



IT 技术专业群

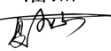
2026 级信息安全技术应用专业

人才培养方案

专业负责人： 杨荣进
二级学院： 智能制造与信息学院

2026 年 5 月

人才培养方案内容提要及审批表

专业名称	信息安全技术应用		专业代码	510207	
学制	三年制，实行弹性学制 3~6 年				
合作企业	1. 武汉厚溥数字科技有限公司				
目标岗位（毕业 3~5 年的）描述	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				
课程门数	44		专业核心课程门数	6	
专业核心课程名称	办公与企业终端安全运维、操作系统、信息安全等级保护、操作系统安全防护实战、电子数据取证技术应用、渗透测试实战、网络设备配置与安全				
毕业考核方式	考试、考查				
职业技能等级证书	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、全国计算机等级证书（二级）、华为网络安全方向职业技能等级认证（HCIA 初级 HCIP 中级）				
公共必修课程总学分	31.5		公共必修课程总学时	673	
专业必修课程总学分	61.5		专业必修课程总学时	1092	
选修课程总学分	44.5		选修课程总学时	804	
总学时数/总学分	2569/137.5	理论总学时	1048	实践总学时	1521
理论课占学时比例		40.79%	实践课占总学时比例		59.21%
其他说明	本方案严格落实《广东碧桂园职业学院 2026 级人才培养方案制（修）订工作的指导意见》要求，符合国家职业教育专业教学标准，突出产教融合、AI 赋能、五育融通、岗课赛证融通特色。将“三有”课堂教学改革实践路径融入人才培养方案，在教学方法、学习评价等环节予以体现，形成学校人才培养特色亮点。				
编制（签名）	1. 广东碧桂园职业学院：陈道贺 潘杰 2. 武汉厚溥数字科技有限公司： 				
审核（签名）					

专业教学指导 委员会主任 (签章)		二级学院 部门负责人 (签章)	
教务处负责人 (签章)		学校教学工作 委员会主任 (签章)	
校 长 (签章)		学校党委书记 (签章)	

目录

一、专业名称及代码	2
二、入学要求	2
三、修业年限	2
四、职业面向	2
五、培养目标与培养规格	2
(一) 培养目标	2
(二) 培养规格	3
六、专业组群	4
(一) 人工智能技术应用专业群人才培养对应新一代信息技术产业(链) ...	4
(二) 专业群人才培养定位	5
(三) 群内专业的逻辑性	6
七、课程设置及要求	6
(一) 公共基础课程	8
(二) 专业课程	8
(三) 实践性教学环节	11
(四) 职业技能等级(资格)证书与相关专业课程的关系	12
(五) 职业院校技能竞赛与相关专业课程的关系	12
(六) 引产入校企业驻校生产项目体系	13
八、教学进程总体安排	15
(一) 全学程教学周分配	15
(二) 教学进程表	16
(三) 学时比例	16
九、师资队伍	16
(一) 队伍结构	16
(二) 专业带头人	17
(三) 专任教师	17
(四) 兼职教师	17
十、实施保障	18
(一) 校企共育人才培养机制	18
(二) 教学设施	18
(三) 教学资源	20
(四) 教学方法	21
(五) 学习评价	23
十一、质量保障和毕业要求	24
(一) 质量保障	24
(二) 毕业要求	25
十二、专业能力图谱	26
十三、课程思政矩阵	32
十四、人才培养特色	33
十五、附录	34

人工智能技术应用专业群

2026 级信息安全技术应用专业人才培养方案

为深入学习贯彻习近平新时代中国特色社会主义思想，贯彻党的二十大精神 and 二十届历次全会精神，落实立德树人根本任务，培养德智体美劳全面发展的社会主义建设者和接班人，根据《教育部关于职业院校专业人才培养方案制订与实施工作的指导意见》（教职成〔2019〕13 号）《关于组织做好职业院校专业人才培养方案制订与实施工作的通知》（教职成司函〔2019〕61 号）《教育部关于深化职业教育教学关键要素改革的意见》（教职成〔2026〕1 号）等文件精神，落实《广东碧桂园职业学院关于做好 2026 级人才培养方案制（修）订工作的通知》（校教字〔2026〕32 号）《以“三有”课堂引领“课堂革命”：广东碧桂园职业学院深化教学改革实施方案（2026—2028 年）》等文件要求，践行“慈心善行、爱教乐学、勤德砺能”办学理念，深化教育教学关键要素改革，推进“三有”课堂建设，着力培养“会做人、会做事”“对人好、对社会好”服务基层一线技术和管理的高技能人才，组织开展 2026 级人才培养方案的制定工作。

为适应科技发展、技术进步对行业生产、建设、管理、服务等领域带来的新变化，顺应互联网和相关服务、软件和信息技术服务业等行业数字化、网络化、智能化发展新趋势，对接新产业、新业态、新模式下网络安全运维、网络安全渗透测试、等级保护测评、网络设备配置与安全、数据存储与容灾等岗位（群）的新要求，不断满足信息安全产业高质量发展对高技能人才的需求，推动职业教育专业升级和数字化改造，提高人才培养质量，遵循推进现代职业

教育高质量发展的总体要求，参照国家相关标准编制要求，制订本专业人才培养方案。

一、专业名称及代码

专业名称：信息安全技术应用

专业代码：510207

二、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。

三、修业年限

基本修业年限 3 年，最长不超过 6 年（含休学）。

四、职业面向

表 1 职业面向

所属专业大类（代码）	电子与信息类（51）
所属专业类（代码）	计算机类（5102）
对应行业（代码）	互联网和相关服务（64）、软件和信息技术服务业（65）
主要职业类别（代码）	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）
主要岗位（群）或技术领域	网络安全运维、网络安全渗透测试、等级保护测评等 网络设备配置与安全、数据存储与容灾
职业类证书	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、全国计算机等级证书（二级）、华为 HCIA/HCIP 网络安全认证

五、培养目标与培养规格

（一）培养目标

本专业培养理想信念坚定，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，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，掌握本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、数据安全治理等工作的高技能人才，毕业 3—5 年可成长为企业网络安全技术骨干或基层管理干部。

（二）培养规格

本专业学生应在系统学习本专业知识和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）坚定拥护中国共产党领导和中国特色社会主义制度，以习近平新时代中国特色社会主义思想为指导，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）掌握与本专业对应职业活动相关的国家法律、行业规定，掌握绿色生产、环境保护、安全防护、质量管理等相关知识与技能，了解相关行业文化，具有爱岗敬业的职业精神，遵守职业道德准则和行为规范，具备社会责任感 and 担当精神；

（3）掌握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）、信息技术等文化基础知识，具有良好的人文素养与科学素养，具备职业生涯规划能力；

（4）具有良好的语言表达能力、文字表达能力、沟通合作能力，具有较强的集体意识和团队合作意识，学习 1 门外语并结合本专业加以运用；

（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，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；

(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技能；

(8) 掌握数据备份与恢复、数据存储与容灾等技术技能，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；

(9) 掌握信息技术基础知识，具有适应本行业数字化和智能化发展需求的数字技能；

(10) 具有探究学习、终身学习和可持续发展的能力，具有整合知识和综合运用知识分析问题和解决问题的能力；

(11) 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，养成良好的运动习惯、卫生习惯和行为习惯，具备一定的心理调适能力；

(12) 掌握必备的美育知识，具有一定的文化修养、审美能力，形成至少 1 项艺术特长或爱好；

(13) 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。

六、专业组群

(一) 人工智能技术应用专业群人才培养对应新一代信息技术产业（链）

人工智能技术应用专业群以人工智能技术应用专业为核心，整合大数据技术、云计算技术应用、软件技术及信息安全技术应用专

业组建而成。人才培养对应新一代信息技术人才需求，服务领域包括金融分析、市场预测、医疗健康、智慧城市建设、企业数字化转型等，岗位涵盖服务链：数据采集、数据存储、数据处理、数据分析、数据安全、数据可视化、AI 模型开发与部署、云服务运维等，各专业就业岗位各有特色，又相互关联，协同支撑数据驱动决策及区域数字经济发展。

本专业作为专业群内的安全保障核心专业，覆盖数据全生命周期的安全防护环节，为专业群内其他专业的技术应用提供安全支撑，共同构建“数据采集-存储-处理-分析-应用-安全防护”的全链条人才培养体系，服务广东省新一代信息技术产业、数字经济产业的高质量发展需求。

（二）专业群人才培养定位

专业群紧扣新一代信息技术产业链，面向人工智能、大数据、云计算、信息安全、软件开发等领域，培养具有良好的人文和信息素养、具备创新精神和实践能力的技术技能型人才团队，以保障区域经济发展和产业转型升级对高素质 IT 人才的需求为人才培养宗旨。，聚焦核心技能培养、团队协作能力和职业素养提升，打造“产教融合、校企共育、AI 赋能、岗课赛证融通”的特色专业群，为广东省数字经济发展培养高素质、复合型、创新型技术技能人才。

本专业在专业群内的定位为：聚焦网络安全与数据安全领域，培养具备全场景安全防护能力的技术技能人才，为专业群内其他专业的技术落地提供安全保障，同时面向各行业的数字化转型需求，提供网络安全、数据安全领域的专业人才支撑。

（三）群内专业的逻辑性

专业基础相通，教学资源共享。群内专业均为电子信息大类下的计算机类，课程体系中开设有 4 门相同的专业群基础平台课，共享 6 个校内实训基地、4 个校外实习基地：

技术领域相近，职业岗位相关。群内专业均主要面向新一代信息技术产业，为人工智能、大数据分析师、云计算技术员、信息安全专家和软件开发等职业岗位培养人才，提供技术研发、数据分析、云服务管理、安全防护和软件开发等全方位服务。

表 2 专业群内专业及对接区域主要重点产业情况表

专业名称	专业代码	对接重点产业	备注
人工智能技术应用	510209	新一代信息技术产业	牵头专业
大数据技术	510205	新一代信息技术产业、数字经济产业	
云计算技术应用	510206	新一代信息技术产业、云计算产业	
软件技术	510203	新一代信息技术产业、软件和信息技术服务业	
信息安全技术应用	510207	新一代信息技术产业、网络安全产业、数据安全产业	

七、课程设置及要求

按照遵循规律、体现培养特色的原则，结合本专业实施“三段递进，校企共育”和采用“三段式”教学组织方式，培养理想信念坚定、身心健康、具有良好的人文素养、职业道德和创新意识的基层一线技术骨干（或管理干部）的要求，构建“三段式”课程体系：

第一阶段（第 1-3 学期）的公共基础课和专业技术平台课，围绕培养学生坚定的理想信念，良好的人文、职业素养和专业基础能力目标，设置公共基础课程和专业技术平台课课程模块。专业技术平台课程模块体现精准对接岗位需求特色，依据岗位需求整合传统课程，精选课程内容，融入 AI 赋能教学内容，夯实学生的专业基础。

第二阶段（第 4-5 学期）的岗位知识深化学习和技能强化训练课程，围绕提升学生完成分流岗位典型工作任务的专业实践能力，构建以典型工作任务为载体的岗位专业知识应用深化学习和技能强化训练项目，聚焦学生分流岗位专业实践能力，突出专业知识应用与实践，并通过深入企业，采用工学交替的教学模式，开展企业课堂学习，在实践中及时收集并解决学生岗位职务工作中共性问题，培养学生职业能力与职业精神，落实“五育融通、校企共育”要求。

第三阶段（第 6 学期）的专业岗位职务能力企业实践教学培养课程，围绕提升学生专业岗位职务能力，通过岗位实习，实现本专业培养基层一线管理干部或技术骨干的目标，并将对学生的创新思维和创新能力的培养，落实到指导学生毕业设计之中，同时融入职业发展规划指导，提升学生的就业竞争力和职业发展能力。

本专业的核心课程包括“操作系统安全防护实战”“电子数据取证技术应用”“渗透测试实战”“网络设备配置与安全”“信息安全等级保护”等课程。

本专业要构建与“产教融合，校企共育”人才培养模式相配套、具有学校办学特色的课程思政、思政课程、思想教育三者相融合的“大思政”体系，形成协同效应。将“价值塑造、知识传授和能力培养”三者有机融入每一门课程中，突出产教融合、职业技能和时代精神并重，让课程思政真正成为塑造学生灵魂、培养时代新人的有效载体。

在每门课程的“课程标准”中，设立独立的“课程思政主线”，并与具体的知识点、技能点、教学情境（如实训、实习、项目等）紧密结合，做到“一课程一特色”，充分挖掘本专业、本行业特有

的思政资源（如行业楷模、行业历史、行业法规、行业文化、优秀企业文化等），形成独具特色的课程思政案例库。通过“如盐化水、润物无声”，自然融合且有机渗透到人才培养的全过程、各环节，通过案例教学、项目教学等方法，以及评教和考核，确保课程思政落地见效，全面落实“三段递进、三全育人”课程思政建设要求。

（一）公共基础课程

按照国家有关规定开齐开足公共基础课程。将习近平新时代中国特色社会主义思想概论、马克思主义理论等思想政治理论课程、体育、军事理论与军训、心理健康教育、劳动教育、创新创业教育、美育教育、人工智能导论、职业发展与就业指导、国家安全教育、安全急救教育、企业文化教育等列为公共基础必修课程。将中华优秀传统文化、人文素养、科学素养和创新创业实践等列为限定选修课程。同时，根据广东省教育厅文件，新增1门《走在前列的广东实践》课程。

（二）专业课程

包括专业基础课程、专业核心课程和专业拓展课程。专业基础课程是需要前置学习的基础性理论知识和技能构成的课程，是为专业核心课程提供理论和技能支撑的基础课程；专业核心课程是根据岗位工作内容、典型工作任务设置的课程，是培养核心职业能力的主干课程；专业拓展课程是根据学生发展需求横向拓展和纵向深化的课程，是提升综合职业能力的延展课程。

本专业结合区域/行业实际、办学定位和人才培养需要确定课程，进行模块化课程设计，依托体现新方法、新技术、新工艺、新标准的真实生产项目和典型工作任务等，开展项目式、情境式教学，结

合人工智能等技术实施课程教学的数字化转型，探索创新课程体系。专业课程教学全面落实“三有”课堂建设要求：专业基础课程融入积分、徽章等趣味教学元素，专业核心课程落地岗位模拟、任务清单式教学，全面落实小组合作加翻转课堂模式，每节课设置2至3个课堂互动环节、课堂互动时长占比不低于30%，全面普及项目化、任务驱动教学法。

（1）专业基础课程

专业基础课程是为专业核心课程提供理论和技能支撑的前置课程，培养学生的专业基础能力，共4门课程，总学分14，总学时246，全部为专业群平台共享课程，实现专业群内教学资源共享。

专业基础课程包括：Python 编程基础、计算机技术基础、网页设计与制作、数据库技术。

（2）专业核心课程

专业核心课程是根据岗位工作内容、典型工作任务设置的主干课程，培养学生的核心职业能力，共7门课程，总学分24，总学时432，全部为理实一体化课程，突出实践能力培养，融入企业真实项目和行业最新技术标准。

表 3 专业核心课程主要教学内容与要求

序号	课程涉及的主要领域	典型工作任务描述	主要教学内容与要求
1	办公与企业终端安全运维	①企业终端安全现状风险识别与安全基线梳理 ②Windows/Linux 终端账号、权限、组策略安全配置加固 ③终端恶意软件、勒索病毒防范、查杀与应急处置 ④企业移动办公、U 盘、外设接入安全管控 ⑤终端数据防泄露、文件加密、数据备份与恢复实操 ⑥企业终端安全巡检、安全台账整理与安全整改报告编制	①掌握企业终端安全常见风险类型、终端安全基线规范，能够完成办公终端安全风险排查；②熟练使用 Windows 组策略、本地安全策略完成账号权限、密码策略、登录安全、外设管控等终端加固操作，掌握 Linux 终端账号、日志、权限安全配置方法；③掌握主流杀毒软件、EDR 终端防护工具部署策略，能够完成勒索病毒、木马病毒的查杀、隔离、应急处置流程；④熟悉企业移动办公、U 盘、打印机等外接设备安全管控方案，能够制定终端外设安全管理制度；⑤掌握办公文档加密、重要业务数据备份、误删数据基础恢复操作，具备企业办公场景下数据防泄露实操能力；⑥能够开展企业批量终端安全巡检，规范填写安全巡检台账，根据安全漏洞撰写终端安全整改方案与安全运维报告，具备面向中小企业的终端安全运维岗位实操能力。
2	操作系统	① 操作系统安装与初始化配置② 系统进程与内存管理③ 设备与文件系统管理④ 用户与权限管理⑤ 系统服务与进程调度⑥ 操作系统故障排查与应急处置	① 掌握操作系统的基本概念、发展历程与体系结构② 熟练掌握 Windows、Linux 及国产操作系统的安装、初始化与基础配置方法③ 理解进程管理、内存管理、设备管理、文件系统的核心原理与实现机制④ 掌握用户账户管理、权限配置、访问控制的方法与技巧⑤ 熟悉系统服务管理、进程调度、性能监控与优化的方法⑥ 具备操作系统常见故障排查、应急处置与系统优化的能力，为后续操作系统安全防护课程奠定基础
3	信息安全等级保护	① 定级备案：分析业务信息与系统服务安全，确定保护等级，编制定级报告并完成公安机关备案② 差距测评：对照等保 2.0 通用要求开展现场测评，识别不合规项，出具差距分析报告③ 整改设计：针对高危漏洞设计技术整改方案和管理措施，编制整改计划④ 体系建设：编写安全管理制度、操作规程，建立安全管理机构，落实人员安全管理要求⑤ 测评运维：配合第三方测评机构完成现场测评与复测，建立应急响应机制，形成持续改进闭环	① 法规标准：掌握《网络安全法》等核心法规，理解等保 2.0 通用要求与扩展要求（云计算、物联网等）② 定级备案：使用矩阵法确定系统等级，掌握定级报告与备案表编制规范③ 技术要求：掌握机房物理安全、网络边界防护（防火墙 / IDS/IPS）、通信加密、访问控制等配置④ 计算环境：配置身份鉴别、安全审计（日志留存 6 个月）、数据加密、集中管控（SOC）等措施⑤ 测评实践：熟练使用测评工具箱（漏洞扫描、渗透测试），编制测评报告，完成二级 / 三级系统等保建设全流程
4	操作系统安全防护实战	① 操作系统漏洞扫描与修复② 系统账户与权限安全配置③ 系统日志审计与异常监测④ 恶意代码防范与清除⑤ 国产操作系统安全部署	① 掌握 Windows、Linux 及国产操作系统安全基础原理② 熟练使用漏洞扫描工具进行系统检测与修复③ 掌握账户权限管理、密码策略配置方法④ 能进行系统日志分析与异常行为排查⑤ 具备恶意代码防范与应急处置能力⑥ 掌握国产操作系统安全部署与运维技巧
5	电子数据取证技术应用	① 电子数据取证准备与现场保护② 存储介质数据提取与固定③ 数据恢复与分析④ 取证报告撰写⑤ 取证工具操作与应用	① 掌握电子数据取证的基本原则与流程② 熟悉常见存储介质（硬盘、U 盘、手机）的取证方法③ 能使用专业取证工具提取、固定电子数据④ 具备数据恢复、数据解密与分析能力⑤ 掌握取证报告的规范撰写要求⑥ 了解电子数据取证相关法律法规

序号	课程涉及的主要领域	典型工作任务描述	主要教学内容与要求
6	渗透测试实战	① 渗透测试环境搭建② 信息收集与端口扫描③ Web 漏洞挖掘与利用④ 系统提权与持久控制⑤ 渗透测试报告撰写⑥ 漏洞修复建议提出	① 掌握渗透测试的流程、方法与工具② 能完成目标信息收集、端口扫描与漏洞探测③ 熟练挖掘 Web 常见漏洞（SQL 注入、XSS 等）并利用④ 掌握系统提权、持久化控制的常用技巧⑤ 能规范撰写渗透测试报告并提出合理修复建议⑥ 树立合法渗透测试的职业意识
7	网络设备配置与安全	① 网络设备（交换机、路由器）初始化配置② VLAN 划分与 trunk 链路配置③ 静态路由、动态路由配置与调试④ 防火墙基础配置与访问控制策略部署⑤ 网络设备安全加固与日志审计⑥ 网络故障排查与应急处置	① 掌握交换机、路由器的工作原理与基本配置方法② 熟练完成 VLAN 划分、trunk 链路及路由协议配置③ 掌握防火墙访问控制策略、NAT 等功能配置④ 能对网络设备进行安全加固，配置设备日志审计⑤ 具备网络故障排查与应急处置能力⑥ 了解华为、华三主流网络设备的配置差异

（3）专业拓展课程

主要包括：数据安全治理实战、云安全技术与应用等领域的内容。

（三）实践性教学环节

实践性教学应贯穿于人才培养全过程，落实“产教融合、校企共育”要求，学时设计符合国家教学标准中“实践性教学学时占总学时 50%以上”的要求。实践性教学主要包括实验、实习实训、毕业设计、社会实践活动等形式，公共基础课程和专业课程等都要加强实践性教学。

（1）实训

在校内外进行操作系统安全、信息安全产品配置与应用、数据存储与容灾、Web 应用安全与防护、渗透测试、电子数据取证等实训，包括单项技能实训、综合能力实训、生产性实训等。实训环节全部采用理实一体化教学模式，依托校内实训基地和校外企业实训平台，以企业真实项目为载体，培养学生的实操能力和岗位适应能力。由学校专任教师和企业兼职教师共同指导。

（2）实习

严格执行《职业学校学生实习管理规定》和相关专业岗位实习标准要求。在软件和信息技术服务、互联网和相关服务行业的通信设备生产、信息安全设备生产、信息安全服务等企业进行信息安全技术应用专业对口实习，包括认识实习和岗位实习。选派专门的实习指导教师和人员，对学生实习的指导、管理和考核。

认识实习：安排在第2学期，为期1周，组织学生到校企合作企业参观学习，了解行业发展趋势、企业岗位需求和工作环境，培养学生的职业认知。

岗位实习：安排在第6学期，为期20周，学生进入校企合作企业的对应岗位进行顶岗实习，由企业指导教师和学校指导教师共同管理和指导，完成岗位工作任务和实习报告，提升学生的岗位实践能力和职业素养。

（四）职业技能等级（资格）证书与相关专业课程的关系

落实“岗课赛证融通”要求，将职业技能等级证书内容融入专业课程教学，学生获得以下职业技能等级（资格）证书（经提交证书原件验证），可获得本专业相关1门专业课程学分。（若有多个职业技能等级证书，以最高等级核定为准）

表4 IT技术专业职业技能等级（资格）证书与相关专业课程的关系

序号	证书名称	证书等级	颁证单位	置换课程名称	学分	备注
1	华为 ICT 认证	HCIP	华为	华为 HCIA 实践	2.5	
2	全国计算机等级考试	一级	教育部教育考试院	计算机技术基础	2	
3	全国计算机等级考试	二级	教育部教育考试院	Python 编程基础	3	

（五）职业院校技能竞赛与相关专业课程的关系

将各级职业技能大赛赛项标准、考核内容融入日常教学与引产项目实训。学生参加市级及以上职业院校技能大赛获奖，可获得本专业相关1门或多门专业课程学分。（若获多个级别职业技能大赛奖项，以最高等级核定为准）

（六）引产入校 企业驻校生产项目体系

为深化产教融合，落实引产入校建设要求，联合武汉厚溥数字科技有限公司、政企信息化服务合作单位等，将真实生产、运维项目引入校园，打造校内即厂区、实训即生产、学生即准员工的培养模式。项目按照学段分层、岗位分类设计，实行校企双师共管、工单化运作、学分认定制度。

1. 项目整体设计框架

培养阶段	对应学期	项目层级	参与对象	实施场地	指导团队	核心培养目标
第一阶段（基础夯实）	1-3 学期	基础辅助类项目	全体大一学生	校内专业实训基地、政企运维模拟工区	校内专任教师 + 企业驻校导师	熟悉企业工作规范，掌握基础实操技能，培养职业素养
第二阶段（能力进阶）	4-5 学期	综合服务类项目	全体大二学生（按岗位分组）	校内联合实训中心	校企双师 + 企业项目负责人	完成模块化生产任务，匹配岗位核心能力
第三阶段（岗位落地）	6 学期	全真驻场类项目	优选大三学生	校内驻场工区 + 合作单位现场	企业项目经理 + 校内督导	对标正式岗位，衔接顶岗实习与就业

2. 项目整体分类

结合合作单位业务，项目分为运维保障类、安全检测类等保测评类、数据安全类、政企综合 IT 运维类，全面覆盖本专业就业岗位。

3. 分阶段具体项目清单

（1）第一阶段（1-3 学期）基础辅助类项目

企业终端安全巡检项目：终端加固、病毒查杀、补丁更新、日志整理；对接课程：操作系统安全防护实战

网络基础配置辅助项目：交换机、路由器基础调试、链路检测；对接课程：网络设备配置与安全

安全情报整理项目：漏洞信息、安全事件台账编制；对接课程：信息安全标准与法规

政企桌面运维模拟项目：PC、打印机、投影仪故障处理；对接课程：计算机基础、办公设备运维

设备巡检项目：设备日常检查、简单排障；对接课程：综合 IT 运维拓展课

（2）第二阶段（4-5 学期）综合服务类项目

通用项目：中小型服务器安全加固项目、常规 Web 站点安全检测项目

岗位专项项目：

- ①网络安全运维方向：企业云节点值守、故障应急处置
- ②等保测评方向：等保资料收集、差距分析
- ③数据安全方向：数据资产梳理、分类分级、脱敏测试
- ④电子取证方向：模拟介质取证、数据分析
- ⑤政企综合 IT 运维方向：办公网络排障、模拟驻场值守

（3）第三阶段（6 学期）全真驻场类项目

- ①政企常态化安全运维项目
- ②授权渗透测试与风险评估项目
- ③信息安全等级保护全流程测评项目
- ④数据备份与容灾运维项目
- ⑤政企 IT 驻场运维项目

4. 政企综合 IT 运维专项说明

本项目聚焦政企单位日常 IT 运维业务，核心工作包含 PC 软硬件检修、外设故障处理、会议室及监控设备运维、基础网络排障。

采用校内模拟实训 + 校外定岗实习两种形式，校外岗位实行标准作息制度，管理规范，岗位要求责任心强、吃苦耐劳、具备良好服务意识。

5. 运行管理机制

组织架构：设立驻校项目管理中心，企业派驻项目经理、技术导师，校方配备实训管理员与督导教师；

管理制度：沿用企业考勤、工位、保密、工单制度，全员签订保密协议；

任务流程：企业派单→小组分工→实操作业→自检→企业验收→成果交付；

学分规则：项目考核合格可置换实训、选修课程学分，优秀项目经历可作为竞赛、证书加分项。

6. 安全与合规要求

所有网络、渗透、数据类操作必须取得企业书面授权，严格遵守《网络安全法》《数据安全法》。涉密区域物理隔离，客户信息严格保密，岗前合规培训考核合格后方可上岗。

八、教学进程总体安排

（一）全学程教学周分配

表 5 全学程教学周分配表

按学期/周数分配									
第一学 年	第一学期（20 周）				寒 假	第二学期（20 周）			暑 假
	新生入学、军训及入 学教育	课程教 学	考试	机动	6	课程教学	考试	机动	6
	周数	3	15	1		1	18	1	
第二学 年	第三学期（20 周）				寒 假	第四学期（20 周）			暑 假
	课程教学		考试	机动	5	课程教学	考试	机动	7
	周数	18		1		1	18	1	
第三学 年	第五学期（20 周）				寒 假	第六学期（20 周）			暑 假
	岗位能力强化训练		岗位实践共性问题 解析		春 节	岗位实习与毕业 设计		毕业教育与 离校	7

按学期/周数分配						
周数	18	2	1	20	3	

（二）教学进程表

见附件 1。

（三）学时比例

表 6 学时比例表

课程类别与性质		学时分配			课程类别总计	占总学时比例 (%)
		总学时	理论学时	实践学时		
公共基础课	必修课	673	343	330	817	31.80%
	限选课	72	40	32		
	任选课	72	40	32		
专业（技能）课	专业群平台课（必修）	306	152	154	1752	68.20%
	专业技术平台课（必修）	426	209	217		
	专业群拓展课（限选）	72	48	24		
	专业岗位课（限选）	588	144	444		
	岗位实习与毕业设计（必修）	360	72	288		
学时合计		2569	1048	1521	——	
学时比例		100%	40.79%	59.21%		

九、师资队伍

按照“四有好老师”“四个相统一”“四个引路人”的要求建设专业教师队伍，将师德师风作为教师队伍建设的第一标准。

（一）队伍结构

学生数与本专业专任教师数比例不高于 25：1，“双师型”教师占专业课教师数比例一般不低于 60%，高级职称专任教师的比例

不低于 20%，专兼职教师年龄、学历结构合理。现有专任教师 8 人，其中高级职称 4 人，占 50%；双师素质 5 人，占 62.5%。

（二）专业带头人

原则上应具有本专业及相关专业副高及以上职称和较强的实践能力，能够较好地把握国内外互联网和相关服务、软件和信息技术服务等行业、专业发展，能广泛联系行业企业，了解行业企业对本专业人才的需求实际，主持专业建设、开展教育教学改革、教科研工作和社会服务能力，在本专业改革发展中起引领作用。

（三）专任教师

具有高校教师资格；原则上具有计算机科学与技术、软件工程、网络工程、信息安全等相关专业本科及以上学历；具有一定年限的相应工作经历或者实践经验，达到相应的技术技能水平；具有本专业理论和实践能力；能够落实课程思政要求，挖掘专业课程中的思政教育元素和资源；能够运用信息技术开展混合式教学等教法改革；能够跟踪新经济、新技术发展前沿，开展技术研发与社会服务；专业教师每年至少 1 个月在企业或生产性实训基地锻炼，每 5 年累计不少于 6 个月的企业实践经历。教师每年参加“三有”课堂建设与教学改革专项培训，年度教改专项培训学时不低于 40 学时，持续提升“三有”课堂教学设计、实施与评价能力。

（四）兼职教师

主要从本专业相关行业企业的高技能人才中聘任，应具有扎实的专业知识和丰富的实际工作经验，一般应具有中级及以上专业技术职务（职称）或高级工及以上职业技能等级，了解教育教学规律，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专

业教学任务。根据需要聘请技能大师、劳动模范、能工巧匠等高技能人才，根据国家有关要求制定针对兼职教师聘任与管理的具体实施办法。

十、实施保障

（一）校企共育人才培养机制

依托以学校为主、牵头成立的“产教融合校企共育理事会”，根据《加强“产教融合、校企共育”人才培养工作实施办法》，持续深化“产教融合、校企共育”人才培养模式，建立本专业与武汉厚溥数字科技有限公司、华为等企业之间的校企共同育人工作机制，包括签订战略合作框架协议，建立专业教学指导委员会，建立产业学院，校企共同制（修）订专业人才培养方案、岗位职务工作标准、课程标准和共同编写教材，建立企业兼职教师、岗位导师教学培训制度、企业实践教学培养教学管理和学生管理制度等，确保校企共同育人各项工作规范有序扎实推进。

（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、实训室和实习实训基地。

1. 专业教室基本要求

具备利用信息化手段开展混合式教学的条件。一般配备黑（白）板、多媒体计算机、投影设备、音响设备，具有互联网接入或无线网络环境及网络安全防护措施。安装应急照明装置并保持良好状态，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. 校内外实验、实训场所基本要求

实验、实训场所面积、设备设施、安全、环境、管理等符合教育部有关标准（规定、办法），实验、实训环境与设备设施对接真实职业场景或工作情境，实训项目注重工学结合、理实一体化，实验、实训指导教师配备合理，实验、实训管理及实施规章制度齐全，确保能够顺利开展操作系统安全、信息安全产品配置与应用、数据存储与容灾、Web 应用安全与防护等实验、实训活动。鼓励在实训中运用大数据、云计算、人工智能、虚拟仿真等前沿信息技术。

表 7 实训基地一览表

序号	实训室名称	实训项目	设备配置要求	
			主要设备名称	数量
1	信息安全 实训室	1、操作系统安全防护实战 2、电子数据取证技术应用 3、渗透测试实战 4、网络设备配置与安全 5、华为 HCIA 实践	防火墙	1
			企业出口路由器	3
			互联交换机	1
			无线控制器	1
			无线接入点	1
			Anti-DDos 检测	1
			Anti-DDos 清洗	1
			Anti-DDos 管理中心	1
			入侵防御与检测系统	1
			计算机	56

3. 实习场所基本要求

本专业的实习场所符合《职业学校学生实习管理规定》《职业学校校企合作促进办法》等对实习单位的有关要求，经实地考察后，确定合法经营、管理规范，实习条件完备且符合产业发展实际、符合安全生产法律法规要求，与学校建立稳定合作关系的单位成为实习基地，并签署学校、学生、实习单位三方协议。

根据本专业人才培养的需要和未来就业需求，实习基地提供网络安全运维、网络安全渗透测试、等级保护测评、网络设备配置与安全、数据存储与容灾等与专业对口的相关实习岗位，涵盖当前相关产业发展的主流技术，接纳一定规模的学生实习；学校和实习单位双方共同制订实习计划，配备相应数量的指导教师对学生实习进行指导和管理，实习单位安排有经验的技术或管理人员担任实习指

导教师，开展专业教学和职业技能训练，完成实习质量评价，做好学生实习服务和管理工作的，建立保证实习学生日常工作、学习、生活的规章制度，依法依规保障学生的基本权益。

（三）教学资源

主要包括能够满足学生专业学习、教师专业教学研究和教学实施需要的教材、图书及数字资源等。

1. 教材选用基本要求

按照国家规定，经过规范程序选用教材，优先选用国家规划教材和国家优秀教材。专业课程教材应体现本行业新技术、新规范、新标准、新形态，并通过数字教材、活页式教材等多种方式进行动态更新。

2. 图书文献配备基本要求

图书文献配备能满足人才培养、专业建设、教科研等工作的需要。专业类图书文献主要包括：信息安全行业的政策法规、行业标准、技术规范；信息安全技术、大数据技术、人工智能技术、云计算技术、物联网技术和实务案例类图书；5 种以上信息安全技术类专业学术期刊。

3. 数字教学资源配置基本要求

本专业建设了完善的数字化教学资源库，包括专业课程教学课件、教学视频、实训项目、虚拟仿真资源、习题库、案例库等，所有核心课程均建设了完整的数字化教学资源，能够支撑线上线下混合式教学、学生自主学习、远程教学等需要。同时，本专业引入了行业企业优质数字化教学资源、虚拟仿真实训平台、在线学习平台，

为学生提供了丰富的学习资源和实践平台，落实 AI 赋能教学要求，提升教学效果和学生学习体验。

（四）教学方法

信息安全技术应用专业聚焦“五育融合”“三全育人”“三教改革”和人才培养目标和定位，依据“三段递进、校企共育”人才培养模式改革和实施“三段式”教学培养的需要，结合教学目标和教学环境不同，采用不同的教学组织方式和教学方法：

1. 第一阶段（第 1-3 学期）教学组织方式与教学方法

第一阶段教学根据企业主要岗位群共性基础知识的特点，实施相应的教学组织方式与教学方法。

（1）以理论教学为主的职业素养类课程，主要采用讲授法为主，并结合案例法辅助教学；

（2）对于专业基础类、专业平台类和专业拓展类的课程，将真实的工程贯穿到专业教学的过程中，采用“教、学、做”合一的教学法、情景教学法、项目教学法、案例教学法、讨论式教学法、启发引导式教学法、现场教学法等实施教学；

（3）对于专业专项技能类的课程，要突出学生的主体地位，采用理论实操一体化、分小组实训方式组织教学和过程考核、操作考核、答辩等方式。引导学生动脑动手、独立实践，提高体验、感受、领悟的能力和水平，增强学生动手能力和发现问题、分析问题、解决问题的能力。

2. 第二阶段（第 4-5 学期）教学组织方式与教学方法

第二阶段教学聚焦专业岗位，进行专业岗位分流知识深化学习与岗位技能强化训练课程，采用工学交替的方式组织教学。以信息

安全岗位为教学单位开展岗位课程包教学。选择合作企业开发建设的项目为载体，以讲解、讨论、指导、实操等方式，训练学生应用专业知识开展岗位工作、分析问题、解决问题能力和技能操作水平。

（1）专业岗位分流知识深化学习。根据岗位设置的课程，采用“教、学、做”合一的教学法、情景教学法、项目教学法、案例教学法、讨论式教学法、启发引导式教学法、现场教学法等实施教学。

（2）专业岗位技能强化训练。本阶段课程安排在企业课堂以岗位实践学习与集中授课交替的方式组织教学。企业课堂期间统一设置两门课程，即“专业岗位能力强化训练”和“岗位实践共性问题解析”。其中“专业岗位能力强化训练”课程须以岗位典型工作任务为训练项目构建课程内容，采用项目化教学，任务驱动的模式组织学生进行专业岗位技能现场实操训练，完成相应的岗位任务；“岗位实践共性问题解析”须紧密结合学生的实际，根据学生在企业实践教学过程中共性问题的梳理和总结，收集和准确分析学生的共性问题，针对共性问题设计线上/线下集中授课方式，采用混合式教学的方法开展教学，培养学生在工作中分析问题、解决问题的能力。

3. 第三阶段（第6学期）教学组织方式与教学方法

第三阶段的“专业岗位职务能力企业实践教学培养”，是“产教融合、校企合作、工学结合、知行合一”的共同育人机制向企业的延伸，是由在校学生变为基层一线管理干部或技术骨干的过渡阶段，是适应专业岗位的切入点。根据企业基层的网络安全运维、渗透测试等岗位职务工作标准和学生在工作中遇到的共性问题，采取分阶段集中授课、企业导师指导、学校指导教师实践教学管理平台

线上指导交流、毕业设计指导等方式组织教学，并进行过程考核，提升学生岗位实践能力。

教师及教师团队要与时俱进，积极围绕教、学、评、研、育五大教育教学主场景，以学生为中心，以问题为导向，深化教学改革，聚焦职业教育教学典型场景应用，以各类通用、垂直类人工智能平台工具为抓手，以人工智能赋能教学。进一步实施人工智能赋能“五金”建设，试点开展人工智能赋能专业教学及人才培养工作；推进人工智能教学实训实习场所建设，构建技术赋能的教学生态环境等。

全面落实“三有”课堂教学改革，将“三有”课堂教学改革实践路径贯穿教学方法改革全过程。一是抓实有趣课堂，激活学习内生动力：全面推行情境化、游戏化、项目化教学设计，依托校级微课资源库完善本专业碎片化知识点资源建设，支持学生个性化学习；二是抓实有效课堂，构建闭环教学管控体系：每节课明确素质、知识、能力三维目标，依托智慧职教平台实现课前预习、课中学情监测、课后精准巩固，实施项目教学五步法（项目启动—任务分解—探究实施—成果展示—评价反思）与阶梯式目标拆解教学，落实分层分类教学；三是抓实有用课堂，锚定岗位需求深化产教融合：将企业真实项目和行业“五新”（新技术、新工艺、新标准、新装备、新方法）融入教学内容，推动AI工具在备课、授课、答疑、评价等教学全流程常态化应用，建设AI智慧课堂。

（五）学习评价

按照过程性评价、结果性评价和增值评价相结合的原则，全面考核学生的素质、能力、知识等掌握情况。建议：

1. 评价内容“注重”能力，在考查学生基础理论知识的基础上，注重考查学生网络安全运维、安全测试、系统加固、数据防护等解决实际问题的能力。

2. 评价形式“注重”多样化，结合课程的特点，坚持正确的命题原则和灵活多样的考试形式相结合，笔试与上机考试相结合，平时考查与期末考试相结合。

3. 评价考核“注重”过程，跟踪记录学生运用完成任务、案例或项目的过程，评价学生操作过程及操作结果的准确性、合理性、熟练性及全面性。对学生整个学习过程的动态情况，进行量化考核。

4. 评价机制“注重”“三有”导向，落实“三有”课堂评价改革，课程过程性评价权重不低于 50%，综合采用过程、结果、增值、综合等多元评价方法；探索构建“教师、学生、机器、企业”多主体评价体系，引入智能学习平台数据分析和行业企业导师评价；对照专业课、通识课两套百分制评价细则常态化开展课堂自评，配合学校开展课程分级评定，持续优化课堂教学质量，在学习评价环节充分体现“三有”课堂建设要求。

十一、质量保障和毕业要求

（一）质量保障

1. 按照学校《关于进一步加强“产教融合、校企共育”人才培养的实施意见》文件精神，建立校企共同育人工作机制，校企双方协同做好育人过程管理，强化对人才培养实施的全过程监控，确保人才培养质量。同时，信息安全技术应用专业在学院教学质量管理机制下，严格执行教学质量管理制度，形成常态化的人才培养质量管控体系，以确保专业人才培养质量，全面实现专业人才培养目标。

2. 学校和二级学院建立专业人才培养质量保障机制，健全专业教学质量监控管理制度，改进结果评价，强化过程评价，探索增值评价，吸纳行业组织、企业等参与评价，并及时公开相关信息，接受教育督导和社会监督，健全综合评价。完善人才培养方案、课程标准、课堂评价、实验教学、实习实训、毕业设计以及资源建设等质量保障建设，通过教学实施、过程监控、质量评价和持续改进，达到人才培养规格要求。

3. 学校和二级学院完善教学管理机制，加强日常教学组织运行与管理，定期开展课程建设、日常教学、人才培养质量的诊断与改进，建立健全巡课、听课、评教、评学等制度，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。将“三有”课堂建设成效纳入教学质量监控与课堂评价体系，常态化开展推门听课和课堂督导巡查，配合学校完成课程分级评定与“三有”课堂评价数据采集、分析。

4. 专业教研组织建立线上线下相结合的集中备课制度，定期召开教学研讨会议，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。

5. 学校建立毕业生跟踪反馈机制及社会评价机制，并对生源情况、职业道德、技术技能水平、就业质量等进行分析，定期评价人才培养质量和培养目标达成情况。

（二）毕业要求

1. 学分要求

学生最低要求修满总学分 137.5 学分，其中公共限选课 4 学分，公共任选课 4 学分；此外，素质拓展学分不低于 12 分。学生可参照学校相关学分认定和转换办法获得素质拓展和课程学分。

2. 体能测试要求

体能测试成绩须达到《国家学生体质健康标准（2014 年修订）》合格标准的要求，成绩未达标者按结业或肄业处理。

十二、专业能力图谱

（一）前言

本表根据信息安全产业升级趋势与行业头部企业对人才及岗位的实际需求，结合国家/行业信息安全行业企业职业标准、网络安全行业职业标准、网络安全运维、渗透测试、等级保护测评等岗位能力要求及课程思政建设要求，系统梳理专业核心能力体系。

为顺应信息安全行业国产化、数智化、实战化转型趋势，本图谱将 AI 安全、数据安全、国产化安全理念融入人才培养全过程，采用基础打底—核心筑基—岗位专精—拓展赋能的递进式逻辑框架，将人才能力拆解为四大层级：

第一层：基础通用能力层（职业底色）。聚焦思想政治素养、法治合规意识、数字化办公、AI 基础应用、准职业人素养，完成从“学生”到“准职场人”的转变。

第二层：专业核心能力层（行业基石）。覆盖信息安全全流程通用技能，重点培养网络安全运维、安全产品配置、漏洞检测、数据安全防护等保合规等跨岗位通用核心能力，支撑课程严格对照专业教学进程表专业必修课程设置。

第三层：岗位专项能力层（核心竞争力）。对应专业岗位分流，聚焦网络安全运维、渗透测试、等级保护测评、数据存储与容灾、网络设备安全五大岗位，形成岗位专属技能体系，支撑课程严格对照专业教学进程表岗位分流必修课程设置。

第四层：综合拓展能力层（职场进阶）。依托企业真实攻防场景、校企双导师制，培养复杂安全事件处置、安全架构规划、应急响应、国产化安全落地等高阶实战能力，支撑课程严格对照专业教学进程表实践类必修课程设置。

以下“能力图谱与教学要素联动明细表”以四大能力层级为主线，将能力指标点与典型生产任务、支撑课程、教材资源、教师能力要求及评价手段逐一对应，推动岗课赛证融通与产教深度融合，确保教学实施与专业能力提升精准联动。



信息安全技术应用专业能力层级模型

（二）基础通用能力层（职业底色 · 全岗位必备）

支撑学生完成从“学生”到“准职场人”的转变，建立数智素养与职业底线。

能力项 (一级)	能力指标点 (二级/三级)	对应典型生产 任务/职业场景	支撑课程(模块 化/项目化) (模块化/项目 化)	支撑教材与资源 (模块化/项目 化)	对应教师能力要 求 (含思政育人能 力)	评价/观测手段 (含素养评价)
职业素养(课 程思政)	二级: 思想政治素养 三级: ①践行社会主义核 心价值观②恪守网络安全 职业道德③保守企业数据 与隐私秘密④团队协作与 责任担当	新员工入职合 规培训、安全 事件协同处 置、保密协议 签署、安全项 目团队协作	思想道德与法 治、习近平新时 代中国特色社会 主义思想概论、 形势与政策、大 学生职业发展与 就业指导、国家 安全教育	马工程系列教 材、网络安全行 业职业道德案例 库、思政微课、 网络安全保密规 范	具备课程思政设 计能力; 能结合 安全实战案例开 展价值引领; 熟 悉行业保密与合 规要求	主题班会、素质 拓展评分、职场 模拟考核、综合 素养测评(贯穿 全学程≥12 学 分)
通用数 字化工 具能力	二级: 数字化办公与 AI 基础应用 三级: ①熟练使用 Office/WPS 完成安全报 告撰写②能使用 AI 工具 辅助安全资料整理与漏洞 分析③掌握基础计算机操 作与系统环境部署④规范 书写安全日志与工作台账 ⑤遵守网络安全法律法规	安全巡检报告 撰写、漏洞资 料整理、工作 台账记录、计 算机基础环境 部署、法规条 款应用	人工智能导论、 计算机导论	办公软件手册、 安全报告模板、 网络安全法规文 本、AI 安全辅 助工具指南	具备数字化办公 与 AI 基础应用能 力; 熟悉安全文 书规范; 能结合 法规开展教学	办公软件操作测 试、安全文书写 作、法规案例研 讨、情景模拟
法治与 安全基 础能力	二级: 安全合规意识 三级: ①掌握网络安全 法、数据安全法核心条款 ②识别基础安全风险与合 规隐患③具备安全防护与 应急基础意识	日常安全合规 检查、基础风 险识别、安全 事件初步上报	国家安全教育、 安全急救教育	网络安全法规汇 编等保 2.0 标 准、安全风险案 例库	熟悉信息安全法 律法规; 能开展 合规意识教育	法规考试、风险 识别测试、安全 意识考核

(三) 专业核心能力层(专业基石·跨岗位通用)

覆盖信息安全全生命周期, 是所有安全岗位通用的核心专业技能。

能力项 (一级)	能力指标点 (二级/三级)	对应典型生产任务/职业场景	支撑课程 (模块化/项目化)	支撑教材与资源 (含思政资源库)	对应教师能力要求 (含思政育人能力)	评价/观测手段 (含素养评价)
网络安全运维能力	二级：系统与网络安全运维 三级：①完成操作系统安全加固②开展网络设备基础安全配置③执行漏洞扫描与基础修复④监控网络安全状态	服务器安全加固、交换机/路由器安全配置、漏洞扫描、日常安全巡检	操作系统、操作系统安全防护实战★、网络设备配置与安全★	操作系统安全教材、网络设备配置手册、漏洞扫描工具指南、企业安全运维案例库	具备网络安全运维实战经验；双师素质；能开展实训教学	安全加固实操、漏洞扫描考核、运维实训评分
安全产品配置能力	二级：安全设备部署与调试 三级：①安装配置防火墙、VPN、入侵检测系统②完成安全策略优化与日志分析③实施防病毒与上网行为管理	防火墙部署、VPN配置、入侵检测调试、安全策略优化	网络设备配置与安全★、华为HCIA 实践	安全产品操作手册、防火墙/VPN 配置教程、企业安全部署案例	熟悉主流安全产品；具备设备调试能力；能指导实操	产品配置实操、策略优化考核、设备部署评分
安全检测与防护能力	二级：漏洞与 Web 安全防护 三级：①识别 Web 常见漏洞②实施 Web 安全防护措施③开展基础渗透测试与风险验证	SQL 注入检测、XSS 防护、漏洞验证、网站安全加固	网页设计与制作、渗透测试实战★、电子数据取证技术应用★	Web 安全教材、漏洞防护手册、渗透测试基础案例、电子数据取证教程	掌握 Web 安全原理；具备漏洞检测能力；能开展攻防教学	Web 漏洞检测、安全防护实操、渗透基础考核
数据安全与容灾能力	二级：数据安全的管理 三级：①实施数据备份与恢复②设计基础容灾方案③开展数据安全检查与防护	数据备份执行、容灾方案设计、数据安全巡检	数据库技术、Python 编程基础、电子数据取证技术应用★	数据容灾教材、备份软件手册、数据安全规范、数据库操作手册	具备数据存储与容灾经验；能指导备份与恢复实操	备份恢复实操、容灾方案设计评分、数据取证考核
等级保护合规能力	二级：等保合规实施 三级：①解读等保 2.0 标准②开展等保基础测评与整改③编制合规检查报告	等保合规检查、测评报告编制、安全整改实施	信息安全等级保护★、信息安全风险评估★	等保 2.0 标准文本、合规检查模板、测评案例库、风险评估指南	熟悉等保流程；具备测评实施能力；能指导合规教学	等保检查实操、报告编制评分、法规考核

(四) 岗位专项能力层 (岗位核心精准匹配)

对应专业岗位分流，聚焦信息安全主流高价值岗位，实现技能与岗位精准匹配。

核心岗位	能力指标点 (二级/三级)	对应典型生产任务/ 职业场景	支撑课程 (模块化/项目化)	支撑教材与资源 (含思政资源库)	对应教师能力要求 (含思政育人能力)	评价/观测手段 (含素养评价)
网络安全运维岗	二级：安全运维与监控 三级：①7×24安全状态监控②安全事件初步响应与处置③设备日常巡检与维护④安全日志审计与分析	安全监控值守、事件响应、设备巡检、日志审计	企业级网络安全实施、网络安全技术与实训、信息安全项目管理、岗位能力强化训练、岗位实践共性问题解析	运维手册、日志分析模板、安全事件处置案例、大数据安全运维教程	具备企业安全运维经验；熟悉监控与响应流程；双师素质	运维实操、日志分析考核、事件响应评分、岗位实践评价
网络与信息安全管理员岗	二级：等保测评与安全管理 三级：①开展等保测评与整改②实施信息安全风险评估★③进行Web源码审计④强化岗位实操能力	等保测评实施、风险评估、Web源码审计、安全整改、岗位实操训练	信息安全等级保护★、信息安全风险评估★、Web源码审计、岗位能力强化训练、岗位实践共性问题解析	等保测评手册、风险评估指南、Web源码审计教程、岗位实操手册	熟悉等保流程与风险评估方法；具备源码审计能力；能指导岗位实践	等保测评实操、风险评估报告评分、源码审计考核、岗位实践评价
渗透测试岗	二级：渗透与漏洞验证 三级：①执行规范渗透测试流程②识别高危漏洞并验证③编写渗透测试报告④提出修复加固方案	授权渗透测试、漏洞验证、报告编制、加固方案设计	渗透测试实战★、电子数据取证技术应用★、Web应用开发、操作系统安全防护实战★★	渗透测试教程、漏洞验证手册、渗透报告模板、电子数据取证案例	具备渗透测试实战★经验；掌握漏洞原理；能指导渗透实操	渗透实操考核、漏洞验证评分、渗透报告评审
网络设备配置与安全岗	二级：网络安全架构部署 三级：①规划网络安全拓扑②配置路由交换安全策略③部署网络边界安全设备④优化网络访问控制	网络拓扑规划、ACL/VRRP/OSPF安全配置、边界防护部署	网络设备配置与安全★、操作系统、华为HCIA实践	网络设备配置手册、华为HCIA培训教材、网络拓扑设计案例	具备网络设备配置与安全★部署经验；熟悉华为设备操作；能指导实操	设备配置实操、拓扑设计评分、安全策略优化考核
数据存储与容灾岗	二级：数据安全与备份容灾 三级：①设计企业级备份方案②实施RAID与存储部署③搭建容灾系统④数据恢复演练	存储方案设计、备份部署、容灾搭建、恢复演练	数据库技术、电子数据取证技术应用★、数据安全治理实战	数据存储教材、备份软件手册、容灾系统搭建教程、数据恢复案例	具备数据存储与容灾经验；能指导备份与恢复实操；熟悉混合云存储技术	备份恢复实操、容灾方案设计评分、存储部署考核

（五）综合拓展能力层（竞争力提升·面向未来发展）

面向企业真实复杂场景与长期职业发展，培养高阶综合能力与创新能力。

能力项 (一级)	能力指标点 (二级/三级)	对应典型生产任务/职业场景	支撑课程 (模块化/项目化)	支撑教材与资源 (含思政资源库)	对应教师能力要求 (含思政育人能力)	评价/观测手段 (含素养评价)
安全应急响应能力	二级：安全事件应急处置 三级：①制定应急响应预案②勒索病毒/数据泄露事件处置③攻击溯源与损失评估④应急演练组织实施	安全事件应急处置、攻击溯源、应急演练、预案编制	岗位能力强化训练、电子数据取证技术应用★、渗透测试实战★	应急响应手册、溯源教程、演练方案模板、安全事件处置案例	具备应急处置实战经验；能组织演练教学；双师素质	应急演练考核、预案设计评分、事件处置实操
国产化安全应用能力	二级：国产系统与密码应用 三级：①部署国产操作系统与数据库②应用国产密码技术③落实国产化安全合规要求	国产化环境部署、国密应用、合规改造	操作系统、操作系统安全防护实战★、数据库技术、华为 HCIA 实践	国产系统手册、国密标准、国产化案例库、华为国产化设备教程	熟悉国产化安全技术；具备部署经验；能指导国产化实操	国产化部署实操、国密应用考核、合规改造评分
安全架构与规划能力	二级：企业安全方案设计 三级：①设计中小企业安全架构②制定整体安全建设方案③开展安全风险评估与规划	安全架构设计、方案编制、风险评估、建设规划	网络设备配置与安全★、信息安全风险评估★、信息安全等级保护★	安全架构案例、风险评估指南、方案模板等保标准文本	具备安全规划与架构设计经验；能指导方案设计；熟悉行业标准	方案评审、架构设计评分、风险评估报告考核
AI 安全与数智化能力	二级：AI 赋能安全应用 三级：①利用 AI 工具辅助漏洞检测②实现安全日志智能分析③防范 AI 相关安全风险	AI 辅助漏洞检测、日志智能分析、AI 安全风险防控	人工智能导论、Python 编程基础	AI 安全工具、智能分析教程、风险案例、Python AI 脚本案例	熟悉 AI 与安全融合技术；能开展数智化教学；具备 AI 工具应用能力	AI 工具实操、分析报告评分、风险识别考核
企业实践与综合输出能力	二级：岗位实习与毕业设计 三级：①独立完成企业安全岗位任务②解决现场实际安全问题③撰写实习总结与毕业设计④通过企业与学校双重评价	企业岗位实习、现场问题解决、毕业设计、岗位综合考核	岗位实习与毕业设计、岗位实践共性问题解析	实习指导手册、毕业设计指导书、企业评价标准、岗位实践案例	双师素质；企业挂职经历；能担任企业实践导师；具备毕业设计指导能力	企业导师评价、实习周志、毕业设计答辩、用人单位评价

说明：

★为核心课程，考试课程

(1) 本图谱严格遵循数字化、模块化、实战化要求，能力指标点全部采用结果驱动型描述，无模糊表述。

(2) 所有能力点均对接行业典型任务与企业真实场景，满足校企协同编制要求。

(3) 融入课程思政、数智赋能、动态优化要求，适配信息安全行业发展趋势。

(4) 标注为核心考试课程，素养评价贯穿全学程且不低于 12 学分，支持 1+X 证书、华为 HCIA/HCIP 安全方向等学分置换。

十三、课程思政矩阵

课程思政面与 课程思政线	思政面 1（家国情怀）			思政面 2（职业道德）			思政面 3（职业精神）			思政面 4（个人品格）			思政面 5（专业素养）	
	思政线 1	思政线 2	思政线 3	思政线 1	思政线 2	思政线 3	思政线 1	思政线 2	思政线 3	思政线 1	思政线 2	思政线 3	思政线 1	思政线 2
	网络安全强国： 使命	信息主权： 守护	数据安全： 国策	等保合规： 守法	隐私保护： 底线	职业诚信： 守责	攻防工匠： 精神	操作严谨： 规范	安全责任： 担当	攻防创新： 探索	应急协作： 配合	廉洁自律： 守规	攻防求真： 务实	攻坚守土： 实干
专业 课程														
办公与企业终端安全运维★			●		●				●					
Python 编程基础							●			●			●	
操作系统★				●				●			●		●	
计算机技术基础									●				●	●
网页设计与制作						●	●			●				
数据库技术			●		●			●					●	
信息安全等级保护★	●		●	●	●		●	●		●		●		
操作系统安全防护实战★		●		●		●		●						
电子数据取证技术应用★				●	●		●			●			●	●
渗透测试实战★		●		●	●		●							
网络设备配置与安全★			●	●								●		
华为 HCIA 实践		●				●			●					●

数据安全治理 实战		●		●									●	
网络安全检测 与应急响应		●						●			●			
云安全技术与 应用		●		●				●						
企业级网络安全 实施★					●			●			●			
网络安全技术 与实训				●			●			●				
信息安全项目 管理				●			●			●				
岗位能力强化 训练						●						●		●
岗位实践共性 问题解析						●						●	●	

十四、人才培养特色

（一）“八共同”协同育人机制

校企双方围绕信息安全技术应用专业，共同制定贴合产业需求的人才培养方案、联合委派师资、共同研发教学资源、共建实训室、共同监管培养质量、共同组织技能竞赛、共同承担师资培训、共享就业资源，实现校企资源统筹、人才共育、责任共担。

（二）“五化”落地实施路径

落实师资队伍双师化、实行教材选用动态化、实习内容方向化、实训进程项目化、实习就业一体化，确保理论与实践深度融合，贴合院校“工学交替、岗课融通”的教学改革方向。

（三）“岗课赛证”四维融合体系

以岗位需求反向定制课程，以技能竞赛驱动能力提升，以职业证书强化专业素养，落实“学-训-练-考-赛-证”一体化落地。

（四）产教融合与课程思政深度融入

将企业真实安全项目、行业标准、法治规范融入教学全过程；同步将课程思政贯穿人才培养各环节，结合网络空间主权、关键信息基础设施保护、红客精神等内容，培育学生家国情怀与职业担当，实现德技并修。

（五）真实项目驱动，实战能力突出

按“攻防—运维—应急”三类设计实训任务分层，采用“项目任务式”交付模式，学生参与企业内网安全加固、数据泄露应急响应、工控系统安全防护等真实项目，提升漏洞检测、入侵防御、应急处置能力。

（六）“三有”课堂引领，形成人才培养特色亮点

将有趣、有效、有用“三有”课堂教学改革实践路径融入人才培养全过程。以项目化教学贯穿教育教学，推动教法与学法协同变革、课程思政精准融入、AI技术全场景应用和教学评价改革，在教学方法、学习评价等环节全面体现，形成学校人才培养特色亮点。

十五、附录

1. 专业教学进程表

广东碧桂园职业学院（IT 技术专业群）2026 级信息安全技术应用专业教学进程表

专业方向：

人才培养阶段	课程类别	课程性质	课程编码	课程名称	课程类型	总学分	总学时	学时分配		核心课程	考核方式	学期周学时安排						
								理论学时	实践学时			1	2	3	4	5	6	
第一阶段 职业素养培养与专业岗位基础能力训练	公共基础课	必修	991110010	思想道德与法治	A	3	54	45	9*			3						
			991110033	毛泽东思想和中国特色社会主义理论体系概论	A	2	36	32	4		▲		2					
			991110030	习近平新时代中国特色社会主义思想概论	A	3	54	48	6		▲			3				
			991130006	走在前列的广东实践	B	1	18	10	8					1				
			991110011	形势与政策	A	1	48	48				每学期 8 学时						
			981120017	军体融合课	C	6	108	8	100			3	3	1	1			
			981120008	军事技能	C	2	112		112			2w						
			981110013	军事理论	A	2	36	36						2				
			984130010	大学生心理健康教育	A	2	36	24	6+6*			2						
			981110022	大学生职业发展与就业指导	B	2	38	18	20*			每学期 6 学时						
			981130005	大学生创新创业	B	2	36	18	18*				2					
			981110012	国家安全教育	A	1	18	18							1			
			981120058	体育体质健康测试	C	0.5	9		9			每学年 3 学时						
			981120019	劳动教育	C	1	18	4	14*				1					
			981110024	美育概论	A	1	18	18				1						
			111110001	人工智能导论	B	1	18	8	10			1						
			981110023	碧桂园企业文化	B	0.5	8	8				每学期 2 学时						
			981120077	安全急救教育	C	0.5	8		8			2						
			小计				31.5	673	343	330			12	8	7	2		
			限选	---	中华优秀传统文化类课程	A	2	36	20	16			课程设置面向全校，学生在限定课程中选择修学					
				---	创新创业类课程	A	2	36	20	16								
				小计				4	72	40	32							
			任选	---	人文素养类课程	A	2	36	20	16			课程设置面向全校，学生在给定范围内任选					
				---	科学素养类课程	A	2	36	20	16								
				小计				4	72	40	32							
			公共课合计				39.5	817	423	394			12	8	7	2		
	专业群平台课 (必修)			104130045	Python 编程基础	B	4	72	32	40				4				
				104130003	操作系统	B	3.5	60	30	30			4					
				214130021	计算机技术基础	B	3.5	60	30	30		▲	4					
				104110010	网页设计与制作	A	3.5	60	36	24		▲	4					
				214130009	数据库技术	B	3	54	24	30				3				
				小计				17.5	306	152	154			12	7			

	专业 技术 平台 课 (必修)		104130038	信息安全等级保护	B	3.5	60	24	36	★	▲		4				
			104130047	办公与企业终端安全运维	B	3.5	60	30	30	★	▲		3				
			104130036	操作系统安全防护实战	B	3	54	27	27	★	▲			3			
			104130037	电子数据取证技术应用	B	3	54	30	24	★	▲			3			
			104120006	渗透测试实战	B	4	72	32	40	★	▲			4			
			104130021	网络设备配置与安全	B	4	72	32	40	★	▲			4			
			104120005	华为 HCIA 实践	A	3	54	34	20					3			
			小计			24	426	209	217			0	7	17			
	专业 群 拓 展 课 (限 选)	模块一 (人工 智能技 术应用 专业)	980070014	交互界面设计	A	2	36	24	12						2		
			980070015	智能终端系统集成与测试	A	2	36	24	12						2		
		模块二 (软件 技术专 业)	980070016	前端项目与交互实战	A	2	36	24	12						2		
			980070017	Web 后端项目实战开发	A	2	36	24	12						2		
		模块三 (云计 算技术 应用专 业)	980070018	企业 IT 环境构建与运维实战	A	2	36	24	12						2		
			980070019	网络安全技术与实训	A	2	36	24	12						2		
		模块四 (大数 据应用 技术专 业)	104130031	大数据实时计算实战	A	2	36	24	12						2		
			104130032	数据仓库开发实战	A	2	36	24	12						2		
		模块五 (信息 安全专 业)	104130033	数据安全治理实战	A	2	36	24	12						2		
			104110019	云安全技术与应用	A	2	36	24	12						2		
			小计			4	72	48	24						4		
第二阶 段 岗 位 分 流 专 业 知 识 深 化 学 习 和 专 业 技 能 强 化 训 练	岗 位 课 (限 选)		104130034	企业级网络安全实施	B	3	54	24	30		▲			4			
			104130049	网络安全检测与应急响应	B	3	54	24	30						4		
			104130040	信息安全项目管理	B	3	54	24	30						4		
			104130039	信息安全风险评估	B	3	54	24	30						4		
			104130041	岗位能力强化训练	C	18	324		324							18w	
			104130042	岗位实践共性问题解析	A	2.5	48	48								2w	
			小计			32.5	588	144	444						16		
第三阶 段 基 层 管 理 干 部 (技 术 骨 干) 岗 位 职 务 能 力 企 业 实 践 教 学 培 养	岗 位 企 业 实 践 教 学 培 养 (必 修)	104130045	岗位实习与毕业设计(必修)	C	20	360	72	288							20w		
		小计			20	360	72	288									
	专业（技能）课合计					98	1752	625	1127			12	14	17	20		
学时、学分及学期周学时总计						137.5	2569	1048	1521			24	22	24	22		

注：*表示课外实践；★表示核心课程；▲表示考试课程，其余为考查；w 表示集中实践教学周
学生素质拓展贯穿全学程，素质拓展学分为 12 学分以上
专业技术拓展课程，群内一个专业一个模块，应列明所有专业的专业技术拓展课程，学生可自由选择其中一个或多个模块学习。