北京市人力资源和社会保障局文件

京人社发〔2024〕2号

北京市人力资源和社会保障局关于增设网络空间安全职称评审专业的通告

为推进网络空间安全产业高质量发展，拓展网络空间安全领域专业技术人才职业发展通道，助力北京“四个中心”建设，经研究，决定在工程技术系列增设网络空间安全职称评审专业。

本通告自2024年5月1日起执行，由市人力资源社会保障局负责解释。

特此通告。

附件：1. 北京市网络空间安全专业职称评价试行办法

2. 北京市网络空间安全专业职称申报标准条件

北京市人力资源和社会保障局

2024 年 4 月 10 日

（此件主动公开）

北京市人力资源和社会保障局办公室　　2024 年 4 月 12 日印发

附件 1

北京市网络空间安全专业职称评价试行办法

为拓展网络空间安全领域专业技术人才职业发展通道，提升首都城市网络空间安全应对处理能力，助力北京“四个中心”建设，根据《关于进一步加强和改进职称工作的通知》（京人社事业发〔2023〕10号）、《北京市职称评审管理暂行办法》（京人社事业发〔2020〕12号）、《北京市深化工程技术人才职称制度改革实施办法》（京人社事业发〔2020〕17号）等文件规定，结合实际，制定本办法。

一、适用范围

本办法适用于本市国有企业事业单位、非公有制经济组织、社会组织等机构中，在网络与系统安全、信息内容安全、数据安全、业务安全等领域从事研发、服务、应用和监管等工作的专业技术人才。

二、层级设置

北京市网络空间安全专业职称纳入工程技术职称系列，设置初级、中级、高级。初级只设助理级，高级分设副高级和正高级。助理级、中级、副高级和正高级职称名称依次为助理工程师、工程师、高级工程师和正高级工程师。

三、专业方向

北京市网络空间安全专业包括网络与系统安全、信息内容安全、数据安全、业务安全等四个方向。

1.网络与系统安全专业方向。包括从事通信安全、芯片安全、主板安全、存储器安全、外设安全、嵌入式系统安全、系统软件安全、云安全、可信计算与虚拟化安全、网络与系统安全标准研究与制修订、网络与系统安全系统建设、网络与系统安全系统运维、网络与系统安全监管、风险评估、恶意代码分析与防护、事件检测、漏洞挖掘与逆向分析、系统与网络安全评测、攻防对抗技术、攻击行为检测、分析与处置、应急响应、数据备份、灾难恢复、技术成果转化等工作。

2.信息内容安全专业方向。包括从事多模态信息获取与识别、多模态信息筛选与过滤、信息内容安全标准研究与制修订、网络信息安全管理、内容理解与舆情分析、信息与情报分析、信息挖掘、社交网络安全、数字版权保护、信息隐藏、信息内容审查、信息内容安全系统评测、信息内容安全系统建设、信息内容安全系统运维、信息内容安全监管、技术成果转化等工作。

3.数据安全专业方向。包括从事数据库安全、身份认证与管理、数据隐私保护、数据分类分级、数据识别与追踪溯源、安全多方计算、同态加密、共识机制安全、智能合约安全、信息泄漏分析、加密协议软硬件研发、加密模块安全防护研发、加密产品开发、数据安全与加密标准研究与制修订、数据安全及加密系统建设、数据安全及加密系统运维、数据安全及加密监管、应用系

统规划、管理、测评与检查、系统监测、应急演练、事件处置能力评估、技术成果转化等工作。

4.业务安全专业方向。包括从事电子政务系统安全、电子商务系统安全、电子支付安全、工业控制系统安全、车联网安全、智慧城市安全、大数据平台安全、人工智能安全、软件定义安全、网络虚拟化安全、业务安全标准研究与制修订、业务安全系统建设、业务安全系统运维、业务安全监管、技术成果转化等工作。

四、评价方式

按照“个人自主申报、单位择优推荐、多方共同评价、促进评用结合、政府指导监管”的方式实行社会化评价，纳入本市年度职称评价工作安排，每年组织一次，可适时开展专项评审，实现产业链、人才链、创新链融合发展。经评审通过的人员取得相应职称证书后，用人单位根据需要，自主、择优聘任专业技术职务。具体评审程序及要求见各年度职称评审工作安排。

五、评审委员会

经市人力资源社会保障局授权备案的评审服务机构，组建北京市工程技术系列（网络空间安全专业）正高级、高级、中级、初级评审委员会，负责网络空间安全专业正高级、副高级、中级和初级职称的评审工作。

六、其他有关事项

（一）市人力资源社会保障局负责北京市工程技术系列网络空间安全专业职称评价政策制定、制度建设、协调落实、监督检

查和工作评估；评审服务机构负责落实政策、完善评价标准和办法、组织开展日常评价工作。

（二）职称评审结果将作为确定岗位、考核、晋升、绩效、薪酬等的依据，鼓励各用人单位对取得网络空间安全专业职称的人才给予奖励。

附件 2

北京市网络空间安全专业职称申报标准条件

申报北京市工程技术系列网络空间安全专业职称资格的专业技术人才，应遵守宪法和法律法规，贯彻落实党和国家的相关方针政策，坚持德才兼备、以德为先，具有良好的职业道德和敬业精神，从事网络空间安全专业工作，具备正常履行岗位职责必须的身体条件和心理素质，按要求参加继续教育。

申报北京市工程技术系列网络空间安全专业职称，需同时满足基本条件、学历和专业经历条件、业绩条件、成果条件，其中成果条件为在以往职称评审过程中未使用过的成果。具体如下：

一、助理工程师

（一）基本条件

掌握本专业的基础理论知识和专业技术知识，了解与本专业相关的法律、法规和政策，具有独立完成一般性技术工作的能力，能处理本专业范围内一般性技术问题。

（二）学历和专业工作经历条件（符合下列条件之一）：

1.具备硕士学位或硕士研究生毕业，从事本专业技术工作；

2.具备大学本科学历或技工院校预备技师（技师）班毕业，从事本专业技术工作满 1 年；

3.具备大学专科学历或技工院校高级工班毕业，从事本专业

技术工作满3年；

4.具备中等职业学校毕业学历或技工院校中级工班毕业，从事本专业技术工作满5年。

二、工程师

（一）基本条件

1.熟练掌握并能够灵活运用本专业基础理论知识和专业技术知识、业务工作基本方法和技能；熟悉本专业技术标准和规程，掌握与本专业相关的法律、法规和政策；了解本专业新技术、新工艺、新设备、新材料的现状和发展趋势；具有指导助理工程师工作的能力。

2.学历和专业工作经历条件（符合下列条件之一）：

（1）具备博士学位或博士研究生毕业，从事本专业技术工作；

（2）具备硕士学位或硕士研究生毕业，从事本专业技术工作满2年；

（3）具备大学本科学历或技工院校预备技师（技师）班毕业，从事本专业技术工作满5年；

（4）具备大学专科及以上学历或技工院校高级工班以上毕业、取得初级职称后，从事本专业技术工作满4年。

（二）业绩条件

1.从事网络与系统安全专业技术工作，熟悉网络与系统安全的开发流程和建设方法，具备承担本专业方向的标准制修订，网络与系统安全的研发设计、验证测试、产品开发、软件开发和应

用推广等相关工作的能力。

2.从事信息内容安全专业技术工作，熟悉信息内容的获取、识别、筛选和过滤的技术理论和研究方法；具备承担本专业方向的信息内容安全标准制修订，舆情分析、情报分析、内容评测、信息挖掘、版权保护、信息隐藏、内容审查、内容建设、内容运维、技术成果转让等相关技术工作的能力。

3.从事数据安全专业技术工作，熟悉数据安全识别、跟踪、评估和治理的技术理论和研究方法，具备承担本专业方向的标准制修订，数据安全分析和事后评估、风险治理（数据脱敏、敏感数据归一化、API 治理、数据资产地图、数据加密、隐私管理等）等相关技术工作的能力。

4.从事业务安全专业技术工作，熟悉新一代电子应用业务的技术理论和研究方法；具备承担本专业方向的标准制修订，电子政务、电子商务、电子支付、工业控制、物联网、智慧城市、人工智能、软件定义、网络虚拟化等业务安全相关技术工作的能力。

（三）成果条件（应具备下列 8 项成果中 2 项及以上，同一类型的多个成果可累计计算）

1.参与完成在单位内具有较大影响的攻关项目 1 项及以上，研究成果通过相关部门鉴定或验收；

2.参与完成行业内较大影响的研究报告、评估报告、工程咨询报告和工程设计文件等，并得到地市级及以上相关部门技术推广；

3.参与完成行业内较大影响的新产品、新设备、新工艺，并已投入生产；

4.参与完成已获得授权的发明专利；

5.参与完成下列之一：国家标准、行业标准、团体标准、地方标准或企业标准；

6.参与发现较大风险隐患，或参与较严重的安全事件处置工作；

7.参与完成技术成果转移转化项目，并取得较好经济和社会效益。

8.参与完成公开出版的专著或编著；

9.作为排名前三的作者在国内外公开发行学术刊物上发表有学术价值的专业论文。

三、高级工程师

（一）基本条件

1.系统掌握本专业基础理论知识和专业技术知识，掌握与本专业相关的法律、法规和政策，掌握国内外网络空间安全领域现状和发展趋势，具有跟踪网络空间安全专业科技发展前沿水平的能力；认真履行工作职责，履职成效良好，有较高的行业认可度；在指导、培养中青年学术技术骨干方面发挥重要作用，能够指导工程师工作和学习。

2.学历和专业工作经历条件（应符合下列条件之一）：

（1）具备博士学位或博士研究生毕业，从事本专业技术工

作满2年；

（2）具备硕士学位或硕士研究生毕业，从事本专业技术工作满7年；

（3）具备大学本科及以上学历或技工院校预备技师（技师）班毕业，取得中级职称后，从事本专业技术工作满5年；

（4）已取得非本系列（专业）副高级职称后，从事本专业技术工作满3年。

（二）业绩条件

作为主要完成人能够完成本单位本专业项目的规划和实施工作，或制定本单位本专业的管理标准、战略规划、管理制度，在项目管理、科研开发、技术推广应用等工作中取得较好成效。

1.从事网络与系统安全专业技术工作，系统掌握网络与系统安全的开发流程和建设方法，具备承担较复杂的网络与系统安全的研发设计、验证测试、产品开发、软件开发和应用推广等相关工作的能力。

2.从事信息内容安全专业技术工作，系统掌握信息内容的获取、识别、筛选和过滤的技术理论和研究方法，具备承担较为复杂的舆情分析、情报分析、内容评测、信息挖掘、版权保护、信息隐藏、内容审查、内容建设、内容运维、技术成果转让等相关技术工作的能力。

3.从事数据安全专业技术工作，系统掌握数据安全识别、跟踪、评估和治理的技术理论和研究方法，具备承担较复杂的数据

安全分析和事后评估、风险治理（数据脱敏、敏感数据归一化、API 治理、数据资产地图、数据加密、隐私管理等）等相关技术工作的能力。

4.从事业务安全专业技术工作，系统掌握新一代电子应用业务的安全技术理论和研究方法；具备承担较复杂的电子政务、电子商务、电子支付、工业控制、物联网、智慧城市、人工智能、软件定义、网络虚拟化等业务安全相关技术工作的能力。

（三）成果条件（应具备下列 8 项成果中 3 项及以上，同一类型的多个成果可累计计算）

1.作为排名前三的负责人完成在行业内具有较大影响的攻关项目，其研究成果通过省部级及以上行业主管部门鉴定或验收；

2.作为排名前三的负责人完成开发具有较高技术水平的新产品、新设备、新工艺等 2 项及以上，并在相关领域实际应用，取得了较大经济和社会效益；

3.作为第一发明人获得已授权的发明专利 1 项；

4.作为主要完成人完成行业内较大影响的研究报告、评估报告、工程咨询报告和工程设计文件等，并得到省部级以上部门技术推广；

5.作为排名前三完成人编写行业内具有较大影响力的专著或编著，并出版发行；

6.作为主要完成人发现较大风险隐患，或作为主要负责人处

置了较严重的安全事件；

7.作为主要完成人完成技术成果转移转化项目，并取得了经济和社会效益；

8.作为排名前三的作者在国内外核心期刊上发表有重要学术价值的专业论文。

（四）破格申报高级工程师

具备下列条件之一，可不受学历和专业工作经历限制，破格申报高级工程师：

1.获得网络空间安全领域省部级及以上科技奖项（一等奖排名前五、二等奖排名前三）；

2.作为排名前三完成人，获得中国专利银奖及以上；

3.作为排名前五完成人编写国家标准；

4.作为排名前三完成人，参与完成省级及以上网络安全重大项目；

5.网络安全产业相关国家重点实验室、国家技术创新中心、科技领军企业、行业龙头企业等单位的技术负责人；

6.承担国家级重大活动网络安全保障任务，成绩突出且个人受到省部级及以上行业主管部门表扬或感谢；

7.作为主要负责人发现系统中存在的重要漏洞，得到CNVD、CNNVD等国家漏洞管理部门书面认可。

四、正高级工程师

（一）基本条件

1.具有全面系统的专业理论知识和实践功底，全面掌握本专业国内外前沿发展动态，精通与本专业相关的法律、法规和政策，科研水平、学术造诣或科学实践能力强，在本专业领域具有很高的知名度和影响力，在突破关键核心技术和自主创新方面做出突出贡献，发挥较强的引领和示范作用；在指导、培养中青年学术技术骨干方面作出突出贡献，能够有效指导高级工程师工作和学习。

2.学历和专业工作经历条件（符合下列条件之一）：

（1）具备大学本科以上学历或技工院校预备技师（技师）班毕业，取得副高级职称后，从事本专业技术工作满5年；

（2）已取得非本系列（专业）正高级职称后，从事本专业技术工作满3年。

（二）业绩条件

主持或承担国家级本专业研究项目、课题，形成的技术报告经同行专家评议具有国内领先水平，并取得显著经济或社会效益；或主持制定国家、省部、行业本专业中长期发展规划、重大战略决策等相关政策、标准、规范，并颁布实施；或作为主要负责人发表本专业研究成果，经同行专家评议具有较高学术价值，推动本专业发展。

1.从事网络与系统安全专业技术工作，全面系统掌握网络与系统安全的开发流程和建设方法；掌握国内外本专业的技术研发、应用与服务、行业监管和科技成果转化等的发展动态和发展方向；具备主持完成本专业方向难度很高的研发设计、验证测试、

软件开发等相关工作的能力；能够推动本专业的发展，并在领域中所展现出的技术达到国内一流水平。

2.从事信息内容安全专业技术工作，全面系统掌握信息获取、识别、筛选和过滤的技术理论和研究方法，掌握国内外本专业的技术研发、应用与服务、行业监管和科技成果转化等的发展动态和发展方向；具备主持完成本专业难度很高的舆情分析、情报分析、内容评测、信息挖掘、版权保护、信息隐藏、内容审查、内容建设、内容运维、技术成果转让等相关技术工作的能力；能够推动本专业的发展，并在领域中所展现出的技术达到国内一流水平。

3.从事数据安全专业技术工作，全面系统掌握数据安全识别、跟踪、评估和治理的技术理论和研究方法；掌握国内外本专业的技术研发、应用与服务、行业监管和科技成果转化等的发展动态和发展方向；具备主持完成本专业难度很高的数据安全分析和事后评估、风险治理（数据脱敏、敏感数据归一化、API 治理、数据资产地图、数据加密、隐私管理等）等相关技术工作的能力；能够推动本专业的发展，并在领域中所展现出的技术达到国内一流水平。

4.从事业务安全专业技术工作，全面系统掌握新一代电子应用业务的安全技术理论和研究方法；掌握国内外本专业的技术研发、应用与服务、行业监管和科技成果转化等的发展动态和发展方向；具备主持完成本专业难度很高的电子政务、电子商务、电子支付、工业控制、物联网、智慧城市、人工智能、软件定义、

网络虚拟化等业务安全相关技术工作的能力；能够推动本专业的发展，并在领域中所展现出的技术达到国内一流水平。

（三）成果条件（应具备下列成果8项中的3项及以上，同一类型的多个成果可累计计算）

1.作为主要负责人完成行业内具有较大影响的攻关项目，其研究成果通过国家级行业主管部门鉴定或验收；

2.作为主要负责人完成开发具有较高技术水平的新产品、新设备、新工艺等2项及以上，并在相关领域实际应用，取得了较大经济和社会效益；

3.作为第一发明人获得已授权的发明专利2项及以上；

4.作为主要负责人完成行业内较大影响的相关专业研究报告、评估报告、工程咨询报告和工程设计文件等，并得到省级及以上部门技术推广；

5.作为第一完成人编写行业内具有较大影响力的专著或编著，并出版发行；

6.作为主要负责人发现了较大网络安全风险隐患2项及以上，或作为主要负责人处置了较严重网络安全事件2项及以上；

7.作为主要负责人完成网络安全技术成果转移转化项目，并取得了较大的经济和社会效益；

8.作为第一作者在国内外核心期刊上发表有重要学术价值的相关专业论文。