**(单位)**

**系统**

**等级保护三级测评**

**现场检测表**

测试对象范围：安全管理

测试对象名称：安全管理机构

配合人员签字：

测试人员签字：

核实人员签字：

测试日期：

**结果统计:**

|  |  |  |
| --- | --- | --- |
|  | 测评项 | 测评结果 |
|  | 岗位设置 | □符合 □部分符合 □不符合 |
|  | 人员配备 | □符合 □部分符合 □不符合 |
|  | 授权和审批 | □符合 □部分符合 □不符合 |
|  | 沟通和合作 | □符合 □部分符合 □不符合 |
|  | 审核和检查 | □符合 □部分符合 □不符合 |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（三级）** |
| **测试对象** | **安全管理** |
| **测 试 类** | 安全管理机构 |
| **测 试 项** | 岗位设置 |
| **测试要求：**   1. 应设立信息安全管理工作的职能部门，设立安全主管人、安全管理各个方面的负责人，定义各负责人的职责； 2. 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责； 3. 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权； 4. 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。 | |
| **测试记录：**   1. 是否设立指导和管理信息安全工作的委员会或领导小组？   否 □  是 □ 〇 最高领导是否由单位主管领导委任或授权的人员担任？  否 □ 是 □   1. 是否设立专职的安全管理机构（即信息安全管理工作的职能部门）？   否 □  是 □ 〇 机构内部门设置情况如何？  〇 是否明确各部门职责分工?  否 □ 是 □   1. 是否设立安全管理各个方面的负责人，设置了哪些工作岗位?   〇安全主管 □ 〇安全管理各个方面的负责人 □  〇机房管理员 □ 〇系统管理员 □  〇网络管理员 □ 〇安全员 □  是否明确各个岗位的职责分工?  否 □ 是 □   1. 访谈安全主管、安全管理某方面的负责人、信息安全管理委员会或领导小组日常管理工作的负责人、系统管理员、网络管理员和安全员，询问其岗位职责的内容，表述是否与文件描述一致：   否 □ 是 □   1. 检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责？   否 □  是 □ 〇是否明确机构内各部门的职责和分工？  否 □ 是 □  〇部门职责是否涵盖物理、网络和系统等各个方面？  否 □ 是 □  〇是否明确设置安全主管、安全管理各个方面的负责人、机房管理员、系  统管理员、网络管理员、安全员等各个岗位？  否 □ 是 □  〇各个岗位的职责范围是否清晰、明确？  否 □ 是 □  〇文件是否明确各个岗位人员应具有的技能要求？  否 □ 是 □   1. 检查信息安全管理委员会或领导小组是否具有单位主管领导对其最高领导的委任授权书？   否 □ 是 □   1. 检查信息安全管理委员会职责文件，查看是否明确描述委员会的职责和其最高领导岗位的职责？   否 □ 是 □   1. 安全管理各部门和信息安全管理委员会或领导小组是否具有日常管理工作执行情况的文件或工作记录（如会议记录/纪要和信息安全工作决策文档等）？   否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**  测试记录4被访谈人员表述与文件描述一致，则该项为肯定；  测试记录1-8项全部符合即视为符合； | |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（三级）** |
| **测试对象** | **安全管理** |
| **测 试 类** | 安全管理机构 |
| **测 试 项** | 人员配备 |
| **测试要求：**   1. 应配备一定数量的系统管理人员、网络管理人员、安全管理人员等； 2. 应配备专职安全管理人员不可兼任； 3. 关键岗位应定期轮岗。 | |
| **测试记录：**   1. 机房管理员： 〇 数量 〇 专职□ 兼职□   系统管理员： 〇 数量 〇 专职□ 兼职□  数据库管理员 〇 数量 〇 专职□ 兼职□  网络管理员 〇 数量 〇 专职□ 兼职□  安全员 〇 数量 〇 专职□ 兼职□   1. 实行定期轮岗的关键岗位有： ；   轮岗情况如何： ：  轮岗周期多长： ；  轮岗手续如何：   1. 安全管理人员是否包括：   机房管理员 □ 系统管理员 □ 数据库管理员 □  网络管理员 □ 安全员 □  是否明确配备专职的安全员？  否 □ 是 □  哪些关键岗位（应有列表）实行定期轮岗：  轮岗周期：   1. 是否明确机房管理员、系统管理员、数据库管理员、网络管理员、安全员等重要岗位人员的信息？   否 □  是 □ 〇安全员是否是专职人员。  否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**  如果测试记录1设置的安全员是专职的，则该项为肯定；  测试记录1-4项全部符合即视为符合。 | |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（三级）** |
| **测试对象** | **安全管理** |
| **测 试 类** | 安全管理机构 |
| **测 试 项** | 授权和审批 |
| 测试要求：   1. 应授权审批部门及批准人，对关键活动进行审批； 2. 应列表说明须审批的事项、审批部门和可批准人； 3. 应建立各审批事项的审批程序，按照审批程序执行审批过程； 4. 应建立关键活动的双重审批制度； 5. 不再适用的权限应及时取消授权； 6. 应定期审查、更新需授权和审批的项目； 7. 应记录授权过程并保存授权文档。 | |
| **测试记录：**   1. 是否规定对信息系统中的关键活动进行审批？   否 □  是 □ 〇 审批部门是何部门？  〇 批准人是何人  〇 他们的审批活动是否得到授权？  否 □  是 □  〇 是否定期审查、更新审批项目？  否 □  是 □ 〇 审查周期多长？   1. 对关键活动的审批范围包括哪些？   〇网络系统 □ 〇应用系统 □ 〇数据库管理系统 □  〇重要服务器和设备等重要资源的访问 □  〇重要管理制度的制定和发布 □  〇人员的配备、培训 □ 〇产品的采购 □  〇第三方人员的访问、管理 □ 〇与合作单位的合作项目 □  〇其他  审批程序如何：   1. 授权管理文件是否包含需审批事项列表？（如列表说明哪些事项应经过信息安全领导小组审批，哪些事项应经过安全管理机构审批，哪些关键活动应经过哪些部门双重审批等）   否 □  是 □ 〇列表是否明确：  审批事项和双重审批事项 □  审批部门 □ 批准人及审批程序 □  〇文件是否说明应定期审查、更新需审批的项目和审查周期等：  否 □ 是 □   1. 经双重审批的文档是否具有双重批准人的签字和审批部门的盖章？   否 □ 是 □   1. 检查关键活动的审批过程记录，关键活动的审批过程记录的审批程序与文件要求是否一致？   否 □ 是 □   1. 检查是否具有对不再适用的权限及时取消授权的记录   否 □ 是 □   1. 检查审查记录，审查记录日期是否与审查周期一致？   否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**  测试记录1-7项全部符合即视为符合 | |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（三级）** |
| **测试对象** | **安全管理** |
| **测 试 类** | 安全管理机构 |
| **测 试 项** | 沟通和合作 |
| 测试要求：   1. 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题； 2. 信息安全职能部门应定期或不定期召集相关部门和人员召开安全工作会议，协调安全工作的实施； 3. 信息安全领导小组或者安全管理委员会定期召开例会，对信息安全工作进行指导、决策； 4. 应加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持； 5. 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，获取信息安全的最新发展动态，当发生紧急事件的时候能够及时得到支持和帮助； 6. 应文件说明外联单位、合作内容和联系方式； 7. 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。 | |
| **测试记录：**   1. 是否建立与外单位（公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司、安全组织等），与组织机构内其它部门之间及内部各部门管理人员之间的沟通、合作机制?   否 □  是 □ 〇与外单位和其他部门有哪些合作内容  〇沟通、合作方式   1. 是否召开过部门间协调会议，组织其它部门人员共同协助处理信息系统安全有关问题?   否 □ 是 □  安全管理机构内部是否召开过安全工作会议部署安全工作的实施?  否 □  是 □ 〇 参加会议的部门和人员有 ，  〇 会议结果 ；  〇 信息安全领导小组或者安全管理委员会是否定期召开例会?  否 □ 是 □   1. 是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等?   否 □ 是 □   1. 与外单位人员，与组织机构内其他部门人员，内部各部门管理人员之间的沟通方式有：     主要沟通内容有：   1. 部门间协调会议文件或会议记录是否有会议内容、会议时间、参加人员和结果等的描述?   否 □ 是 □   1. 安全工作会议文件或会议记录是否有会议内容、会议时间、参加人员和会议结果等的描述?   否 □ 是 □   1. 信息安全领导小组或者安全管理委员会定期例会会议文件或会议记录是否有会议内容、会议时间、参加人员、会议结果等的描述?   否 □ 是 □   1. 外联单位是否包含公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司、安全组织等?   否 □  是 □ 〇 是否说明外联单位的联系人和联系方式等内容?  否 □ 是 □   1. 是否具有安全顾问名单或者聘请安全顾问的证明文件?   否 □  是 □ 〇 由安全顾问指导信息安全建设、参与安全规划和安全评审的相关文档或记录是否具有由安全顾问签字的相关建议?  否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**  测试记录1-9项全部符合即视为符合 | |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（三级）** |
| **测试对象** | **安全管理** |
| **测 试 类** | 安全管理机构 |
| **测 试 项** | 审核与检查 |
| 测试要求：   1. 应由安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统测试情况等； 2. 应由安全管理部门组织相关人员定期进行全面检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； 3. 应由安全管理部门组织相关人员定期分析、评审异常行为的测试记录，发现可疑行为,形成测试分析报告，并采取必要的应对措施； 4. 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报； 5. 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。 | |
| **测试记录：**   1. 是否组织人员定期对信息系统进行安全检查？   否 □  是 □ 〇检查周期多长？  〇是否定期分析、评审异常行为的测试记录？  否 □ 是 □   1. 安全检查包含哪些内容？   〇检查人员有哪些？  〇检查程序是否按照系统相关策略和要求进行？  否 □ 是 □  〇是否制定安全检查表格实施安全检查？  否 □ 是 □  〇检查结果如何？  〇是否对检查结果进行通报？  否 □  是 □ 〇通报形式、范围如何？   1. 安全检查制度文档是否规定检查内容、检查程序和检查周期等？   否 □  是 □ 〇检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等？  否 □ 是 □  〇是否包括用户账号情况、系统漏洞情况、系统测试情况等？  否 □ 是 □   1. 安全检查报告日期与检查周期是否一致？   否 □  是 □ 〇报告中是否有检查内容、检查人员、检查数据汇总表、检查结果等的描述？  否 □ 是 □   1. 检查安全检查过程记录，安全检查过程记录的检查程序与文件要求是否一致？   否 □ 是 □   1. 检查测试分析报告，查看测试分析报告报告日期与检查周期是否一致？   否 □  是 □ 〇报告中是否有分析人员、异常问题和分析结果等的描述？  否 □ 是 □  〇是否对发现的问题提出相应的措施？  否 □ 是 □   1. 是否具有安全检查表格?   否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**  测试记录1-7项全部符合即视为符合 | |