

附件1:

秦农银行2024年金融科技劳务派遣人员招聘岗位需求明细表

序号	岗位编号	岗位分类	职位描述	任职条件	招聘人数
1	QN1	管理类	<ol style="list-style-type: none">参与信息科技项目的组织级监管与规划工作（包含项目管理、PMO、质量管理方向等）；参与制定组织级相关管理工作的规范及标准；负责开展信息科技项目相关管理工作的实施与落地。	<ol style="list-style-type: none">年龄45周岁（含）以下，全日制大学本科及以上学历；具有3年以上计算机信息科技相关工作经验，其中1年以上管理类工作经验；至少具备项目管理、PMO、质量管理等方向之一的专业知识和深入理解，并有丰富的实践经验；具有较强的综合分析能力和组织协调能力，有较好表达沟通和文字组织能力；具有金融行业背景、具有相关项目管理资质证书者优先。	20
2	QN2	研发类	<ol style="list-style-type: none">负责业务需求评估、功能设计、核心模块代码开发等工作；负责开展代码审查，识别并解决项目技术风险，确保研发质量优良；负责解决研发中出现的问题，对技术难点进行攻关，并能够解决疑难问题；在研发过程中运用相关管理制度、流程、规范，推动研发标准在负责的领域内落地；完成领导交办的其他事项。	<ol style="list-style-type: none">年龄40周岁（含）以下，全日制大学本科及以上学历；具有2年以上计算机信息科技相关工作经验，其中1年以上研发类工作经验；至少具备交易类系统的前端开发或后端开发、数据类系统的数据治理和数据研发等技能，并有丰富的实践经验；具备应用级系统的规划与设计能力，掌握或精通领域内研发工具与方法；具有高度责任心、抗压能力和团队合作精神，善于诊断技术问题、洞察技术风险，驱动问题解决；具有银行业系统研发经验的优先。	127
3	QN3	基础设施管理类	<ol style="list-style-type: none">负责网络、主机、虚拟化平台、云平台、操作系统、中间件、数据库系统整体规划、架构设计和建设实施；制定和落实网络、主机、虚拟化平台、云平台、操作系统、中间件、数据库系统相关管理制度规范；负责网络、主机、虚拟化平台、云平台、操作系统、中间件、数据库系统的日常管理维护工作；负责网络、主机、虚拟化平台、云平台、操作系统、中间件、数据库系统相关自动化工具的设计和开发工作；保障重要业务系统网络、主机、虚拟化平台、云平台、操作系统、中间件、数据库系统稳定运行；完成交办的其他工作事项。	<ol style="list-style-type: none">年龄40周岁（含）以下，全日制大学本科及以上学历，计算机相关专业；需满足以下条件中的一项：<ol style="list-style-type: none">2年以上网络维护工作经验；2年以上主机和操作系统维护工作经验；4年以上数据库维护工作经验；需满足以下要求中的一项：<ol style="list-style-type: none">精通网络交换和路由技术，熟悉TCP/IP协议，掌握各类常见路由器和交换机、负载均衡等设备的调试和管理；熟悉小型机、X86、C86、ARM等计算机系统架构，熟悉AIX、LINUX等操作系统，熟悉块、对象、文件等存储知识，熟悉Openstack、KVM等架构，掌握一种虚拟化平台和云平台的使用；需熟悉Oracle、Mysql、DB2、OB、TDSQL等数据库原理和高可用架构，能独立完成高可用架构的搭建以及数据库的优化工作；具有金融行业实践经验者优先。	15

秦农银行2024年金融科技劳务派遣人员招聘岗位需求明细表

序号	岗位编号	岗位分类	职位描述	任职条件	招聘人数
4	QN4	测试类	<ol style="list-style-type: none"> 1. 承担应用系统的测试任务，参与测试需求分析与测试案例设计等工作； 2. 参与测试管理配套的平台和工具的设计和建设，负责对测试人员进行业务及技术方面的测试指导； 3. 负责产品生命周期各阶段测试，进行功能或非功能测试实施； 4. 负责编写和执行测试案例； 5. 负责组织进行测试结果分析，编写测试报告，进行测试进展和结果汇报； 6. 负责撰写测试文档。 	<ol style="list-style-type: none"> 1. 年龄40周岁（含）以下，全日制大学本科及以上学历； 2. 具有2年以上计算机信息科技相关工作经验，其中1年以上测试类工作经验； 3. 至少具备功能测试、自动化测试、性能测试、测试管理、配置管理等方向之一的测试经验，并有丰富的实践经验； 4. 熟悉测试相关知识，熟练使用测试工具； 5. 熟悉MySQL/Oracle等主流数据库，能够编写测试sql； 6. 熟悉JAVA/Python等计算机语言，熟练使用Git、QTP、Selenium、Jenkins等开源工具； 7. 熟悉Linux操作系统常用命令和基础计算机网络知识； 8. 具有金融行业背景、具有相关专业资质证书者优先。 	10
5	QN5	网络安全类	<ol style="list-style-type: none"> 1. 参与网络安全规划，并负责落实网络安全相关工作； 2. 负责制定网络安全加固方案，并负责落实； 3. 参与技术方案制定，负责网络安全风险相关角度提出技术控制措施； 4. 负责安全事件分析、响应及处置（如网站入侵、网站后门、页面篡改等），从安全事件中分析提取IOC（入侵指标）并开展溯源； 5. 开展威胁情报和风险提示分析，对安全漏洞、攻击活动提供预警，组织排查和防范工作； 6. 负责渗透测试、漏洞扫描、代码审计工作，发现漏洞并督促相关方整改，确保网络安全技术防护水平能够有效抵御安全威胁； 7. 负责信息系统渗透测试、代码审计等安全测评工作； 8. 负责终端安全管理，包括终端桌面管理、防病毒、终端准入、终端操作系统管理等，负责终端安全整体策略及基线的制定和推广工作，负责相关系统的规划建设和运行维护等工作，包括日常巡检、故障诊断与处理、事件联动处置、应急响应、数据统计与分析以及日常维护工作； 9. 负责主机安全管理，包括相关系统规划建设和运行维护等工作，负责管理流程建设、平台建设日常检查、安全事件处置； 10. 负责制定安全配置基线、审核安全策略并负责落实； 11. 负责网络安全日常运营、运维。 	<ol style="list-style-type: none"> 1. 年龄35周岁（含）以下，全日制大学本科及以上学历； 2. 具有2年以上网络安全相关工作经验； 3. 掌握信息安全管理和技术各领域的基础知识，具有良好的计算机基础，熟悉信息安全相关法律法规、标准、技术规范； 4. 熟悉常见漏洞的机制原理，具备独立分析、评估和提供漏洞处置建议的能力； 5. 熟练使用Burpsuite、AWVS、NMAP、MSF、IDA、ADB等常用漏洞分析工具； 6. 掌握安全运维基本知识，熟悉金融机构安全架构及所使用的主要安全产品（如：防火墙、入侵检测（防护）、WAF应用防火墙、终端检测与响应、流量分析、蜜罐、态势感知等）； 7. 熟悉常见的APP、Web、操作系统及各类软件高危漏洞（SQL注入、XSS、CSRF、缓冲区溢出、命令执行、反序列化等）原理及实践，并具有漏洞挖掘经验； 8. 熟悉渗透测试步骤、方法、流程，熟练使用一定量的渗透测试工具；至少熟练掌握一门编程语言，熟悉C、JAVA、PHP、Python、SHELL语言，有测试代码或脚本编写经验，能独立做代码审计； 9. 能够根据已知威胁的TTP（战术、技术和过程）和入侵行为特征设计检测规则者优先考虑；具有CISSP/CISP/CISA网络安全相关证书或其他国家认可的网络安全资质证书者优先考虑。 	10
合计					182