# 2 部门职责描述

## 2.1 技术部门

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 部门编号 |  | 部门名称 | 技术部门 | 直接上级 | 国资管理处 |
| 部门性质 | 技术 | 部门级别 | 2 | 编制人员 | 4 |
| 下属部门 | 数据库管理部门、网络安全保障部门 | | | | |
| 部门职能 | 一、数据库管理员  （1）规划设计：根据业务需求，制定数据库的逻辑结构和物理结构，设计数据库的存储方案和索引方案等。  （2）建立和管理：负责数据库的安装、配置、调试和管理等工作，保证数据库系统的稳定运行和可靠性。  （3）优化和维护：对数据库进行性能调优和数据维护，包括索引优化、查询优化、空间管理、数据清理等方面的工作。  （4）故障排除：对数据库故障进行及时排查和解决，保证数据库系统的稳定运行。  （5）备份和恢复：制定数据库备份和恢复策略，定期进行备份，并能够在数据丢失或损坏时及时恢复数据。  二、网络安全工程师  （1）制定和实施网络安全策略：对网络进行规划和设计，制定网络安全策略和规范，确保网络的安全性和可靠性。  （2）监控和检测：对网络进行实时监控和检测，及时发现和处理网络安全漏洞和威胁，包括加固防火墙设置、加强网络访问控制、加密传输等工作。  （3）网络安全事件的应急处理和处置：对网络安全事件进行及时响应和处置，采取措施防止事件扩散和损害。  （4）网络安全培训和教育：为项目成员提供网络安全培训和教育，提高员工的安全意识和网络安全知识。  （5）网络安全管理和监督：对项目团队的网络安全进行管理和监督，包括网络安全政策的制定和执行、安全事件的记录和报告等工作。 | | | | |
| 具备条件 | 1. 运作机制高效：技术部门需要建立高效的运作机制，包括项目管理、运维管理、安全管理等，能够保证信息化建设和管理的质量和效率。   2. 专业化人才队伍：打造一支专业化的技术团队，提供系统设计、安全保障等服务，满足不同层次的要求。同时，需要注重人才的培养和引进，以提高整个团队的专业化水平和能力。  3. 先进的技术设备：拥有现代化的信息技术设备，包括计算机、服务器、网络设备、存储设备、软件等，能够满足国资管理平台信息化建设和管理的需求。 | | | | |

# 3 岗位职责描述

## 3.1 数据库管理员

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 职位编号 |  | 职位名称 | | 数据库管理员 | | 所属部门 | 技术部门 |
| 职位类型 | 数据库管理 | 上级职位 | | 国资管理处主任 | | 编制日期 |  |
| 具体工作职责 | | | | | | | |
| 序号 | 工作职责（按重要程度排序） | | | | | 时间比例 | 关键的绩效指标 |
| 1 | 建立和管理 | | | | | 60% | 50% |
| 2 | 规划设计 | | | | | 15% | 20% |
| 3 | 优化和维护 | | | | | 10% | 15% |
| 4 | 故障排除 | | | | | 10% | 10% |
| 5 | 备份和恢复 | | | | | 5% | 5% |
| 内部工作接口 | 交往对象 | | 工作内容 | | | 性质 | 频率（天/周/月/季/年） |
| 经营部门 | | 根据业务需求制定数据库规划和设计方案 | | | 接收项目 | 月/季/年 |
| 提供业务数据支持，包括数据导出和数据分析等 | | | 信息反馈 | 月 |
| 财务部门 | | 提交数据库相关的费用预算申请 | | | 信息反馈 | 季/年 |
| 提供数据库管理相关费用的支出明细，供财务部门核算和报销。 | | | 信息反馈 | 季/年 |
| 提供财务数据支持，包括数据导出和数据分析等 | | | 信息反馈 | 月 |
| 监管部门 | | 提交数据库管理工作记录，保证数据安全、管理合规。 | | | 接受监督 | 季/年 |
| 提供监管数据支持，包括数据导出和数据分析等 | | | 信息反馈 | 月 |
| 资产管理部门 | | 提交数据库管理部门的资产清单，供资产管理部门清点核算 | | | 信息反馈 | 季/年 |
| 提供资产数据支持，包括数据导出和数据分析等 | | | 信息反馈 | 月 |
| 外部工作接口 | 交往对象 | | 工作内容 | | | 性质 | 频率（天/周/月/季/年） |
| 数据库供应商 | | 评估数据库供应商的产品和服务，选取合适的数据库系统 | | | 业务往来 | 周/月/季 |
| 外部技术顾问 | | 寻求专业的数据库技术咨询和支持 | | | 业务往来 | 季/年 |
| 工作条件 | 工作时间 | | 8小时 | | | | |
| 工作场所 | | 办公室 | | | | |
| 使用设备 | | 计算机、数据库服务器、网络设备、硬盘等存储设备、监控摄像头等监控设备及打印机、扫描仪等外设 | | | | |
| 任职资格要求 | | | | | | | |
| 一般条件 | 最佳学历 | | 研究生 | | | 最低学历 | 大学本科 |
| 专业要求 | | 计算机科学与技术、软件工程 | | | | |
| 资格证书 | | 有OCP、MCSE等资格证书优先 | | | | |
| 工作经验  必要知识 | 工作经验 | | 有1-3年相关领域的工作经验经验者优先 | | | | |
| 必要知识 | | 1. 掌握数据库原理和设计，包括数据库系统的架构、数据模型、数据结构等基础知识 2. 熟悉至少一种主流的数据库管理系统，如Oracle、MySQL、SQL Server等。 3. 熟练掌握SQL、T-SQL 等编程语言，以及数据库编程工具和框架。 4. 了解数据库系统的安全原理和技术，能够制定和实施安全策略，防范安全威胁和攻击。 5. 了解团队业务和流程，熟悉数据库在业务中的应用场景和要求。 | | | | |
| 外语要求 | | CET-6 | | | | |
| 计算机要求 | | 数据库管理员应具备较高的计算机职业素养，以保证能够胜任日常工作。包括良好的编程能力、掌握常见算法和数据结构知识、了解计算机操作系统和网络的基本原理和实现方式等。 | | | | |
| 相关资料的收集和整理 | 1.收集和整理平台的系统架构图，包括主要的硬件设备、网络拓扑结构、软件框架等信息。  2.收集和整理数据库的设计和规划文档，包括数据库模型、表结构、索引等信息，以及数据库的容量规划、备份和恢复策略等。  3.收集和整理数据库的管理运维文档，包括数据库的安装、配置、监控、优化等方面的技术文档。  4.收集和整理数据备份与恢复的文档，包括备份策略、备份工具、备份周期、备份验证等信息。  5.收集和整理相关技术标准和规范，如SQL标准、数据库编码规范、安全标准等。 | | | | | | |
| 任职者签名：  日 期： | | | | | 直接上级签名：  日 期： | | |

## 3.2 网络安全工程师

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 职位编号 |  | 职位名称 | | 网络安全工程师 | | 所属部门 | 技术部门 |
| 职位类型 | 网络安全管理 | 上级职位 | | 国资管理处主任 | | 编制日期 |  |
| 具体工作职责 | | | | | | | |
| 序号 | 工作职责（按重要程度排序） | | | | | 时间比例 | 关键的绩效指标 |
| 1 | 监控和检测 | | | | | 30% | 35% |
| 2 | 制定和实施网络安全策略 | | | | | 25% | 25% |
| 3 | 网络安全事件应急处理和处置 | | | | | 20% | 25% |
| 4 | 网络安全管理和监督 | | | | | 15% | 10% |
| 5 | 网络安全培训和教育 | | | | | 10% | 5% |
| 内部工作接口 | 交往对象 | | 工作内容 | | | 性质 | 频率（天/周/月/季/年） |
| 财务部门 | | 提交网络安全方面的采购需求和预算申请 | | | 信息反馈 | 季/年 |
| 获取有关财务数据，如公司的财务预算、成本和支出情况等，以便更好地制定网络安全策略和规划 | | | 信息反馈 | 季/年 |
| 提供安全支持，确保经营部门的业务和数据得到充分的保护 | | | 技术支持 | 天 |
| 监管部门 | | 协作制定团队内部网络安全标准 | | | 合作 | 年 |
| 提供网络安全报告，以便监督企业的网络安全情况。 | | | 信息反馈 | 月 |
| 协助监管部门进行网络安全检查 | | | 协助 | 季/年 |
| 提供安全支持，确保监管部门的业务和数据得到充分的保护 | | | 技术支持 | 天 |
| 经营部门 | | 根据业务需求制定数据库规划和设计方案 | | | 接收项目 | 月/季/年 |
| 提供安全支持，确保经营部门的业务和数据得到充分的保护 | | | 技术支持 | 天 |
|  | 资产管理部门 | | 提交网络安全保障部门的资产清单，供资产管理部门清点核算 | | | 信息反馈 | 季/年 |
| 提供安全支持，确保资产管理部门的业务和数据得到充分的保护 | | | 技术支持 | 天 |
| 外部工作接口 | 交往对象 | | 工作内容 | | | 性质 | 频率（天/周/月/季/年） |
| IT服务提供商 | | 网络安全审计、漏洞扫描和修复 | | | 业务往来 | 季/年 |
| 外部安全机构 | | 寻求安全咨询和支持 | | | 业务往来 | 季/年 |
| 行业协会 | | 参与网络安全标准制定和修订 | | | 业务往来 | 季/年 |
| 工作条件 | 工作时间 | | 8小时 | | | | |
| 工作场所 | | 办公室 | | | | |
| 使用设备 | | 计算机、网络测试设备、数据加密设备等安全设备、监控摄像头等监控设备、打印机、扫描仪等外设等外设 | | | | |
| 任职资格要求 | | | | | | | |
| 一般条件 | 最佳学历 | | 研究生 | | | 最低学历 | 大学本科 |
| 专业要求 | | 网络空间安全、信息安全、计算机科学与技术 | | | | |
| 资格证书 | | 有CISSP、CISM、OSCP等资格证书优先 | | | | |
| 工作经验  必要知识 | 工作经验 | | 有1-3年相关领域的工作经验经验者优先 | | | | |
| 必要知识 | | 1. 掌握计算机网络原理和架构，包括计算机网络的基本原理，包括网络拓扑、网络协议、网络安全等方面的知识。 2. 熟悉各种网络安全技术和工具，如防火墙、入侵检测系统、漏洞扫描器、加密技术等 3. 了解社交工程和恶意软件的攻击手段和防范方法，能够制定有效的防范措施。 4. 熟悉渗透测试和漏洞修复的基本流程和方法，能够针对网络安全漏洞进行分析和修复。 5. 熟悉安全管理和合规要求，如ISO 27001、GDPR等，能够制定企业安全策略和合规措施。 | | | | |
| 外语要求 | | CET-6 | | | | |
| 计算机要求 | | 网络安全工程师应具备较高的计算机职业素养，以保证能够胜任日常工作。包括良好的编程能力、掌握常见算法和数据结构知识、了解计算机操作系统和网络的基本原理和实现方式等。 | | | | |
| 相关资料的收集和整理 | 1. 制定和整理企业安全策略和规范，包括安全管理流程、安全控制措施、合规要求等，以便有效执行和监督。 2. 准确绘制网络拓扑图和制定资产清单，包括网络设备、服务器、应用程序等，以便进行安全管理和监控。 3. 定期进行漏洞扫描和测试，并整理相关报告，以便及时修复和弥补安全漏洞。 4. 记录和整理安全事件的响应和处理记录，包括事件发生时间、影响范围、处理措施、修复结果等，以便进行安全事件分析和总结 5. 整理安全培训相关资料，包括安全知识、安全行为规范、安全警示、应急处理等，以便进行安全教育和培训。 | | | | | | |
| 任职者签名：  日 期： | | | | | 直接上级签名：  日 期： | | |