**(单位)**

**系统**

**等级保护二级测评**

**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:**

|  |  |  |
| --- | --- | --- |
| 序号 | 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（二级）** |
| **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. 访谈安全主管，询问是否设立安全管理机构（即信息安全管理工作的职能部门，可以由其它部门兼职）？   否 □  是 □ 〇机构内部门设置情况如何：    〇是否明确机构内各部门的职责分工？  否 □ 是 □   1. 访谈安全主管，询问是否设立安全管理各个方面的负责人？   否 □  是 □ 〇设置了哪些工作岗位（如安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员和安全员等重要岗位）：    〇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，询问其岗位职责包括哪些内容?      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 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**   1. 如果3被访谈人员表述与文件描述一致，则该项为肯定； 2. 1-4均为肯定，则信息系统符合本单元测评项要求。 | |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（二级）** |
| **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. 安全管理人员不能兼任网络管理员、系统管理员、数据库管理员等； | |
| **测试记录：**   1. 访谈安全主管，询问   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. 检查人员配备要求的相关文档，查看是否明确应配备哪些安全管理人员，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、安全员等重要岗位人员：   否 □ 是 □   1. 检查管理人员名单，查看其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 □  确认安全员是否没有兼任网络管理员、系统管理员、数据库管理员等？  否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**   1. 如果1设置的安全员没有兼任网络管理员、系统管理员、数据库管理员等，则该项为肯定； 2. 1-3均为肯定，则信息系统符合本单元测评项要求。 | |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（二级）** |
| **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； | |
| **测试记录：**   1. 访谈安全主管，询问其是否对信息系统中的关键活动进行审批:   否 □  是 □ 审批部门是何部门:  批准人是何人:  他们的审批活动是否得到授权:  否 □ 是 □   1. 访谈关键活动的批准人，询问其对关键活动的审批范围包括哪些（如网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问，重要管理制度的制定和发布，人员的配备、培训和产品的采购等）:     审批程序如何:   1. 检查审批事项列表，查看列表是否明确须审批事项、审批部门、批准人及审批程序等:   否 □ 是 □   1. 检查经审批的文档，查看是否具有批准人的签字和审批部门的盖章。   否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**  测试记录1-4项全部符合即视为符合 | |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（二级）** |
| **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. 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 | |
| **测试记录：**   1. 访谈安全主管，询问是否经常与公安机关、电信公司和兄弟单位联系:   否 □  是 □ ○联系方式有哪些:  ○与组织机构内其他部门之间有哪些合作内容:  ○沟通、合作方式有哪些:   1. 访谈安全主管，询问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 □ ○参加会议的部门和人员有哪些:  ○会议结果如何:   1. 访谈安全管理人员（从系统管理员和安全员等人员中抽查），询问其与外单位人员，与组织机构内其他部门人员，与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. 检查部门间协调会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述：   否 □ 是 □   1. 检查安全工作会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述：   否 □ 是 □   1. 检查外联单位说明文档，查看外联单位是否包含公安机关、电信公司及兄弟公司：   否 □ 是 □  是否说明外联单位的联系人和联系方式等内容：  否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**  测试记录1-6项全部符合即视为符合 | |

|  |  |
| --- | --- |
| **测试类别** | **等级测评（二级）** |
| **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、系统审计情况等； | |
| **测试记录：**   1. 访谈安全主管，询问是否组织人员定期对信息系统进行安全检查：   否 □  是 □ ○ 检查周期多长：  ○是否明确检查内容：   1. 访谈安全员，询问安全检查包含哪些内容：     检查人员有哪些：  检查程序是否按照系统相关策略和要求进行：  否 □ 是 □  检查结果如何：   1. 检查安全检查记录，查看记录时间与检查周期是否一致：   否 □ 是 □  文档中是否有检查内容、检查人员、检查结果等的描述：  否 □ 是 □ | |
| **测试结果：** □符合 □部分符合 □不符合 | |
| **备注：**  测试记录1-3项全部符合即视为符合 | |