秦农银行2025年金融科技劳务派遣人员招聘岗位需求明细表

序号	岗位分类	岗位描述	资格条件	招聘人数	备注
1	研发类	1.负责业务需求评估、功能设计、核心模块代码开发等工作； 2.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； 3.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； 4.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； 5.完成领导交办的其他事项。	1.年龄40周岁（含）以下，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年以上研发类工作经验； 3.至少具备交易类系统服务端开发、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； 4.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； 5.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； 6.具有银行业系统研发经验的优先； 7.掌握云平台、nginx、redis、tongweb等之中一种或多种平台、组件的管理、配置和优化； 8.熟悉Linux、AIX、CenterOS一种或多种操作系统及常用操作,具备shell脚本编写能力； 9.熟练掌握sql语句编写、有一定sql调优能力。	14人	互联网渠道服务端开发：3人 核心、总账等账务类系统开发：4人 反欺诈系统开发：2人 支付类系统开发：2人 技术支撑类开发：3人
2	安全类-网络安全岗	1.参与网络安全制度、标准规范和日常管理制度的制定； 2.参与网络、web、移动端、端点、云的安全架构设计； 3.参与主机安全、终端安全等的制度建立与检查； 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； 7.负责制定安全配置基线、审核安全策略并负责落实； 8.负责网络安全日常运营、运维。	1.年龄35周岁（含）以下，大学本科及以上学历； 2.具有5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。	1人	
3	安全类-渗透开发岗	1.渗透测试执行 制定计划：依据银行信息系统架构和业务特点，制定详细渗透测试计划，明确测试目标、范围、方法和时间安排。 漏洞扫描：运用Nmap、AWVS等工具对银行内部网络、服务器、应用系统进行定期扫描，识别潜在漏洞，如弱口令、SQL注入点、XSS漏洞等。 手工测试：针对关键业务系统和高风险区域，进行手工渗透测试，模拟黑客攻击手法，深入挖掘复杂漏洞，验证漏洞的可利用性。 报告编写：整理测试结果，编写专业渗透测试报告，清晰描述漏洞详情、危害程度、修复建议等，为银行安全加固提供依据。 2.渗透工具开发与维护 工具开发：根据银行安全需求和实际情况，运用C、Python等编程语言开发定制化渗透工具，提升渗透测试效率和准确性。 工具优化：持续关注安全技术发展和行业动态，对现有渗透工具进行优化升级，添加新功能，以适应不断变化的安全环境。 工具管理：负责渗透工具的日常管理和维护，确保工具的稳定性和安全性，防止工具被滥用或泄露。 安全研究与情报分析。 安全研究：深入研究新兴的网络攻击技术和安全漏洞，分析其原理和影响，为银行信息系统提供前瞻性的安全防护建议。 情报分析：收集整理国内外网络安全情报，结合银行实际情况进行分析评估，及时发现潜在安全威胁，为渗透测试和安全防护工作提供方向。 3.协助安全防护与应急响应 防护建议：依据渗透测试结果和安全研究成果，为银行的安全防护体系建设提供技术支持和建议，协助完善安全策略和措施。 应急响应：在银行信息系统遭受安全攻击或出现紧急安全事件时，迅速响应，运用渗透开发技能进行应急处置，如分析攻击路径、查找漏洞根源等。	1.年龄35周岁（含）以下，大学本科及以上学历； 2.具有2年及以上渗透测试或开发相关工作经验； 一、技术专长 1. 编程语言：精通Python、C或C++，能独立完成复杂渗透脚本、工具开发，熟悉常用安全库与框架，如Scapy、pwntools； 2. 操作系统：熟练掌握Windows、Linux系统，可进行系统漏洞挖掘、权限提升，熟悉系统加固与安全配置优化； 3. 数据库知识：熟悉MySQL、Oracle等主流数据库，掌握SQL语言，具备数据库渗透测试、注入攻击及防御能力，了解数据库审计与安全策略； 4. 网络技术：深入理解TCP/IP、HTTP等协议，熟悉网络拓扑，能运用Burp Suite、Nmap等工具进行网络扫描、漏洞探测，具备网络流量分析能力。 二、安全技能 1. 漏洞研究：深入研究常见漏洞原理，如SQL注入、XSS、CSRF、缓冲区溢出等，能及时掌握最新漏洞信息，具备0day漏洞挖掘能力者优先； 2. 渗透测试：熟练运用渗透测试流程与方法，独立完成银行核心业务系统、网络设备、Web应用等渗透测试，精准识别、评估安全风险，出具专业报告。 三、综合素质 1. 分析解决问题：面对复杂安全问题，能快速定位根源，通过多维度分析提出有效解决方案，具备应急响应与处理安全事件能力； 2. 学习能力：紧跟网络安全领域发展，主动学习新知识、新技能，快速掌握新兴攻击技术与防御手段； 3. 沟通协作：具备良好沟通能力，能与开发、运维、业务等团队高效协作，推动安全策略实施与漏洞修复。 四、职业素养 1. 严格遵守国家法律法规、行业规范及银行内部安全制度，确保所有渗透测试活动合规； 2. 对银行信息安全高度负责，妥善保管敏感信息，防止数据泄露 。	1人	

秦农银行2025年金融科技劳务派遣人员招聘岗位需求明细表

序号	岗位分类	岗位描述	资格条件	招聘人数	备注
4	基础设施-数据中心管理岗	1、承担数据中心基础设施建设工作，在设计过程中，提出建设需求、审核图纸;在建设过程中，对暖通或电气基础系统的施工质量、成本、变更等方面进行全过程管理，确保项目的顺利实施;负责制定新建数据中心的维护、应急、标准操作流程及作业指导书; 2、承担数据中心基础设施及系统(高低压供配电系统、备用电源系统、其他电气系统、暖通系统、弱电及监控系统)的运行、维护; 3、负责组织编制设备及系统各种维护计划，制定电气设备及系统、暖通系统，弱电及监控系统的日常运行操作、维护保养、专业检测等工作流程及作业指导书，制定各专业应急预案; 4、负责组织各专业服务商的管理、系统及设备的现场作业实施和管理、各种应急流程实施和演练; 5、负责数据中心监控平台技术支持工作，协调施工单位，完成弱电系统实施、调试、培训工作; 6、根据总行数据中心及分支行机房基础设施运行情况，优化系统运行模式及相关运行管理规则，负责能耗控制，降低运行PUE。	1、年龄35周岁及以下，大学本科及以上学历，职位相关专业领域5年及以上工作经验(包括工业电气、自动化、仪表、供电、暖通、空调、热能动力等)，其中3年及以上大型数据中心设计、工程管理或运维经验(不限于暖通或电气系统或设备的设计、工程施工、安装、调试及维护，或基础设施监控系统建设或运维)，特别优秀者可适当放宽; 2、具有电气专业相关知识基础，熟悉UPS、柴油发电机组高低压配电等设备的操作及维护，有大型电电气系统运行维护、设备管理经验; 3、熟练掌握大型数据中心暖通系统，熟悉各种制冷设备运行原理，有运维冷冻水系统和设备的经验，业务熟练，具有独立完成工作的能力;对空调水系统、风系统及末端设备的运行维护有丰富的经验; 4、具有机房动力环境监控系统、楼控系统(冷冻水系统)电力监控系统、DCIM系统的开发、应用及维护经验; 5、具有高级工程师证书、高低压操作证、高压入网证、注册公用设备或注册电气、UptimeATS、UptimeATD等相关资质证书者优先。	1人	
5	数据类岗位	1、负责根据全行业务发展目标，各机构需求，结合业务场景，进行业务数据的分析挖掘工作，并形成分析挖掘报告; 2、负责建立全行营销、绩效、风控、运营等数据分析挖掘体系，建立数据分析挖掘模型，并持续评估和优化; 3. 负责基于数据分析得到有价值的业务信息，为全行运营决策、产品方向、营销推广、风险管理等提供建设性建议，为各级管理层决策提供价值信息支撑; 4. 牵头规划和建立全行数据分析模型、数据分析工具等，支持技术开发团队完成系统建设，为全行数据分析提供模型、工具. 平台支撑; 5.跟踪联邦学习、隐私计算、大模型等技术在金融数据应用中的实践和落地; 6.负责数据治理体系建设，进行数据管理制度，规范，流程的设计与制定，包括数据标准制定、元数据管理、数据质量管理（问题治理+监控体系），推动数据资产价值最大化，支持银行业务决策和监管要求; 7.设计元数据管理框架，制定元数据采集、存储、维护和应用的规范；维护元数据并确保数据血缘清晰可追溯; 8.制定和维护银行数据标准，并推动标准在系统建设、数据交换中的落地；配合内外部审计和监管检查，确保数据合规性; 9.定位数据质量问题根因，协调业务、科技、风险等部门制定改进方案并跟踪落实；提炼银行业务数据质量要求，监控关键数据指标，推动问题整改; 10.建立并完善数据资产，实现数据资产全生命周期管理及价值评估。	1.年龄40周岁（含）以下，大学本科及以上学历；数学、统计、计算机、金融工程、信息技术等相关专业; 2.精通SQL/Python/R至少一种，熟悉银行常用数据库（Hive、Greenplum）; 3.掌握机器学习算法（如XGBoost、随机森林）在金融风控中的应用案例; 4.熟悉主流的大数据分析方法和计算框架，对预测建模、统计抽样、机器学习和人工智能技术有项目经验; 5、精通金融行业数据仓库架构，熟悉数据治理框架及数据资产管理方法论，具备金融监管报送系统建设经验者优先; 6、熟悉银行重要业务系统业务流程及数据; 7、逻辑清晰，具备问题分析和文档编写能力; 8、优秀的跨部门协调能力，能有效沟通业务、技术及合规部门; 9、持有CDMP、DAMA等数据管理认证证书者优先。	3人	
合计				20人	