**网络与信息安全检查表**

| **类别** | **检测项目** | **检查内容** | **检查要求** | **检查记录** | **检查结果** |
| --- | --- | --- | --- | --- | --- |
| **网络安全基础设施建设****网络安全基础设施建设** | 网络架构安全 | 网络结构设计、网络划分 | 网络结构设计、网络划分符合相关要求 |  |  |
| 是否有不经过防火墙的外联链路（包括拨号外联） | 外网与内网的连接链路（包括拨号外联）必须经过防火墙 |  |  |
| 网络拓扑结构图 | 提供当前网络的网络拓扑结构图 |  |  |
| 网络分区管理 | 生产控制大区和管理信息大区之间是否按电监会5号令要求部署了专用隔离装置 |  |  |
| 网络使用的各种硬件设备、软件等 | 各种硬件设备、软件和网络接口是否经过安全检验、鉴定、认证。 | 各种硬件设备、软件和网络接口均经过安全检验、鉴定、认证。 |  |  |
| 广域网建设情况 | 广域网是否按集团规定进行建设、并按规定进行连接 | 广域网按集团规定进行建设、并按规定进行连接 |  |  |
| 网络承建单位情况 | 网络承建单位是否具有相关资质 | 网络承建单位具有相关资质（查看相关资质文件） |  |  |
| 网络内部数据信息 | 网络内部数据信息的产生、使用、存储和维护是否安全、合理等 | 网络内部数据信息的产生、使用、存储和维护安全、合理 |  |  |
| 机房环境安全 | 主机房是否安装了门禁、监控与报警系统 | 主机房安装了门禁、监控与报警系统 |  |  |
| 是否有详细的机房配线图 | 有详细的机房配线图 |  |  |
| 机房供电系统是否将动力、照明用电与计算机系统供电线路分开 | 机房供电系统已将动力、照明用电与计算机系统供电线路分开 |  |  |
| 机房是否配备应急照明装置 | 机房有配备应急照明装置 |  |  |
| 是否定期对UPS的运行状况进行检测 | 定期对UPS的运行状况进行检测（查看半年内检测记录） |  |  |
| 是否安装机房自动灭火系统，是否配备机房专用灭火器，是否定期对灭火装置进行检测 | 安装机房自动灭火系统，配备机房专用灭火器，定期对灭火装置进行检测 |  |  |
| 是否有防雷措施，机房设备接地电阻是否满足要求，接地线是否牢固可靠 | 机房有防雷措施，机房设备接地电阻满足要求，接地线牢固可靠（直流工作接地≤1欧，接地地位差≤1V；交流工作交流工作接地系统接地电阻：＜4Ω、零地电压＜1V；计算机系统安全保护接地电阻及静电接地电阻：＜4Ω) |  |  |
| 机房温度是否控制在摄氏18-25度以内 | 机房温度控制在摄氏18-25度以内 |  |  |
| **安全技术防范措施****安全技术防范措施****安全技术防范措施** | 核心网络设备、系统安全配置 | 交换机、路由器、防火墙等网络设备的安全设置情况；操作系统的安全配置、版本及补丁升级情况 | 交换机、路由器、防火墙等均根据安全要求进行了正确设置；操作系统的安全配置、版本及补丁升级情况。 |  |  |
| 网络设备配置是否进行了备份（电子、物理介质） | 网络设备配置进行了备份（电子、物理介质） |  |  |
| 应用安全配置 | 应用安全配置、身份鉴别策略 | 相关服务进行正确的安全配置、身份鉴别情况 |  |  |
| WWW服务用户账户、口令是否强健 | WWW服务用户账户、口令强健（查看登录） |  |  |
| 信息发布是否进行了分级审核 | 信息发布进行了分级审核（查看审核记录） |  |  |
| 用于业务系统维护的远程拨号访问是否采取了身份验证、访问操作记录等措施。 | 用于业务系统维护的远程拨号访问采取了身份验证、访问操作记录等措施。 |  |  |
| 用户账户的变更、修改、注销是否有记录 | 用户账户的变更、修改、注销有记录（查看半年记录情况） |  |  |
| 关键应用系统管理员账户、用户账户口令是否定期进行了变更 | 关键应用系统管理员账户、用户账户口令定期进行了变更 |  |  |
| 关键区域或设备是否关闭了HTTP、FTP、TFTP等服务 | 关键区域或设备关闭了HTTP、FTP、TFTP等服务 |  |  |
| 是否删除多余默认账号和无关服务 | 删除多余默认账号和无关服务 |  |  |
| 网络与广域网安全隔离 | 逻辑隔离、物理隔离技术是否安全、合理 | 逻辑隔离、物理隔离技术安全、合理 |  |  |
| 网络与二次网安全隔离 | 逻辑隔离、物理隔离技术是否安全、合理 | 逻辑隔离、物理隔离技术安全、合理 |  |  |
| IP管理 | 是否能对本单位全部IP地址进行授权管理，作到接入可控。 | 能对本单位全部IP地址进行授权管理，作到接入可控 |  |  |
| 是否有IP地址分配记录 | 有IP地址分配记录 |  |  |
| 数据备份与恢复 | 是否建立了明确、合理的备份策略；是否严格按照备份策略对系统数据进行备份 | 建立了明确、合理的备份策略；严格按照备份策略对系统数据进行备份（查看备份策略文件、查看备份记录，或查看备份工具配置） |  |  |
| 是否建立了明确的数据恢复预案 | 建立了明确的数据恢复预案（查看文件） |  |  |
| 是否定期进行数据恢复演练 | 定期进行数据恢复演练（查看半年演练记录） |  |  |
| 储存介质是否存放在安全环境 | 储存介质存放在安全的地方 |  |  |
| 是否有严格的介质存取控制，是否有专人对存储介质进行定期检查 | 有严格的介质存取控制，有专人对存储介质进行定期检查 |  |  |
| 补丁管理 | 是否有补丁管理的手段，或管理制度 | 有补丁管理的手段，或管理制度 |  |  |
| 防病毒管理 | 是否有使用通过公安部及有关测评机构认证的防病毒系统 | 有使用通过公安部及有关测评机构认证的防病毒系统 |  |  |
| 是否有对病毒库及时升级，定期对全网进行病毒查杀 | 定期对全网进行病毒查杀，有对病毒库及时升级（最新病毒库） |  |  |
| 所有服务器和客户端是否都安装防病毒软件 | 所有服务器和客户端都安装防病毒软件 |  |  |
| 是否有专责人员负责维护防病毒系统，并及时发布病毒通告 | 有专责人员负责维护防病毒系统，并及时发布病毒通告 |  |  |
| 防火墙管理 | 网络中的防火墙部署位置是否合理 | 网络中的防火墙部署位置合理 |  |  |
| 防火墙墙规则配置是否符合安全要求 | 防火墙墙规则配置符合安全要求 |  |  |
| 防火墙规则配置的建立、更改是否有规范的申请、审核、审批流程 | 防火墙规则配置的建立、更改有规范的申请、审核、审批流程（查看半年内的记录） |  |  |
| 是否对防火墙日志进行了存储、备份 | 对防火墙日志进行了存储、备份 |  |  |
| 入侵检测管理 | 检查入侵检测系统部署是否合理、能否覆盖主要网络边界与主要服务器 | 入侵检测系统部署合理、能覆盖主要网络边界与主要服务器 |  |  |
| 是否定期更新入侵检测的规则与升级 | 定期更新入侵检测的规则与升级 |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **安****全****组****织****管****理** | **检查项目** | **检查内容** | **检查要求** | **检查记录** | **检查结果** |
| 安全组织管理制度 | 1、单位的信息安全组织领导情况及职责划分情况；2、保密制度；3、信息安全教育与培训计划。 | 1、有信息安全管理的组织领导机构，具有明确的职责划分；2、制定保密制度，与相关人员签订保密协议；3、不定期对相关人员进行信息安全知识培训及保密教育。 |  |  |
| 1. 信息安全规章制度；
2. 信息安全应急制度；
3. 网络安全事件记录情况；

信息安全事件管理规程。 | * 1. 制定相关的信息安全规章制度；
	2. 建立信息安全事故和信息安全故障的应急预案；
	3. 对已发生的网络安全事件进行记录；
1. 若发生安全事件则有相应的系统安全分析、软件故障报告的程序、安全事故报告、安全事故处理报告等。
 |  |  |
| 信息安全培训情况 | 信息安全责任人、管理员是否定期参加有关单位的信息安全培训。对本单位全体人员是否进行了信息安全培训（提供培训计划、培训内容、培训成绩、人员） | 信息安全责任人、管理员定期参加有关单位的信息安全培训。对本单位全体人员进行了信息安全培训（提供培训计划、培训内容、培训成绩、人员） |  |  |
| 信息安全通报机制 | 是否按照集团公司、省公司的要求建立了及时的信息安全信息通报机制 | 按照集团公司、省公司的要求建立了及时的信息安全信息通报机制 |  |  |