《信息安全技术与实施》
课程标准

Curriculum Standards

（2024 年修订）

重庆电子工程职业学院　人工智能与大数据学院 编印
Chongqing college of Electronic Engineering

目　录

开课学院	人工智能与大数据学院
课程名称	信息安全技术与实施
课程代码	6108020042
适用专业（群）及班级	计算机大类专业
学制学历及教育类别	三年制高职教育
课程学分	4 学分
课程学时	64 学时
编制人/修订人	武春岭、梁雪梅
平台/模块主任审核	张靖
系（群）主任审核	鲁先志
二级学院教学院长审定	何欢
制订/修订时间	2024 年 8 月

一、课程性质与任务

（一）课程性质与定位

《信息安全技术与实施》课程是信息安全技术应用专业（校警合作班）二年级第一学期开设的专业核心课程（必修课程）。该课程旨在培养学生对信息系统的安全测试和安全防范技术实施的技能，使学生掌握信息系统的脆弱性及脆弱感性测试的新方法，能够分析信息系统安全需求，选择和运用安全防范技术，同时培养学生的方法能力、社会能力及职业素质。为学生发展成为具有信息安全“攻”、“防”、“测”、“控”、“管”、“评”综合能力的技术技能型网络安全卫士奠定基础。课程内容对接网络安全评估、网络安全运维职业技能等级证书（中级）X 证书的必备知识和技能。

前导课程：程序设计基础、数据库基础、计算机网络基础

后续课程：网络安全攻防技术、网络安全工程项目实践

（二）课程基本教学理念

（1）落实“立德树人”的根本任务。坚持育人为本、德育为先，充分挖掘与系统设计课程思政元素，培养“德智体美劳”全面发展的社会主义建设者和接班人。以学生为中心，关注学生的全面发展、和谐发展、持续发展、终身发展和健康成长。

（2）培养学生系统掌握专业基础知识。根据专业（群）人才培养目标与规格，按照理论实践一体、线上线下结合、岗课赛证相融通的设计理念，将行业的新技术、新工艺、新知识、新标准、新规范及职业资格认证、技能大赛相关知识与内容及时融入课程，培养学生掌握新一代信息技术相关产业链与岗位群所需要的信息网络领域系统的理论基础知识。

（3）培养学生熟练掌握专业核心技能。根据专业（群）人才培养目标与规格，将精益求精的工匠精神、追求卓越的劳动精神与专业信息网络领域技术技能提升相结合，以任务或项目为载体组织序化实习实训内容，坚持学做合一，要求学生掌握行业岗位通用的成熟技术与方法，在实践环节通过角色扮演、团队协同、个体体验、展示交流等手段，培养学生具备信息网络领域扎实的技术能力。

（4）培养学生具备创新性劳动的能力。培养学生产业数字化与数字产业化需要的技术技能创新能力，适应产业技术快速迭代升级与就业结构不断向高端技术层次转化，培养学生持续学习与终身学习能力，增强学生就业适应性。强化学生在具备过硬的思想政治素质、系统的专业理论知识和扎实的专业技能基础上，能够进行技术技能的创新，强调对学生创新创业意识的培养，深入挖掘学生自身的创造力，增强自主创新、原始创新、集成创新能力。

（三）课程任务

紧跟国家网络空间安全战略，响应时代需求，把控人才缺口，培养一批具有高水平网络空间安全“管理能力”与“技术能力”的复合型人才，有效促进我国网络安全行业蓬勃发展,为国家经济的转型升级发展提供网络安全保障。打磨课程内容，紧紧围绕信息安全技术应用国家高水平专业群信息安全技术应用专业网络安全运维工程师、风险评估工程师、网络安全测试工程师、数据安全工程师等职业岗位，培养学生具备 “网络安全策略配置能力”、“网络安全应急服务能力”、“网络安全测试”、“数据安全防护”等工作需求。立足课堂教学，培养学生网络安全设备基础设置和信息系统安全加固,为多分支机构企业的复杂基础网络架构进行安全策略设计和实施的基本能力,提高学生的独立思考能力和解决问题的能力，引导教育学生树立正确的网络安全观，培养学生精益求精的工匠精神和不畏艰难的劳动精神。

二、课程目标与要求

基于信息安全技术应用专业群人才培养方案,对接高等职业学校信息安全技术应用专业教学标准、网络与信息安全管理员国家职业技能标准、信息安全测试员国家职业技能标准、高等职业学校信息安全技术应用专业顶岗实习标准，以及网络安全运维工程师、风险评估工程师、网络安全测试工程师、数据安全工程师等岗位的相关要求；有机融入网络安全等级保护 2.0 新标准、世界技能大赛网络安全项目新规范、《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》新要求、网络安全评估、网络安全运维职业技能等级证书（中级）X 证书新技术，确定了三维教学目标和重难点，具体内容如下：

（一）知识目标

1. 熟悉信息安全要素、安全模型、技术体系及安全评估标准等基础知识；
2. 熟悉机房建设的安全等级及场地建设、电磁防护、存储介质保护、物理隔离等相关安全要求等知识；
3. 理解防火墙的概念、功能与缺陷、工作原理、体系结构等知识；
4. 熟悉入侵检测组成模型、工作原理、性能指标等知识；
5. 了解无线局域网的标准、理解无线局域网的安全协议和无线网络防护措施的知识；
6. 熟悉常见操作系统、域控服务器的安全机制等知识；
7. 理解计算机病毒的概念、分类、特点、作用机制与病毒传染过程等知识；
8. 熟悉应用系统渗透测试方法等知识；
9. 掌握常见漏洞产生、利用原理及防护方法等知识；
10. 理解数据泄漏、修复、防护的方法等知识；

11. 掌握古典密码、对称密码、非对称密码的工作机制以及数据加解密、数字签名、数字认证等密码技术应用工作机制等知识。

（二）能力目标

1. 能分析机房建设中网络系统的拓扑结构存在的安全隐患，并提出解决方案的能力；
2. 能根据网络安全需求制定网络安全设备设置方案的能力；
3. 能对防火墙、入侵检测系统、无线设备等网络设备进行安全策略配置的能力；
4. 能配置域控服务安全策略的能力；
5. 能根据实际需求配置操作系统的用户管理、文件管理、安全策略的能力；
6. 能检测恶意代码并提供解决方案的能力；
7. 能够熟练配置并使用各种网络安全渗透工具的能力；
8. 能根据目标系统的安全防护状态，开展有效的安全安全测试工作的能力；
9. 能针对所发现的系统弱点和网络攻击行为，制定并实施有效安全防护措施的能力；
10. 能够分析数据泄漏的原因，制定数据修复、数据安全保护措施等解决方案的能力；
11. 能根据安全需求对文件、系统等进行加解密、数字签名和数字认证等工作的能力。

（三）素质目标

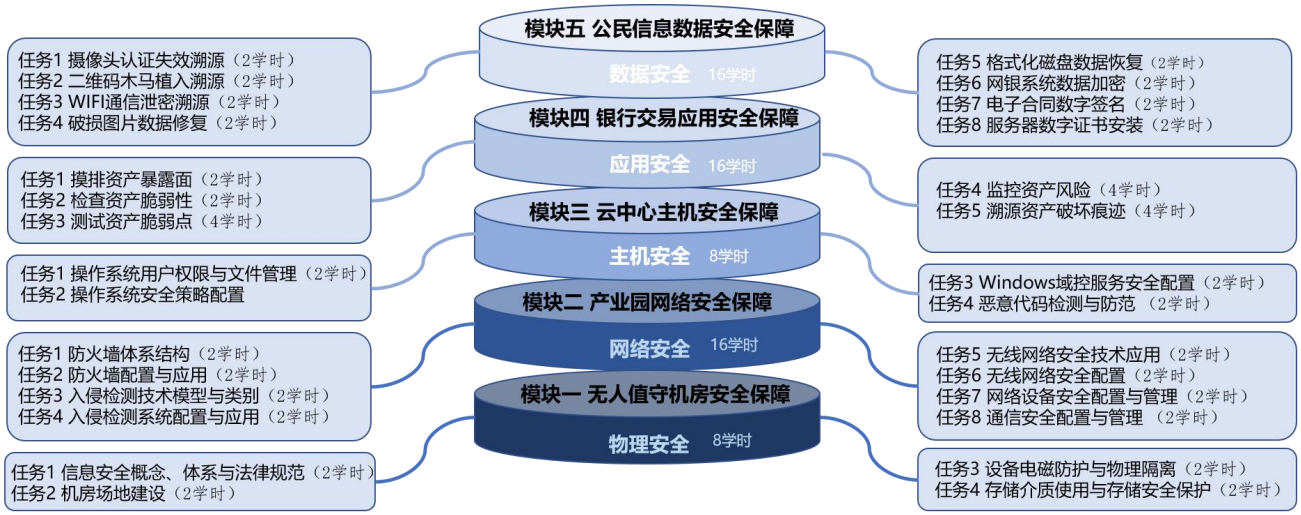
1. 具备精益求精的工匠精神；
2. 具备不畏艰难、爱劳动、讲节约的劳动精神；
3. 备求真务实、科学质疑精神、创新思维和创业精神；
4. 具备互联网思维和计算思维；
5. 具备学习新技术、新知识的能力；
6. 具备分析、计划、实施和监控工作任务的工程管理能力；
7. 具备从事网络安全行业工作的良好个人隐私保护意识和信息安全职业道德；
8. 具备遵守网络安全行业法律法规和行业标准的合规意识；
9. 具有在推动国产化、数字化方面国家安全战略意识；
10. 具备正确的网络安全观。

三、课程结构与内容

（一）课程结构

课程结构以网络安全运维工程师、风险评估工程师、网络安全测试工程师、数据安全工程师等岗位中安全评估、渗透测试、安全产品策略配置、数据安全保护等典型工作任务为核心。

依托我校与重庆市公安局成立的网络空间安全联合工程技术研究中心、与重庆市司法局成立的司法鉴定所的实际工作项目作为教学载体和教学案例。有机结合信息安全渗透测试员、网络与信息安全管理员职业标准、网络安全评估职业技能等级证书（1+X、中级）、网络安全运维职业技能等级证书（1+X、中级）内容要点，融入世界技能竞赛网络安全项目 A、B、C 三个模块和全国职业院校技能大赛信息安全管理与评估赛项的技能要求。依据网络安全等级保护 2.0 的网络安全技术防护体系，结合学生的身心发展规律、认知特点、专业特性、兴趣喜好，将教学内容分为五个层次化教学模块。模块划分为物理安全、网络安全、主机安全、应用安全、数据安全五个层次，帮助学生掌握信息安全防护相关的技术。



（二）课程内容与要求

表 2 课程内容与要求

教学模块	学习任务	学习内容与要求	学时
模块一 无人值守机房安全保障	任务 1 信息安全概念、体系与法律规范 任务 2 无人值守机房场地建设 任务 3 设备电磁防护与物理隔离 任务 4 存储介质使用与存储安全保护	1.了解黑客精神、黑客准则，树立网络安全报国情怀； 2.了解信息安全相关法律法规，树立知法、懂法、守法的法治观念； 3.熟悉信息安全体系架构与安全模型； 4.熟悉机房建设中防火、防盗、防水、温度、湿度、洁净度等安全要求，树立安全意识及劳动意识； 5.掌握机房建设信息安全等级标准要求，能判断机房建设图中存在的安全隐患。 6.通过“修改公交卡储值信息非法充值案例”分析，了解电磁干扰的隐患； 7.掌握电磁防护措施，能够提出电磁防护的解决方案； 8.熟悉物理隔离的技术路线和实现方法；	8

		9.熟悉硬盘、光盘等存储介质的保护措施。	
模块二 产业园网络安全保障	任务 1 防火墙体系结构 任务 2 产业园边界防火墙配置与应用 任务 3 入侵检测技术模型与类别 任务 4 核心服务器入侵检测系统配置与应用 任务 5 无线网络安全技术应用 任务 6 产业园区公共无线网络安全配置 任务 7 网络设备安全配置与管理 任务 8 通信安全配置与管理	1.在网络安全配置过程中，养成精益求精的工匠精神，了解安全标准，树立标准化意识； 2.了解防火墙及其相关概念，熟悉防火墙的功能与缺陷； 3.掌握包过滤防火墙、应用防火墙、电路级防火墙、规则检查防火墙四种类型防火墙应用层级及作用，以及防火墙的三种体系结构； 4.掌握 pfsense 防火墙和个人电脑防火墙的配置方法，能够根据产业园区网络划分状况配置防火墙策略； 5.了解入侵检测系统的概念和分类，掌握通用入侵检测系统的模型、功能和工作过程； 6.掌握异常检测模型、误用检测模型的作用及优缺点，能够区分两种模型的异同； 7.理解入侵检测系统的性能指标，能够根据产业园资产特点合理配合 snort 入侵检测系统； 8.了解无线网络的概念和无线局域网标准； 9.理解无线局域网安全协议的概念、性能指标等基本内容； 10.掌握无线网络扩频技术、用户认证和口令控制、数据加密等信息安全技术； 11.能配置产业园区无线网络设备，实现产业园区无线网络全覆盖； 12.掌握无线网络的缺陷和安全防护措施。 13.能配置通信设备，并根据需求进行设备日常运维管理。	16
模块三 云中心主机安全保障	任务 1 云服务器操作系统用户权限与文件管理 任务 2 云服务器操作系统安全策略配置 任务 3 Windows 域控服务安全配置 任务 4 恶意代码检测与防范	1.感知使用国产操作系统的重要性和振兴国产操作系统的民族责任感。 2.熟悉 Windows、Linux 等网络操作系统特性，能够区分 Windows、Linux 系统的安全机制的不同； 3.掌握网络操作系统用户权限管理方法，能够配置云中心机房主机用户权限策略； 4.掌握网络操作系统文件安全管理方法，能够配置	8

		云中心机房主机网络操作系统文件策略； 5.掌握网络操作系统安全策略配置方法，能够配置云中心机房主机操作系统安全策略； 6.掌握域控服务安全配置方法，能够配置云中心机房主机域控服务安全策略； 7.了解恶意代码的概念、分类、发展趋势及作用机制； 8.掌握预防和清除恶意代码的方法，能够使用杀毒软件检测并清除恶意代码； 9.能够对传播计算机病毒破坏主机安全案例分析，及网络安全法律要求。	
模块四 银行交易应用安全保障	任务 1 摸排资产暴露面 任务 2 检查资产脆弱性 任务 3 测试资产脆弱点 任务 4 监控资产风险 任务 5 溯源资产破坏痕迹	1.熟悉网络安全测试流程及实施规范，熟悉《GB/T 36627-2018 信息安全技术 网络安全等级保护测试评估技术指南》要求，树立标准规范意识和不触碰安全界限的职业底线； 2.在渗透测试过程中，树立合规、界限意识，树立严谨、创新、精益求精的工匠精神。 3.熟悉端口扫描等网络侦察手段及工作原理，掌握端口扫描操作方法及反侦查措施； 4.能够对水电气管理系统开展资产排查，梳理信息资产清单。 5.熟悉漏洞、漏洞扫描的概念，及漏洞扫描的工作原理，掌握漏洞扫描的方法。 6.能够使用 AWVS 等应用程序漏洞扫描器，获取水电气管理系统漏洞情况，并进行分析。 7.掌握 SQL 注入、XSS 等常见 Web 应用系统漏洞产生的机理和漏洞利用方法。 8.能够针对 SQL 注入、XSS 等常见应用漏洞利用工具进行渗透测试，评估漏洞对水电气应用系统带来的影响。 9.熟悉典型目标控制所使用的网络后门技术，掌握后门技术检测及清除方法； 10.熟悉入侵行为典型隐藏技术，掌握入侵行为追踪方法，能够针对 Web 服务器日志发现入侵行为； 11.掌握安全防护体系构建内容及方法； 12.熟悉网络安全事件应急响应流程，能够制定网络安全应急响应预案。	16
模块五 公民信息数据安全保障	任务 1 摄像头认证失效溯源 任务 2 二维码木马植入溯源 任务 3 WIFI 通信泄密溯源 任务 4 破损图片数据修复 任务 5 格式化磁盘数据恢复 任务 6 网银系统数据加密 任务 7 电子合同数字签名 任务 8 服务器数字证书安装	1.熟悉数据安全的相关知识，提升个人隐私数据保护意识、职业信息安全伦理道德、国家数据安全法律、法规和标准的要求。 2.在数据安全知识和技能学习的过程中，提升学生的求真务实、科学质疑、创新创造、诚信、责任担当、劳动伟大等优良传统美德。 3.了解“密码”和口令的区别，能够区分口令和“密码”，掌握口令复杂度的要求，能够编制、配置满	16

		足等级保护标准要求的高强度口令，能够检测口令的强度。 4.通过二维码、智能摄像头、免费 WIFI 等案例，掌握数据泄漏的途径，能够对常见数据泄漏现象进行溯源分析。 5.了解个人隐私数据的内容，掌握木马等后门程序的工作原理，能够制作二维码木马，并提出防范措施。 6.掌握流量分析等方法，能够发现流量中数据泄漏的问题。 7.掌握图片文件的格式，能够分析图片损坏原因，并进行修复。 8.掌握磁盘、文件目录的格式，能够对磁盘格式进行文件恢复。 9.理解并掌握古典密码、对称密码、非对称密码的工作机制，能够使用工具实现对数据进行加解密，实现隐私数据的保密性安全保障。 10.理解并掌握散列函数、数字摘要、数字签名的概念和工作机制，能够对电子数据进行数字签名，实现隐私数据的真实性保障要求。 11.理解并掌握数字证书的相关概念及工作原理，能够搭建具有数字证书的 Web 服务器，实现数据完整性保护功能。	
合计			64

四、学生考核与评价

（一）考核方式

以学生、任课教师、网安警官、项目导师构成四个评价主体，利用学习通平台、竞技考核平台全程采集学生学习数据，涵盖学习进度、课堂表现、攻防对抗演习等评价要素；考核评价标准数据安全工程师岗位能力要求，对接世赛网络安全项目、国赛信息安全管理与评估赛项、网络安全运维X证书、网络安全评估中级X证书、网络安全等级保护测评等标准；构建“多主体、多维度、国际化”考核评价体系，进行教与学全过程行为数据采集与分析，根据学生“职业性+意识性”素质提升情况探索个性化成长增值，优化结果评价，健全综合评价。

（二）考核指标与占比

表 3 考核指标与占比

评价构成	评价要素	评价主体	评价手段
过程性评价（60%）	出勤（5%）	教师	学习通平台

	资源学习（5%）	教师	学习通平台
	师生互动（10%）	教师+学生	学习通平台
	实践考核（30%）	教师	竞技考核平台
	理论测验（20%）	教师	学习通平台
	课后作业（10%）	教师+学生	学习通平台
	模块考核（20%）	教师	学习通平台
结果性评价（40%）	期末考试	教师	学习通平台
增值性评价（素质增值）	网络安全意识	教师	学习通平台
	操作规范性	项目导师 （国赛金牌获得者）	竞技考核平台
	职业规范性	网安警官	学习通平台

五、教学实施与保障

（一）实施过程

1.教学要求

（1）场地要求

学习场地、设施要求可根据实际情况分为本地教学要求和远程教学要求，在条件允许的情况下建议使用本地教学要求，如遇突发情况，无法开展本地教学的，则可以实行网络远程教学，采用远程教学要求。

本地教学要求：

① 具有计算机设备的实训室，计算机设备生均1台或笔记本生均1台；

② 具有良好的局域网环境；

③ 在局域网内具有网络攻防虚拟靶场平台设备，平台运行良好；

④ 在局域网内具有竞技考核平台，平台运行良好。

⑤ 远程教学要求：

⑥ 学生具备个人台式计算机或者笔记本电脑，生均1台，且学生所处环境具有良好的互联网环境；

⑦ 具有连接互联网的网络攻防虚拟靶场平台，平台运行良好。

⑧ 在局域网内具有竞技考核平台，平台运行良好。

2.教学组织

根据培养目标和教学内容，结合“互联网+”“智能+”信息化手段，教学团队基于“5E”（参与（Engagement）、探究（Exploration）、解释（Explanation）、迁移（elaboration）和评价（evaluation））教学模式创新性地提出了“情境竞技式”教学策略，将教学过程分为“感

→探→演→展→拓”五个环节，以项目任务为教学单元进行案例建构、情境创设和问题探究，实施启发式、参与式和探究式的课堂，运用情境导入法、角色扮演法、任务驱动法、直观演示法、启发式等教学方法按照五个环节、十个步骤动态组织教学。帮助学生从“感性、知性、理性”层层升级。实现个人学习与小组协作相结合，激发学生的学习兴趣，有效化解重难点，充分延伸学习时空，提高学生的专业能力、创新能力和素质能力，实现创新型、发展型、复合型的高素质技术技能人才的培养。

（二）实施保障

1.课程教学资源

（1）教材

教材选取应遵循“重庆电子科技职业大学教材建设与管理办法”的教材选用原则。必须依据本课程标准的要求选用或编写教材；教材应充分体现课程设计思想，满足课程内容的需要和岗位职责的要求，教材内容应符合国家职业标准，体现教学过程的实践性、开放性和职业性，要将本专业领域新技术、新工艺、新设备纳入教材中，体现教材的时代性。鼓励编写与教学相适应的学习指导教材，吸纳企业专家与学校教师合作编写教材。

推荐教材：“十四五”职业教育国家规划教材：信息安全技术与实施（第3版） [M].北京:电子工业出版社

（2）网络资源

学校提供了必要的软硬件支撑，为学生提供多元、丰富、优质的教学资源，实现人人皆学、处处可学、时时能学的智慧校园环境，为学生提供良好的学习条件和环境，满足网络安全实践的需要。

网络攻防虚拟靶场平台是按照世界技能大赛网络安全项目中规定的行业规范，联合网络安全企业进行联合开发设计。平台能够真实重现复杂企业网络环境，并且能够开展课程要求的所有网络安全场景。

竞技考核平台将教学任务颗粒化细分成了不同难度级别的竞技比赛关卡，授课中通过竞技考核平台发布网络安全攻防比赛场景，分步骤完成攻防闯关比赛。该平台可实时实现攻防态势变化，通过闯关积分作为技能评价依据。

学习通、中国大学生慕课、重庆市高校在线开放课程等课程学习资源，课程资源来自于信息安全技术应用国家级教学资源库。

大学生mooc网资源：

https://www.icourse163.org/course/cqcet-1461942168?from=searchPage&outVendor=zw_mooc_pcssjg_

2.设施、场地资源

（1）世界技能大赛集训基地

配有网络攻防虚拟靶场平台7套、竞技考核平台7套、核心交换机、汇聚交换机、接入交换机等设施设备，能够满足世界技能大赛网络安全项目应急响应、计算机取证、代码审计、CTF、网络流量分析等集训及培训任务，能够满足信息安全技术与实施、网络安全攻防技术、网络安全工程项目实践、系统渗透测试用例开发等课程教学任务。

（2）工业控制网络安全实训室

工业控制网络安全实训室。配有电力系统工业控制仿真平台一套，核心交换机、汇聚交换机、接入交换机、Web 应用防火墙的等设施设备。主要完成网络安全攻防技术、信息安全技术与实施、网络安全工程项目实践等课程实训教学任务。

（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、投影仪与幕布、白板、交换机（二层、三层）、路由器、Web 应用防火墙、VPN 设备、信息安全攻防竞技平台、上网行为监控设备、堡垒服务器、日志服务器、计算机（工作站）、操作系统（Windows、Linux）和数据库等相关软件。用于信息安全技术与实施、网络安全设备配置、网络安全系统集成、数据存储与容灾、操作系统安全等课程教学与实训。

（4）智慧网联安全实训室

配有智慧交通网联设施一套，1:1智慧交通网联数字孪生平台一套，虚拟靶场1套、竞技考核平台1套。能够满足网络安全攻防、数据安全防护、应急响应等实训任务，能够满足信息安全技术与实施、网络攻防实训、系统渗透测试用例开发等课程教学任务。

（5）计算机取证实训室

该实训室投资一千余万，具有Talon E取证拷贝机、UltraKit III型取证工具箱等专业取证设备，以及EnCase Forensics、X_ways Forensics等专业取证分析工具。主要完成信息安全技术与实施、计算机取证与司法鉴定、网络安全工程项目实践等课程实训教学任务。该实训室集科研与教学为一体，重点进行计算机取证与司法鉴定相关方面的研究并针对我校信息安全技术应用专业学生进行相关方面的教学工作。

3.教学督导机制

学院形成了由院督导办、各系（院、部）督导小组以及学生信息督导员组成的三级教学督导模式，对学院的教学质量评价和监控进行了全覆盖，有效地保证了专业核心课的教学质量。

4.师资保障

担任本课程教学团队的主讲教师应具备较丰富的教学经验，鼓励教学名师、技能大师、全国技术能手参与、指导教学活动。在教学组织能力方面，本课程的主讲教师应具备基本的设计能力，即根据本课程标准制订详细的课程授课计划，对每一堂课的教学过程精心设计，做出详细、具体的安排写入教案;还应该具备较强的施教能力，即掌握扎实的教学基本功并能够因材施教，在教学过程中还应具备一定的课堂控制能力和应变能力。同时还应具备以下相关知识、能力和资质：

（1）熟悉《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》，并具有正确的网络安全法律意识和责任；

（2）熟练掌握本课程所要求的所有前导课程的知识;

（3）具备操作系统安全加固、网络安全测试、网络安全应急响应等能力;

（4）熟悉网络安全等级保护2.0各安全等级保护新规范；

（5）具有网络安全测评、风险评估、网络安全运维等实际项目经验；

（6）具有“双师型”；

（7）获得教师资格证；

（8）教师团队部分成员具有国家信息安全测评工程师证书（CISP）；

（9）熟悉相应行业标准和工艺规范。

六、授课进程与安排

表 4 授课进度与安排

模块	授课章节及内容	学时	授课方式
模块一 无人值守机房安全保障	任务 1：信息安全概念、体系与法律规范	2	讲授
	任务 2：无人值守机房场地建设 实训项目 1：无人值守机房环境设计	2	讲授+实训
	任务 3：设备电磁防护与物理隔离 实训项目 2：无人值守机房网闸设备的配置	2	讲授+实训
	任务 4：存储介质使用与存储安全保护 实训项目 3：无人值守机房介质保护方案设计	2	讲授+实训
模块二 产业园网络安全保障	任务 1：防火墙体系结构 实训项目 4：网络防火墙体系结构的选择	2	讲授+实训

	任务 2：产业园边界防火墙配置与应用 实训项目 5：内网防火墙安全策略配置	2	讲授+实训
	任务 3：入侵检测技术模型与类别	2	讲授
	任务 4：核心服务器入侵检测系统配置与应用 实训项目 6：内网入侵检测系统的配置使用	2	讲授+实训
	任务 5：无线网络安全技术应用	2	讲授
	任务 6：产业园区公共无线网络安全配置 实训项目 7：产业园区公共无线网络的安全设置	2	讲授+实训
	任务 7：网络设备安全配置与管理 实训项目 8：安全路由器的配置与管理	2	讲授+实训
	任务 8：通信安全配置与管理	2	讲授+实训
模块三 云中心主机安全保障	任务 1：云服务器操作系统用户权限与文件管理 实训项目 9：云中心 Web 服务器操作系统的用户权限与文件安全设置	2	实训
	任务 2：云服务器操作系统安全策略配置 实训项目 10：云中心 Web 服务器操作系统的安全策略配置	2	实训
	任务 3：Windows 域控服务安全配置 实训项目 11：云中心域控服务安全配置	2	实训
	任务 4：恶意代码检测与防范 实训项目 12：云中心电脑主机的病毒、木马查杀	2	讲授+实训
模块四 银行交易应用安全保障	任务 1：摸排资产暴露面 实训项目 13：电力公司内网资产发现与防范	2	讲授+实训
	任务 2：检查资产脆弱性 实训项目 14：内网服务与漏洞扫描	2	讲授+实训
	任务 3-1：测试 Web 漏洞 实训项目 15：内网 Web 服务漏洞测试	2	讲授+实训
	任务 3-2：测试系统漏洞 实训项目 16：内网服务器漏洞测试	2	讲授+实训
	任务 4-1：检测 Web 木马 实训项目 17： Web 系统木马后门检测	2	讲授+实训
	任务 4-2：检测系统木马 实训项目 18：服务器木马后门检测	2	讲授+实训
	任务 5-1：流量分析 实训项目 19：安全防护设备流量分析	2	讲授+实训
	任务 5-2：日志分析 实训项目 20：服务器日志分析	2	讲授+实训
模块五 公民信息数据安全保障	任务 1 摄像头认证失效溯源 实训项目 22：智慧交通摄像头认证机制设置	2	讲授+实训
	任务 2 二维码木马植入溯源 实训项目 21：手机木马制作与防范	2	讲授+实训

	任务 3 WIFI 通信泄密溯源 实训项目 23：免费 WIFI 数据泄漏分析	2	讲授+实训
	任务 4 破损图片数据修复 实训项目 24：摄影图片数据修复	2	讲授+实训
	任务 5 格式化磁盘数据恢复 实训项目 25：司法鉴定数据恢复	2	讲授+实训
	任务 6 网银系统数据加密 实训项目 26：银行通讯数据加密防破解	2	讲授+实训
	任务 7 电子合同数字签名 实训项目 27：企业电子合同数字签名	2	讲授+实训
	任务 8 服务器数字证书安装 实训项目 28：数字证书服务器搭建	2	讲授+实训

七、实施建议

（一）完善丰富教学资源

不断的完善丰富现有教学资源，加大教学中课程资源的开发、投入和利用，有选择性的使用优质教学资源，利用更多的新媒体和信息化资源来丰富教学内容，构建教学多元化智慧学习环境。

（二）加强教师技能培训

每年组织一次专业人员对教师进行教育教学能力的培训，更新教师的思想观念和教学理念，熟练运用各类软件进行线上线下教学。促进高职信息安全与管理专业教学改革与创新，在教学设计中融入网络安全观内容的同时，积极探索满足学生升学和职业生涯发展需要的途径。

八、课程标准编制委员会

表 5 课程标准编制委员会成员

序号	姓名	职称	职务
1	武春岭	教授	课程负责人/党总支副书记（课程负责人）
2	梁雪梅	副教授	网络空间安全系专任教师
2	张靖	副教授	网络空间安全系副主任
3	胡兵	副教授	网络空间安全系第二党支部书记
4	江林鑫	高工	网御星云信息技术有限公司技术总监
5	王之涵	工程师	网安分院教育事业部负责人
6	马渊	高工	网警
7	王聃黎	副教授	软件系副主任
8	周璐璐	副教授	网络空间安全系专任教师
9	黄将诚	讲师	网络空间安全系专任教师
9	尹宽	讲师	人工智能系专任教师