**7 安全与合规性分析**

**密码应用合规性对照表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **指标要求** | **密码技术应用点** | **GB/T 39786密码应用基本要求** | **适用情况（适用/不适用）** | **采取的密码保障措施** | **说明**  **（如采取的缓解及替代性措施）** | **自评结果（通过/不通过）** |
| 物理和环境安全 | 身份鉴别 | 宜 | 适用 |  |  | 通过 |
| 电子门禁记录数据存储完整性 | 宜 | 适用 |  |  | 通过 |
| 视频监控记录数据存储完整性 | 宜 | 适用 |  |  | 通过 |
| 网络和通信安全 | 身份鉴别 | 应 | 适用 |  |  | 通过 |
| 通信数据完整性 | 宜 | 适用 |  |  | 通过 |
| 敏感信息或通信报文的机密性 | 应 | 适用 |  |  | 通过 |
| 网络边界访问控制信息的完整性 | 宜 | 适用 |  |  | 通过 |
| 安全接入认证 | 可 | 不适用 |  |  | 通过 |
| 设备和计算安全 | 身份鉴别 | 应 | 适用 |  |  | 通过 |
| 安全的信息传输通道 | 应 | 适用 |  |  | 通过 |
| 系统资源访问控制信息完整性 | 宜 | 适用 |  |  | 通过 |
| 重要信息资源安全标记完整性 | 宜 | 不适用 |  |  | 通过 |
| 日志记录完整性 | 宜 | 适用 |  |  | 通过 |
| 重要可执行程序完整性、重要可执行程序来源真实性 | 宜 | 适用 |  |  | 通过 |
| 应用和数据安全 | 身份鉴别 | 应 | 适用 |  |  | 通过 |
| 访问控制信息完整性 | 宜 | 适用 |  |  | 通过 |
| 重要信息资源安全标记完整性 | 宜 | 不适用 |  |  | 通过 |
| 重要数据传输机密性 | 应 | 适用 |  |  | 通过 |
| 重要数据存储机密性 | 应 | 适用 |  |  | 通过 |
| 重要数据传输完整性 | 宜 | 适用 |  |  | 通过 |
| 重要数据存储完整性 | 宜 | 适用 |  |  | 通过 |
| 不可否认性 | 宜 | 不适用 |  |  | 通过 |
| 管理制度 | 具备密码应用安全管理制度 | 应 | 适用 | 建立密码应用安全管理制度 | 无 | 通过 |
| 密钥管理规则 | 应 | 适用 | 建立密钥管理规则 | 无 | 通过 |
| 建立操作规程 | 应 | 适用 | 建立密码操作规程 | 无 | 通过 |
| 定期修订安全管理制度 | 应 | 适用 | 定期修订安全管理制度 | 无 | 通过 |
| 明确管理制度发布流程 | 应 | 适用 | 明确制度发布流程 | 无 | 通过 |
| 制度执行过程记录留存 | 应 | 适用 | 制度执行过程记录留存 | 无 | 通过 |
| 人员管理 | 了解并遵守密码相关法律法规和密码管理制度 | 应 | 适用 | 要求相关人员了解并遵守密码相关法律法规和密码管理制度 | 无 | 通过 |
| 建立密码应用岗位责任制度 | 应 | 适用 | 建立密码应用岗位责任制度 | 无 | 通过 |
| 建立上岗人员培训制度 | 应 | 适用 | 建立上岗人员培训无制度 | 无 | 通过 |
| 定期进行安全岗位人员考核 | 应 | 适用 | 定期进行安全岗位人员培训 | 无 | 通过 |
| 建立关键岗位人员保密制度和调离制度 | 应 | 适用 | 明确制度发布流程 | 无 | 通过 |
| 建设运行 | 制定密码应用方案 | 应 | 适用 | 制定密码应用方案 | 无 | 通过 |
| 制定密钥安全管理策略 | 应 | 适用 | 制定密钥安全管理策略 | 无 | 通过 |
| 制定实施方案 | 应 | 适用 | 制定实施方案 | 无 | 通过 |
| 投入运行前进行密码应用安全性评估 | 应 | 适用 | 投入运行前密码应用安全性评估 | 无 | 通过 |
| 定期开展密码应用安全性评估及攻防对抗演习 | 应 | 适用 | 定期开展密码应用安全性评估及攻防对抗演习 | 无 | 通过 |
| 应急处置 | 应急策略 | 应 | 适用 | 制定应急策略 | 无 | 通过 |
| 事件处置 | 应 | 适用 | 制度事件处置流程 | 无 | 通过 |
| 向有关主管部门上报处置情况 | 应 | 适用 | 向有关主管部门上报处置情况 | 无 | 通过 |