附件 1

# 非涉密政务信息系统开发安全管理指南

（征求意见稿）

## 第一章 总则

**第一条** 为规范非涉密政务信息系统开发全生命周期安全管控工作，防范因开发阶段管理不善导致的安全风险，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》《关键信息基础设施安全保护条例》《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** 非涉密政务信息系统（以下简称“政务信息系统”）开发时，应当将安全工作贯穿于系统开发全生命周期，明确安全管理职责，坚持同步规划、同步设计、同步建设、同步验收、同步使用原则，制定相应安全防护措施，严禁未经安全检测、不符合安全要求的政务信息系统“带病运行”。涉及工作秘密的政务信息系统开发应当符合相关安全保密管理规定。

**第三条** 按照“谁建设谁负责、谁参与谁负责”的原则，建设单位承担政务信息系统网络和数据安全主体责任，设计、承建等单位分别承担各自安全责任，共同保障政务信息系统开发

安全。

本指南所述的建设单位是指实施政务信息化项目的政务部门，设计单位、承建单位分别是指承接政务信息系统设计、建设工作的相关企事业单位。

**第四条** 本指南所述的政务信息系统开发共划分为四个阶段，分别是规划设计阶段、开发阶段、测试阶段、上线阶段。

## 第二章 规划设计阶段

**第五条** 建设单位应当统筹政务信息系统开发安全监管工作，督促设计、承建单位落实政务信息系统开发安全措施，加强与密码、保密、网信、公安等部门的沟通协调，确保政务信息系统在密码应用、保密管理、网络安全、数据安全、等级保护等方面符合国家法律法规和监管要求。对分开采购基础设施、应用系统、安全防护等建设内容的政务信息系统，建设单位应当建立协同工作机制，确保各承建单位之间的开发安全责任、工作流程、技术规范等衔接顺畅。

**第六条** 建设单位应当依据 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》，组织开展政务信息系统网络安全等级保护定级工作，对政务信息系统业务类型、应用范围、系统结构等情况进行全面分析，明确安全保护等级。根据所确定级别明确安全保护需求，依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》，规划安全保护措施并按规定

开展等级保护备案。被认定为关键信息基础设施的，应当参照GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》等标准，同步规划安全保护措施。

**第七条** 建设单位应当依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》提出明确的密码合规性保护要求，制定商用密码应用方案，规划商用密码保障系统，并对商用密码应用方案进行商用密码应用安全性评估，确保政务信息系统在密码算法、技术、产品和管理上符合国家密码法律法规与主管部门要求。商用密码应用方案未通过商用密码应用安全性评估的，不得作为商用密码保障系统的建设依据。

设计单位应当在安全设计方案中明确密码应用安全保障体系设计，包括但不限于:

（一）明确规定应当采用符合国家密码管理要求的商用密码算法、产品和服务。

（二）设计密钥安全管理方案，密钥应当与业务数据分离存储，明确密钥定期更换机制和严格的访问控制策略。

**第八条** 建设单位在编制政务信息系统项目建设方案时，应当组织开展安全需求分析，向设计、承建单位提供必要的业务、管理信息，通过组织专题会议、联合评审等方式，确保所有参与方对安全需求的理解达成一致。

**第九条** 设计单位应当为政务信息系统开发提供合规、可靠

的安全设计能力保障，准确识别政务信息系统建设安全需求，根据系统业务流、数据流和政务信息系统安全合规要求，分析研判网络和数据安全风险，编制全面、准确、可行的政务信息系统安全设计方案，并确保整体设计方案符合国家和行业标准。

**第十条** 建设单位应当组织制定政务信息系统身份认证和访问安全管理制度，明确权限分配、变更、收回审批流程，定期进行账号权限审查，在人员调岗或离职时同步收回相应的权限。

设计单位应当遵循最小权限原则，在安全设计方案中明确身份认证与访问安全管理措施，包括但不限于:

（一）采取多因素认证的身份鉴别机制。

（二）设定口令长度不低于 8 位且包含大小写字母、数字及特殊字符的复杂度要求，每 90 天强制更换。

（三）首次登录强制修改口令，并要求定期更换不重复的密码，限制错误登录次数，设置合理的账号锁定机制。

（四）记录所有账户完整操作日志，包括时间戳、用户 ID、操作类型等信息；特权账户应当独立管理，严格审计和监控特权账户的相关操作。

**第十一条** 建设单位应当按照数据分类分级保护制度要求，编制核心数据、重要数据、一般数据目录，明确数据分类分级保护和容灾备份需求。

设计单位应当在安全设计方案中明确数据安全架构设计，包括但不限于:

（一）制定数据差异化保护措施，明确不同级别数据的加密传输、加密存储及访问控制策略。

（二）设计数据脱敏技术方案，防范因数据汇聚、关联分析引发的泄密风险。

（三）明确输入数据的过滤策略和有效性验证规则，用户输入需要进行合法性校验，文件上传功能应当限制文件类型、大小，文件下载应当进行病毒扫描。

（四）限制输出数据内容，不得直接输出未经脱敏处理的敏感信息，错误提示信息应当经过安全处理，不得包含政务信息系统内部技术细节。

（五）数据出境活动应当严格遵守国家法律法规要求，未经安全评估和主管机关批准的，严禁数据跨境传输。

**第十二条** 建设单位应当明确日志管理要求，包括但不限于:

（一）完整记录用户登录、权限变更、数据导出、批量查询等关键操作，包含操作时间、操作者、操作内容、源 IP 等关键要素，保存周期一般不少于 6 个月。

（二）与互联网政务应用相关的防火墙、主机等设备的运行日志，以及政务信息系统的访问日志、数据库的操作日志，

留存时间不少于1年。

（三）明确日志定期备份要求，确保日志的完整性、保密性和可用性。

设计单位应当在安全设计方案中完成日志管理体系设计，确保关键操作要素记录无遗漏，保存周期、备份策略、传输加密方案和访问控制机制符合安全需求，明确日志存储至专用、安全的服务器或平台，确保日志的完整性、保密性和不可篡改性，并设计必要的日志查询、统计分析和告警功能。

**第十三条** 建设单位应当明确政务信息系统部署必须符合政务云安全架构和管理要求，接入电子政务外网或者需要与电子政务外网进行数据交换的，应当按照国家政务外网的要求采取相应的安全保障措施。

设计单位应当在安全设计方案中明确选用安全可控的操作系统、数据库、中间件等基础软件，设计政务信息系统在政务云、电子政务外网等环境下的边界防护安全策略、数据交换与接口调用安全管理体系，并配备相应的安全组件，确保所有跨域访问行为记录完整、可被审计。

## 第三章 开发阶段

**第十四条** 承建单位应当组建专业安全团队，建立系统开发安全管理制度和机制，编制安全开发编码规范，组织开发安全培训，严格管理政务信息系统安全责任重点人员，提供统一的

开发平台、开发工具及相关支撑软件，选用符合相关安全标准的第三方产品，明确开发各阶段责任人，定期开展安全检查，确保开发过程符合安全规范。

**第十五条** 承建单位应当确保开发过程在安全、受控的环境中进行。对开发和测试环境采取物理或逻辑隔离措施，使用正版开发工具并定期更新安全补丁。用于开发的服务器、个人电脑等终端设备应当安装防病毒软件，落实移动存储介质管理、安全准入控制等安全防护措施，所有终端设备应当通过安全检查，使用相关准入软件接入开发环境。

**第十六条** 承建单位应当严格按照安全设计方案要求和安全开发编码规范进行开发，建立配置管理、代码审计和无效代码的识别与清理机制，及时备份项目文档和代码，使用专门的源代码管理服务器保存所有源代码的历史版本，确保代码的可读性、可维护性、可扩展性和可溯源性。所有源代码应当进行规范性、安全性和功能符合性检查，禁止将加密密钥、管理员账户口令等敏感信息直接写入源代码或配置文件中。所有安全隐患修复后，代码方可投入使用。

**第十七条** 承建单位应当对使用的第三方产品进行安全评估，禁止使用存在法律风险、停止维护的组件。建立第三方组件管理清单，记录使用版本、使用范围和许可证信息。

**第十八条** 承建单位用于开发、测试、演示的数据应当经过

有效脱敏，确保不可被识别特定信息且不可复原。在非生产环境中严禁直接使用生产数据，并严格限制访问权限。

**第十九条** 承建单位应当建立资产台账和常态化检查机制，持续识别并清理政务信息系统中的废弃资产，包括模块、功能、API 接口以及暴露在互联网的无效 IP、端口、URL 路径等，及时完成下线和归档，主动收敛暴露面，降低安全风险。

**第二十条** 承建单位应当严格遵循最小权限原则管理开发人员，其访问权限严格限定于完成指定任务所必需的范围，原则上不得授予高级别权限。确需临时性高级别权限的，应当履行严格的申请、审批与授权流程，保证操作全过程受到监控与审计，任务完成后立即收回权限。

## 第四章 测试阶段

**第二十一条** 建设单位应当依据软件测试相关国家标准要求和 GB/T 30276-2020《信息安全技术 网络安全漏洞管理规范》，组织第三方机构开展安全测试，通过代码审计、漏洞扫描、渗透测试等方式，发现政务信息系统存在的安全漏洞，形成包含漏洞等级、复现步骤和修复建议的漏洞台账。

（一）在开展代码审计时应当采用专业源代码审查工具和人工审查相结合的方式，对敏感函数调用、输入输出过滤逻辑、第三方组件合规性、数据库加密存储、安全策略配置等内容进行审计，形成代码审计报告。

（二）在开展漏洞扫描、渗透测试时应当对 SQL 注入、越权访问、任意文件上传等问题进行检查，形成漏洞扫描和渗透测试报告。

**第二十二条** 建设单位应当依据 GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》，组织开展商用密码应用安全性评估。未通过商用密码应用安全性评估的，应当进行改造，改造期间不得上线运行。

**第二十三条** 建设单位应当督促承建单位建立漏洞全生命周期管理机制，督促承建单位完成漏洞处置工作，将漏洞修复情况、源代码变更情况统一归档，并严格控制漏洞相关信息知悉范围。

## 第五章 上线阶段

**第二十四条** 承建单位应当建立完善的版本管理制度，部署方案、管理员操作手册、用户手册、源代码、配置文件、账号权限清单等文档需统一归档保管。政务信息系统上线部署时应当明确系统版本、上线或变更内容、回退方案和安全测试结果，履行相关审批手续。

**第二十五条** 承建单位应当落实政务信息系统部署过程中的安全管控措施，包括但不限于:

（一）生产环境与开发、测试环境隔离。

（二）系统服务启用和切换、系统配置设置和变更、核心

功能部署和更新、数据批量处理等高风险操作，应当建立“双人确认”机制，留存操作过程日志记录，杜绝单人误操作或越权行为引发的安全事件。

（三）所有服务器在部署前应当完成关闭非必要服务、设置安全基线配置、安装最新补丁等安全加固工作，部署完成后立即验证业务功能和安全配置，确认无误后方可开放访问权限。

（四）及时回收开发过程中使用的特权账户、测试账户、超级管理员等临时账号和权限。

**第二十六条** 承建单位应当严格政务信息系统访问管控，不面向公众、无互联网访问需求的政务信息系统，禁止在互联网环境直接部署与开放，因业务需求确需提供互联网访问的，应当经建设单位审批同意，并采取白名单访问控制机制限制访问来源。

## 第六章 附则

**第二十七条** 本指南由河南省行政审批和政务信息管理局负责解释。

**第二十八条** 本指南自印发之日起施行。