信息安全岗位职责

. 相关推荐

信息安全岗位职责（精选 26 篇）

在生活中，岗位职责在生活中的使用越来越广泛，岗位职责可以明确每个人工作职责是什么内容，该承担什么样的工作、担当什么样的责任、如何更好的去做、什么是不该做的等等。相信很多朋友都对制定岗位职责感到非常苦恼吧，以下是店铺为大家收集的信息安全岗位职责，仅供参考，欢迎大家阅读。

信息安全岗位职责 篇 1

岗位职责：

1、负责制定信息安全技术体系的'规划和实施，负责安全管理制度制定实施和监督；

2、负责处理信息安全事件，参与安全专项保障工作，提供信息安全技术支撑；

3、负责公司网络和网络安全系统的建设、巡检、维护、故障处理等管理工作；

岗位要求：

1、本科及以上学历，信息安全、计算机、通信等相关专业，优秀应届生也可接受；

2、了解计算机网络体系，了解 TCP/IP 协议，对计算机网络感兴趣；

3、了解至少一门编程语言，了解安全运维扫描工具；

4、良好的沟通能力、团队合作精神，工作主动、认真，能承受一定压力。

信息安全岗位职责 篇 2

岗位职责：

1、管理、维护长期客户关系和资源，促成合作的进行；

2、评估客户需求，为客户定制信息安全服务方案；

3、与技术团队对接，根据客户需求，制订技术方案；

4、售后客户关系维护、客户满意度维护。

岗位要求：

1、熟悉网络架构和信息安全体系框架；

2、具备 2 年以上的.信息安全领域从业经验；

3、拥有优秀的沟通、展示能力；

4、计算机技术、信息安全、软件工程或相关领域本科、硕士学位优先。

信息安全岗位职责 篇 3

岗位职责：

1、熟练使用常用渗透测试工具，负责实施 app 、web 、系统服务器的安全性测试、渗透测试；

2、对渗透测试中存在的网络安全问题进行及时修补与加固；

3、响应公司发生的应急安全事件，对安全事件及时处理、分析、报告、溯源；

4、跟进业内以及第三方通报的最新安全漏洞，驱动业务团队修复和协助检验；

5、对开发工具进行线上的`安全扫描。

任职要求：

1、至少精通一门脚本语言；

2、熟习各种 web 安全攻防手法；

3、精通 web 应用程序渗透测试方法和定制攻击自动化；

4、深入理解 owasp 风险评估中前十位 web 攻击模式和评估方法；

5、善于挖掘 web 安全漏洞或有安全工具开发经验者优先；

6、2—3 年渗透测试经验，具备独立开展渗透工作的能力；

7、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；

8、熟悉攻击的各类技术及方法，对各类操作系统、应用平台的弱点有较深入的理解；

9、主动性强，具有良好的沟通、协调组织能力以及文档编写能力，逻辑性强。

信息安全岗位职责 篇 4

1.具有两年或两年以上工作经验,在操作系统、数据库、网络和安全产品等方面有扎实的'技术功底和项目实践。

2.熟悉流行的网络及主机类安全产品的部署情况,并熟练使用 VISO 。

3.负责等级保护,风险评估、安全咨询等各种项目的整个项目过程管理、协调。

4.性格活泼开朗,有较强的沟通协调能力,有主动学习意识、沟通和学习能力强、工作耐心、细心、负责,适应出差者优先考虑。

5.有 PMP 证书、CISA 、ISO27001LA 、cisp、cissp者优先。

6.具有华为、思科或等级测评师证书者优先。

信息安全岗位职责 篇 5

(一)岗位要求:

1、学历本科及以上;

2、熟练掌握英语,国家六级及以上水平,听说读写能力强,能够翻译英文资料;

3、熟悉有关信息安全相关知识,具有较强的业务学习能力;

4、参加工作 2 年或从事标准化工作 1 年以上;

5、具有国家或行业标准化工作经验优先;

6、具备良好的文字表达能力和沟通协调能力,责任心强,有良好的`团队合作精神。

(二)岗位职责:

1、跟踪国内国际信息安全标准化发展趋势,提出信息安全标准化工作建议;

2、开展国际信息安全标准在国内的应用落地实施工作;

3、宣传推广国家(行业)信息安全标准;

4、参与标准化项目,在项目组中负责与标准化项目主管单位沟通、协助项目经理制定项目计划和研究方案;

5、参与项目研究,撰写标准文档及项目方案;

6、根据要求组织与项目有关的各种会议和培训。

信息安全岗位职责 篇 6

岗位职责：

1 负责构建公司整体信息安全架构，制定未来的信息安全规划蓝图

2 负责督促并监控信息安全流程所涉及的各个部门的流程和制度的.执行，承担内部 it审计

工作 3 负责对公司所有信息系统的用户，角色，权限的合理性的审核与校正工作

4 对外信息发布流程及内容的安全审核工作

6 负责对整体 it信息架构安全隐患的挖掘，追踪与消除

7 信息安全问题导致的紧急与突发事件需定制应急预案，负责必要的紧急响应协调与危机公关工作

8 完成整体信息安全制度梳理，以及完成信息安全各个职能部门的相关培训

任职资格：

1 本科及本科以上学历 2 3~5 年工作经验，有信息安全方面管理经验

3 熟悉 sox404 ， iso

4 熟悉主流安全产品以及安全管理体系

5 良好的沟通能力，领导才能

信息安全岗位职责 篇 7

岗位描述

1、负责车联网数据服务运维工作的整体规划

2、负责规划组建运维团队以及定义角定分工

3、建立和完善规范化的运维体系，保证运维质量

4、制定突发事件处理响应机制，解决实际突发问题

5、负责与供应商运维团队协作完成平台的整体运维工作

6、负责自动化运维能力的'设计、开发和优化，及监控体系的建设

岗位要求

1、全日制大学本科及以上学历，计算机或相关专业，8 年以上工作经验，5 年以上运维工作经验

2、熟练使用 APM　监控工具 Dynatrace

3、熟练使用 Java、Python 等语言，精通 Java 开发

4、有 CMDB　，Zabbix，ELK，Saltstack 等自动化运维软件的开发经验

5、熟悉使用工具 Jenkins、Git、GitLab、SVN　中的任一种或任多种

6、精通容器技术，熟练运用 Docker ，熟悉至少一种容器编排引擎

7、熟悉阿里公有云相关 PaaS 组件

信息安全岗位职责 篇 8

网络安全员岗位职责

为了贯彻落实国务院办公室《关于加强计算机信息网络国际联网信息安全管理的紧急通知》和国家教育部《中国教育和科研计算机网暂行管理办法》等文件精神，进一步加强我校校园网安全管理，特制定网络安全管理员工作守则如下。

一、网络安全管理任职条件

网络安全管理员是负责学校网络安全运行，保证学校教学、办公、学习、生活等提供安全、畅通的高速信息通道。网络安全管理员必须具备以下条件：

1、坚持“四项基本原则”，遵照国家公安部关于使用网络的管理条例及国家教委有关网络工作的规定，严守国家机密。

2、思想端正，作风严谨，虚心好学，不断追求。

3、服从领导，团结协作，雷厉风行，完成本职。

4、熟悉本单位情况，掌握本单位信息知识及一定的计算机基础知识，具有一定的计算机网络管理技能。

二、网络安全管理员工作职责

在学校领导和网管中心领导指导下，负责学校校园网的安全管理工作，具体职责如下：

1、每天实时监控校园网运行情况，定时巡察校园网内各服务器，各子网的运行状态，及时做好值班记录。

2、每天监控防火墙、过滤网及杀毒软件的运行，并做好记录。在学校网站上及时公布目前互联网上病毒及防病毒的动态及我校防病毒方面的.要求及措施。 3、定时做好校园网各种运行软件的记录文档备份工作，做好保密工作，不得泄密。记录文档每季度整理一次，并刻录成光盘保存，并根据制度只提供一定部门人员查看。

4、对学校及上级机关文档要根据密级进行保护，对校内教学、办公等文档要求内部使用的，不得任意往外泄露。

5、要努力学习，不断更新自己计算机网络知识，努力提高计算机网络水平，参加各种网络安全管理培训班学习，提高自己网络安全管理水平。

6、热心网络安全管理工作，能及时向领导反映本人对网络安全管理工作的意见、建议等。

信息安全岗位职责 篇 9

岗位职责：

1、负责售前顾问工作，配合销售人员参与投标项目，完成整个投标过程；

2、与用户进行现场交流，包括初次交流、具体项目交流和投标交流；

3、为用户在项目启动前撰写和提供相关的技术文件，包括公司资料、技术建议书、长期规划建议等；

4、参与投标项目，负责撰写投标方案技术文件部分和过程中的技术应答文件；

5、负责和参与对用户的短期培训和讲座；

6、作为对销售部门售前过程的唯一接口，负责帮助销售协调测试和其他部门的资源；

7、根据公司安排，支持各分支机构的重要项目。

任职要求：

1、本科以上学历，网络安全或计算机相关专业；

2、具有规范编写专业文档的’能力，包括申报材料、宣传软文、分析报告、解决方案、成功案例分析等；

3、熟悉信息安全理论、主流信息安全技术、产品的应用部署及方案设计；

4、了解国家信息安全相关政策法规与标准规范；

5、具有良好的沟通、表达、总结归纳和文档撰写能力；

6、具有一定行业业务分析和行业解决方案设计的能力。

信息安全岗位职责 篇 10

职责描述：

1、负责落实监管部门和公司有关信息安全及科技风险管理要求；

2、负责制订、落实公司信息安全政策、制度和技术标准；

3、建立健全公司信息系统安全防护体系,完善系统和数据的备份、恢复机制,完善数据加密手段,落实系统三防(防篡改、防攻击、防泄露)安全措施；

4、监测公司信息安全管理水平和安全隐患,制定相应应急预案并定期演练,积极预防及处理信息安全事件；

5、指导网络硬件、软件开发等技术人员,实现符合安全等级保护工作标准或产品；对待上线软件进行安全检测,定期对公司网络、服务器及应用进行渗透测试；

6、负责研究跟踪最新信息科技安全动态,掌握运用有效的`网络攻防技术；

7、负责员工信息安全及科技风险教育培训。

任职要求：

1、本科(第一学历为 985 、211)及以上学历,计算机信息安全相关专业；

2、3 年以上信息安全管理工作经验；

3、精通信息安全评估理论,熟悉安全加固和安全审计技术,有丰富的实践经验；

4、掌握主要软硬件的信息安全点和攻防技术,熟悉安全控制技术并运用相关工具；

5、精通网络架构设计,熟悉路由器、防火墙、IDS/IPS/WAF　等配置及数据加密技术；

6、精通 Unix、Windows　等操作系统环境下的管理工具、服务和安全防护,熟悉主流数据库配置和管理;

7、良好的团队协作能力和学习能力;

8、有金融背景工作经验,CISSP、CISA 、ISO27000　等资历优先。

信息安全岗位职责 篇 11

任职要求:

1、有一定的计算机技能，能够处理 excel 等办公软件;

2、责任心强，具有团队协作意识;

3、工作态度积极乐观，能够承受一定的工作压力。

岗位要求:

1、一年以上信息安全工作经验,有一定的信息安全技术功底和先进的信息安全理念;

2、具有风险评估、安全策略设计、安全体系、安全规划等信息安全资讯服务项目的售前交流、撰写项目标书等售前能力实施经验，有 1 年以上安全服务项目实施与管理经验;

3、熟悉主流的网络安全产品（FW 、IDS、SCANNER　、AUDIT 等）的基本原理和基本技术;

4、熟悉国内外信息安全标准和规范，对信息安全风险评估、等级保护、ISO17799/27001　等有深刻理解;

5、负责数据中心所有网站接入的`备案信息收集、网站审核与网站备案资料的管理维护;

6、负责为内部人员进行备案流程的培训;

7、定期统计和整理涉及工作内容的数据，并完成工作报告;

8、协助公司相关部门开展网站备案咨询工作，解答用户问题。

岗位要求:

1、计算机应用、计算机网络、通信、信息安全等相关专业，一年以上网络安全领域工作经验，优秀应届生亦可;

2、了解网络安全技术：包括端口、服务漏洞扫描、程序漏洞分析检测、权限管理、入侵和攻击分析追踪、网站渗透、病毒木马防范等;

3、了解 tcp/ip协议，熟悉 sql 注入原理和手工检测、熟悉内存缓

冲区溢出原理和防范措施、熟悉信息存储和传输安全、熟悉数据包结构、熟悉 ddos 攻击类型和原理有一定的 ddos 攻防经验，熟悉 iis安全设置、熟悉 ipsec、组策略等系统安全设置；

4、了解 windows 或 linux系统；

5、了解主流网络安全产品（如 fw、ids、scanner 、audit 等）的配置及使用；

6、善于表达沟通，诚实守信，责任心强，讲求效率，具有良好的团队协作精神。

岗位职责：

1、网络信息安全工程师的工作主要是为企业量身定做合理且经济的信息网络安全解决方案，维护日常网络安全管理，预防网络安全隐患等；

2、通过运用各种安全产品和技术，设置防火墙、防病毒、IDS、PKI、攻防技术等，进行安全制度建设与安全技术规划、日常维护管理、信息安全检查与审计系统帐号管理与系统日志检查等；

3、能适应两班倒，9:00-16:30 16:00-24:00（做五休二，包住宿）。

信息安全岗位职责 篇 12

1、协助现代教育技术中心领导制定本校校园网建设及网络发展总体规划和项目计划，并贯彻落实。

2、负责校园网域名与 IP 地址注册审核等业务,并与上级相关技术部门积极沟通协调。

3、负责校园网服务器、交换机、集线器、路由器、防火墙等各种网络设施的维护和管理,定期对网络设施进行巡查。

4、协助完成 DNS 、WEB 、FTP 、教学、数据库等各种服务器及应用系统的安装、配置、维护和调整及更新，协助解决校园网应用和管理中的关键技术。

5、确定网络安全及资源共享策略；协助完成公共信息服务器的安全监控和日常管理，及时排除各种故障。

6、负责监察网络运行状况，调整网络参数，调度网络资源，保障

网络安全、稳定、畅通。

7、负责计算机网络设备资料的整理和归档。

8、负责收集整理网络拓扑图、网络接线图表、设备规格及配置清单、网络管理记录、网络运行记录、网络检修记录等网络资料。

9、负责为全校教职员工与学生提供网络技术支持与咨询。

10、管理和维护用户计费系统，协助办理网络费用的收缴工作。

11、每年对本单位计算机网络的.效能进行评价，提出网络结构、网络技术和网络管理的改进措施。

12、认真履行职责，严格遵守网络管理各项规章制度，积极主动配合、协助中心其他岗位的工作

13、完成领导交办的其他工作任务。

信息安全岗位职责 篇 13

职责描述：

1、负责日常信息安全事件处理

2、负责公司突发安全事件的应急响应调度和处理

3、负责应用系统漏洞验证、提交整改建议并验证整改结果

4、负责信息安全监控审计，包括审计发现，核实，处理和出具审计报告

5、改进现有安全事件处理流程，优化公司安全事件管理规范

任职要求：

1、本科及以上学历，对信息安全攻防技术有浓厚的兴趣，年龄 35 岁以下

2、熟悉常见的 Web　漏洞、系统漏洞以及原理

3、熟悉常见安全攻防技术，熟悉渗透测试，能够较熟练使用相关工具

4、熟悉主流操作系统、网络产品、应用系统日志收集和分析

5、有一定编程能力，至少掌握一门程序语言（Java/shell/Python/PHP/Perl 等）；

6、具有较强的`表达能力，能主动沟通、并进行团队协作

7、工作主动性强，自学能力强，能承受一定的工作压力