

中央电化教育馆函件

教电馆[2020]24号

中央电化教育馆关于开展职业院校 网络与信息安全专业校企合作建设项目的通知

各省、自治区、直辖市电教馆（中心）、新疆生产建设兵团中小学电教馆，有关职业院校：

为深入贯彻《关于加强网络安全学科建设和人才培养的意见》（中网办发文〔2016〕4号）、《国务院办公厅关于深化产教融合的若干意见》（国办发〔2017〕95号）和《国家职业教育改革实施方案》（国发〔2019〕4号）精神，促进职业院校在信息安全与管理（高职）、网络信息安全（中职）专业领域的人才培养，开展产学合作，经研究，我馆决定在职业院校中开展“职业教育网络与信息安全专业校企合作建设”项目（以下简称“项目”）。现将有关事项通知如下：

一、目标任务

项目以产教融合为指导思想，以学生高水平就业为导向，为职业院校网络与信息安全专业建设提供支持服务，促进职业院校网络与信息安全专业人才培养。

项目将为职业院校提供网络与信息安全专业课程与师资培训，并根据院校专业建设的需要，提供人才培养方案、实验室建设、实训实习、帮助就业等支持服务。项目通过开

展系列交流活动，引入行业企业优质资源，提升学生专业技能水平，助力其高质量就业。

各有关省级电教部门、有关职业院校应对项目予以重视，积极参与，认真组织落实，推动项目实施。项目具体内容及实施办法详见项目《指南》（见附件1）。

二、组织实施

1. 中央电教馆负责项目的组织、实施和管理；
2. 各省级电教部门在本省（区、市）教育行政部门的指导下，做好本地项目的组织、实施和管理工作；
3. 相关单位（机构）提供技术支持和服务；
4. 项目专家团队为项目提供智力支持，如：教师培训、实地指导等。

三、项目院校申报

（一）申报条件

项目院校应为开设或拟开设网络与信息安全专业的职业院校。

（二）申报方式

1. 请有关职业院校于2020年7月3日前将申报表（见附件2）盖章扫描件pdf版和word电子版发至我馆联系人邮箱，并报所在省（区、市）的省级电教部门备案；
2. 我馆将于7月15日前发文公布项目院校名单。

四、联系方式

联系人：中央电教馆职业教育教学资源部 姜博仑

电 话：010-66490216

地 址：北京复兴门内大街160号609室，邮编：100031

邮 箱：jiangbl@moe.edu.cn

本通知电子版可在我馆网站 (<http://www.ncet.edu.cn>) 下载。

附件:

1. 中央电化教育馆“职业院校网络与信息安全专业校企合作建设项目”指南
2. 职业院校网络与信息安全专业校企合作建设项目院校申报表



附件 1:

中央电化教育馆
“职业院校网络与信息安全专业校企合作建设项目”
指南

目 录

一、项目背景 2

二、项目目标 2

三、项目内容 3

四、项目实施 8

五、项目组织 8

一、项目背景

党的十八大以来，在以习近平总书记为总书记的党中央的坚强领导下，国家网络安全建设以及人才培养取得重要进展，受到空前重视。习近平总书记在全国网信工作会议讲话中指出，“没有网络安全就没有国家安全”。

随着信息化的快速发展，网络安全问题更加突出，对网络安全人才建设不断提出新的要求。从总体上看，我国网络安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。网络安全学科建设刚刚起步，迫切需要加大投入力度，加强网络安全专业建设和人才培养。

2019年6月，教育部组织开展了《中等职业学校专业目录(2010)》修订工作，在信息技术类专业中新增网络信息安全专业，为职业教育网络信息安全专业发展提供了契机。

为深入贯彻《关于加强网络安全学科建设和人才培养的意见》(中网办发文〔2016〕4号)、《国务院办公厅关于深化产教融合的若干意见》(国办发〔2017〕95号)和《国家职业教育改革实施方案》(国发[2019]4号)精神，促进职业院校在信息安全与管理(高职)、网络信息安全(中职)专业领域的人才培养、开展产学合作，我馆决定在职业院校中开展职业教育网络与信息安全专业校企合作建设项目。

二、项目目标

以产教融合、校企合作为指导思想，以学生高水平就业为导向，为职业院校网络与信息安全专业建设提供支持服务，

促进职业院校网络与信息安全专业人才培养。

三、项目内容

本项目计划为职业院校网络与信息安全专业建设提供实践性课程教学资源以及人才培养方案、实验室建设、“双师型”师资培养、实训实习、帮助就业等支持服务。

（一）专业课程

通过对工作岗位职业能力的分析与设计，并结合一线工程师与职业院校专家的经验，设计开发的实训类课程资源，包括：教材、大纲、ppt、实验指导书、初始题库等。

涉及的核心课程包括：《web 安全原理与分析实践》《web 应用防火墙技术及应用》《防火墙技术及实践》《漏洞扫描与防护》《漏洞扫描与防护实验指导》《日志审计与分析》《日志审计与分析实验指导》《VPN 技术原理与实践》《windows 安全加固》《Linux 安全加固》《中间件安全》《漏洞验证》《风险评估》《网络安全运维》《安全接入技术》《数据库安全》等。院校可根据自身需求选购使用。

（二）人才培养方案建设

与企业用人需求对接，根据院校需求和实际情况，选择培养方向，与院校共同定制人才培养方案。覆盖岗位包括：网络安全分析、安全产品运维、渗透测试、应急处置、等保测评、风险评估等。

（三）实验室建设

可提供的实验室方案包括：网络安全教学实验室、网络攻防竞技实验室、代码安全实验室、大数据与云安全实验室、应急演练网络靶场、综合测试网络靶场。

1. 网络安全教学实验室

实验室可集合训、练、考、评一体化设计的网络安全对抗训练平台。基于高度仿真的虚拟网络，模拟物理环境组网，提供网络安全攻防知识培训及实操解题练习和测评功能，并形成完整的人才能力评价体系。在此平台之上，还提供了一套完整的网络安全能力提升知识体系，覆盖上百个安全方向，可以针对不同需求进行培训内容的训练。网络安全人员可按照学习日程安排的课程学习，课程内容包含基础知识、虚拟仿真实验、项目实训实验、基础内容考核等，能完全覆盖网络安全教学课程和人才培养方案。

2. 网络攻防竞技实验室

网络安全竞技实验室承担了攻防实训的考核功能，通过竞技系统可以针对实训的内容进行阶段性的测试考核，通过考核分析来检验学习效果，找到学习的难点重点，此外竞技系统还可以组建竞赛比赛，通过比赛选拔人才，同时以赛促练，以赛代练提高网络安全人员的攻防知识的水平，实现安全人才的高效选拔、信息安全人才的水准认证等。多样化的赛事模式，提供在线 CTF 赛事及攻防混战等多种赛事模式，检测选手对攻防、技术的答题速度、答题水平及综合渗透能力。同时又需提供多样化竞赛题目类型，以及大量经典赛事题目，通过实战、CTF、红蓝对抗赛，满足赛事组织者及参与者各方面要求。

3. 代码安全实验室

代码安全作为网络信息安全的一项基础性学科，该项技术应当让学生在校期间系统掌握。特别是源代码安全缺陷类型和模式的学习对于他们打牢网络空间安全的专业基

础，培养专业意识、提高专业素养有非常重要的作用。

建设代码安全实验室，以源代码安全检测平台和案例设计实训为依托，通过全面开展实验实训，面对 C/C++、Java 语言软件的源代码开展安全检测工作，培训学生借助工具分析代码安全问题、修复安全缺陷的能力。一方面实验室可促进提升学生掌握源代码安全检测的基础知识和实现技能，提高代码安全意识，为软件安全分析和代码安全分析的智能缺口提供人才储备。另一方面实验室平台为教师进行研究的平台。例如，源代码缺陷与软件漏洞关联关系分析、源代码缺陷误报分析等。同时也触发教师将源代码安全检测方法融入到网络空间安全其他相关学科中，与其他技术结合，探索更好的安全解决方案。

4. 大数据与云安全实验室

大数据与云安全实验室的建设可以搭建理论与实践的桥梁，为学生提供大数据与云安全技术的实验及实训平台，深化学生对大数据与云安全技术理论的理解，提高学生的操作能力，同时，利用所学知识对云安全技术进行创新型研究。大数据与云安全实验室包括云安全基础教学、云安全技术实战教学、真实实验云平台，为学生提供理论知识实验环境、大数据技术、云技术的知识实际应用实验案例，又可以涵盖真实大数据与云平台，使学生可以在真实环境中进行技术体验与研究。

大数据与云安全实验室提供了一套集成了完整云计算、大数据等课程资源的实践教学系统平台，针对当前云计算大数据专业建设，采用 Docker 容器化技术一站式提供性能可靠、环境完整、界面交互良好的实验和案例操作

环境，实验室以理论+实践、平台+资源的全新模式为教师和学生提供立体化、全周期的实践教学环节的支撑和辅助。

5. 应急演练网络靶场

应急演练网络安全靶场可以在真实的网络攻击环境中进行网络攻防演练，犹如置身于真正的网络战。像战斗机飞行员一样训练网络安全团队，尽可能接近现实世界的网络战争。通过智能自定义的攻击模拟和威胁场景建立，快速实现包含 IT/OT/IoT 的自动化攻防场景转换，在商用的 SOC/FW/IPS/工控/网络设备组成的实际网络中，实现包含红红对抗/红蓝对抗/蓝蓝对抗/自定义实网攻击对抗的全天候对抗，培养实战化的网络安全攻防能力。网络靶场可提供沉浸式的网络安全场景，实现自动且无缝地网络攻击与防御实践，让参训人员有机会在理论课堂学习的基础上，增强自己的网络安全操作技能，满足网络安全人员对于网络空间基础设施安全体系的建设与科研试验、网络空间安全学科体系规划、测试评估、人才教育培养等需求。

6. 综合测试网络靶场

支持学、练、赛、测一体的网络靶场平台，包括实操、视频、图文一体的网络安全技能学习，复杂、综合、逼真的网络安全场景演练，丰富多样的网络安全竞赛支撑，灵活、便捷、全面的测试与科研环境，在同一平台可满足人才培养、人才选拔、系统安全测试、网络安全试验、新技术验证等各种网络靶场应用场景。具备开放的第三方接入支撑，包括第三方虚拟节点采集探针接入、流量仿真接入、用户行为仿真接入、流量分析接入、网络安全

态势分析接入、网络安全态势展示接入等。具备开放、便捷的场景设计能力，可迅速构建需要的演练、竞赛、测试场景，支持统一的场景描述语言，可迅速导入第三方靶标和场景。配有强大的管理系统，能够为攻防竞演、护网演习，安全研究提供一个完整的、一体化的网络攻防竞演环境。

（四）“双师型”师资培训

目标为培养具有独立授课能力的“双师型”师资队伍。针对岗位核心能力课程，进行专项师资培训，使受训教师掌握专业课所需专业技术、授课方法、实验操作等。可根据院校自身工作安排，吸收教师参与企业实践，积累工程经验。

（五）实训与实习

本项目组建网络安全企业联盟，支持该项目开展。支持企业包括：北京翰博众安科技有限公司、北京奇安信科技集团股份有限公司、北京启明星辰信息技术有限公司等十几家企业。

上述企业可作为校外实训基地，集中承担合作院校的学生岗前实训。学生实训分为两个阶段，第一阶段在校内完成，完成后可以考取助理工程师认证。获得认证并且通过人力资源面试，学员可以选择校外实训基地参与岗前实训。实训合格的学员，企业提供顶岗实习岗位。

（六）就业指导

为在校生提供职业能力素养课程培训，职业素养课内容包括职业规划、简历编写、面试技巧、职场适应与职业发展等。对于获得岗位能力认证的学生，可推荐至上述产

业联盟中的企业就业。

四、项目实施

（一）试点实验

我馆将分批组织职业院校申报项目试点院校，就校企合作开展网络信息安全人才培养的课程、教学、实训、实习以及合作模式开展试点实验，试点院校由我馆确定为“职业教育网络与信息安全专业校企合作建设基地”。

（二）专家指导

项目组建“职业教育网络与信息安全专业校企合作项目专家组”，组织专家开展面向项目院校的实地指导、讲座培训等活动。

（三）活动推动

结合项目实施的情况，开展观摩和交流活动，促进区域和校际间的沟通与协作，分享项目实施经验，推进网络与信息安全专业建设协同发展；组织项目院校学生参加网络与信息安全领域的赛事活动。

（四）案例推广

在项目开展过程中对项目院校的实施情况进行调研，及时收集、整理项目实施过程中的典型案例，形成项目的示范、培育、推广效应。在开展上述活动并取得成果的基础上，进一步吸纳更多院校参与。

五、项目组织

本项目由中央电教馆组织实施，馆所属电化教育电子音像出版社负责课程开发及推广，网络安全企业联盟提供技术

支持。组建“职业教育网络与信息安全专业校企合作项目专家组”为项目提供专家指导。

联系方式：

联系人：中央电教馆职业教育教学资源部 姜博仑

电 话：010-66490216

邮 箱：jiangbl@moe.edu.cn

附件 2:

职业院校网络与信息安全专业校企合作建设项目
院校申报表

基本信息			
院校名称（全称）			
省（自治区、直辖市）		中职/高职	
通讯地址			
官方网站			
联系方式			
项目负责人		项目联系人	
姓名		姓名	
职务		职务	
联系电话		联系电话	
电子邮箱		电子邮箱	
院校情况			
1. 院校开设网络与信息安全专业情况 （是否开设；已经开设的，开设了什么专业，有关专业的授课教师、学生人数、软硬件等信息）			

2. 院校对本校建设网络与信息安全专业的预期	
3. 院校对本项目在本校开展的计划与保障	
4. 其它需要说明的内容	
<div data-bbox="879 1597 1054 1644">院校盖章:</div> <div data-bbox="957 1736 1054 1783">日期:</div>	

备注：项目负责人应由校长或副校长担任，项目联系人应由具体负责项目工作的教务部门或信息化部门负责同志担任。