**信息系统安全检查表**

编号：HJRD-2-D-05

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **信息系统安全检查表** | | | | |
| **序号** | **安全域** | **子域** | **要求** | **备注** |
| 1 | 安全制度落实情况 | 安全管理制度 | 1. 是否建立了相应信息安全策略：□有 □无 ，策略中是否包括信息安全的总体目标、范围、原则和总体安全框架等。□有 □无 2. 已制订机房管理制度：□有 □无，是否正式印发：□是 □否 3. 已制订网络管理制度：□有 □无，是否正式印发：□是 □否 4. 已制订应用系统管理制度：□有 □无，是否正式印发：□是□否 5. 已制订变更管理制度：□有 □无，是否正式印发：□是 □否 6. 已制订运维管理制度：□有 □无，是否正式印发：□是 □否 7. 已制订设备管理制度：□有 □无，是否正式印发：□是 □否 已正式印发的信息安全管理制度有 份。 |  |
| 安全管理机构 | 1. 是否设置了专门的职能部门对信息安全进行管理：□是 □否 2. 是否设置了相应的职责岗位：□是 □否，每个岗位的责任人是否明确：□是 □否 3. 是否配备了相应的系统管理人员、网络管理人员、安全管理人员：□是 □否 4. 安全管理人员是否同时兼任网络管理员、系统管理员、数据库管理员等□是 □否 |  |
| 人员安全管理 | ①已制订重要岗位信息安全和保密责任制度：□ 是 □ 否 ②已制订人员离岗离职时信息安全管理规定：□ 是 □ 否 ③是否定期对所有人员进行安全技能及安全知识考核：□ 是 □ 否，是否对重点、敏感岗位的人员进行全面严格的安全审查：□ 是 □ 否 |  |
| 保密管理 | ①是否与从事关键岗位的人员签署保密协议，保密协议内容包括保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容。□ 是 □ 否 |  |
| 密码管理 | ①是否建立了密码使用管理制度，并使用符合国家密码管理规定的密码技术和产品；□ 是 □ 否 |  |
| 等级保护 | 1. 是否指定专门的部门或人员负责管理系统定级的相关材料 □ 是 □ 否 ； 2. 是否将系统等级及相关材料报系统主管部门备案□ 是 □ 否； 3. 是否将系统等级及其他要求的备案材料报相应公安机关备案□ 是 □ 否 ； 4. 是否选择具有国家相关技术资质和安全资质的测评单位进行等级测评□ 是 □ 否； 5. 是否指定或授权专门的部门或人员负责等级测评的管理□ 是 □ 否； 6. 是否至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改□ 是 □ 否 ； 7. 是否在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改□ 是 □ 否 。 8. 是否采用等级保护管理工具对等级保护的工作进行常态化管理□ 是 □ 否。 |  |
| 2 | 安全防范措施 | 身份认证 | ①安装了身份认证系统：□ 有 □ 无 设备厂家和型号：\_\_\_\_\_\_ |  |
| 访问控制 | ①安装了访问控制设备：□ 有 □ 无 设备厂家和型号：\_\_\_\_\_\_ |  |
| 数据加密 | ①安装了数据加密系统：□ 有 □ 无 设备厂家和型号：\_\_\_\_\_\_ |  |
| 安全审计 | ①安装了网络审计系统，能对所有应用系统的使用情况进行记录：□ 全部安装 □ 部分安装 □ 没有 |  |
| 防篡改 | ①安装了网站防篡改系统：□ 有 □ 无 设备厂家和型号： \_\_\_\_\_\_  网站IP地址和名称： \_\_\_\_\_\_ |  |
| 防病毒 | ①安装了数据加密系统：□ 有 □ 无 设备厂家和型号：\_\_\_\_\_\_ |  |
| 防攻击 | ①安装了防攻击设备：□ 有 □ 无 设备厂家和型号：\_\_\_\_\_\_ |  |
| 防瘫痪 | ①是否做了防瘫痪防护措施：□ 有 □ 无 具体措施：\_\_\_\_\_\_ |  |
| 防泄密 | ①是否做了防泄密防护措施：□ 有 □ 无 具体措施：\_\_\_\_\_\_ |  |
| 计算机 | ①是否采取技术措施进行计算机管理： □ 是 □ 否具体措施：\_\_\_\_\_\_ |  |
| 移动存储设备 | ①是否采取技术措施进行移动存储介质管理： □ 是 □ 否 具体措施：\_\_\_\_\_\_ |  |
| 电子文档 | ①是否采取技术措施进行电子文档管理： □ 是 □ 否 具体措施：\_\_\_\_\_\_ |  |
| 3 | 应急响应机制 | 应急预案的制定 | 1. 信息安全应急预案：□有 □无，是否正式印发：□是 □否； 2. 应急预案是否包括了所有的应用系统和网络：□是 □否； 3. 应急预案框架下是否制定了不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容：□是 □否 |  |
| 应急预案的演练 | 1. 年度应急演练情况：□ 已开展 □ 未开展； 2. 是否定期进行应急演练：□ 是 □ 否，演练的内容和演练方式请在自查报告中描述。 |  |
| 应急队伍 | ①应急技术支持队伍：□内部 □外部 □内外联合 □无 |  |
| 数据备份 | ①是否有完整的信息系统（网络、主机操作系统、应用系统、数据库系统）备份方案：□ 是 □ 否 ②在网络关键环节（核心交换机、路由器）出现故障，是否需采用人工干预方式导换至备份设备：□ 是 □ 否 ③是否建立异地备份系统：□ 是 □ 否，异地备份系统的功能：□ 数据级 □ 应用级 ④重要数据备份介质是否在同一安全区域存放：□ 是 □ 否 ⑤是否有检查备份措施有效性和数据完整性的专用测试环境： □ 是 □ 否 |  |
| 4 | 安全隐患排查及整改 | 漏洞扫描 | 1. 是否定期对信息系统、主机系统、网络系统进行漏洞扫描：□定期扫描，每周一次 □定期扫描，每月一次 □定期扫描，每季度一次 □未进行定期扫描 2. 是否对扫描过程中发现的问题进行过整改和修复： □ 全部整改 □未整改 □部分整改 |  |
| 渗透测试 | 1. 是否定期对业务系统（如网站系统、数据库系统）进行的渗透测试，测试周期为：□ 一季度 □一个月 □一年 □未测试 2. 是否对渗透测试结果中发现的问题进行过整改和修复： □ 全部整改 □未整改 □部分整改 |  |
| 安全巡检 | ①系统管理员、数据库管理员、网络管理员是否定期对系统配置、数据库配置、网络设备配置等方面进行安全巡检：□定期巡检，每周一次 □定期巡检，每月一次 □定期巡检，每季度一次 □未进行定期巡检 ②是否对巡检过程中发现的问题进行过整改和修复： □ 全部整改 □未整改 □部分整改 |  |
| 风险评估 | 1. 是否定期对信息系统进行风险评估：□定期评估，季度一次 □定期评估，每半年一次 □定期评估，每年一次 □未进行过风险评估 2. 是否对风险评估过程中，存在的风险进行整改和加固：□ 全部整改 □未整改 □部分整改 |  |