奉贤区教育局对基层单位网络与信息安全考核评价表

**单位名称（盖章）：** **考评学年度：** **学年**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **考核项目** | **考核内容及标准** | **分** **值** | **单位****自评** | **得** **分** |
| **一、体制机制建设****（** **11** **分）** | 1. 成立网络安全与信息化工作小组（ 1 分） ， 党政主要负责人签署《网络安全承诺书》 ，并签字盖章 报信息中心备案（ 1 分）。 | 2 |  |  |
| 2. 制定学年度网络安全与信息化工作计划（ 1 分） ， 党政主要负责人签字盖章报信息中心备案（ 1 分） ，按季度自查推进情况（ 1 分）。 | 3 |  |  |
| 3. 制定机房管理制度（ 1 分）、 终端管理制度（ 1 分）、 业务系统平台管理制度（ 1 分）、 人员（ 网管 员、 第三方运维人员等 ）管理制度（ 1 分）、 应急预案（ 1 分）、 数据管理制度（ 1 分）。 | 6 |  |  |
| **二、技术防护与设施****管理（** **19** **分）** | 1. 核心业务系统配备防火墙、 IDS/IPS 和日志审计等安全设备（ 3 分）； 所有服务器安装防病毒软件并 定期更新（ 2 分）。 | 5 |  |  |
| 2. 定期进行漏洞扫描和系统补丁修复（ 2 分）； 对于通报的漏洞扫描和补丁及时修复（ 3 分）。 | 5 |  |  |
| 3. 机房整洁（ 1 分） ， 配备精密空调（ 1 分）、 专业防静电地板（ 1 分）、 UPS（ 1 分）、 PDU 插排（ 1 分）。 | 5 |  |  |
| 4. 机房配备消防措施 ，例如烟感探测器、 报警系统、 灭火器等（ 2 分）。 | 2 |  |  |
| 5. 机房出入口配备电子门禁或门锁 ， 能对进出人员进行鉴别、 记录（ 2 分）。 | 2 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **三、人员与经费保障****（9** **分）** | 1. 配备专职网络安全人员（ 2 分）,【配备兼职网络安全员（ 1 分） 】， 并持有相关证书（ 1 分）； 参 加上级部门或本单位组织的网络安全培训（ 2 分）。 | 5 |  |  |
| 2. 保障网络安全经费 ，设备更新、 运维等费用纳入本单位预算（ 2 分）； 网络安全相关预算不低于本 单位信息化项目总预算的 5%（ 1 分）。 | 3 |  |  |
| 3. 将网络安全工作纳入绩效考核 ， 落实网络安全岗位津贴（ 1 分）。 | 1 |  |  |
| **四、信息化项目管理****（** **11** **分）** | 1. 与第三方服务单位签订《网络安全责任书》（ 2 分）； 与第三方运维技术人员签订信息保密协议（ 2 分）。 | 4 |  |  |
| 2. 落实《奉贤区教育系统使用单位对第三方服务单位网络与信息安全考核制度》（ 2 分） ，考评表报 信息中心（ 1 分）。 | 3 |  |  |
| 3. 重要系统完成定级、 备案、 测评、 整改（ 2 分） ， 二级系统每 2 年测评（ 1 分） ， 三级系统每年测评 （ 1分）。 | 4 |  |  |
| **五、用户与终端管理****（23** **分）** | 1. 落实网络用户实名制 ，对各类网络接入终端设备认证管理 ，未经认证设备禁止入网。（ 2 分） | 2 |  |  |
| 2. 所有终端安装防病毒软件（ 2 分） ，及时更新病毒库和修复系统补丁（ 2 分） ，对通报的风险设备及 时查杀处理（ 2 分）。 | 6 |  |  |
| 3. 留存网络日志 ≥ 6 个月（含上网行为、 认证信息等）（ 2 分）； 每年更新 IP/Mac 地址与使用人对应表 （ 2分）。 | 4 |  |  |
| 4. 安装正版操作系统和软件（ 2 分） ，建立正版软件资产台账（ 1 分）。 | 3 |  |  |
| 5. 每学期开展网络安全宣传主题活动（ 2 分）； 网络安全培训普通人员≥ 4 学时/年（ 2 分） ， 网络安 全专职人员≥ 8 学时/年（ 2 分）。 | 6 |  |  |
| 6. 非工作时间段关闭非必要网站、 平台、 电子屏、 计算机等（ 2 分）。 | 2 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **六、数据安全管理****（15** **分）** | 1. 建立数据备份机制（ 2 分） ， 重要数据定期全量 / 增量备份（ 2 分）。 | 4 |  |  |
| 2.每学年梳理数据资产（ 2 分） ，制定数据分类分级目录及防护措施（ 2 分）。 | 4 |  |  |
| 3.平台账号密码设置符合强制修改要求（ 1 分） ， 强制 90 天更换（ 1 分） ，加密储存（ 1 分）。 | 3 |  |  |
| 4.数据发布前脱敏审核（ 2 分） ，公示后及时撤回敏感信息（ 2 分）。 | 4 |  |  |
| **七、应急预案与处置****（2** **分）** | 1. 每学年至少开展 1 次应急演练（桌面推演或实战演练）（ 1 分） ，演练报告包含改进措施（ 1 分）。 | 2 |  |  |
| **八、** **电子屏管理****（10** **分）** | 1. 电子屏播控系统、 播控终端放置位置可控（ 1 分） ， 出入口配备电子门禁或门锁 ， 能对进出人员进 行鉴别、 记录（ 1 分）。 | 2 |  |  |
| 2. 播控系统开启必要的防护功能 ， 如设置登录密码、 开启操作日志等（ 2 分）。 | 2 |  |  |
| 3. 电子屏运营责任单位制定的应急处置预案 ， 预案场景需覆盖信息误发或篡改、 设备故障等场景（ 1 分） ，建立应急人员名单 ，包括联系人、 联系方式等内容（ 1 分）。 | 2 |  |  |
| 4. 播控终端安装防病毒软件（ 1 分） ，定期进行病毒库更新（ 1 分）。 | 2 |  |  |
| 5. 大屏粘贴管理二维码（ 1 分） ， 二维码有效并有已填报数据（ 1 分）。 | 2 |  |  |
|  | **合计** | 100 |  |  |

评价结论：

□ 优秀 ( ≥90 分） □ 良好（ 80-89 分） □ 合格（ 60-79 分） □ 不合格（ <60 分）

检查组评价人签字：

日期： 年 月 日