附件3

关键信息基础设施管理单位网络安全工作责任制落实考核指标

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **考核对象： 考核时间： 年 月 日** | | | | | |
| **考核指标** | **考核内容** | **考核项** | | **分值** | **得分** |
| 一、政策法规 | 1.贯彻落实工作 | 1 | □贯彻落实中央和省委、市委的决策部署 | 3 |  |
| 2 | □制定网络安全工作相关规划、落实措施 | 3 |  |
| 3 | □制定落实相关政策的工作方案、实施办法等 | 2 |  |
| 4 | □按时完成上年度网络安全工作总结 | 2 |  |
| 5 | □明确本年度网络安全工作安排、重点任务等 | 2 |  |
| 二、制度建设 | 2.组织机构 | 6 | □明确网络安全工作机构 | 3 |  |
| 7 | □明确网络安全工作机构职责 | 2 |  |
| 8 | □及时报告网络安全工作机构负责人和联系人变动情况 | 3 |  |
| 9 | □将网络安全工作纳入重要议事日程 | 3 |  |
| 10 | □落实网络安全工作经费 | 2 |  |
| 3.网络安全工作报告 | 11 | □按时报送年度网络安全工作报告 | 5 |  |
| 4.表彰奖励 | 12 | □获得上级相关工作得表彰和奖励 | 3 |  |
| 5.人才培养 | 13 | □制定网络安全人才引进、使用和培养相关政策措施 | 3 |  |
| **考核指标** | **考核内容** | **考核项** | | **分值** | **得分** |
| 二、制度建设 | 6.落实网络安全责任制 | 14 | □开展网络安全责任制考核 | 3 |  |
| 15 | □考核结果作为领导班子和有关领导干部综合考核评价重要内容 | 2 |  |
| 16 | □将网络安全建设和绩效纳入审计范围 | 2 |  |
| 7.对网络安全职能部门支持和保障 | 17 | □为网络安全职能部门开展工作提供支持和保障 | 3 |  |
| 三、系统运行 | 8.重大事件 | 18 | □建立本单位网络安全和信息化重大事项报告制度 | 2 |  |
| 19 | □以下事件本单位本年度均未发生  ①网络与信息系统被攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，且没有及时报告和组织处理的；  ②网站受攻击后没有及时组织处置，且瘫痪6小时以上的；  ③国家秘密泄露、大面积个人信息泄露或者大量地理、人口、资源等国家基础数据泄露的；  ④关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；  ⑤其他有严重不良社会影响网络安全事件。 | 6 |  |
| 9.安全保障 | 20 | □及时向行业主管监管部门报送新建、停运关键信息基础设施或关键信息基础设施发生重大变化的情况 | 1 |  |
| 21 | □网络安全关键岗位施行持证上岗，并组织从业人员定期进行岗位技能培训 | 1 |  |
| **考核指标** | **考核内容** | **考核项** | | **分值** | **得分** |
| 三、系统运行 | 9.安全保障 | 22 | □采购网络产品和服务，与提供者明确安全和保密义务与责任 | 1 |  |
| 23 | □信息系统在境内运营中收集或产生的个人信息和重要数据在境内存储 | 1 |  |
| 24 | □自行或委托网络安全服务机构对网络与信息系统的安全性和风险隐患每年至少进行一次检测评估，对发现的问题及时整改，并将有关情况报告行业主管或监管部门 | 3 |  |
| 10.管理制度 | 25 | □制定全面的网络安全管理制度 | 3 |  |
| 26 | □网络安全管理制度执行记录完整 | 2 |  |
| 11.人员安全 | 27 | □与重点岗位人员签订网络安全保密协议 | 1 |  |
| 28 | □外部人员访问重要区域时采取访问控制措施 | 1 |  |
| 12.物理安全 | 29 | □机房安全措施满足相关要求，并明确维护部门和人员 | 2 |  |
| 13.网络安全 | 30 | □网络边界防护具备阻止木马攻击、拒绝服务攻击、网络蠕虫攻击等能力 | 2 |  |
| 31 | □在网络边界部署访问控制设备，启用访问控制功能 | 2 |  |
| 14.系统安全 | 32 | □启用系统访问控制功能，依据安全策略控制用户对资源的访问 | 2 |  |
| 33 | □具备恶意代码防护能力 | 2 |  |
| 15.数据安全 | 34 | □应根据数据的重要性及其对系统的影响，制定备份恢复策略 | 3 |  |
| 16.应用安全 | 35 | □具备用户身份鉴别功能 | 2 |  |
| 36 | □提供应用访问控制功能，依据安全策略控制用户的访问权限 | 2 |  |
| **考核指标** | **考核内容** | **考核项** | | **分值** | **得分** |
| 三、系统运行 | 16.应用安全 | 37 | □有网站信息发布审核机制 | 1 |  |
| 17.运维安全 | 38 | □开展网络安全监测预警 | 2 |  |
| 39 | □定期开展网络安全自查并对发现的问题及时整改 | 1 |  |
| 40 | □有完善的网络、应用、数据备份恢复措施和策略 | 1 |  |
| 四、应急处置 | 18.应急管理 | 41 | □制定网络安全应急预案 | 4 |  |
| 42 | □组织应急演练 | 2 |  |
| 43 | □发生网络安全事件及时按照应急预案进行处置并按要求报告行业主管监管部门或网络安全和信息化部门 | 4 |  |