管理内容，明确身份鉴别、口令管控、登录控制、操作校验、会话管理、账号审计等具体安全设计措施，包括但不限于：

（一）明确系统身份鉴别设计，采用多因素认证方式实现用户身份核验，杜绝单一身份认证风险。

（二）细化账号口令安全管控规则，明确口令最小长度、复杂度、定期更换频次、历史口令复用限制、首次登录强制改密等

配置要求。

（三）明确系统登录安全管控设计，设置合理的账号锁定策略，限制错误登录次数及同时在线用户数，禁止账号共用。

（四）明确系统高危关键操作范围，针对核心配置变更、批量数据处理、特权指令执行等操作，明确强制二次身份认证的触发场景与校验方式。

（五）明确系统会话超时管控设计，设置合理的登录闲置超时阈值，超时后强制销毁登录令牌、清除客户端敏感缓存、终止有效会话，禁止恢复登录状态，用户须重新完成身份认证后方可登录使用。

（六）明确账号操作日志留存与审计设计，完整记录所有账号登录、操作、变更等行为日志，对特权管理账号单独制定专项管控、独立审计、实时监控的落地措施。

第十一条 建设方案应当包含接口安全防护内容，细化明确接口风险防控、网关管控、开发基线、访问控制、传输存储防护等具体设计措施，包括但不限于：

（一）明确外部接口安全风险评估及防护设计，部署身份认证、流量限流、防重放攻击等安全防护措施，并规划安全测试，明确接口安全测试范围、测试内容及校验标准。

（二）明确接口统一网关管控设计，制定统一安全管控策略，实现接口统一接入、请求流量限速、请求内容过滤、运行状态可视化监控、超限阈值熔断等安全管控功能。

（三）明确接口安全开发基线设计，制定接口开发安全规范，对接口输入合法性验证、输出内容编码、异常错误处置等关键环节设定强制性安全管控要求。

（四）明确接口访问安全控制设计，配置接口访问频率限制、请求签名校验、跨域资源精准管控等安全能力，有效防范接口非法调用、滥用访问、越权操作等安全风险。

（五）明确接口数据传输与存储安全设计，跨服务接口调用采用“授权认证＋数据签名”双重校验机制，对接口请求参数实施签名核验，实现接口密钥加密存储、会话超时自动销毁等安全防护能力，保障接口数据传输可信、可溯。

第十二条 建设方案应当明确系统高可用性保障措施，采用双活集群、同城灾备、异地容灾等方案，部署在政务云的系统，可依托政务云平台的灾备能力规划实施，确保服务连续性和数据可靠性。

第十三条 涉及升级改造的建设方案，应当全面评估新建系统与已建系统安全防护体系的衔接关系，明确与已有安全设备在技术接口、协议标准、管理规范等层面的兼容性，制定安全设备的利旧、整合或替代方案，确保防护能力无缝覆盖，避免重复建设和防护缺失。

第十四条 建设方案应当明确系统采用软硬件产品和服务的安全管理要求，保障系统自主可控，包括但不限于：

（一）系统采用的软硬件产品和服务，应当符合国家及行业

现行有效安全标准，且具备相应安全认证资质。

（二）CPU 芯片、操作系统、数据库等关键部件，应当通过安全可靠测评，并符合政府采购相关标准。

（三）应当包含系统国产化适配专项内容。

第十五条 建设方案应当包含供应链安全管控内容，明确系统使用的开源及第三方软件或组件来源，制定开源及第三方组件的安全管理策略，包括引入审查、版本更新、漏洞扫描等，并明确在项目建设和运维阶段采用技术手段对组件清单进行动态管理和监控。

第十六条 建设方案应当明确源代码的安全管理要求，包括版本控制、安全托管与访问控制，确保源代码在整个生命周期内的完整性、保密性和可追溯性。

第十七条 采用人工智能、物联网、区块链等新兴技术的系统，建设方案中应当设专项章节阐述新兴技术应用各环节的潜在风险隐患，制定针对性风险防控措施，保障系统建设合规可控、安全可靠。

第三章 安全管理制度

第十八条 建设方案应当包含安全审计规划内容，细化明确审计覆盖范围、审计实施规则、日志存储规范、问题处置流程等具体设计内容，包括但不限于：

（一）明确安全审计覆盖范围，审计日志全面涵盖网络设备、

主机操作系统、业务应用系统、数据库、安全防护设备等各类主体，实现业务操作、设备运行、权限变更等核心环节审计无死角、无遗漏。

（二）明确安全审计实施频次与触发规则，制定常态化定期审计工作周期，明确重大安全事件、系统架构重大调整等特殊场景的专项审计启动条件。

（三）明确审计日志留存期限及安全存储标准，规范日志存储方式与防护要求，确保审计日志留存时长不少于6个月，保障日志数据完整、真实、可追溯、可核验。

（四）明确审计问题闭环处置设计，列明审计问题整改责任主体、整改时限、验证标准，制定审计责任认定、责任追究相关流程，依托审计结果落实常态化安全整改优化工作。

第十九条 建设方案应当制定系统安全测试计划，明确系统上线前应当开展网络安全风险评估，评估内容涵盖渗透测试、漏洞扫描、基线安全检查、源代码安全检测、供应链安全检查等。

第二十条 建设方案应当制定项目建成后的试运行计划，包括试运行准备、流程、注意事项、试运行期间风险评估与应对策略等。

第二十一条 建设方案应当制定项目建成后的安全运维移交计划，明确移交流程及系统资产与对应清单、运维操作规范、核心风险点位等移交内容，确保上线前，运维团队全面掌握系统的安全状况与运维要求，保障运维工作规范衔接、有序落地。

第二十二条 建设方案应当制定常态化安全监测计划，采用技术工具与人工分析相结合的方式，对系统运行状态和安全威胁进行持续监控，确保及时发现并处置软硬件服务中断供应、停止授权、停止提供产品升级等供应链安全风险，防范漏洞、后门等技术安全风险和信息泄露、数据篡改等数据安全风险。

第二十三条 建设方案中应当制定常态化安全检查计划，细化全流程定期自查和专业第三方评估的具体范围、评估标准及实施频次，确保系统全生命周期持续符合国家、行业相关法律法规及有关规定要求。

第二十四条 建设方案应当明确在国家重要活动、重大会议、法定节假日以及特殊敏感时期等重要时段的网络安全保障措施，涵盖值班值守、安全监测与应急响应等内容。

第二十五条 建设方案中应当编制完善的安全事件应急预案，明确应急管控全流程设计，保障安全事件快速响应、规范处置，确保预案具备针对性与实战性，包括但不限于：

（一）明确安全事件分级应急响应机制，明确网络攻击、数据泄露、系统瘫痪等典型安全事件的分级判定标准，细化各等级事件的预案启动条件、应急响应时限、技术支撑储备及应急人员配置，确保应急响应措施与事件风险等级精准适配。

（二）明确安全事件全流程处置规范机制，明确事件发现研判、逐级上报、溯源分析、闭环处置各环节操作要求，清晰划定各环节责任主体、关键时间节点及全程留痕记录标准，保障处置

流程可落地、可执行、可追溯。

（三）明确应急处置复盘优化闭环设计，制定安全事件事后复盘工作机制，明确复盘时限、整改要求、报告编制规范，同步迭代更新应急预案及安全防护策略，持续完善系统应急处置能力。

第二十六条 建设方案应当明确变更管理流程规范，包括变更前影响评估、系统版本更新与安全配置修改等场景的合规审批、安全测试、上线验证等全流程管控要求，制定变更回滚预案，确保变更失败或引发安全问题时可快速恢复至稳定状态。

第二十七条 建设方案应当明确安全防护体系的持续改进机制，根据网络安全形势、技术发展、业务变化和管理要求，对安全策略和措施进行定期评审和动态优化。

第四章 安全组织保障

第二十八条 建设方案应当明确项目安全主管领导及其承担的安全工作统筹决策职责，明确承担日常安全管理和协调工作的安全责任部门及其具体职责。

第二十九条 建设方案应当明确关键岗位安全责任，明确系统管理员、安全管理员、审计管理员等关键角色的安全职责和权限划分。

第三十条 建设方案应当制定安全培训计划，明确对开发、运维等不同岗位人员的培训内容、频次等要求，确保其具备岗位

所需的安全意识和技能。

第三十一条 建设方案应当编制清晰、完整的安全经费预算及使用计划，包括但不限于：

（一）预算构成清晰。单独列支网络安全防护专项预算，分类细化列明安全软硬件设备采购、安全服务等各类经费明细，预算科目划分规范、层级清晰、无交叉遗漏。

（二）预算依据充分。预算金额应当与系统规模、安全防护需求相匹配，并涵盖项目免费运维期内的网络安全等级保护、商用密码应用安全性评估、第三方软件测试费等安全支出。

（三）使用计划合理。制定项目建设期安全预算使用实施计划，明确各环节安全投入分配比例，建设阶段预算应当重点保障安全设备采购、安全集成实施、安全测试测评等建设类安全支出，确保预算使用有序高效。

第五章 附 则

第三十二条 本指南由河南省数据局负责解释。

第三十三条 本指南自印发之日起施行。

河南省数据局 2026 年 8 月 11 日印发