漯河职业技术学院
LUO HE VOCATIONAL TECHNOLOGY COLLEGE

漯河职业技术学院（群内）专业人才培养方案

（2025版）

专业名称：信息安全技术应用专业

专业代码：510207

专业大类：电子信息大类

所属学院：人工智能学院

所属专业群：大数据技术专业群

二〇二五年八月

目　录

漯河职业技术学院信息安全技术应用专业(群内)人才培养方案

(2025 版)

一、专业描述

专业名称：信息安全技术应用

专业代码：510207

入学要求：中等职业学校毕业、普通高级中学毕业或具备同等学力

基本修业年限：三年

教育类型：高等职业教育

学历层次：专科

所属专业群名称：大数据技术专业群

二、职业面向

（一）职业面向岗位

表 1　信息安全技术应用专业职业面向岗位一览表

所属专业大类（代码）	所属专业类（代码）	对应行业（代码）	主要职业类别（代码）	主要岗位群或技术领域	职业资格证书和技能等级证书
电子信息大类（51）	计算机类（5102）	互联网及相关服务（64）、软件和信息技术服务业（65）	网络与信息安全管理员 S（4-04-04-02）、信息安全测试员 S（4-04-04-04）、电子数据取证分析师 S（4-04-05-08）、网络安全等级保护测评师（4-04-04-06）、信息系统分析工程技术人员 S（2-02-10-05）、信息安全工程技术人员 S（2-02-10-07）	网络安全运维、网络安全渗透测试、等级保护测评、网络设备配置与安全、数据存储与容灾	计算机技术与软件专业技术资格、Web 安全测试、网络安全运维、网络安全评估、信息安全渗透测试工程师、华为 HCIA 和 HCIP 认证、国家信息安全水平考试 NISP 认证

（二）职业发展路径及职业能力分析

表 2　信息安全技术应用专业职业岗位及其岗位能力分析

序号	岗位群	岗位类别		岗位任务描述与核心能力要求	
		入职岗位	发展岗位	岗位任务描述	核心能力要求
1	安全运维	安全运维员	安全运维工程师	1.监控网络、服务器、安全设备运行状态，及时响应告警并初步排查故障，如防火墙策略冲突、入侵检测系统告警等； 2.按周期执行安全设备日常巡检，检查配置合规性、日志完整性，协助完成设备策略优化； 3.参与安全事件应急响应，配合上级对病毒感染终端、小规模网络攻击进行隔离、查杀，记录处置过程； 4.维护基础安全文档，如设备台账、简单操作手册更新。	1.掌握防火墙、IDS/IPS 基础配置，能通过 Web 界面/命令行完成策略增删改； 2.Windows/Linux 系统常规安全检查命令，定位基础系统安全问题； 3.了解常见网络攻击特征，识别初级安全威胁。
2	渗透测试	渗透测试员	高级渗透测试工程师	1.依据授权对 Web 系统、小型网络开展渗透测试，执行信息收集、漏洞扫描； 2.验证漏洞可利用性，编写测试报告，清晰描述漏洞位置、危害、复现步骤及修复建议； 3.协助开发安全加固方案，参与企业安全防护体系优化； 4.跟踪漏洞库更新，学习新型漏洞原理与检测方法，应用于测试工作。	1.熟练使用渗透测试工具，完成常规 Web 漏洞检测； 2. 掌握 OWASP TOP10 漏洞原理与手工检测方法，区分误报漏洞； 3.具备基础脚本编写能力，辅助漏洞验证。
3	等保测评	等保测评助理	等保测评工程师	1.协助开展信息系统等级保护测评，收集系统资料，执行现场测评； 2.依据等保标准，编写测评项结果记录、初步分析不合规点； 3.参与整改方案制定，跟踪整改实施，验证整改效果； 4.维护测评项目文档，整理过程记录、证据材料，协助编制最终测评报告。	1.熟悉等级保护基本流程与要求，背诵等保二级/三级核心测评项； 2.熟练操作等保测评工具，导出漏洞扫描、配置核查结果； 3.理解常见不合规场景，给出基础整改建议方向。
4	应急响应	应急响应专员	应急响应高级工程师	1.接收安全事件预警，快速启动响应流程，进行事件定级； 2.开展初步调查，通过流量分析工具、日志系统定位攻击源、攻击路径，判断影响范围； 3.执行防护措施，如隔离感染终端、切断攻击 IP 访问，阻止事件	1.熟悉应急响应标准流程，快速响应不同级别事件； 2.掌握基础流量分析、日志检索技能； 3.了解常见恶意样本分析思路，识别样本类型；

				扩大； 4.协助进行事件溯源，编写应急响应报告，输出整改建议； 5.参与企业应急演练策划，编制演练脚本、流程，组织桌面推演/实战演练。	4.能使用开源/商用工具辅助事件处置。
5	电子数据取证	电子数据取证技术员	电子数据取证分析师	1.对提取到的电子数据进行深度分析，恢复被删除、隐藏的数据； 2.识别与案件相关的电子证据，如文档、邮件、聊天记录、上网痕迹等； 3.编写电子数据取证分析报告，清晰阐述取证过程、分析结果和证据链。	1.熟练运用专业的取证分析工具； 2.掌握不同操作系统及移动设备的文件系统结构和数据存储特点； 3.具备较强的逻辑分析和证据关联性分析能力，能够构建完整的电子证据链； 4.熟悉电子数据取证相关法律法规，确保取证过程和结果的合法性。

三、培养目标与培养规格

（一）培养目标

本专业依托漯河及豫中南地区互联网产业、软件信息技术服务产业集群优势，紧跟网络安全攻防技术迭代、数字经济安全保障需求的发展趋势，培养能够践行社会主义核心价值观，传承技能文明，德智体美劳全面发展，具有一定的科学文化水平，良好的人文素养、科学素养、数字素养、职业道德、创新意识，具备爱岗敬业的职业精神和精益求精的工匠精神，较强的就业创业能力和可持续发展的能力；掌握网络安全防护、渗透测试、等级保护测评、数据备份与容灾等专业知识和技术技能，具备职业综合素质和行动能力，面向互联网和相关服务、软件和信息技术服务等行业的网络安全运维、网络安全渗透测试、等级保护测评、网络设备配置与安全、数据存储与容灾等技术领域，能够从事网络安全管理、网络安全运维、数据备份与恢复等工作的高技能人才。

（二）培养规格

本专业学生应在系统学习本专业知识并完成有关实习实训基础上，全面提升知识、能力、素质，掌握并实际运用岗位（群）需要的专业核心技术技能，实现德智体美劳全面发展，总体上须达到以下要求：

1.素质

（1）坚定拥护中国共产党领导和中国特色社会主义制度，在习近平新时代中国特色社会主义思想指引下，践行社会主义核心价值观，具有坚定的理想信念、深厚的爱国情感和中华民族自豪感；

（2）崇尚宪法、遵法守纪、崇德向善、诚实守信、尊重生命、热爱劳动，履行道德准则和行为规范，具有社会责任感、担当精神和社会参与意识；

（3）具有质量意识、环保意识、安全意识、信息素养、工匠精神、创新思维，具有学以致用、爱岗敬业的职业理念和服务网络强国战略与数字经济发展的职业理想；

（4）具有自我管理能力、职业生涯规划的意识，有较强的集体意识和团队合作精神，能适应团队协作开展专业工作；

（5）具有健康的体魄、心理和健全的人格，掌握身体运动的基本知识和至少 1 项体育运动技能，达到国家大学生体质健康测试合格标准，养成良好的健身、卫生习惯和行为习惯，具备一定的心理调适能力；

（6）具有一定的审美和人文素养，掌握必备的美育知识，具有一定的文化修养、审美能力，能够形成至少 1 项艺术特长或爱好；

（7）树立正确的劳动观，尊重劳动，热爱劳动，具备与本专业职业发展相适应的劳动素养，弘扬劳模精神、劳动精神、工匠精神，弘扬劳动光荣、技能宝贵、创造伟大的时代风尚。

2.知识

（1）掌握必备的思想政治理论、科学文化基础知识、中华优秀传统文化知识，以及支撑本专业学习和可持续发展必备的语文、数学、外语（英语等）等文化基础知识；

（2）熟悉与本专业相关的法律法规、行业规定，以及环境保护、安全消防、文明生产、绿色生产、安全防护、质量管理等相关知识，了解相关行业文化；

（3）掌握信息技术基础知识，以及计算机网络体系结构、TCP/IP 协议栈原理及网络协议分析技术；

（4）具备 Windows Server 与 Linux 系统的配置管理知识，掌握操作系统安全加固技术（权限管理、日志审计、漏洞修补等）相关知识；

（5）掌握信息安全技术与实施、信息安全标准与法规、计算机网络、数据库、程序设计等方面的专业基础理论知识；

（6）掌握网络安全运维、网络安全渗透等技术技能相关知识，以及信息安全风险评估、信息安全产品配置管理的实践知识；

（7）掌握国产操作系统、国产数据库、国产密码体系、国产信息安全产品等部署与应用相关知识；

（8）掌握数据备份与恢复、数据存储与容灾等技术技能相关知识，了解数据备份、存储介质数据恢复及信息系统的数据存储、数据容灾设计与实施的知识；

（9）掌握 CTF 竞赛中 MISC 杂项、流量分析、密码学、Web 等题型解法相关知识；

（10）掌握取证工具基础操作及数据固定、提取、分析流程知识，具备司法取证规范与报告撰写认知，知晓新型场景取证适配思路；

（11）了解企业级网络架构设计与安全建设规范，掌握网络安全风险评估与安全运营管理方法，具备安全方案设计及等级保护测评实施相关知识。

3.能力

（1）具有探究学习、终身学习和可持续发展的能力，能整合知识并综合运用知识分析问题和解决问题，适应行业技术快速发展需求；

（2）具有良好的语言、文字表达能力和沟通合作能力，学习 1 门外语并结合本专业加以运用，能清晰传递专业信息、开展协作交流；

（3）具有较强的集体意识和团队合作意识，能与团队成员配合完成专业项目，具备协调团队资源推进项目实施的安全项目管理与实践能力；

（4）具有良好的人文素养与科学素养，具备职业生涯规划能力，能结合行业发展规划个人职业路径；

（5）具有适应本行业数字化和智能化发展需求的数字技能，能运用数字化工具开展专业工作；

（6）具备网络安全防护的实践能力，能够熟练配置防火墙、入侵检测系统等网络安全设备，制定并实施有效的安全防护策略；

（7）具备系统安全管理能力，能够对系统权限进行管理、漏洞修复等核心安全运维技能，同时掌握网络安全运维、网络安全渗透等技术技能，具有信息安全风险评估、信息安全产品配置管理的实践能力；

（8）具备网络攻防实战能力，能够开展渗透测试、漏洞挖掘分析以及网络安全事件的应急响应工作；

（9）具有国产操作系统、国产数据库、国产密码体系、国产信息安全产品等部署与应用能力；

（10）具有数据备份、存储介质数据恢复的实践能力和信息系统的数据存储、数据容灾的

设计与实施能力；

（11）具有学习取证新技术、分析复杂场景问题的能力，可依规范分析数据构建证据链，具备撰写规范报告及应对新型场景取证的能力。

4.职业态度

（1）自觉遵守相关法律法规、行业标准和管理规定，在专业工作中坚守法律与职业底线；

（2）具有吃苦耐劳、爱岗敬业的精神，秉持精益求精的工作态度，认真完成各项专业任务；

（3）具有强烈的团队合作意识，主动与团队成员沟通配合，共同推进项目落地，助力团队目标达成；

（4）具有积极向上的态度和创新精神，主动探索网络安全领域新技术、新方法，勇于尝试解决行业新问题；

（5）具备高度的风险防范意识和严谨细致的工作作风，能够在安全运维、漏洞排查等工作中保持警惕性和操作规范性，避免因疏忽导致安全隐患；

（6）树立主动学习的职业态度，保持对网络安全技术发展的敏锐度，主动参与行业培训与技术交流，适应快速变化的行业需求；

（7）具备客户服务意识，能够从用户需求出发设计安全方案，注重保护客户数据隐私，并在服务过程中体现专业性、耐心与责任感；

（8）树立网络安全社会责任意识，主动参与网络空间安全治理，积极向公众普及防范网络诈骗、数据泄露等安全知识，维护清朗网络环境；

（9）具备抗压与应变能力，在应对突发安全事件时保持冷静，恪守职业道德底线，坚决抵制利用技术手段谋取非法利益的行为。

四、人才培养模式

根据专业人才培养目标，本专业采用“产教融合、岗课赛证、理实一体”的人才培养模式。

联合漯河及豫中南地区网络安全企业（如河南奇联西智能科技有限公司漯河分公司、河南信安世纪科技有限公司）共建实训基地，对标网络安全运维、渗透测试、等级保护测评等岗位核心能力重构课程体系；同步融入“1+X”网络安全应用、数据安全与备份等职业技能等级证书标准，实现“课证融通”。推行“理论解析+实践实操”交替教学：理论课结合真实网络攻击案例、企业安全事件解析技术原理；实践课依托校内虚拟仿真平台与企业真实运维环境，开展 Web 漏洞检测、应急响应、数据备份与容灾等场景化实训。以省级以上网络安全竞赛为牵引，强化技能突破与创新能力培养。建立“校内专业教师+企业技术导师”双指导机制，全程参与课程教

学、实训指导与岗位实习，通过项目实战提升学生岗位适配能力，最终培养具备扎实专业能力、符合区域网络安全产业需求的高技能人才。

通过关联“漯河及豫中南地区企业”，进一步体现专业服务区域产业的定位，同时让“理论—实践—竞赛—实习”的逻辑衔接更顺畅，能更精准支撑信息安全技术应用专业的人才培养目标落地。

五、课程设置及要求

主要包括公共基础课程和专业（技能）课程。

1.公共基础课程

见大数据技术专业群公共基础课程内容。

2.专业（技能）课程

（1）专业群共享及专业基础课程

本专业开设专业群共享课程有 5 门，包括计算机应用基础、数据库技术、Python 编程基础、计算机网络基础、Web 前端技术，见大数据技术专业群共享课程内容。

本专业基础课程为信息安全技术。

表 3 专业基础课程描述

课程代码	课程名称	课程目标	主要内容	教学要求
023637	信息安全技术	1.掌握密码学基本原理、数据加密核心技术及网络流量分析基础方法； 2.能准确识别不同密码算法的特性、加密数据的安全级别以及网络流量中的正常与异常模式； 3.熟练运用密码学工具进行数据加密、解密操作，运用流量分析工具排查网络安全隐患； 4.具备将密码学和流量分析知识应用于实际信息安全防护与数据保密的专业素养。	1.密码学与信息安全基础：信息安全基本概念、密码学发展历程、对称加密、非对称加密、哈希函数及应用场景； 2.数据加密技术：数据加密流程、密钥管理、加密算法的选择与实现、常见加密工具的使用； 3. 流量分析技术：网络流量结构、Wireshark 工具使用、流量协议分析、异常流量识别与分析； 4.综合实践：数据加密实战（对文件、数据进行加密解密）、流量分析实战（捕获并分析网络流量，识别安全风险）。	1.能独立分析不同密码算法的应用场景及安全性，准确率不低于 90%； 2. 可运用 Wireshark 对网络流量进行协议分析与异常识别，准确率达 85% 以上； 3. 能熟练使用至少两种加密工具完成数据加密解密操作，操作准确率不低于 80%；4. 完成 1 个数据加密与流量分析结合的综合项目，提交规范的项目报告并给出可落地的信息安全改进建议。

（2）专业核心课程

本专业开设 6 门专业核心课程，包括 Web 应用安全与防护、操作系统安全、电子数据取证技术应用、网络设备配置与安全、信息安全产品配置与管理、信息安全风险评估。

表 4　专业核心课程描述

课程代码	课程名称	课程目标	主要内容	教学要求
023638	Web 应用安全与防护	1.掌握 Web 应用安全基础原理及 HTTP 协议安全特性； 2.能精准识别 SQL 注入、XSS、CSRF 等常见 Web 漏洞的成因与特征； 3.熟练运用 Web 安全防护技术进行漏洞修复与安全加固； 4.具备 Web 应用安全评估的基础能力与漏洞处置的职业素养。	1.Web 安全基础：HTTP 协议安全机制、Web 应用架构与安全风险； 2.核心漏洞解析：SQL 注入（类型、检测与利用）、XSS（存储型 / 反射型/ DOM 型）、CSRF 攻击原理与场景； 3.防护技术实践：输入过滤与输出编码实现、安全框架配置、验证码与 Token 防伪造机制； 4.安全评估实训：使用 Burp Suite 等工具进行漏洞扫描，编写简易安全评估报告。	1.能独立分析 HTTP 请求包并识别协议层安全隐患，准确率不低于 90%； 2.可运用手工检测与工具扫描（Burp Suite）定位 3 类以上 Web 漏洞，漏洞识别率达 85% 以上； 3.能针对具体漏洞编写防护代码，安全加固方案有效率不低于 80%； 4.完成 1 个完整 Web 应用的安全评估实训，提交规范的漏洞报告并给出可落地的修复建议。
023639	操作系统安全	1.掌握 Windows 和 Linux 操作系统安全核心知识，包括账户管理、权限控制、数据保护逻辑； 2.能独立完成操作系统安全配置、应用服务安全部署； 3.具备操作系统安全监控（日志分析）、软件限制、备份与恢复的实操能力，能定位基础系统安全问题； 4.了解系统安全分析与风险排查思路，能制定简单的操作系统安全防护方案。	1.操作系统安全基础：Windows/Linux 安全架构差异、账户安全、密码策略； 2.核心安全配置：数据安全（文件加密、权限设置）、网络与应用服务安全、系统软件限制（软件安装白名单、进程权限管控）； 3.监控审计：Windows 事件日志分析、Linux /var/log 日志检索、安全审计工具配置； 4. 备份与恢复：Windows 备份工具、Linux tar/rsync 命令实操、故障恢复（如系统修复模式、数据恢复软件使用）。	1. 能独立完成 Windows/Linux 的安全配置，配置合规率不低于 90%； 2.能通过日志分析定位 3 类以上系统安全问题，问题定位准确率达 85%以上； 3.能独立完成操作系统数据备份与故障恢复，恢复数据完整性达 95%以上，恢复耗时不超过 30 分钟；4.完成 1 个操作系统安全加固项目，提交加固方案与验证报告，方案有效率达 80%以上。
023640	电子数据取证技术应用	1.掌握电子数据取证标准流程（准备—提取— 分析—固化—报告）与核心技术	1. 取证基础：电子数据取证概念、标准流程、取证设备介绍； 2.存储与文件系统：计	1.能独立完成计算机或移动设备的数据提取，提取成功率不低于 90%；

		原理； 2.能精准分析计算机、移动设备的存储结构与文件系统特征； 3.具备使用专业工具完成数据提取、文件恢复、证据固化的实操能力，能处理简单取证场景； 4.熟知电子数据取证法律法规（如《电子数据取证规则》）与合规要求，能编制规范的电子数据取证报告。	算机硬盘分区结构、Windows NTFS/Linux ext4 文件系统、Android/iOS 存储分区； 3.核心技术实操：逻辑提取（文件复制、日志导出）、哈希计算、文件恢复、镜像制作； 4.工具应用：免费取证工具实操、镜像文件分析、数据检索技巧； 5.案例与合规：文件误删恢复、微信/ QQ 聊天记录提取等模拟案例实践、取证过程录像与文档记录规范、《刑事诉讼法》中电子证据合法性要求。	2.能使用工具恢复 3 类以上被删除/隐藏数据（如文档、聊天记录、上网痕迹），恢复准确率不低 85%； 3.能正确计算数据哈希值进行证据固化，固化正确率 100%，无数据篡改风险； 4.完成 1 个模拟取证案例（如“办公电脑误删重要文档”），提交取证流程记录与规范报告，报告合规率达 100%，证据链完整性达 90%以上。
023641	网络设备配置与安全	1.掌握路由器、交换机的工作原理（如路由转发、VLAN 隔离）与基本配置方法（命令行 / Web 界面）； 2.能独立完成路由协议配置、NAT 转换、VLAN 划分与 Trunk 配置、链路聚合实操； 3.具备中小型网络拓扑搭建、安全配置（如端口安全、ACL 访问控制）与故障排查的实操能力； 4.了解生成树协议（STP/RSTP）原理与网络冗余配置逻辑，能通过综合组网项目优化网络安全性。	1.路由器配置：路由器工作原理、静态路由配置、OSPF 协议配置、NAT 转换实操； 2.交换机配置：交换机工作原理、VLAN 划分与 Trunk 链路配置、链路聚合配置、端口安全； 3.网络安全配置：ACL 访问控制列表配置、生成树协议配置、网络设备密码策略； 4.组网与故障排查：中小型网络拓扑规划、ENSP 仿真软件实操、综合组网项目（如企业内网搭建）、故障模拟与排查。	1.能搭建中小型网络拓扑，配置完成率不低于 90%； 2.能独立完成 OSPF 协议配置、 NAT 转换与 ACL 访问控制，网络连通性达 100%，数据转发延迟不超过 10ms； 3.能定位并排除 常见网络故障，排查成功率不低于 85%； 4.完成 1 个综合组网安全项目，提交配置文档与测试报告，网络运行稳定性达 95%以上。
023642	信息安全产品配置与管理	1.掌握防火墙、入侵检测系统（IDS）、安全审计系统的工作原理与典型应用场景（如企业边界防护、内网监控） 2.能独立完成主流安全产品（华为 USG 防火墙）的基础配置（策略新增/修改、规则优化）；	1.产品基础：防火墙、IDS、安全审计系统的工作原理、核心功能与应用场景； 2.防火墙配置：华为 USG 防火墙访问控制策略、NAT 配置、VPN（IPsec/L2TP）搭建、攻击防护； 3. IDS 配置：IDS 规则编写（基础规则语法）、	1.能独立完成华为 USG 防火墙访问控制策略/ IDS 检测规则配置，配置有效性不低于 90%； 2.能通过安全审计系统日志定位 2 类以上异常行为（如异常 IP 访问、敏感操作），定位准确率不低于 85%；

		3.具备安全产品日常管理（设备状态监控、日志查看）、异常行为分析（如攻击流量识别）与故障处置的实操能力； 4.了解不同安全产品的协同防护逻辑（如防火墙 + IDS 联动），能搭建基础的企业安全防护体系。	检测模式设置、告警日志查看与分析、误报 / 漏报优化； 4.安全审计配置：安恒明御安全审计系统日志采集、审计报表生成、异常行为告警设置； 5.协同与管理：防火墙与 IDS 联动配置、安全产品状态监控（CPU/内存使用率、接口状态）、日常维护（配置备份/恢复）。	3.能独立完成安全产品配置备份与恢复，恢复成功率达 90%； 4.完成 1 个安全产品协同防护场景配置，提交配置文档与测试报告，防护策略有效率达 90% 以上。
023643	信息安全风险评估	1.掌握信息安全风险评估标准（GB/T 23694）、网络安全等级保护测评标准（GB/T 22239）核心要求与风险评估核心流程； 2.能精准识别物理、数据、主机、网络、应用层的资产与脆弱性，同时结合等保 2.0 对应级别（二级/三级）要求识别合规性差距； 3.具备使用评估工具开展风险检测、结合等保测评要点编制风险评估与合规性测评报告的实操能力； 4.了解应急响应策略制定逻辑，能针对评估结果及等保合规要求提出可行的风险处置与合规整改方案。	1.评估基础：信息安全风险评估概念、GB/T 23694 标准框架、网络安全等级保护 2.0 体系、风险评估全流程； 2.资产与威胁识别：资产分类与价值评估、威胁来源分析，结合等保测评资产核查要求开展资产清查与等级确定； 3.脆弱性与专项测评：脆弱性识别方法，物理安全、数据安全、主机安全、网络安全、应用安全专项测评要点，同步对照等保 2.0 对应级别安全要求开展合规性测评； 4.风险计算与处置：风险值计算方法、风险等级划分，等保合规性判定规则，风险处置策略与等保合规整改方案制定、应急响应基础； 5.案例与报告：中小型企业风险评估与等保测评融合模拟案例，风险评估报告结构编写，含等保合规性差距分析与整改建议章节。	1.能完成 1 个中小型企业的资产识别与等保等级确定，资产识别覆盖率不低于 90%，等级判定符合等保要求； 2.能使用工具扫描并评估 3 类以上层面的脆弱性，结合等保 2.0 对应级别测评项开展合规性检查，脆弱性识别率不低于 85%，风险等级与合规性判定准确率达 90%； 3.能独立计算风险值，结合等保合规要求制定对应的风险处置与合规整改方案，方案可行性与合规性不低于 80%； 4.完成 1 份模拟企业风险评估与等保合规性测评融合报告，提交资产清单、风险矩阵、合规性差距分析与处置整改方案，报告完整性、逻辑性与合规性达 90%以上。

（3）专业拓展课程

本专业开设 4 门专业拓展课程，包括数据备份与恢复、网络渗透测试、无线网络安全技术、信息安全项目管理，学生任选 2 门。

表 5　专业拓展课程描述

课程代码	课程名称	课程目标	主要内容	教学要求
023644	数据备份与恢复	1.掌握数据备份与恢复基础理论，包括信息系统存储架构、文件系统安全特性及数据丢失风险分析逻辑； 2.熟悉主流备份技术差异，能区分全量/增量/差异备份适用场景，掌握快照、容灾备份的核心原理； 3.具备针对不同场景制定备份方案的能力； 4.熟练执行数据恢复操作，可完成故障诊断、完整恢复等，具备备份方案落地与应急演练组织能力。	1.数据存储基础：信息系统存储架构、文件系统数据存储逻辑、数据丢失类型与风险成因； 2.备份技术与工具：全量备份、增量备份、差异备份的操作流程与适用场景，及主流工具实操； 3.备份方案设计：数据库备份策略、业务系统备份周期规划、异地容灾方案设计； 4.数据恢复流程：故障诊断、数据校验、恢复操作； 5.容灾与演练：容灾备份体系构建逻辑、应急演练方案、演练记录与方案优化。	1.能独立分析 3 类以上数据丢失场景的风险成因，分析准确率不低于 90%； 2.可针对数据库或业务系统制定备份方案，方案可行性达 90% 以上； 3.能使用 Veeam 或备份一体机完成模拟数据恢复，恢复数据完整性达 95% 以上； 4.完成 1 次容灾应急演练，含演练方案、执行记录、复盘报告，演练流程合规率达 100%，复盘报告可落地优化建议不少于 3 条。
023645	网络渗透测试	1.掌握网络渗透测试标准流程，包括信息收集、漏洞检测、漏洞利用、权限维持、痕迹清除、报告编写全环节逻辑； 2.能精准运用渗透测试工具完成信息收集、漏洞检测与漏洞验证； 3.熟悉常见攻击技术，可实现密码攻击、社会工程学攻击、内网横向渗透的基础操作； 4.具备网络渗透测试全流程执行能力，能规范编写渗透测试报告，具备漏洞处置的职业素养。	1.渗透测试基础：渗透测试定义与合规性、核心战术、渗透测试文档规范； 2.信息收集技术：被动信息收集、主动信息收集； 3.漏洞检测与利用：Web 漏洞检测、系统漏洞检测；漏洞利用；4.专项攻击技术：密码攻击、社会工程学、规避技术； 5.深度渗透与报告：内网横向渗透、痕迹清除、渗透测试报告编写。	1.能独立完成 1 个目标网络的信息收集，资产识别覆盖率不低于 90%，端口扫描准确率达 85%以上； 2.可运用工具+手工检测定位 3 类以上漏洞，漏洞利用成功率不低于 70%； 3.能编写渗透测试报告，报告包含漏洞截图、复现步骤、修复建议，报告完整性与逻辑性达 90%以上； 4.完成 1 个中小型网络的模拟渗透测试项目，提交测试计划、过程记录与最终报告，项目完成合规率达 100%。
023646	无线网络安全技术	1.掌握无线网络原理，包括 802.11 系列协议特性、无线网络架构及数据传输逻辑； 2.熟悉无线网络安	1.无线网络基础：802.11 系列协议速率 / 频段差异、无线网络架构、数据帧类型及传输流程； 2.安全机制解析：	1.能独立分析无线网络协议帧，识别协议层安全隐患，准确率不低于 90%； 2.可使用 Aircrack-ng/Wireshark

		全机制差异，能区分 WPA/ WPA2/ WPA3 加密原理，识别 WEP 协议安全缺陷； 3.能精准识别常见无线网络攻击手段，掌握攻击检测工具的使用方法； 4.具备无线网络安全配置与管理能力，可完成 AP 安全配置、无线路由器防护策略部署，能制定无线网络安全运维方案。	WEP/WPA/WPA2/WPA3 协议的加密流程与安全优势； 3.攻击手段与检测：抓包破解攻击、ARP 欺骗攻击；攻击检测； 4.防护技术与配置：无线网络安全配置、无线路由器防护、企业级防护； 5.运维方案设计：无线网络覆盖规划、定期安全巡检、安全事件响应。	检测 2 类以上无线网络攻击，攻击识别准确率达 85%以上； 3.能完成 AP 安全配置，配置合规率达 100%，无线连接稳定性达 95% 以上； 4.完成 1 个中小型无线网络的安全配置与攻击检测实训，提交配置文档与攻击检测报告，方案有效率达 80% 以上。
023647	信息安全项目管理	1.掌握信息安全项目管理标准框架，理解信息安全项目的特殊性； 2.具备信息安全项目全生命周期管理能力，可完成项目立项、计划制定、资源协调； 3.能开展项目执行与风险管控，识别信息安全项目常见风险，制定风险应对策略，具备项目质量监督与变更管理能力； 4.熟练完成项目收尾工作，能编写项目总结报告，具备协调多方解决项目问题的职业素养。	1.项目管理基础：信息安全项目定义与特点、核心过程组和分类； 2.项目启动与规划：立项可行性分析、项目需求调研、计划制定； 3.项目执行与团队管理：项目团队构建、沟通管理、信息安全需求转化； 4.风险与质量管控：信息安全项目常见风险、风险识别与评估、应对策略；项目质量监督； 5.项目收尾与案例：项目验收、文档归档、项目总结；典型案例。	1.能独立完成 1 个信息安全项目的 WBS 工作分解，分解颗粒度符合项目执行需求，完整性达 90% 以上； 2. 可识别信息安全项目 3 类以上常见风险，制定对应的应对策略，策略可行性达 85%以上； 3. 能编写规范的项目计划与验收报告，文档包含核心要素，合规率达 100%； 4.以小组形式完成 1 个虚拟安全项目全流程管理，提交项目计划、风险报告、验收文档，项目按时交付率达 100%，团队协作评分不低于 85 分。

六、教学进程总体安排

见附录一：信息安全技术应用专业教学进程表；附录二：学时与学分分配表。

七、实施保障

（一）师资队伍

表 6　师资队伍结构与配置表

类别	数量	具体要求
师资队伍结构	8	学生数与本专业专兼任教师数比例为 18:1，双师素质教师占专业教师比为 75%。
专业负责人	1	副教授职称，能够较好地把握国内外网络安全行业、专业发展动态，能广泛联系行业企业，了解行业企业对信息安全技术应用专业人才的需求实际，教学设计、专业研究能力强，组织开展教科研工作能力强，在区域或全国信息安全职业教育领域具有一定的专业影响力。
专任教师	5	具有高校教师资格和本专业领域有关证书； 有理想信念、有道德情操、有扎实学识、有仁爱之心； 具有全日制研究生等相关专业本科及以上学历； 具有扎实的本专业相关理论功底和实践能力； 具有较强的信息化教学能力，能够开展课程教学改革和科学研究； 每 5 年累计不少于 6 个月的企业实践经历。
兼职教师	2	主要从网络安全企业、安全测评机构、网络安全监管机构等相关企业、机构聘任，具备良好的思想政治素质、职业道德和工匠精神，具有扎实的信息安全技术应用专业知识和丰富的实际工作经验，具有中级及以上相关专业职称或行业权威认证，能承担专业课程教学、实习实训指导和学生职业发展规划指导等教学任务。

（二）教学设施

主要包括能够满足正常的课程教学、实习实训所需的专业教室、实训室和实训基地。

1.专业教室基本条件

具备利用信息化手段开展混合式教学的条件。配备了黑板、多媒体计算机、投影设备、音响设备，具有互联网接入和无线网络环境及网络安全防护措施。安装有应急照明装置，状态良好，符合紧急疏散要求，安防标志明显，保持逃生通道畅通无阻。

2.校内实训室基本要求

（1）网络组建实训室

配备中控台及功放系统、多媒体教学系统、投影仪与幕布、白板，以及计算机、交换机、路由器、服务器、Web 应用防火墙、防火墙、入侵检测系统、漏洞扫描设备、日志审计设备、上网行为管理监控等设备。用于计算机网络基础、数据备份与恢复、网络设备配置与安全、信息安全产品配置与管理等课程实训教学。

（2）操作系统安全实训室

配备中控台及功放系统、多媒体教学系统，以及投影仪与幕布、白板、交换机、计算机 （工作站）、服务器等设备，安装操作系统（Windows、Linux）和数据库、软件开发、网页设计等相关软件，用于 Web 前端技术、操作系统安全、数据库技术、电子数据取证技术应用、Python 编程基础等实训教学。

（3）网络安全攻防实训室

配备中控台及功放系统、多媒体教学系统，以及投影仪与幕布、白板、Web 应用防火墙、堡垒服务器、日志服务器、Web 攻防平台、计算机（工作站）等设备，安装渗透测试工具、虚拟机等相关软件，用于 Web 应用安全与防护、网络渗透测试、信息安全风险评估、信息安全项目管理等实训教学。

表 7　校内实践教学条件配置

序号	实验室或实训室名称	实验实训项目名称	主要实验实训仪器设备	备注
1	网络组建实训室	中小型网络组建、综合路由交换、信息安全产品配置、数据备份与恢复等	50 台高规格多媒体电脑、核心交换机、汇聚交换机、接入交换机、防火墙、入侵检测系统、漏洞扫描设备、上网行为管理监控设备	相关配套器材
2	操作系统安全实训室	Linux 操作系统配置、Windows Server 操作系统配置、系统安全加固、网站开发、数据库设计等	50 台高规格多媒体电脑、操作系统虚拟化功能的软件	相关配套器材
3	网络安全攻防实训室	信息安全风险评估、网络渗透、电子数据取证、Web 应用安全与防护、流量分析等	50 台高规格多媒体电脑、Web 攻防平台、服务器、Web 应用防火墙	相关配套器材

3.学生实习基地基本要求

校外实训基地基本要求为：具有稳定的校外实训基地；能够开展信息安全技术与应用专业相关实训活动，实训设施齐备，实训岗位、实训指导教师确定，实训管理及实施规章制度齐全。

表 8　校外实践教学条件配置

序号	实习实训基地名称	实习实训项目名称	备注
1	河南信安世纪科技有限公司	网络安全应急响应、网络安全运维	
2	河南网训科技有限公司	路由与交换、网络安全	
3	河南奇联西智能科技有限公司漯河分公司	网络安全运维	

（三）教学资源

1.教材选用

教材选用按照国家规定及学校教材选用规范程序，优先选用“十四五”职业教育国家规划教材、信息安全领域优秀教材；专业核心课程教材需体现网络安全攻防新技术（如 APT 攻击防御、零信任架构）、行业新规范（《网络安全等级保护基本要求》）、职业技能新标准（“1+X”网络安全应用证书标准），并联合河南信安世纪合作企业开发 Web 安全技术、数据安全防护等活页式教材、数字化讲义，通过“纸质教材+数字资源”组合实现内容动态更新。

2.图书文献配置

图书文献配置图书文献需满足人才培养、专业建设与教科研需求，核心配置三大类：一是信息安全技术类（如《网络安全实践指南》和《渗透测试实战》）、行业标准类（如《信息安全技术》和《数据安全分级指南》）；二是实务案例类（如企业网络安全事件处置案例集、网络安全赛项案例汇编）；三是新技术前沿类（如零信任安全、AI 驱动的威胁检测相关图书），每年更新专业图书占比不低于 15%，同步补充信息安全工程师证书培训、攻防竞赛相关参考资料，支撑师生课内外学习。

3.数字资源配置

数字资源配置构建“实战导向”的专业数字资源库：一是基础教学资源，含信息安全核心课程音视频素材（如漏洞复现视频）、PPT 课件、数字化习题；二是实战实训资源，配备网络攻防虚拟仿真平台（如 Web 漏洞靶场、CTF 竞赛模拟环境）、安全运维模拟软件（如 ENSP 和 GNS3 模拟器）、企业真实案例库（如电商平台数据泄露应急处置案例）；三是协同资源，接入国家高等教育智慧教育平台信息安全精品课程、合作企业（如河南信安世纪科技有限公司）共享的运维日志数据集，资源库需定期更新（每学期补充新技术案例），支持学生自主实训、教师项目化教学，满足“攻防实操、漏洞演练”等专业核心能力培养需求。

（四）教学方法

通过“项目筑基、赛证进阶、产教落地、数字赋能”四阶联动的教学方法，实现从理论到岗位实战的能力培养闭环。具体四阶划分及联动逻辑如下：

第一阶：项目化教学——岗位能力筑基

以真实岗位任务为载体，完成“理论→实操”的基础转化，依托 6 门专业核心课程（如《Web 应用安全与防护》），将 SQL 注入原理、WAF 防火墙配置等理论拆解为“企业官网安全评估”

和“边界防护搭建”等项目任务。

第二阶：岗赛证融合教学——能力标准进阶

对接行业标准与竞赛要求，实现“基础能力→高阶技能”的跃升。将 NISP、CISP、HCIP 等证书的考点嵌入《Web 应用安全与防护》和《信息安全产品配置与管理》等课程，以实现证书与课程内容衔接。把省级攻防赛的“流量分析”和“电子数据恢复”题型转化为实训项目，如 2 小时内完成“中小型网络渗透”全流程，以赛促练强化实战突破能力。

第三阶：产教协同教学——真实场景落地

引入企业资源，完成“校内实训→岗位实战”的场景迁移。邀请河南信安世纪、奇联西智能等行业导师进课堂，讲解真实应急响应案例，指导等保测评项目规划，以实现双师指导。同时与企业实施实训联动，先在校内完成 Web 渗透与防护、Linux 服务器加固等基础训练，再赴企业参与安全巡检、应急响应等岗位实训，还原岗位真实工作流程。

第四阶：数字赋能教学——技术迭代保障

依托数字化工具，破解“场景有限、技术更新快”的痛点。通过虚拟仿真平台（如 Web 漏洞靶场、CTF 模拟环境）复现 APT 攻击、勒索病毒等高危场景，供学生反复实操演练，降低实体设备风险。借助专业数字资源库，推送 Log4j2 等新型漏洞的复现视频，教师通过平台数据定位学生流量分析等薄弱环节，开展精准辅导。

（五）学习评价

对于公共基础课程，完全服从学院安排进行考核；对于专业基础课程和主干核心课程，以专业“岗位能力适配”为核心，构建“过程性评价+终结性评价+补充评价”三维评价。

第一维：过程性评价（占比 60%）

聚焦日常能力养成，覆盖学习全环节。以“边学边评”为原则，重点评估学生在课程学习、实训中的实操能力与职业素养，避免“期末一次性考核”的局限性。主要包括实操评价（30%）、项目报告评价（20%）和职业素养评价（10%）。

第二维：终结性评价（占比 40%）

聚焦岗位实战能力，检验综合应用水平。以“模拟真实岗位场景”为核心，评估学生综合运用知识解决复杂问题的能力，突出 “实战性” 与 “项目落地性”。包括岗位实操考核（25%）和综合项目答辩（15%）。

第三维：补充评价

衔接行业标准与企业需求，拓展评价维度。作为核心评价的补充，强化“证书—竞赛—实

习”与岗位能力的关联，提升评价的行业适配性。包括证书与竞赛加分和企业导师实习评价。

（六）质量管理

1.建立了专业建设和教学质量诊断与改进机制、专业教学质量监控管理制度，制定了课堂教学、教学评价、实习实训、毕业设计以及专业调研、人才培养方案更新、资源建设等方面标准，通过教学实施、过程监控、质量评价和持续改进，实现人才培养规格。

2.建立了教学管理机制，加强日常教学组织运行与管理，定期开展课程建设水平和教学质量诊断与改进，建立了巡课、听课、评教、评学等制度，已建立与企业联动的实践教学环节督导制度，严明教学纪律，强化教学组织功能，定期开展公开课、示范课等教研活动。

3.建立了毕业生跟踪反馈机制及社会评价机制，并对生源情况、在校生学业水平、毕业生就业情况等进行分析，定期评价人才培养质量和培养目标达成情况。

4.专业教研室充分利用评价分析结果，有效改进专业教学，持续提高人才培养质量。

八、毕业要求

本专业学生毕业时应达到培养目标及培养规格的素质、知识和能力等方面要求，同时满足以下条件。

（一）学分条件

本专业学生在毕业前总学分须取得 148 学分，最低学分要求及所包括内容如下表。

表 9 最低学分要求

课程类别		最低学分
公共基础及素质教育课程	必修课程	38
	限选课程	8
	任选课程	4
	合计	50
专业课程	专业群共享及专业基础课	28
	专业核心课程	30
	专业拓展课程	8
	合计	66
岗位实习及单列实习实训		32
总计		148

（二）证书

学生在校期间，应考取必要的基本能力证书及职业资格证书，鼓励学生考取多项职（执）

业资格证书。

表 10　考取证书一览表

证书类别	证书名称	考证等级要求	备注
基本能力证书	英语等级证书	B 级以上	任选其中 1 项
	普通话证书	乙级以上	
	计算机等级考试	一级以上	
职（执）业资格证书	华为 HCIA	初级	任选其中 1 项
	华为 HCIP	中级	
	国家注册信息安全渗透测试工程师（CISP-PTE）	高级	
	国家信息安全水平考试（NISP）	一级	
	国家信息安全水平考试（NISP）	二级	
	国家信息安全水平考试（NISP）	三级	
	信息安全工程师（软考）	中级	
	网络安全管理员	三级	

附录一　信息安全技术应用专业教学进程表

课程类别		序号	课程名称	课程代码	学时		学分	开课学期与周学时						开课单位	考核方式
					理论	实践		一	二	三	四	五	六		
公共基础及素质教育课程	必修课	1	思想道德与法治	161010	44	4	3	4/12						马院	考试
		2	毛泽东思想与中国特色社会主义理论体系概论	18010013	32	4	2		2						考试
		3	习近平新时代中国特色社会主义思想概论	161008	46	8	3			4/14					考试
		4	※形势与政策㈠	161004	8	0	0.25								考查
		5	※形势与政策㈡	161005	8	0	0.25								考查
		6	※形势与政策㈢	161006	8	0	0.25								考查
		7	※形势与政策㈣	161007	8	0	0.25								考查
		8	中国共产党历史	161011	16	0	1		1						考试
		9	※军事理论	231001	36	0	2		2					学工部	考查
		10	军事技能	231006	0	112	2	2 周							考查
		11	劳动教育	231003	6	30	2	1	1						考查
		12	※大学生心理健康	231005	36	0	2	2						公共教学部	考查
		13	大学体育㈠	101001	10	26	2	2						公共体育部	考试
		14	大学体育㈡	101002	10	26	2		2						考试
		15	大学体育㈢	101003	10	26	2			2					考试
		16	大学英语㈠	201001	64	0	4	4						公共教学部	考试
		17	大学英语㈡	201002	72	0	4		4						考查
		18	职业生涯规划	181001	18	4	1	1						招生就业处	考查
		19	创新创业教育	181002	16	16	2		1						考查
		20	大学生就业指导	181003	12	4	1				1				考查
		21	※实验室安全教育	141001	8	8	1	1						教务处	考查
		22	国家安全教育	161012	18	0	1			1				马院	考查
		小计			**486**	**268**	**38**	**11**	**11**	**6**	**1**				
	限选课	23	※美学与艺术史论		16	0	0.5	0.5						公共艺术部	考查
		24	※艺术鉴赏和评论		16	0	0.5	0.5							考查
		25	艺术体验和实践		0	16	1		1						考查

		26	高等数学	101007	72	0	4		4					公共教学部	考试
		27	※职业人文素养	101009	36	0	2	2							考查
		小计			**140**	**16**	**8**	**0**	**5**						
	任选课	28	公共任选课程		64	0	4							教务处	考查
		小计			**64**	**0**	**4**								
专业技能课程	专业共享及专业基础课	29	计算机应用基础	023632	24	40	4	4						人工智能学院	考试
		30	数据库技术	023633	36	36	4			4					考试
		31	Python 编程基础	023634	32	64	6	6							考试
		32	计算机网络基础	023635	32	32	4	4							考试
		33	Web 前端技术	023636	36	72	6		6						考查
		34	信息安全技术	023637	36	36	4		4						考试
		小计			**196**	**280**	**28**	**14**	**10**	**4**					
	专业核心课	35	Web 应用安全与防护	023638	36	72	6			6				人工智能学院	考试
		36	操作系统安全	023639	36	72	6				6				考试
		37	电子数据取证技术应用	023640	24	48	4				4				考查
		38	网络设备配置与安全	023641	36	72	6			6					考试
		39	信息安全产品配置与应用	023642	24	48	4				4				考试
		40	信息安全风险评估	023643	24	48	4				4				考试
		小计			**180**	**360**	**30**			**12**	**18**				
	专业拓展课	41	数据备份与恢复	023644	24	48	4			4				人工智能学院	考查
		42	网络渗透测试	023645	24	48	4			4					考查
		43	无线网络安全技术	023646	24	48	4				4				考查
		44	信息安全项目管理	023647	24	48	4				4				考查
		小计			**48**	**96**	**8**			**4**	**4**				
岗位实习及单列实习实训		45	毕业设计	024121	0	108	6					18/6		人工智能学院	考查
		46	岗位实习㈠	024122	0	180	10					18/10			考查
		47	岗位实习㈡	024123	0	288	16						18/16		考查
		小计			**0**	**576**	**32**								
教学计划总计					**1114**	**1596**	**148**	**25**	**26**	**26**	**23**				

备注：1.※表示线上教学课程，课时数不计入周学时，计入总学时☆表示线上、线下混合教学课

程，公共任选课程每学期初由教务处提供公共任选课程目录，学生自由选择。

2.每学期安排 20 周的教学活动，其中第 19、20 周为复习考试时间。

3.美学和艺术史论类含《美术欣赏》《音乐欣赏》2 门课程，学生任选 1 门；艺术鉴赏和评论类含《书法鉴赏》、《影视鉴赏》、《艺术导论》、《舞蹈鉴赏》、《戏剧鉴赏》、《戏曲鉴赏》6 门课程，学生任选 1 门；艺术体验和实践类含《手工剪纸》《硬笔书法》《手机摄影》《手工编织》《戏剧教育》《现代舞》《歌曲演唱》《大学美育》8 门课程，学生任选 1 门。

附录二　学时与学分分配表

课程类型	学分数	学时数	占总学时百分比(%)	实践学时	占总学时百分比(%)	选修课学时	占总学时百分比(%)
公共基础及素质教育课程	50	974	35.94	284	10.48	220	8.12
专业（技能）课程	66	1160	42.80	736	27.16	144	5.31
岗位实习及单列实习实训	32	576	21.26	576	21.25	0	0.00
总　计	148	2710	100	1596	58.89	364	13.43

编制说明

本专业人才培养方案适用于三年全日制高职信息安全技术应用专业，由漯河职业技术学院人工智能学院专业建设委员会组织专业教师，与河南信安世纪科技有限公司、河南网训科技有限公司、河南奇联西智能科技有限公司漯河分公司等合作企业的专家共同制订，经学校党委会审定，批准从2025级信息安全技术应用专业学生开始实施。

主要编制人员一览表

序号	姓　名	所 在 单 位	职称/职务	签　名
1	李会凯	漯河职业技术学院	副教授/人工智能学院院长	
2	王鸿飞	漯河职业技术学院	副教授/人工智能学院副院长	
3	王淑娟	漯河职业技术学院	副教授/教研室主任	
4	赵永乐	漯河职业技术学院	副教授/教研室主任	
5	孙祥春	漯河职业技术学院	讲师	
6	左晓静	漯河职业技术学院	副教授	
7	谭会君	漯河职业技术学院	副教授	
8	欧阳玉峰	漯河职业技术学院	讲师	
9	韩银贺	漯河职业技术学院	助教	
10	常玉存	河南信安世纪科技有限公司	工程师/部门经理	
11	郑西刚	河南网训科技有限公司	高级工程师/总经理	
12	杨小龙	河南奇联西智能科技有限公司漯河分公司	工程师/总经理	

专业负责人：

复核人：

人工智能学院院长：

漯河职业技术学院

专业人才培养方案论证与审定意见表

	姓　名	单　位	职务/职称	签　名
专业建设指导委员会成员	李会凯	漯河职业技术学院	人工智能学院院长/副教授	李会凯
	王鸿飞	漯河职业技术学院	人工智能学院副院长/副教授	王鸿飞
	赵永乐	漯河职业技术学院	秘书/副教授	赵永乐
	程学军	漯河职业技术学院	教研室主任/教授	程学军
	李娜	漯河职业技术学院	教研室主任/教授	李娜
	王红纪	漯河职业技术学院	教研室主任/副教授	王红纪
	武世栋	中国移动漯河分公司	部门经理/高级工程师	武世栋
	吴铭烨	中国电信漯河分公司	云中台总师/高级工程师	吴铭烨
	王宇光	漯河市大数据运营有限公司	部门经理/工程师	王宇光

论证意见：

本专业群人才培养方案编制规范，科学合理，符合《国家职业投育改革实施方案》《河南省职业教育改革实施方案》《职业教育专业教学标准(2025 版)》文件要求，能够满足三年全日制高职信息安全技术应用专业培养需要，同意从 2025 级信息安全技术应用专业学生开始实施。

专业建设指导委员会主任签名：李会凯

2025 年 8 月 19 日

审定意见：

中共漯河职业技术学院委员会（签章）

年　月　日