# 一、附表

## （一）等级保护技术3级技术要求

#### （1）物理安全环境

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 物理位置选择 | a)机房场地应选择在具有防震、防风和防雨等能力的建筑内； | 记录类文档和机房 | 1、应核查所在建筑物是否有建筑抗震设防审批文档； 2、应核查机房是否不存在雨水渗漏； 3、应核查门窗是否不存在因风导致的尘土严重；4、应核查屋顶、墙体、门窗和地面等是否不存在破损开裂。 |
| b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 | 机房 | 应核查机房是否不位于所在建筑的顶层或地下室，如果否，则核查机房是否采取了防水和防潮措施。 |
| 物理访问控制 | 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 | 机房电子门禁系统 | 1、应核查出入口是否配置电子门禁系统； 2、应核查电子门禁系统是否可以鉴别、记录进入的人员信息。 |
| 防盗窃和防破坏 | a)应将设备或主要部件进行固定，并设置明显的不易除去的标识； | 机房设备或主要部件 | 1、应核查机房内设备或主要部件是否固定； 2、应核查机房内设备或主要部件上是否设置了明显且不易除去的标识。 |
| b)应将通信线缆铺设在隐蔽安全处。 | 机房通信线缆 | 应核查机房内通信线缆是否铺设在隐蔽安全处，如桥架中等。 |
| 防雷击 | 应将各类机柜、设施和设备等通过接地系统安全接地。 | 机房 | 应核查机房内机柜、设施和设备等是否进行接地处理。 |
| 防火 | a)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； | 机房防火设施 | 1、应核查机房内是否设置火灾自动消防系统； 2、应核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火。 |
| b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。 | 机房验收类文档 | 应核查机房验收文档是否明确相关建筑材料的耐火性。 |
| 防水和防潮 | a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 机房 | 应核查窗户、屋顶和墙壁是否采取了防雨水渗透的措施。 |
| b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。 | 机房 | 1、应核查机房内是否采取了防止水蒸气结露的措施； 2、应核查机房内是否采取了排泄地下积水，防止地下积水渗透的措施。 |
| 防静电 | 应采用防静电地板或地面并采用必要的接地防静电措施。 | 机房 | 1、应核查机房内是否安装了防静电地板或地面； 2、应核查机房内是否采用了防静电措施。 |
| 温湿度控制 | 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 | 机房温湿度调解设施 | 1、应核查机房内是否配备了专业空调； 2、应核查机房内温湿度是否在设备运行所允许的范围内之内。 |
| 电力供应 | a)应在机房供电线路上配置稳压器和过电压防护设备； | 机房供电设施 | 应核查供电线路上是否配置了稳压器和过电压防护设备。 |
| b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。 | 机房备用供电设施 | 1、应核查是否配备UPS等后备电源系统； 2、应核查UPS等后备电源系统是否满足设备在断电情况下的正常运行要求。 |
| 电磁防护 | 电源线和通信线缆应隔离铺设，避免互相干扰。 | 机房线缆 | 应核查机房内电源线缆和通信线缆是否隔离铺设。 |

#### （2）安全通信网络

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 网络架构 | a)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； | 路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件。 | 1、应核查是否依据重要性、部门等因素划分不同的网络区域； 2、应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。 |
| b)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。 | 网络拓扑 | 1、应核查网络拓扑图是否与实际网络运行环境一致； 2、应核查重要网络区域是否未部署在网络边界处； 3、应核查重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表（ACL）等。 |
| 通信传输 | 应采用校验技术或密码技术保证通信过程中数据的完整性。 | 提供校验技术和密码技术功能的设备或组件 | 1、应核查是否在数据传输过程中使用校验技术或密码技术保证其完整性； 2、应测试验证密码技术设备或组件能否保证通信过程中数据的完整性。 |
| 可信验证 | 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 提供可信验证的设备或组件、提供集中审计功能的系统。 | 1、应核查是否基于可信对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证； 2、应核查是否在应用程序的关键执行环节进行动态可信验证； 3、应测试验证当检测到通信设备的可信性受到破坏后是否进行报警； 4、应测试验证结果是否以审计记录的形式送至安全管理中心。 |

#### （3）安全区域边界

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 边界防护 | 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。 | 网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件 | 1、应核查在网络边界处是否部署访问控制设备； 2、应核查设备配置信息是否指定端口进行跨越边界的网络通信，指定端口是否配置并启用了安全策略； 3、应采用其他技术手段（如非法无线网络设备定位、核查设备配置信息等）核查或测试验证是否不存在其他未受控端口进行跨越边界的网络通信。 |
| 访问控制 | a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | 网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件 | 1、应核查在网络边界或区域之间是否部署访问控制设备并启用访问控制策略； 2、应核查设备的最后一条访问控制策略是否为禁止所有网络通信。 |
| b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件 | 1、应核查是否不存在多余或无效的访问控制策略； 2、应核查不同的访问控制策略之间的逻辑关系及前后排列顺序是否合理。 |
| c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； | 网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件 | 1、应核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数； 2、应测试验证访问控制策略中设定的相关配置参数是否有效。 |
| d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。 | 网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件 | 1、应核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力； 2、应测试验证是否为进出数据流提供明确的允许/拒绝访问的能力。 |
| 入侵防范 | 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。 | 抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击和入侵保护系统或相关组件 | 1、应核查相关系统或组件是否能够检测从外部发起的网络攻击行为； 2、应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本； 3、应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点； 4、应测试验证相关系统或组件的配置信息或安全策略是否有效。 |
| 恶意代码防范 | 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。 | 防病毒网关和UTM等提供防恶意代码功能的系统或相关组件 | 1、应核查在关键网络节点处是否部署防恶意代码产品等技术措施； 2、应核查防恶意代码产品运行是否正常，恶意代码库是否已更新到最新； 3、应测试验证相关系统或组件的安全策略是否有效。 |
| 安全审计 | a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 综合安全审计系统等 | 1、应核查是否部署了综合安全审计系统或类似功能的系统平台； 2、应核查安全审计范围是否覆盖到每个用户； 3、应核查是否对重要的用户行为和重要安全事件进行了审计。 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 综合安全审计系统等 | 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 |
| c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 | 综合安全审计系统等 | 1、应核查是否采取了技术措施对审计记录进行保护； 2、应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。 |
| 可信验证 | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 提供可信验证的设备或组件、提供集中审计功能的系统 | 1、应核查是否基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证； 2、应核查是否在应用程序的关键执行环节进行动态可信验证； 3、应测试验证当检测到边界设备的可信性受到破坏后是否进行报警； 4、应测试验证结果是否以审计记录的形式发送至安全管理中心。 |

#### （4）安全计算环境

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 身份鉴别 | a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应核查用户在登陆时是否采用了身份鉴别措施； 2、应核查用户列表确认用户身份标识是否具有唯一性； 3、应核查用户配置信息或测试验证是否不存在空口令用户； 4、应核查用户鉴别信息是否具有复杂度要求并定期更换。 |
| b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应核查是否配置并启用了登录失败处理功能； 2、应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账号锁定等； 3、应核查是否配置并启用了登录连续超时及自动退出功能。 |
| c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听。 |
| 访问控制 | a)应对登录的用户分配账户和权限； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应核查是否为用户分配了账户和权限及相关设置情况； 2、应核查是否已禁用或限制匿名、默认账户的访问权限。 |
| b)应重命名或删除默认账户，修改默认账户的默认口令； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应核查是否已经重命名默认账户或默认账户已被删除； 2、应核查是否已修改默认账户的默认口令。 |
| c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应； 2、应测试验证多余的、过期的账户是否被删除或停用。 |
| d)应授予管理用户所需的最小权限，实现管理用户的权限分离。 | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应核查是否进行角色划分； 2、应核查管理用户的权限是否已进行分离； 3、应核查管理用户权限是否为其工作任务所需的最小权限。 |
| 安全审计 | a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应核查是否开启了安全审计功能； 2、应核查安全审计范围是否覆盖到每个用户； 3、应核查是否对重要的用户行为和重要安全事件进行审计。 |
| b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 |
| c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应核查是否采取了保护措施对审计记录进行保护； 2、应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。 |
| 入侵防范 | a)应遵循最小安装的原则，仅安装需要的组件和应用程序； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备等 | 1、应核查是否遵循最小安装原则； 2、应核查是否未安装非必要的组件和应用程序。 |
| b)应关闭不需要的系统服务、默认共享和高危端口； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备等 | 1、应核查是否关闭了非必要的系统服务和默认共享； 2、应核查是否不存在非必要的高危端口。 |
| c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备等 | 应核查配置文件或参数是否对终端接入范围进行限制。 |
| d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 业务应用系统、中间件和系统管理软件及系统设计文档等 | 1、应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块； 2、应测试验证是否对人机接口或通信接口输入的内容进行有效性检验。 |
| e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟机网络设备）、安全设备（包括虚拟机安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 1、应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞； 2、应核查是否在经过充分测试评估后及时修补漏洞。 |
| 恶意代码防范 | 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。 | 终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、移动终端、移动终端管系统、移动终端管理客户端和控制设备等 | 1、应核查是否安装了防恶意代码软件或相应功能的软件； 2、应核查是否定期进行升级和更新防恶意代码库。 |
| 可信验证 | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 提供可信验证的设备或组价、提供集中审计功能的系统 | 1、应核查是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证； 2、应测试验证当检测到计算设备的可信性受到破坏后是否进行报警； 3、应测试验证结果是否以审计记录的形式送至安全管理中心。 |
| 数据完整性 | 应采用校验技术保证重要数据在传输过程中的完整性。 | 业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等 | 1、应核查系统设计文档，重要管理数据、重要业务数据在传输过程中是否采用了校验技术或密码技术保证完整性。 |
| 数据备份恢复 | a)应提供重要数据的本地数据备份与恢复功能； | 配置数据和业务数据 | 1、应核查是否安装备份策略进行本地备份； 2、应核查备份策略设置是否合理、配置是否正确； 3、应核查备份结果是否与备份策略一致； 4、应核查近期恢复测试记录是否能够进行正常的数据恢复。 |
| b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。 | 配置数据和业务数据 | 应核查是否提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地。 |
| 剩余信息保护 | 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。 | 终端和服务器等设备中的操作系统、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 | 应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。 |
| 个人信息保护 | a)应仅采集和保存业务必需的用户个人信息； | 业务应用系统和数据库管理系统等 | 1、应核查采集的用户个人信息是否是业务应用必须的； 2、应核查是否制定了相关用户个人信息保护的管理制度和流程。 |
| b)应禁止未授权访问和非法使用用户个人信息。 | 业务应用系统和数据库管理系统等 | 1、应核查是否采用技术措施限制对用户个人信息的访问和使用； 2、应核查是否制定了有关用户个人信息保护的管理制度和流程。 |

#### （5）安全管理中心

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 系统管理 | a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； | 提供集中系统管理功能的系统 | 1、应核查是否对系统管理员进行身份鉴别； 2、应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作； 3、应核查是否对系统管理的操作进行审计。 |
| b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 | 提供集中系统管理功能的系统 | 应核查是否通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 |
| 审计管理 | a)应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； | 综合安全审计系统、数据库审计系统等提供集中审计功能的系统 | 1、应核查是否对审计管理员进行身份鉴别； 2、应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作； 3、应核查是否安全审计操作进行审计。 |
| b)应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 | 综合安全审计系统、数据库审计系统等提供集中审计功能的系统 | 应核查是否通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |

#### （6）安全管理制度

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 安全策略 | 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。 | 总体方针策略类文档 | 应核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略。 |
| 管理制度 | a)应对安全管理活动中的各类管理内容建立安全管理制度； | 安全管理制度类文档 | 应核实各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容。 |
| b)应对管理人员或操作人员执行的日常管理操作建立操作规程。 | 操作规程类文档 | 应核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等。 |
| 制定和发布 | a)应指定或授权专门的部门或人员负责安全管理制度的制定； | 部门/人员职责文件等 | 应核查是否由专门的部门或人员负责制定安全管理制度。 |
| b)安全管理制度应通过正式、有效的方式发布，并进行版本控制。 | 管理制度类文档和记录表单类文档 | 1、应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容； 2、应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等。 |
| 评审和修订 | 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 | 信息/网络安全主管和记录表单类文档 | 1、应访谈信息/网络安全主管是否定期对安全管理制度的合理性和适用性进行审定； 2、应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。 |

#### （7）安全管理机构

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 岗位设置 | a)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； | 信息/网络安全主管、管理制度类文档和记录表单类文档 | 1、应访谈信息/信息网络安全主管是否设立网络安全管理工作的只能部门； 2、应核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责； 3、应核查岗位职责文档是否有岗位划分情况和岗位职责。 |
| b)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 | 信息/网络安全主管、管理制度类文档和记录表单类文档 | 1、应访谈信息/网络安全主管是否进行了安全管理岗位的划分； 2、应核查岗位职责文档是否明确了各部门及岗位职责。 |
| 人员配备 | 应配备一定数量的系统管理员、审计管理员和安全管理员等。 | 信息/网络安全主管、管理制度类文档和记录表单类文档 | 1、应访谈信息/网络安全主管是否配备系统管理员、审计管理员和安全管理员； 2、应核查人员配备文档是否明确各岗位人员配备情况。 |
| 授权和审批 | a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； | 管理制度类文档和记录表单类文档 | 1、应核查部门职责文档是否明确各部门审批事项； 2、应核查岗位职责文档是否明确各岗位审批事项。 |
| b)应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。 | 操作规程类文档和记录表单类文档 | 应核查各类审批记录是否针对系统变更、重要操作、物理访问和系统接入等事项进行审批。 |
| 沟通和合作 | a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； | 信息/网络安全主管、管理制度类文档和记录表单类文档 | 1、应访谈信息/网络安全主管是否建立了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制； 2、应核查会议记录是否明确各类管理员、组织内部机构和网络安全管理部门之间开展了合作与沟通。 |
| b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； | 信息/网络安全主管、管理制度类文档和记录表单类文档 | 1、应访谈信息/网络安全主管是否建立了与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制； 2、应核查会议记录是否与网络安全职能部门、各类供应商、业界专家及安全组织开展了合作与沟通。 |
| c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 | 记录表单类文档 | 应核查外联单位联系列表是否记录了外联单位名称、合作内容、联系人和联系方式等信息。 |
| 审核和检查 | 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 | 信息/网络安全主管、管理制度类文档和记录表单类文档 | 1、应访谈信息/网络安全主管是否定期进行了常规安全检查； 2、应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。 |

#### （8）安全管理人员

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 人员录用 | a)应指定或授权专门的部门或人员负责人员录用； | 信息/网络安全主管 | 应访谈信息/网络安全主管是否由专门的部门或人员负责人员的录用工作。 |
| b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。 | 管理制度类文档和记录表单类文档 | 1、应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）； 2、应核查是否具有人员录用时对录用人身份、安全背景、专业资格或资质等进行审查的相关文档或记录，是否记录审查内容和审查结果等）； 3、应核查人员录用时的能考核文档或记录是否记录考核内容和考核结果等。 |
| 人员离岗 | 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。 | 记录表单类文档 | 应核查是否具有离职人员终止其访问权限、交还身份证件、软硬件设备等的登录记录。 |
| 安全意识教育和培训 | 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。 | 管理制度类文档 | 1、应核查安全意识教育及岗位技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容； 2、应核查安全责任和惩戒措施管理文档或培训文档是否包含具体的安全职责和惩戒措施。 |
| 外部人员访问管理 | a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； | 管理制度类文档和记录表单类文档 | 1、应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等； 2、应核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等； 3、应核查外部人员访问重要区域的登录记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等； |
| b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； | 管理制度类文档和记录表单类文档 | 1、应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程； 2、应核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限、是否具有允许访问的批准签字等； 3、应核查外部人员访问系统的登录记录是否记录了外部人员访问的权限、时限、账户等。 |
| c)外部人员离场后应及时清除其所有的访问权限。 | 管理制度类文档和记录表单类文档 | 1、应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限； 2、应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。 |

#### （9）安全建设管理

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 定级和备案 | a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； | 记录表单类文档 | 应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由。 |
| b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； | 记录表单类文档 | 应核查定级结果的论证评审会议记录是否有相关部门和相关安全技术专家对定级结果的论证意见。 |
| c)应保证定级结果经过相关部门的批准； | 记录表单类文档 | 应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见。 |
| d)应将备案材料报主管部门和相应公安机关备案。 | 记录表单类文档 | 应核查是否具有公安机关出具的备案证明文档。 |
| 安全方案设计 | a)应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； | 安全规划设计类文档 | 应核查安全设计文档是否根据安全保护等级选择安全措施，是否跟安全需求调整安全措施。 |
| b)应根据保护对象的安全保护等级进行安全方案设计； | 安全规划设计类文档 | 应核查安全设计方案是否有根据安全保护等级进行设计规划。 |
| c)应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。 | 记录表单类文档 | 应核查配套文件的论证评审记录或文档是否有相关部门和相关安全技术专家对总体安全规划、安全设计方案等相关配套文件的批准意见和论证意见。 |
| 产品采购和使用 | a)应确保网络安全产品采购和使用符合国家的有关规定； | 记录表单类文档 | 应核查有关网络安全产品是否符合国家的相关规定，如网络安全产品获得了销售许可等。 |
| b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。 | 建设负责人和记录表单类文档 | 1、应访谈建设负责人是否采用了密码产品及相关服务； 2、应核查密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。 |
| 自行软件开发 | a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； | 建设负责人 | 1、应访谈建设负责人自主开发软件是否在独立的物理环境中完成编写和调试，与实际运行环境分开； 2、应核查测试数据和结果是否受控使用。 |
| b)应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。 | 记录表单类文档 | 应核查是否具有软件安全测试报告和代码审计报告，明确软件存在的安全问题及可能存在的恶意代码。 |
| 外包软件开发 | a)应在软件交付前检测其中可能存在的恶意代码； | 记录表单类文档 | 应核查是否具有交付前的恶意代码检查报告。 |
| b)应保证开发单位提供软件设计文档和使用指南。 | 操作规程类文档和记录表单类文档 | 应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南。 |
| 工程实施 | a)应指定或授权专门的部门或人员负责工程实施过程的管理； | 记录表单类文档 | 应核查是否指定专门部门或人员对工程实施进行进度和质量控制。 |
| b)应制定安全工程实施方案控制工程实施过程。 | 记录表单类文档 | 应核查安全工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。 |
| 测试验收 | a)应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； | 记录表单类文档 | 1、应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容； 2、应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。 |
| b)应进行上线前的安全性测试，并出具安全测试报告。 | 记录表单类文档 | 应核查是否具有上线前的安全测试报告。 |
| 系统交付 | a)应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； | 记录表单类文档 | 应核查交付清单是否说明交付的各类设备、软件、文档等。 |
| b)应对负责运行维护的技术人员进行相应的技能培训； | 记录表单类文档 | 应核查系统交付技术培训记录是否包括培训内容、培训时间和参与人员等。 |
| c)应提供建设过程文档和运行维护文档。 | 记录表单类文档 | 应核查交付文档是否包括建设过程文档和运行维护文档等，提供的文档是否符合管理规定的要求。 |
| 等级测评 | a)应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； | 运维负责人和记录表单类文档 | 1、应访谈运维负责人本次测评是否为首次，若非首次，是否根据以往测评结果进行相应的安全整改； 2、应核查是否具有以往等级测评报告和安全整改方案。 |
| b)应在发生重大变更或级别发生变化时进行等级测评； | 运维负责人和记录表单类文档 | 1、应核查是否有过重大变更或级别发生过变化及是否进行相应的等级测评； 2、应核查是否具有相应情况下的等级测评报告。 |
| c)应确保测评机构的选择符合国家有关规定。 | 等级测评报告和相关资质文件 | 应核查以往等级测评的测评单位是否具有等级测评机构资质。 |
| 服务供应商选择 | a)应确保服务供应商的选择符合国家的有关规定； | 建设负责人 | 应访谈建设负责人选择的安全服务商是否符合国家相关规定。 |
| b)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。 | 记录表单类文档 | 应核查与服务供应商签订的服务合同或安全责任书是否明确了后期的技术支持和服务承诺等内容。 |

#### （10）安全运维管理

|  |  |  |  |
| --- | --- | --- | --- |
| 控制点 | 测评项 | 测评对象 | 测评方法和步骤 |
| 环境管理 | a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； | 物理安全负责人和记录表单类文档 | 1、应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理、对基础设施（如空调、供电设备、灭火器等）进行定期维护； 2、应核查部门或人员岗位职责文档是否定期明确机房安全的责任部门及人员； 3、应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息； 4、应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。 |
| b)应建立机房安全管理制度，包括物理访问、物品进出和环境安全等方面； | 管理制度类文档和记录表单类文档 | 1、应核查机房安全管理制度是否覆盖物理访问、物品进出和环境安全等方面内容； 2、应核查物理访问、物品进出和环境安全等相关记录是否与制度相符。 |
| c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 | 管理制度类文档和办公环境 | 1、应核查机房安全管理制度是否明确来访人员的接待区域； 2、应核查办公桌面上等位置是否未随意放置了敏感信息的纸档文件和移动介质等。 |
| 资产管理 | 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。 | 记录表单类文档 | 应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容。 |
| 介质管理 | a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； | 资产管理员和记录表单类文档 | 1、应访谈资产管理员介质存放环境是否安全，存放环境是否由专人管理； 2、应核查介质管理记录是否记录介质归档、使用和定期盘点等情况。 |
| b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 | 资产管理员和记录表单类文档 | 1、应访谈资产管理员介质在物理传输过程中的人员选择、打包、交付等情况是否进行控制； 2、核查是否对介质的归档和查询等进行登记记录。 |
| 设备维护管理 | a)应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； | 设备管理员和管理制度类文档 | 1、应访谈设备管理员是否对各类设备、线路指定专人或专门部门进行定期维护； 2、应核查部门或人员岗位职责文档是否明确设备维护管理的职责部门。 |
| b)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。 | 管理制度类文档和记录表单类文档 | 1、应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容； 2、应核查是否留有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符。 |
| 漏洞和风险管理 | 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。 | 记录表单类文档 | 1、应核查是否有识别安全漏洞和隐患的安全报告或记录（如漏洞扫描报告、渗透测试报告和安全通报等）； 2、应核查相关记录是否对发现的漏洞及时进行修补或评估可能的影响后进行修补。 |
| 网络和系统安全管理 | a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； | 记录表单类文档 | 应核查网络和系统安全管理文档，系统管理员是否划分了不同角色，并定义各个角色的责任和权限。 |
| b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； | 运维负责人和记录表单类文档 | 1、应访谈运维负责人是否指定专门的部门或人员进行账户管理； 2、应核查相关审批记录或流程是否对申请账单、建立账户、删除账户等进行控制。 |
| c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； | 管理制度类文档 | 应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略、账户管理（用户责任、、义务、风险、权限审批、权限分配、账户注销等）、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与打补丁、审计日志管理、登录设备和系统的口令更新周期等方面。 |
| d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； | 操作规程类文档 | 应核查重要设备或系统（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作步骤、参数配置等内容。 |
| e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。 | 记录表单类文档 | 应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容。 |
| 恶意代码防范管理 | a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； | 运维负责人和管理制度类文档 | 1、应访谈运维负责人是否采取培训和告知等方式提升员工的防恶意代码意识； 2、应核查恶意代码防范管理制度是否明确对外来计算机或存储设备接入系统前进行恶意代码检查。 |
| b)应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等； | 管理制度类文档 | 应核查恶意代码防范管理制度是否包括防恶意代码软件的授权使用、恶意代码库升 级、定期查杀等内容。 |
| c)应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。 | 安全管理员和记录表单类文档 | 1、应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否出现过大规模的病毒事件，如何 处理； 2、应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。 |
| 配置管理 | 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等； | 系统管理员 | 应访谈系统管理员是否对基本配置信息进行记录和保存。 |
| 密码管理 | a)应遵循密码相关国家标准和行业标准； | 安全管理员 | 应访谈安全管理员密码管理过程中是否遵循密码相关的国家标准和行业标准要求。 |
| b)应使用国家密码管理主管部门认证核准的密码技术和产品。 | 安全管理员 | 应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。 |
| 变更管理 | 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。 | 记录表单类文档 | 1、应核查变更方案是否包含变更类型、变更原因、变更过程、变更前评估等内容； 2、应核查是否具有变更方案评审记录和变更过程记录文档。 |
| 备份与恢复管理 | a)应识别需要定期备份的重要业务信息、系统数据及软件系统等； | 系统管理员和记录表单类文档 | 1、应访谈系统管理员有哪些需要定期备份的业务信息、系统数据及软件系统； 2、应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。 |
| b)应规定备份信息的备份方式、备份频度、存储介质、保存期等； | 管理制度类文档 | 应核查备份与恢复管理制度是否明确备份方式、频度、介质、保质期等内容。 |
| c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 | 管理制度类文档 | 应核查备份和恢复的策略文档是否根据数据的重要程度制定相应备份恢复策略和程序等。 |
| 安全事件处置 | a)应及时向安全管理部门报告所发现的安全弱点和可疑事件； | 运维负责人和记录表单类文档 | 1、应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告； 2、应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。 |
| b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； | 管理制度类文档 | 应核查安全事件报告和处理管理制度是否明确了与安全事件有关的工作职责、不同安全事件的报告、处置和相应流程等。 |
| c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。 | 记录表单类文档 | 应核查安全事件报告和响应处置记录是否记录引发安全事件的原因、证据、处置过程、经验教训、补救措施等内容。 |
| 应急预案管理 | a)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； | 管理制度类文档 | 应核查制定重要事件的应急预案（如针对机房、系统、网络等各个方面）。 |
| b)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。 | 运维负责人和记录表单类文档 | 1、应访谈运维负责人是否定期对相关人员进行应急预案培训和演练； 2、应核查应急预案培训记录是否明确培训对象、培训内容、培训结果等； 3、应核查应急预案演练记录是否记录演练时间、主要操作内容、演练结果等。 |
| 外包运维管理 | a)应确保外包运维服务商的选择符合国家的有关规定； | 运维负责人 | 1、应访谈运维负责人是否有外包运维服务情况； 2、应访谈运维负责人外包运维服务单位是否符合国家相关规定。 |
| b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。 | 记录表单类文档 | 应核查外部运维服务协议是否明确约定外包运维的范围和工作内容。 |

## （二）软件正版化检查表

#### （1）2024年度省直机关软件使用情况统计表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **2024年度省直机关软件使用情况统计表** | | | | | | | | | |
| 填表单位（盖章）： 填表人： 联系电话： 填表日期： 年 月 日  **一、责任部门情况** | | | | | | | | | |
| 部门名称 | | | | 部门负责人姓名 | | 部门负责人电话 | | 部门传真 | |
|  | | | |  | |  | |  | |
| **二、机关本级情况** | | | | | | | | | |
| 使用正版软件工作总体情况 | | | | □是 □否 全面完成使用正版软件工作 | | | | | |
| 人员情况 | 总人数 |  | | 使用计算机人数 | |  | | | |
| 计算机情况 | 服务器数 |  | | 台式机数 | |  | 便携机数 |  | |
| 2020年 采购软件 情况 | 软件 属性 | 操作系统软件 (不含预装操作系统) | | 办公软件 | | 杀毒软件 | | 总计 | |
| 许可数（个） | 金额 （万元） | 许可数（个） | 金额 （万元） | 许可数（个） | 金额 （万元） | 许可数（个） | 金额 （万元） |
| 国内 |  |  |  |  |  |  |  |  |
| 国外 |  |  |  |  |  |  |  |  |
| 合计 |  |  |  |  |  |  |  |  |
| 累计拥有 软件许可 情况 | 软件 属性 | 操作系统软件 (含预装操作系统) 许可数（个） | | 办公软件 许可数（个） | | 杀毒软件 许可数（个） | | 总计 | |
| 国内 |  | |  | |  | |  | |
| 国外 |  | |  | |  | |  | |
| 合计 |  | |  | |  | |  | |
| **三、直属事业单位情况** | | | | | | | | | |
| 是否有直属事业单位 | | □是 □否 | | 直属事业单位数 | |  | 完成使用正版软件  直属事业单位数 | |  |
| 人员情况 | 总人数 |  | | 使用计算机人数 | |  | | | |
| 计算机情况 | 服务器数 |  | | 台式机数 | |  | 便携机数 |  | |
| 2020年 采购软件 情况 | 软件属性 | 操作系统软件 (不含预装操作系统) | | 办公软件 | | 杀毒软件 | | 总计 | |
| 许可数（个） | 金额 （万元） | 许可数（个） | 金额 （万元） | 许可数（个） | 金额 （万元） | 许可数（个） | 金额 （万元） |
| 国内 |  |  |  |  |  |  |  |  |
| 国外 |  |  |  |  |  |  |  |  |
| 合计 |  |  |  |  |  |  |  |  |
| 累计拥有 软件许可 情况 | 软件属性 | 操作系统软件  (含预装操作系统)  许可数（个） | | 办公软件 许可数（个） | | 杀毒软件 许可数（个） | | 总计 | |
| 国内 |  | |  | |  | |  | |
| 国外 |  | |  | |  | |  | |
| 合计 |  | |  | |  | |  | |

#### （2）2024年度省直机关软件正版化工作自评表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2024年度省直机关软件正版化工作自评表 | | | | | | |
| 单位名称：（公章） 填表人： 联系电话： 时间：年月日 | | | | | | |
| 序号 | 自评项目 | 自评依据 | 内容 | 分值 | 得分 | 说明 |
| 1 | 年度工作总结 | 文件 | 总结本单位本年度软件正版化工作情况，制定下一年度工作计划 | 5 |  | 有总结材料的，此项得满分，没有的不得分。 |
| 2 | 管理监督责任 | 文件、工作记录 | 明确软件正版化工作机构、第一责任人及管理监督责任 | 5 |  | 有机构、责任人和管理监督责任的，此项得满分，缺少一项扣1分；未正式发文的扣2.5分。 |
| 3 | 软件资产统计 | 软件资产统计表 | 单位编制人数，软件拥有种类、数量等 | 5 |  | 有统计表的，此项得满分，没有的不得分。 |
| 4 | 软件规范使用 | 文件、软件资产台账 | 建立软件安装、使用台账 | 5 |  | 有软件安装使用台账的，此项得满分，没有的不得分。 |
| 5 | 软件采购经费 | 文件、经费预算报告、软件采购合同、支付凭证、发票等 | 将软件采购经费纳入预算，采购资金落实情况 | 10 |  | 有采购预算、资金落实相关文件的，本项得满分，没有的不得分。 |
| 6 | 软件资产管理制度 | 文件、通知 | 软件采购、升级、安装使用、报废等方面的规定或制度，软件资产管理制度 | 10 |  | 有软件资产管理制度和安装使用管理制度的，此项得满分，缺少一项扣5分；未正式发文的扣5分。 |
| 7 | 正版软件安装 | 软件授权书（授权序列号）、采购合同 | 拥有正版软件（以操作系统、办公软件和杀毒软件三类为主，其他应用软件不进入统计范围）数量与本单位计算机数量的匹配情况 | 50 |  | 按照正版软件中操作系统、办公软件、杀毒软件的数量之和占本单位计算机总数\*3的百分比计算本项得分。如某单位计算机共60台，正版软件中操作系统50个、办公软件44个、杀毒软件50个，则得分为：(50+44+50)/（60\*3）\*50=40分。 |
| 8 | 软件自查 |  | 使用安装好的正版软件检查工具网络版检查操作系统软件、办公软件和杀毒软件的安装使用情况 | 10 |  | 发现计算机有安装使用盗版软件的每台扣2分，直至扣完本项分值；未安装正版软件检查工具网络版的扣5分。 |
|  |  |  |  | 总计 |  |  |

#### （3）省直机关直属事业单位软件正版化工作完成情况表

省直机关直属事业单位软件正版化工作完成情况表

单位（盖章）： 填表人： 联系电话：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 事业单位名称 | 事业单位类别 | 办公软件正版化率 | 杀毒软件正版化率 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

（注：事业单位类别可填1.参公2.财政核拨3.财政核补4.自收自支5.实行企业化管理）

#### （4）软件正版化工作检查表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 软件正版化工作检查表 | | | | |
| 被查单位名称： 检查组组长签字： | | | | |
| 检 查 时 间：年月日 | | | | |
| 序号 | 检查项目 | 检查内容 | 检查依据 | 检查结果 |
| 1 | 制度建设和责任落实情况 | 软件正版化工作机构和职责落实情况 | 文件、工作记录 | 有□ 无□ |
| 计算机软硬件采购制度建设和落实情况 | 文件、工作记录 | 有□ 无□ |
| 正版软件管理制度建设和落实情况 | 文件、工作记录 | 有□ 无□ |
| 软件正版化工作考核评议制度建设和落实情况 | 文件、工作记录 | 有□ 无□ |
| 使用正版软件承诺书签署情况 | 文件、工作记录 | 有□ 无□ |
| 2 | 软件日常使用管理 情况 | 2020年软件正版化工作总结 | 文件、工作记录 | 有□ 无□ |
| 2021年软件正版化工作计划 | 文件、工作记录 | 有□ 无□ |
| 正版软件使用日常检查情况 | 文件、工作记录 | 有□ 无□ |
| 软件检查工具（网络版）安装使用情况 | 文件、工作记录 | 有□ 无□ |
| 正版软件台账建立情况 | 文件、工作记录 | 有□ 无□ |
| 国产软件采购及使用情况 | 文件、工作记录 | 有□ 无□ |
| 软件采购合同、软件授权协议 | 文件、工作记录 | 有□ 无□ |
| 3 | 现场检查计算机情况 | 检查计算机台数 | **判定安装盗版软件标准：** 安装的软件名称及版本与采购的软件名称及版本不一致（可免费使用的正版软件除外；采购某软件厂商高版本软件，实际使用该软件厂商低版本软件，并且有该软件厂商出具的降级使用授权书的除外） | 台 |
| 安装盗版操作系统软件的计算机台数 | 台 |
| 安装盗版办公软件的计算机台数 | 台 |
| 安装盗版杀毒软件的计算机台数 | 台 |
| 安装Windows8或Window10操作系统软件的计算机台数 | 台 |
| 备注：如有需要说明的事项，可在此栏填写，也可另附页说明。 | | | | |

#### （5）软件使用情况汇总表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 软件使用情况汇总表 | | | | | | | | | | | | |
| 单位名称（盖章）： 填表人： 联系电话： 填表日期：年月日 | | | | | | | | | | | | |
| **人员情况** | | 总人数 |  | | | 使用计算机人数 | |  | | | | |
| **计算机情况** | | 服务器数 |  | | | 台式机数 | |  | | 便携机数 |  | |
| **序号** | **软件编号** | **软件名称** | **软件版本** | **软件类型** | **采购时间** | **采购金额 (单位:元)** | **许可类型** | **许可数量** | **可使用版本** | **许可期限** | **序列号** | **安装数量** |
| 1 |  |  |  | 商业软件 |  |  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 2 |  |  |  | 商业软件 |  |  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 3 |  |  |  | OEM软件 |  | | | | | | |  |
| 4 |  |  |  | OEM软件 |  | | | | | | |  |
| 5 |  |  |  | 免费软件 |  | | | | | | |  |
| 6 |  |  |  | 免费软件 |  | | | | | | |  |
| 说明：1.只填写操作系统、办公和杀毒三类软件使用情况。2.各栏目行数可自行增加，可另附页。 | | | | | | | | | | | | |

#### （6）软件使用情况明细表

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 软件使用情况明细表 | | | | | | | | | | | | | |
| 单位名称（盖章）： 填表人： 联系电话： 填表日期：年月日 | | | | | | | | | | | | | |
| 序号 | 部门 | 姓名 | 计算机编号 | 计算机品牌 | 软件编号 | 软件名称 | 软件版本 | 许可期限 | 软件类型 | | | 安装日期 | 现场核查情况 |
| 商业 软件 | OEM 软件 | 免费 软件 |
| 1 |  |  |  |  |  |  |  |  | □ | □ | □ |  |  |
| 2 |  |  |  |  | □ | □ | □ |  |  |
| 3 |  |  |  |  | □ | □ | □ |  |  |
| 4 |  |  |  |  |  |  |  |  | □ | □ | □ |  |  |
| 5 |  |  |  |  | □ | □ | □ |  |  |
| 6 |  |  |  |  | □ | □ | □ |  |  |
| 7 |  |  |  |  |  |  |  |  | □ | □ | □ |  |  |
| 8 |  |  |  |  | □ | □ | □ |  |  |
| 9 |  |  |  |  | □ | □ | □ |  |  |
| 10 |  |  |  |  |  |  |  |  | □ | □ | □ |  |  |
| 11 |  |  |  |  | □ | □ | □ |  |  |
| 12 |  |  |  |  | □ | □ | □ |  |  |
| 说明：1.只填写操作系统、办公和杀毒三类软件使用情况。  2.各栏目行数可自行增加，可另附页。  3.“现场核查情况”栏目由检查组填写。 | | | | | | | | | | | | | |