# **一、三级系统**

## **A.1物理安全**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 数据中心机房 | 物理位置的选择 | a)机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内； | 机房和办公场地满足基本的防震、防风和防雨要求； | 符合(5分) |
| b)机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。 | 机房未在建筑物高层或地下室，以及用水设备下层或隔壁。 | 符合(5分) |
| 物理访问控制 | a)机房出入口应安排专人值守，控制、鉴别和记录进入的人员； | 制定了机房管理制度；机房有专人值守，有值守记录；有三个出入口，主出入口是玻璃门； | 部分符合(3分) |
| b)需进入机房的外来访人员应经过申请和审批流程，并限制和监控其活动范围； | 外来人员进入机房有审批流程和相应的审批记录，对外部人员的活动范围进行限制； | 符合(5分) |
| c)应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域； | 机房进行了区域划分，并且有隔离措施； | 符合(5分) |
| d)重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。 | 没有有电子门禁系统，只有门口纸质登录记录。 | 符合(5分) |
| 防盗窃和防破坏 | a)应将主要设备放置在机房内； | 主要设备均放置在机房内； | 符合(5分) |
| b)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记； | 设备在机房位置固定，且进行设备标签标注，标识不易去除； | 符合(5分) |
| c)应将通信线缆铺设在隐蔽处，可铺设在地下或管道中； | 通信线缆铺设在走线架中； | 符合(5分) |
| d)应对介质分类标识，存储在介质库或档案室中； | 介质分类标示存储在档案室； | 符合(5分) |
| e)应利用光、电等技术设置机房防盗报警系统； | 机房安装视频监控； | 符合(5分) |
| f)应对机房设置监控报警系统。 | 机房安装视频监控。 | 符合(5分) |
| 防雷击 | a)机房建筑应设置避雷装置； | 机房大楼有避雷针，有建筑防雷设计和验收文档； | 符合(5分) |
| b)应设置防雷保安器，防止感应雷； | 没有安装防雷保安器； | 不符合 |
| c)机房应设置交流电源地线。 | 有交流电源地线，并且有交流电源地线的说明。 | 符合(5分) |
| 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； | 机房有灭火器； | 符合(5分) |
| 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； | 机房采用防火材料装修； | 符合(5分) |
| c)机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。 | 机房重要区域和其他区域之间采取隔离防火措施。 | 符合(5分) |
| 防水和防潮 | a)水管安装，不得穿过机房屋顶和活动地板下； | 活动地板下无水管穿过，屋顶有水管穿过，采取了三层防渗漏措施； | 符合(5分) |
| b)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 屋顶和墙壁未出现漏水、渗透和返潮的现象； | 符合(5分) |
| c)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； | 机房设置了挡水和排水设施； | 符合(5分) |
| d)应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 | 机房安装有漏水检测报警装置。 | 符合(5分) |
| 防静电 | a)主要设备应采用必要的接地防静电措施； | 主要设备采用了接地防静电措施； | 符合(5分) |
| b)机房应采用防静电地板。 | 机房铺设了防静电地板。 | 符合(5分) |
| 温湿度控制 | a)机房应设置温、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。 | 机房使用两台空调调节机房温湿度，且运行正常，机房温湿度满足电子信息设备使用要求。 | 符合(5分) |
| 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； | 设置了稳压器和过电压防护设备，且正常运行，供电电压正常； | 符合(5分) |
| b)应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求； | 设置了短期备用电源（UPS），但无法正常运行； | 符合(5分) |
| c)应设置冗余或并行的电力电缆线路为计算机系统供电； | 机房采用并行电力电缆线路供电； | 符合(5分) |
| d)应建立备用供电系统。 | 机房建立备用供电系统，满足主要设备的正常运行。 | 符合(5分) |
| 电磁防护 | a)应采用接地方式防止外界电磁干扰和设备寄生耦合干扰； | 机房设备外壳有安全接地； | 符合(5分) |
| b)电源线和通信线缆应隔离铺设，避免互相干扰； | 机房电源线和通信线缆隔离铺设； | 符合(5分) |
| c)应对关键设备和磁介质实施电磁屏蔽。 | 对关键设备和磁介质实施电磁屏蔽措施。 | 符合(5分) |

## **A.2网络安全**

### A.2.1 交换机

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 数据网核心交换机 | 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 开启相应安全审计策略，对网络设备的运行状况、网络流量、用户行为等进行日志记录； | 符合(5分) |
| 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； | 开启日志审计，审计记录包括事件的时间、日期、用户、事件类型和事件是否成功，能够进行溯源； | 符合(5分) |
| c)应能够根据记录数据进行分析，并生成审计报表； | 通过人工对设备的日志数据进行分析，可以生成审计报表； | 符合(5分) |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 没有配置日志服务器，日志由本机保存，保存日志记录超过3个月。 | 符合(5分) |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 开启身份鉴别功能，口令不为空； | 符合(5分) |
| b)应对网络设备的管理员登录地址进行限制； | 对网络设备的管理员登录地址进行了限制； | 符合(5分) |
| c)网络设备用户的标识应唯一； | 存在多个用户使用同一个账号登录，（两个管理员使用同一个账号）； | 不符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 未采用双因子鉴别； | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令仅限制至少8个字符，未要求数字加字母组合，未定期修改； | 部分符合(3分) |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 登录超时时间没有限制，登录失败没有次数限制； | 不符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 关闭telnet服务，使用ssh远程登录管理； | 符合(5分) |
| h)应实现设备特权用户的权限分离。 | 根据实际使用情况为不同用户分配不同的权限。 | 符合(5分) |

### A.2.2 路由器

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 路由器 | 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 开启相应安全审计策略，对网络设备的运行状况、网络流量、用户行为等进行日志记录； | 符合(5分) |
| 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； | 开启日志审计，审计记录包括事件的时间、日期、用户、事件类型和事件是否成功，能够进行溯源； | 符合(5分) |
| c)应能够根据记录数据进行分析，并生成审计报表； | 通过人工对设备的日志数据进行分析，可以生成审计报表； | 符合(5分) |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 没有配置日志服务器，日志由本机保存，保存日志记录超过3个月。 | 符合(5分) |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 开启身份鉴别功能，口令不为空； | 符合(5分) |
| b)应对网络设备的管理员登录地址进行限制； | 对网络设备的管理员登录地址进行了限制；； | 符合(5分) |
| c)网络设备用户的标识应唯一； | 存在多个用户使用同一个账号登录，（两个管理员使用同一个账号）； | 不符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 未采用双因子鉴别； | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令仅限制至少8个字符，未要求数字加字母组合，未定期修改； | 部分符合(3分) |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 登录超时时间没有限制，登录失败没有次数限制； | 不符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 关闭telnet服务，使用ssh远程登录管理； | 符合(5分) |
| h)应实现设备特权用户的权限分离。 | 根据实际使用情况为不同用户分配不同的权限。 | 符合(5分) |

### A.2.3 网络结构

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络结构 | 结构安全 | a)应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要； | 未发现设备存在性能瓶颈，主要网络设备业务处理能力基本满足需求； | 符合(5分) |
| b)应保证网络各个部分的带宽满足业务高峰期需要； | 未发现接入网络和核心网络存在瓶颈，系统采用足够的带宽和流量控制措施保证高峰期业务运行需要； | 符合(5分) |
| c)应在业务终端与业务服务器之间进行路由控制建立安全的访问路径； | 路由控制策略使用了静态路由和动态路由混合； | 符合(5分) |
| d)应绘制与当前运行情况相符的网络拓扑结构图； | 已绘制与当前网络结构相符的网络拓扑图，能客观反映实际网络现状的规则； | 符合(5分) |
| e)应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段； | 已根据各部门的工作职能在核心交换机上通过vlan进行了网段划分； | 符合(5分) |
| f)应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段； | 重要网段不位于网络边界处，对重要网段采取可靠的访问控制策略，避免非授权访问； | 符合(5分) |
| g)应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。 | 采用网络掌门流控，对网络带宽进行了控制策略，保障在业务高峰期网络出现拥堵的时候，能优先保护重要业务。 | 符合(5分) |
| 访问控制 | a)应在网络边界部署访问控制设备，启用访问控制功能； | 在网络边界处部署访问控制设备（边界防火墙），启用访问控制功能； | 符合(5分) |
| b)应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； | 边界处访问控制设备的访问控制规则有明确的源IP、目的IP、协议及端口，边界处的网络设备关闭了不必要的服务； | 符合(5分) |
| c)应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制； | 网络层面未对应用层协议进行内容进行内容过滤； | 不符合 |
| d)应在会话处于非活跃一定时间或会话结束后终止网络连接； | 根据业务实际需求在边界或访问节点设置TCP、UDP会话超时时间； | 符合(5分) |
| e)应限制网络最大流量数及网络连接数； | 限制网络最大流量数，未限制网络连接数； | 不符合 |
| f)重要网段应采取技术手段防止地址欺骗； | 重要网段所在的交换机开启防止ARP欺骗的功能； | 符合(5分) |
| g)应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户； | VPN功能没有开启； | 符合(5分) |
| h)应限制具有拨号访问权限的用户数量。 | 限制了拨号用户的数量。 | 符合(5分) |
| 边界完整性检查 | a)应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断； | 没有采取任何技术手段或管理措施对非授权设备私自联到内部网络的行为进行检查、定位和阻断； | 不符合 |
| b)应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。 | 没有采取任何技术手段或管理措施对非法外联行为进行检查、定位和阻断。 | 不符合 |
| 入侵防范 | a)应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等； | 网络边界处没有安装入侵检测设备； | 不符合 |
| b)当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。 | 网络边界处没有安装入侵检测设备。 | 不符合 |
| 恶意代码防护 | a)应在网络边界处对恶意代码进行检测和清除； | 在网络边界处没有安装防病毒网关等措施防范恶意代码； | 不符合 |
| b)应维护恶意代码库的升级和检测系统的更新。 | 在网络边界处没有安装防病毒网关等措施防范恶意代码。 | 不符合 |

## **A.3 主机安全**

### A.3.1 linux主机

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 数据库服务器 | 身份鉴别 | a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别； | 第二字段不为空，各个用户主目录下无.rhosts文件，/etc/hosts.equiv文件不存在； | 符合(5分) |  |
| b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | PASS\_MAX\_DAYS 9999 PASS\_MIN\_DAYS 0 PASS\_MIN\_LENS 5 PASS\_WARN\_AGE 7，minlen=8 ucredit=-1 lcredit=-1 dcredit=-1 等参数没有设置，口令定期更换； | 不符合 |  |
| c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | 未使用pam\_tally.so模块跟踪不成功登录次数； | 不符合 | Cat/etc/pam.d/sshd ?这个需要确定一下 |
| d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 未开启Telnet、Ftp等服务，采用SSH进行远程管理； | 符合(5分) |  |
| e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性； | 无同名账号，UID具有唯一性，UID=0为root账号； | 符合(5分) |  |
| f)应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 | 未使用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 | 不符合 |  |
| 访问控制 | a)应启用访问控制功能，依据安全策略控制用户对资源的访问； | 未制定用户权限表； | 不符合 |  |
| b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限； | 管理员用户权限分离，管理用户最小授权； | 符合(5分) |  |
| c)应实现操作系统和数据库系统特权用户的权限分离； | 操作系统与数据库系统管理员为同一人； | 不符合 |  |
| d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； | 重命名系统默认账号，修改了默认账号口令； | 符合(5分) |  |
| e)应及时删除多余的、过期的帐户，避免共享帐户的存在； | 对多余账号进行了删除、锁定、或禁止其登录； | 符合(5分) |  |
| f)应对重要信息资源设置敏感标记； | 对主机内的重要信息设置敏感标记； | 符合(5分) |  |
| g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 | 定义敏感标记资源的访问策略，并根据策略控制用户对该资源的操作。 | 符合(5分) |  |
| 安全审计 | a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； | 日志进程syslog未开启，开启了日志进程rsyslog，审计进程正常运行； | 符合(5分) |  |
| b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； | /etc/rsyslog文件中包含日志内容，审计规则未配置； | 部分符合(3分) |  |
| c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | Linux系统审计默认符合； | 符合(5分) |  |
| d)应能够根据记录数据进行分析，并生成审计报表； | 未人工对审计日志进行分析，并未生成审计报表； | 不符合 |  |
| e)应保护审计进程，避免受到未预期的中断； | 未安装额外审计进程保护软件； | 不符合 |  |
| f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | /var/log/messages 600 /var/log/secure 600 /var/log/audit/audit.log 600，权限为root账号可读可写。 | 符合(5分) |  |
| 剩余信息保护 | a)应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； | 引用产品测试结果，信息删除后能清除； | 符合(5分) |  |
| b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。 | 引用产品测试结果，信息删除后能清除。 | 符合(5分) |  |
| 入侵防范 | a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警； | 未安装入侵检测系统； | 不符合 | 1. 是否经常命令查看more /var/log/secure | grep refused (centos) 2. more /var/log/auth.log | grep refused (ubuntu) 3. 是否启用主机防火墙、TCP SYN保护机制 4. 是否安全入侵检测软件：ITA、hostsentry、logcheck等 5. 是否有入侵检测系统 |
| b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施； | 未安装完整性检测工具，定期对系统进行备份； | 部分符合(3分) |  |
| c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。 | 系统安全补丁安装，未关闭危险服务网络echo login。 | 部分符合(3分) |  |
| 恶意代码防范 | a)应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库； | 未安装防病毒软件； | 不符合 |  |
| b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库； | 未安装防病毒软件； | 不符合 |  |
| c)应支持防恶意代码的统一管理。 | 未安装防病毒软件。 | 不符合 |  |
| 资源控制 | a)应通过设定终端接入方式、网络地址范围等条件限制终端登录； | /etc/ssh/sshd\_config文件中包含 PermitRootLogin no ，两个文件不为空，未配置限制ip地址信息，配置防火墙规则； | 部分符合(3分) |  |
| b)应根据安全策略设置登录终端的操作超时锁定； | 未设置export TMOUT参数； | 不符合 |  |
| c)应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； | 未对资源进行监控和报警，仅通过人工在重要时段进行查看； | 部分符合(3分) |  |
| d)应限制单个用户对系统资源的最大或最小使用限度； | 未限制单个用户对系统资源的最大最小使用限度； | 不符合 |  |
| e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。 | 未对资源进行监控和报警，仅通过人工在重要时段进行查看。 | 不符合 |  |

备注：（linux密码复杂度分系统）

策略设置：

一、禁止使用旧密码

找到同时有 “password” 和 “pam\_unix.so” 字段并且附加有 “remember=5” 的那行，它表示禁止使用最近用过的5个密码（己使用过的密码会被保存在 /etc/security/opasswd 下面）。

Debian、Ubuntu 或 Linux Mint 系统上：

代码如下:

$ sudo vi /etc/pam.d/common-password  
password [success=1 default=ignore] pam\_unix.so obscure sha512 remember=5

CentOS、Fedora、RHEL 系统上：

代码如下:

$ sudo vi /etc/pam.d/system-auth  
password sufficient pamunix.so sha512 shadow nullok tryfirstpass useauthtok remember=5

二、设置最短密码长度

找到同时有 “password” 和 “pam\_cracklib.so” 字段并且附加有 “minlen=10” 的那行，它表示最小密码长度为（10 - 类型数量）。这里的 “类型数量” 表示不同的字符类型数量。PAM 提供4种类型符号作为密码（大写字母、小写字母、数字和标点符号）。如果密码同时用上了这4种类型的符号，并且 minlen 设为10，那么最短的密码长度允许是6个字符。

Debian、Ubuntu 或 Linux Mint 系统上：

代码如下:

$ sudo vi /etc/pam.d/common-password  
password requisite pam\_cracklib.so retry=3 minlen=10 difok=3

CentOS、Fedora、RHEL 系统上：

代码如下:

$ sudo vi /etc/pam.d/system-auth  
password requisite pam\_cracklib.so retry=3 difok=3 minlen=10

三、设置密码复杂度

找到同时有 “password” 和 “pam\_cracklib.so” 字段并且附加有 “ucredit=-1 lcredit=-2 dcredit=-1 ocredit=-1” 的那行，表示密码必须至少包含一个大写字母（ucredit），两个小写字母（lcredit），一个数字（dcredit）和一个标点符号（ocredit）。

Debian、Ubuntu 或 Linux Mint 系统上：

代码如下:

$ sudo vi /etc/pam.d/common-password  
password requisite pam\_cracklib.so retry=3 minlen=10 difok=3 ucredit=-1 lcredit=-2 dcredit=-1 ocredit=-1

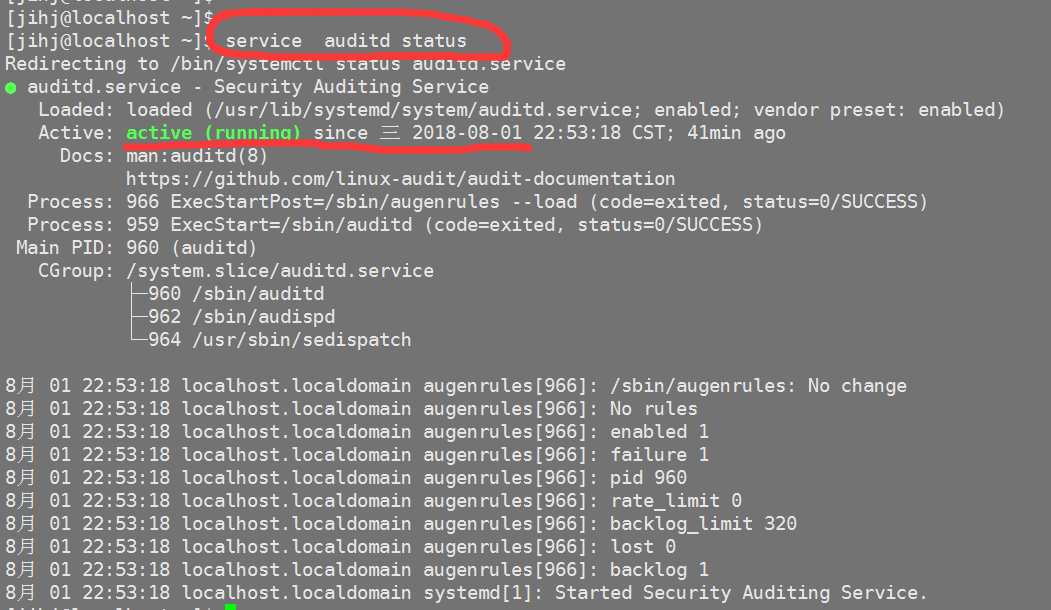
CentOS、Fedora、RHEL 系统上：

代码如下:

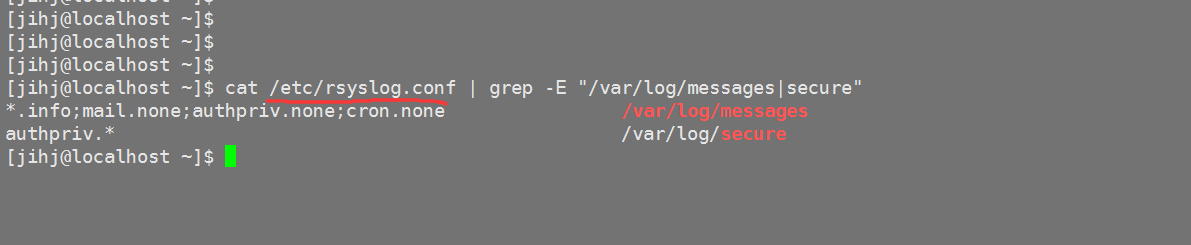
$ sudo vi /etc/pam.d/system-auth  
password requisite pam\_cracklib.so retry=3 difok=3 minlen=10 ucredit=-1 lcredit=-2 dcredit=-1 ocredit=-1

Centos 系统

1. audit进程默认开启



1. 测评过程中需要查看 /var/log/messages 和 /var/log/secure 两个文件的权限，这两个文件是在/var/log/rsyslog.conf中进行配置的，而/var/log/audit/audit.log是audit进程开启就有该文件



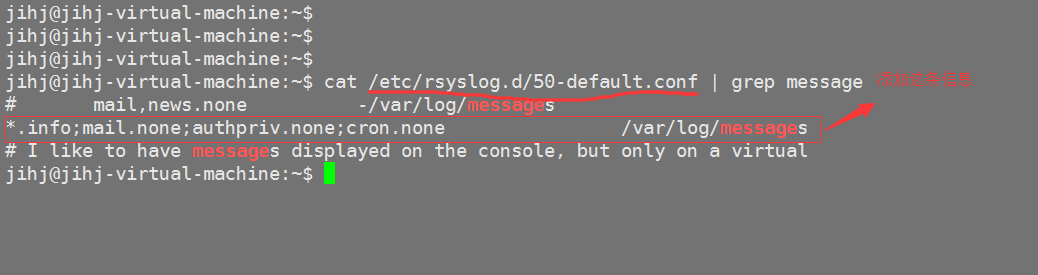
Ubuntu系统

1. auditd默认没有开启

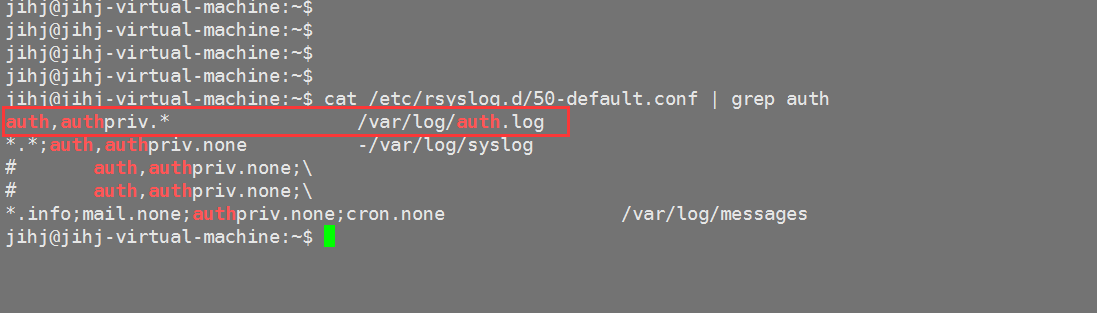
安装命令：sudo apt-get install auditd，安装成功后就有/var/log/audit/audit.log文件

1. 测评过程中需要查看 /var/log/messages 和 /var/log/secure 两个文件的权限

/var/log/messages文件是在/etc/rsyslog.d/50-default.conf文件中添加如下信息后才有该文件：



/var/log/secure这个文件在Ubuntu中是/var/log/auth.log，依据为：



### A.3.2 windows主机

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 教务A.3.2 windows主机 系统存储服务器 | 身份鉴别 | a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别； | 没有勾选“要使用本机，用户必须输入用户名和密码”； | 不符合 | 运行：control userpasswords2 |
| b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 密码必须符合复杂性要求已禁用，密码长度最小值0个字符，密码最短使用期限0天，密码最长使用期限42天，0个记住密码，没有勾选密码永不过期，勾选用户下次登录时必须更改密码； | 不符合 |  |
| c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | 账户锁定时间不适用，账户锁定阈值0次无效登录，重置账户锁定计数器不适用，采用remote desktop organizer远程登录； | 不符合 |  |
| d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 禁用telnet服务，采用remote desktop organizer远程登录； | 符合(5分) |  |
| e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性； | 存在多个用户使用同一账户情况； | 符合(5分) |  |
| f)应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 | 未使用两种鉴别技术对管理用户进行身份鉴别。 | 符合(5分) |  |
| 访问控制 | a)应启用访问控制功能，依据安全策略控制用户对资源的访问； | 未制定用户权限表； | 不符合 |  |
| b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限； | 管理用户权限分离，按照最小原则授权用户权限； | 符合(5分) |  |
| c)应实现操作系统和数据库系统特权用户的权限分离； | 数据库和操作系统管理员为同一个人，操作系统和数据库使用不同账户；登录 | 不符合 |  |
| d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； | 没有重命名管理员账号Administrator，禁用了Guest账户； | 不符合 | 1. 右键单击【我的电脑】→【管理】→【本地用户和组】→【用户】，查看有无“administrator”账号，并检查是否禁用了guest账号，无“administrator”账号且禁用了guest账号则此项为符合 2. 按照测评助手方法 |
| e)应及时删除多余的、过期的帐户，避免共享帐户的存在； | 不存在多余的过期账户； | 符合(5分) |  |
| f)应对重要信息资源设置敏感标记； | 定义了主机中的重要信息资源，为主机内的重要信息设置了敏感标记； | 符合(5分) |  |
| g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 | 定义主机中的敏感标记资源的访问策略，并根据访问策略控制用户对资源的操作。 | 符合(5分) |  |
| 安全审计 | a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； | 所有的审核策略无审核； | 不符合 |  |
| b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； | 所有的审核策略无审核； | 不符合 |  |
| c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | 所有的审核策略无审核； | 不符合 |  |
| d)应能够根据记录数据进行分析，并生成审计报表； | 所有的审核策略无审核 | 不符合 |  |
| e)应保护审计进程，避免受到未预期的中断； | Windows系统具备审计进程自我保护功能； | 符合(5分) |  |
| f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 仅administrator可管理审核和安全日志，RestrictGuestAccess键值均为1。 | 符合(5分) | 1. 根据软件助手的方法检测 2. 右键【我的电脑】→【管理】→【事件查看器】→右键单击任一事件查看器，【属性】，查看关于审计日志的存储大小设置以及是否按要求覆写，根据日志量的大小可酌情设置，但不得低于64M（默认是20M），并询问系统管理员是否对审计日志是否进行备份或者使用其它方式收集日志。达到最大日志量后，默认是覆盖旧日志，这是不符合的。 |
| 剩余信息保护 | a)应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； | 引用产品测试结果，信息删除后能清除； | 符合(5分) |  |
| b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。 | 引用产品测试结果，信息删除后能清除。 | 符合(5分) |  |
| 入侵防范 | a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警； | 未部署主机入侵检测系统； | 不符合 | 1. windows自带防火墙实现入侵防范功能（高级设置） 2. 入侵检测系统（IDS） |
| b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施； | 没有对关键性程序进行完整性检测，检测受到破坏具备备份恢复措施； | 部分符合(3分) |  |
| c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。 | 安装SP1，仅开启必须服务端口，关闭默认共享，系统安全补丁最新一次更新时间为：2017/12/1 最近检查更新时间：从未 安装更新时间：从未。 | 部分符合(3分) |  |
| 恶意代码防范 | a)应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库； | 部署360（免费版）和金山杀毒软件（收费版）； | 符合(5分) |  |
| b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库； | 网络层面未安装恶意代码防护产品； | 不符合 |  |
| c)应支持防恶意代码的统一管理。 | 防病毒软件支持统一管理。 | 符合(5分) |  |
| 资源控制 | a)应通过设定终端接入方式、网络地址范围等条件限制终端登录； | 通过开启主机防火墙限制； | 符合(5分) |  |
| b)应根据安全策略设置登录终端的操作超时锁定； | 启用屏幕保护，未开启会话空闲时间； | 不符合 |  |
| c)应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； | 未对主机cpu、内存、硬盘等状态采取监控措施，仅通过人工定期查看资源的使用情况； | 部分符合(3分) |  |
| d)应限制单个用户对系统资源的最大或最小使用限度； | 未对主机资源使用进行监控，未限制单个用户对资源的最大或最小使用限度； | 不符合 |  |
| e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。 | 未对主机资源进行监控和报警，仅通过人工定期查看系统资源使用情况。 | 部分符合(3分) |  |

### A.3.3 SQL数据库

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网站数据库 | 身份鉴别 | a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别； | 数据库系统对登录用户进行身份标识和鉴别； | 符合(5分) |
| b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | sa用户没有勾选强制实施密码策略，其余账户没有勾选，密码必须符合复杂性要求已禁用，密码长度最小值0个字符，密码最长使用期限42天，密码最短使用期限0天，0个记住密码； | 不符合 |
| c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | 登录用户没有勾选“强制实施密码策略”，账户锁定阈值5次无效登录，账户锁定时间999，重置账户锁定计数器999； | 不符合 |
| d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 使用默认客户端对服务器进行远程管理； | 符合(5分) |
| e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性； | 数据库只有一个管理人员进行登录使用，不存在多个用户使用同一个账户情况； | 符合(5分) |
| f)应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 | 没有采用两种及两种以上身份鉴别机制。 | 符合(5分) |
| 访问控制 | a)应启用访问控制功能，依据安全策略控制用户对资源的访问； | 启用访问控制功能，依据安全策略控制用户对资源的访问； | 符合(5分) |
| b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限； | 普通用户没有服务器角色，管理员用户权限分离，应用连接用户仅授予需要的最小权限； | 符合(5分) |
| c)应实现操作系统和数据库系统特权用户的权限分离； | 操作系统和数据库管理员为同一个人； | 不符合 |
| d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； | sa账号没有禁用，也没有对sa进行重命名； | 不符合 |
| e)应及时删除多余的、过期的帐户，避免共享帐户的存在； | 已经删除多余的、过期的账号，目前有sa、StudBaseInfo、test\_center用户正在使用； | 符合(5分) |
| f)应对重要信息资源设置敏感标记； | 默认SQL Server数据库达不到B1级水平； | 不符合 |
| g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 | 默认SQL Server数据库达不到B1级水平； | 不符合 |
| 安全审计 | a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； | 勾选SQL server和windows身份验证模式， 勾选仅限失败的登录， 没有勾选启用C2审核跟踪； | 不符合 |
| b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； | 勾选SQL server和windows身份验证模式， 勾选仅限失败的登录， 没有勾选启用C2审核跟踪； | 不符合 |
| c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | 勾选SQL server和windows身份验证模式， 勾选仅限失败的登录， 没有勾选启用C2审核跟踪； | 不符合 |
| d)应能够根据记录数据进行分析，并生成审计报表； | 不定期人工审计日志，有审批记录，没有生成报表； | 不符合 |
| e)应保护审计进程，避免受到未预期的中断； | 审计未开启； | 不符合 |
| f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 审计未开启。 | 不符合 |
| 剩余信息保护 | a)应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； | 引用产品测试结果，但信息删除后无法保证完全清除； | 部分符合(3分) |
| b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。 | 引用产品测试结果，但信息删除后无法保证完全清除。 | 部分符合(3分) |
| 入侵防范 | a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警； | sql server数据库 默认不适用； | 不适用 |
| b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施； | sql server数据库 默认不适用； | 不适用 |
| c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。 | 未更新最新补丁。 | 不符合 |
| 资源控制 | a)应通过设定终端接入方式、网络地址范围等条件限制终端登录； | 通过数据库触发器限制登录数据库的网络地址，勾选允许远程连接服务器，最大并发连接数为0 ； | 符合(5分) |
| b)应根据安全策略设置登录终端的操作超时锁定； | 设置远程查询超时时间600秒； | 符合(5分) |
| c)应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； | 没有对数据库的性能进行监控； | 不符合 |
| d)应限制单个用户对系统资源的最大或最小使用限度； | 没有对系统资源的最大或最小使用限度进行限制，但是当前资源充分满足要求(最小服务器内存0，最大服务器内存2147483647，创建索引占用的内存0，每次查询占有的最小内存1024)； | 符合(5分) |
| e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。 | 没有对数据库的性能进行监控，也没有邮箱、短信等方式进行报警。 | 不符合 |

### A.3.4 Oracle数据库

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 教务系统数据库 | 身份鉴别 | a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别； | 显示所有能登录数据库的用户信息，需要用户名和口令； | 符合(5分) |
| b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | PASSWORD\_REUSE\_MAX=UNLIMITED PASSWORD\_REUSE\_TIME=UNLIMITED PASSWORD\_LIFE\_TIME=UNLIMITED PASSWORD\_VERIFY\_FUNCTION=NULL | 不符合 |
| c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | FAILED\_LOGIN\_ATTEMPTS=UNLIMITED,PASSWORD\_GRACE\_TIME=UNLIMITED,PASSWORD\_LOCK\_TIME=UNLIMITED； | 不符合 |
| d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | Oracle默认符合； | 符合(5分) |
| e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性； | 存在多个用户使用同一个账户登录； | 不符合 |
| f)应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 | 未采用两种或者两种以上身份鉴别技术进行身份鉴别。 | 不符合 |
| 访问控制 | a)应启用访问控制功能，依据安全策略控制用户对资源的访问； | 提供用户权限表； | 符合(5分) |
| b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限； | 管理用户权限分离，管理用户最小授权； | 符合(5分) |
| c)应实现操作系统和数据库系统特权用户的权限分离； | 操作系统和数据库管理员是同一人，使用不同账号管理数据库及操作系统； | 不符合 |
| d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； | 未重命名SYS、SYSTEM默认账户，默认角色赋予PUBLIC为 null，未发现弱口令和默认口令； | 部分符合(3分) |
| e)应及时删除多余的、过期的帐户，避免共享帐户的存在； | 删除SCOTT用户，锁定CEXSYS、DMSYS等用户； | 符合(5分) |
| f)应对重要信息资源设置敏感标记； | 对数据库内的重要信息设置敏感标记； | 符合(5分) |
| g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 | 定义敏感标记资源的访问策略。 | 符合(5分) |
| 安全审计 | a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； | 开启审计功能；； | 符合(5分 |
| b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； | 开启部分安全事件的审计功能； | 部分符合(3分) |
| c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | 审计日志开启，则默认符合； | 符合(5分) |
| d)应能够根据记录数据进行分析，并生成审计报表； | 对审计日志进行分析，形成审计报表； | 符合(5分) |
| e)应保护审计进程，避免受到未预期的中断； | 仅DBA管理员可以开启关闭审计进程； | 符合(5分) |
| f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 定期查看分析数据库操作日志，备份审计日志。 | 符合(5分) |
| 剩余信息保护 | a)应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； | 引用产品测试结果，信息删除后能清除； | 符合(5分) |
| b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。 | 引用产品测试结果，信息删除后能清除。 | 符合(5分) |
| 入侵防范 | a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警； | Oracle数据库系统不适用； | 不适用 |
| b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施； | Oracle数据库系统不适用； | 不适用 |
| c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。 | 数据库安装了所需组件，但未更新了补丁，最近一次更新补丁未2016年。 | 部分符合(3分) |
| 资源控制 | a)应通过设定终端接入方式、网络地址范围等条件限制终端登录； | 数据库对访问地址进行了限制，管理核心数据库的终端不能访问互联网； | 符合(5分) |
| b)应根据安全策略设置登录终端的操作超时锁定； | 未设置登录终端的操作超时锁定； | 不符合 |
| c)应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； | 未对资源进行监控和报警，仅通过人工在重要时段进行查看； | 部分符合(3分) |
| d)应限制单个用户对系统资源的最大或最小使用限度； | 未限制单个用户对系统资源的 最大或最小使用度； | 不符合 |
| e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。 | 未对资源进行监控和报警，仅通过人工在重要时段进行查看。 | 部分符合(3分) |

### A.3.5 默认数据库（postgresql、Mongo）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 门户网站数据库 | 身份鉴别 | a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别； | 数据库系统对登录用户进行身份标识和鉴别 | 符合(5分) |
| b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 密码长度14位，由数字和字符组成，密码更换周期42天 | 符合(5分) |
| c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | 连续6次登录失败没有采取任何措施 | 不符合 |
| d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 使用默认客户端对服务器进行远程管理 | 符合(5分) |
| e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性； | 数据库只有一个管理人员进行登录使用，不存在多个用户使用同一个账户情况 | 符合(5分) |
| f)应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 | 没有采用两种及两种以上身份鉴别机制 | 符合(5分) |
| 访问控制 | a)应启用访问控制功能，依据安全策略控制用户对资源的访问； | 启用访问控制功能，依据安全策略控制用户对资源的访问 | 符合(5分) |
| b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限； | 普通用户没有服务器角色，管理员用户权限分离，应用连接用户仅授予需要的最小权限 | 符合(5分) |
| c)应实现操作系统和数据库系统特权用户的权限分离； | 操作系统和数据库管理员为同一个人 | 符合(5分) |
| d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； | 重命名系统默认账户，修改账户默认口令 | 符合(5分) |
| e)应及时删除多余的、过期的帐户，避免共享帐户的存在； | 已经删除多余的、过期的账号 | 符合(5分) |
| f)应对重要信息资源设置敏感标记； | 对重要信息设置敏感标记 | 符合(5分) |
| g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 | 定义了敏感标记资源的访问策略 | 符合(5分) |
| 安全审计 | a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； | 开启审计功能，覆盖到每一个数据库用户 | 符合(5分) |
| b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； | 审计内容包括重要用户行为、系统资源的异常使用等安全相关事件 | 符合(5分) |
| c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | 审计功能包括：日期、时间、类型等 | 符合(5分) |
| d)应能够根据记录数据进行分析，并生成审计报表； | 人工定期分析审计数据，没有定期生成审计报表 | 部分符合(3分) |
| e)应保护审计进程，避免受到未预期的中断； | 对审计进程进行了保护、无法中断 | 符合(5分) |
| f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 审计记录不能删除、修改或覆盖 | 符合(5分) |
| 剩余信息保护 | a)应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； | 没有用户鉴别信息残留 | 符合(5分) |
| b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。 | 没有用户鉴别信息残留 | 符合(5分) |
| 入侵防范 | a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警； | 数据库 默认不适用 | 不适用 |
| b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施； | 数据库 默认不适用 | 不适用 |
| c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。 | 数据库仅安装最小组件，安装补丁前进行了测试验证 | 符合(5分) |
| 资源控制 | a)应通过设定终端接入方式、网络地址范围等条件限制终端登录； | 对终端的接入方式、网络地址范围进行了限制 | 符合(5分) |
| b)应根据安全策略设置登录终端的操作超时锁定； | 设置远程查询超时时间600秒 | 不符合 |
| c)应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； | 没有对数据库的性能进行监控 | 不符合 |
| d)应限制单个用户对系统资源的最大或最小使用限度； | 没有对系统资源的最大或最小使用限度进行限制，但是当前资源充分满足要求 | 不符合 |
| e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。 | 没有对数据库的性能进行监控，也没有邮箱、短信等方式进行报警 | 不符合 |

### A.3.6 MySQL数据库

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| pk-backup1数据库 | 身份鉴别 | a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别； | 所有的user的password字段不为空； | 符合(5分) |
| b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令至少20位，必须由数字，字母，特殊字符组成，且字母必须大小写区分，通过命令脚本一周进行密码修改； | 符合(5分) |
| c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | mysql默认没有该功能； | 不符合 |
| d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 通过跳板机进行远程登录数据库； | 符合(5分) |
| e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性； | 存在多个用户使用同一个账号进行管理情况； | 不符合 |
| f)应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 | 未采取两种或两种以上组合的鉴别技术对管理员身份进行鉴别，目前采取密钥方式进行身份鉴别。 | 不符合 |
| 访问控制 | a)应启用访问控制功能，依据安全策略控制用户对资源的访问； | 管理员通过命令进行用户权限表分配，远程访问的账户进行了IP限制； | 符合(5分) |
| b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限； | 授予管理员账号用户所需的最小权限，实现管理员用户权限分离； | 符合(5分) |
| c)应实现操作系统和数据库系统特权用户的权限分离； | 操作系统和数据库管理员为同一个人； | 不符合 |
| d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； | 修改root口令； | 符合(5分) |
| e)应及时删除多余的、过期的帐户，避免共享帐户的存在； | 删除多余过期账户； | 符合(5分) |
| f)应对重要信息资源设置敏感标记； | MySQL数据库默认不符合； | 符合(5分) |
| g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 | MySQL数据库默认不符合。 | 符合(5分) |
| 安全审计 | a)审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； | my.cnf 文件中有log命令行；（my.ini是windows文件） | 符合(5分) |
| b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； | my.cnf 文件中有log命令行； | 符合(5分) |
| c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | my.cnf 文件中有log命令行； | 符合(5分) |
| d)应能够根据记录数据进行分析，并生成审计报表； | 每一周对MySQL日志进行分析； | 符合(5分) |
| e)应保护审计进程，避免受到未预期的中断； | 有监管进程后台运行，审计经常中断监管进程自动启动审计进程； | 符合(5分) |
| f)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 审计日志通过本地和线上进行备份。 | 符合(5分) |
| 剩余信息保护 | a)应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； | MySQL服务器默认符合； | 符合(5分) |
| b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。 | MySQL服务器默认符合。 | 符合(5分) |
| 入侵防范 | a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警； | MySQL服务器默认不适用； | 不适用 |
| b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施； | MySQL服务器默认不适用； | 不适用 |
| c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。 | 数据库仅安装最小程序，安装最新补丁进行了验证测试。 | 符合(5分) |
| 资源控制 | a)应通过设定终端接入方式、网络地址范围等条件限制终端登录； | 对账号ip进行限制，my.cnf文件中没有限制登录用户数量； | 部分符合(3分) |
| b)应根据安全策略设置登录终端的操作超时锁定； | MySQL数据默认不符合； | 不符合 |
| c)应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； | 通过第三方开源软件zabbix进行数据库性能监控； | 符合(5分) |
| d)应限制单个用户对系统资源的最大或最小使用限度； | MySQL数据默认不符合； | 不符合 |
| e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。 | 通过第三方开源软件zabbix进行数据库性能监控。 | 符合(5分) |

## **A.4 应用安全**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 西华大学教务管理系统 | 身份鉴别 | a)应提供专用的登录控制模块对登录用户进行身份标识和鉴别； | 系统对登录用户进行身份标识和鉴别； | 符合(5分) |
| b)应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别； | 没有采用两种或两种以上组合鉴别技术对身份进行鉴别； | 不符合 |
| c)应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用； | 无法创建同名账户，标识唯一，用户口令长度至少8位，须有字母、数字及特殊符号组合； | 符合(5分) |
| d)应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | 使用不存在的用户名及任意口令和存在的用户名及错误的口令登录应用系统，会提示用户名或口令错误；连续多次登录失败后没有采取锁定账号或退出客户端等措施； | 不符合 |
| e)应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。 | 启用身份鉴别，用户身份标识唯一性检查，没有登录失败处理功能。 | 部分符合(3分) |
| 访问控制 | a)应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问； | 系统权限分离功能有效，不登录系统不可以访问功能页面url，不登录系统，直接输入下载文件的url不可以下载； | 符合(5分) |
| b)访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作； | 系统访问控制功能正常，覆盖范围包括与资源访问相关的主体、客体及他们之间的操作； | 符合(5分) |
| c)应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限； | 由专门用户管理员进行用户权限分离，权限与设置一致，无法进行越权操作，系统不存在默认账户； | 符合(5分) |
| d)应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系； | 系统维护不同管理角色，特权用户权限分离，根据最小原则进行授权，并在各用户之间形成相互制约关系； | 符合(5分) |
| e)应具有对重要信息资源设置敏感标记的功能； | 系统对重要信息资源设置敏感标记； | 符合(5分) |
| f)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 | 系统对具有敏感标记的重要信息进行严格控制，防止被非授权访问。 | 符合(5分) |
| 安全审计 | a)应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计； | 系统提供了覆盖到每个用户的安全审计功能，对重要事件都有审计记录； | 符合(5分) |
| b)应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录； | 应用系统无法删除、修改或覆盖审计记录，审计进程无法被中断，审计记录超过6个月； | 符合(5分) |
| c)审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等； | 审计记录内容包括：视频设备型号、设备名称、设备ip、设备端口、用户名、密码、备注、详细设置和删除； | 符合(5分) |
| d)应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。 | 系统可对审计记录进行统计、查询、分析，未提供生成报表功能。 | 部分符合(3分) |
| 剩余信息保护 | a)应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； | 系统关闭清除用户鉴别信息功能，退出后无法访问先前页面，无残留的用户鉴别信息； | 符合(5分) |
| b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。 | 系统内的文件、目录、和数据库记录等资源所在的存储空间，释放后分配给其他用户使用。 | 符合(5分) |
| 通信完整性 | a)应采用密码技术保证通信过程中数据的完整性。 | 网站系统不适用。 | 符合(5分) |
| 通信保密性 | a)在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证； | 使用swmanager客户端建立会话，满足加密需求； | 符合(5分) |
| b)应对通信过程中的整个报文或会话过程进行加密。 | 系统对通信过程中整个报文或会话过程进行加密。 | 符合(5分) |
| 抗抵赖 | a)应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能； | 系统审计记录较完整，且与用户数据独立，但未在第三方保存； | 部分符合(3分) |
| b)应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。 | 系统审计记录较完整，且与用户数据独立，但未在第三方保存。 | 部分符合(3分) |
| 软件容错 | a)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数据格式或长度符合系统设定要求； | 能创建1=1用户，具有防SQL注入风险； | 不符合 |
| b)应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。 | 系统未提供自动保护恢复功能，系统发生故障通过人工进行恢复。 | 部分符合(3分) |
| 资源控制 | a)当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话； | 系统不具有超时结束会话功能； | 符合(5分) |
| b)应能够对系统的最大并发会话连接数进行限制； | 系统没有设置最大并发会话连接数限制； | 不符合 |
| c)应能够对单个帐户的多重并发会话进行限制； | 系统没有限制单个用户多重并发会话数，同一用户可以同时登录操作系统； | 不符合 |
| d)应能够对一个时间段内可能的并发会话连接数进行限制； | 系统没有对一个时间段内可能的并发会话数进行限制； | 不符合 |
| e)应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额； | 系统没有设置对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额； | 不符合 |
| f)应能够对系统服务水平降低到预先规定的最小值进行检测和报警； | 未监控系统服务水平，达到阀值时没有进行报警； | 不符合 |
| g)应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。 | 系统未提供服务优先级设定功能。 | 不符合 |

## **A.5 数据安全及备份恢复**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 数据安全及备份恢复 | 数据完整性 | a)应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施； | 主要的主机操作系统、网络设备操作系统、数据库管理系统、应用系统数据在传输过程中采取了完整性保护措施，并通过MD5加密算法进行完整性保护； | 符合(5分) |
| b)应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破，并在检测到完整性错误时采取必要的恢复措施。 | 主要的主机操作系统、网络设备操作系统、数据库管理系统、应用系统数据在存储过程中采取了完整性保护措施，并通过MD5加密算法进行完整性保护。 | 符合(5分) |
| 数据保密性 | a)应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性； | 主要网络设备、主机操作系统、数据库管理系统和应用系统的管理数据、鉴别信息和重要业务数据采取加密措施实现传输保密性； | 符合(5分) |
| b)应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。 | 主要网络设备、主机操作系统、数据库管理系统和应用系统的管理数据、鉴别信息和重要业务数据采取加密措施实现存储保密性。 | 符合(5分) |
| 备份和恢复 | a)应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放； | 主要网络设备的配置文件、主机操作系统的重要信息、数据库管理系统的重要数据和应用系统的应用程序提供本地备份和恢复功能，设计文档中明确了针对主要操作系统、网络设备操作系统、数据库管理系统和应用系统配置的本地数据备份和恢复的功能和策略，备份结果与备份策略一致，完全数据备份每天一次； | 符合(5分) |
| b)应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地； | 主要网络设备的配置文件、主机操作系统的重要信息、数据库管理系统的重要数据和应用系统的应用程序未提供异地数据备份，设计文档中明确了针对主要操作系统、网络设备操作系统、数据库管理系统和应用系统配置的异地数据备份和恢复的功能和策略； | 部分符合(3分) |
| c)应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障； | 网络关键点不存在单点故障，采用冗余技术设计网络拓扑机构； | 符合(5分) |
| d)应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。 | 主要的网络设备、通信线路和数据处理系统采取硬件冗余，冗余措施有效。 | 符合(5分) |

## **A.6 安全管理制度**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 安全管理制度 | 管理制度 | a)应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等； | 已制定信息安全工作的总体方针和安全策略。明确了机构安全工作的总体目标、范围、原则和安全框架等； | 符合(5分) |
| b)应对安全管理活动中的各类管理内容建立安全管理制度； | 已对安全管理活动中的各类管理内容建立安全管理制度； | 符合(5分) |
| c)应对要求管理人员或操作人员执行的日常管理操作建立操作规程； | 对安全管理人员执行的日常管理操作建立操作规程； | 符合(5分) |
| d)应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。 | 形成有安全策略、管理制度、操作规程等构成全面的信息安全管理制度体系。 | 符合(5分) |
| 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； | 已指定四川监狱管理局网络信息处负责安全管理制度的制定； | 符合(5分) |
| b)安全管理制度应具有统一的格式，并进行版本控制； | 安全管理制度具有统一的格式，并进行版本控制； | 符合(5分) |
| c)应组织相关人员对制定的安全管理制度进行论证和审定； | 相关安全管理制度均会在制度评审会中进行论证和审定； | 符合(5分) |
| d)安全管理制度应通过正式、有效的方式发布； | 制度正式发布，有专门的发布方式； | 符合(5分) |
| e)安全管理制度应注明发布范围，并对收发文进行登记。 | 安全管理制度发布采用OA系统。 | 符合(5分) |
| 评审和修订 | a)信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定； | 四川监狱管理局网络信息处负责组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，每年评审一次； | 符合(5分) |
| b)应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。 | 定期对安全管理制度进行检查和审定，对不足的地方进行修订，每年一次。 | 符合(5分) |

## **A.7 安全管理机构**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 安全管理机构 | 岗位设置 | a)应设立信息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； | 已设立四川监狱管理局网络信息处负责信息安全管理工作，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； | 符合(5分) |
| b)应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责； | 目前设立了系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责； | 符合(5分) |
| c)应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权； | 设立了信息安全领导小组； | 符合(5分) |
| d)应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。 | 明确各部门职责分工，并将工作要求文件化。 | 符合(5分) |
| 人员配备 | a)应配备一定数量的系统管理员、网络管理员、安全管理员等； | 配备有系统管理员、网络管理员和安全管理员； | 符合(5分) |
| b)应配备专职安全管理员，不可兼任； | 配备了专职的安全管理员； | 符合(5分) |
| c)关键事务岗位应配备多人共同管理。 | 关键岗位未配备多人共同管理。 | 不符合 |
| 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； | 已制定审批事项表，明确审批部门和审批人，并对关键活动进行审批； | 符合(5分) |
| b)应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； | 对系统变更、重要操作、物理访问和系统接入等事项已建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； | 符合(5分) |
| c)应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息； | 定期审批需审批的事项，审批部门和审批人； | 符合(5分) |
| d)应记录审批过程并保存审批文档。 | 保存审批记录，并与文件要求一致。 | 符合(5分) |
| 沟通和合作 | a)应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题； | 内部机构之间以及信息安全职能部门不定期召开信息安全协调会议； | 符合(5分) |
| b)应加强与兄弟单位、公安机关、电信公司的合作与沟通； | 在日常工作中经常同电信，移动，联通，公安机关等保持合作沟通； | 符合(5分) |
| c)应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通； | 与供应商、业界专家、专业的安全公司、安全组织的进行合作与沟通； | 符合(5分) |
| d)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； | 建立了外联单位联系列表； | 符合(5分) |
| e)应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。 | 已聘请信息安全专家作为安全顾问。 | 符合(5分) |
| 审核和检查 | a)安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； | 安全管理员定期进行系统安全检查，检查内容覆盖系统运行相关管理活动； | 符合(5分) |
| b)应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； | 安全管理员定期进行系统安全检查，有检查内容及结果的记录文档； | 符合(5分) |
| c)应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报； | 保存有安全检查记录和检查报告； | 符合(5分) |
| d)应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。 | 已建立安全检查机制度，并遵照执行。 | 符合(5分) |

## **A.8 人员安全管理**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 人员安全管理 | 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； | 已设立专门的人事部门负责人员录用； | 符合(5分) |
| b)应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核； | 严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核； | 符合(5分) |
| c)应签署保密协议； | 相关人员均签署了保密协议； | 符合(5分) |
| d)应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。 | 相关人员均签署了岗位安全协议，进行信用审查，一年一次。 | 符合(5分) |
| 人员离岗 | a)应严格规范人员离岗过程，及时终止离岗员工的所有访问权限； | 人员离职办理离职手续时将终止所有访问权限； | 符合(5分) |
| b)应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； | 人员离岗时收回了身份证件、钥匙、徽章等以及机构提供的软硬件设备； | 符合(5分) |
| c)应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。 | 人员离岗需办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。 | 符合(5分) |
| 人员考核 | a)应定期对各个岗位的人员进行安全技能及安全认知的考核； | 有定期安全技能和知识的考核； | 符合(5分) |
| b)应对关键岗位的人员进行全面、严格的安全审查和技能考核； | 定期对关键岗位人员进行全面、严格的安全审查及技能考核； | 符合(5分) |
| c)应对考核结果进行记录并保存。 | 定期安全技能知识的考核，有考核结果和记录。 | 符合(5分) |
| 安全意识教育和培训 | a)应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训； | 对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，培训记录完整； | 符合(5分) |
| b)应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒； | 制定了对违反违背安全策略和规定的人员进行惩戒措施； | 符合(5分) |
| c)应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训； | 定期对信息安全基础知识、岗位操作规程等进行培训，制定了书面的培训文档； | 符合(5分) |
| d)应对安全教育和培训的情况和结果进行记录并归档保存。 | 对培训记录和结果归档保存。 | 符合(5分) |
| 外部人员访问管理 | a)应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案； | 外部人员访问受控区域前需进行书面申请，有专人陪同，方可进入受控区；机房有进出记录； | 符合(5分) |
| b)对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。 | 对外部人员访问区域进行了书面规定，并按照规定执行。 | 符合(5分) |

## **A.9 系统建设管理**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 系统建设管理 | 系统定级 | a)应明确信息系统的边界和安全保护等级； | 已经完成定级工作，定级报告已明确系统边界和安全保护等级； | 符合(5分) |
| b)应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由； | 在定级报告中明确了信息系统为某个安全保护等级的方法和理由； | 符合(5分) |
| c)应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定； | 已参照《信息系统安全保护等级定级指南》完成定级工作，系统已经备案； | 符合(5分) |
| d)应确保信息系统的定级结果经过相关部门的批准。 | 定级结果无上级主管部门的批准盖章，经过企业安全主管批准。 | 符合(5分) |
| 安全方案设计 | a)应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施； | 目前正在实施信息安全等级保护测评，安全措施会在下一步的整改阶段中进行完善； | 部分符合(3分) |
| b)应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划； | 目前正在实施信息安全等级保护测评，安全保障体系将在等级测评后的整改阶段进行规划； | 部分符合(3分) |
| c)应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件； | 安全设计方案、安全管理策略、安全建设规划文档较齐全，内容不完善； | 部分符合(3分) |
| d)应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施； | 有相关部门和测评专家对相关配套文件进行论证和审定，并出具了评审意见； | 符合(5分) |
| e)应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。 | 根据安全评测、安全评估的结果定期调整和修订，保留评审记录，记录周期和维护周期一致。 | 符合(5分) |
| 产品采购和使用 | a)应确保安全产品采购和使用符合国家的有关规定； | 由四川监狱管理局网络信息处负责采购，在采购合同有明确安全产品采购和使用符合国家的有关要求； | 符合(5分) |
| b)应确保密码产品采购和使用符合国家密码主管部门的要求； | 由四川监狱管理局网络信息处负责采购，在采购合同中明确密码产品采购和使用需符合国家密码主管部门的要求； | 符合(5分) |
| c)应指定或授权专门的部门负责产品的采购； | 由四川监狱管理局网络信息处负责采购； | 符合(5分) |
| d)应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。 | 有产品选型测试报告、候选产品名单，但没有定期更新。 | 部分符合(3分) |
| 自行软件开发 | a)应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制； | 未自行开发软件； | 不适用 |
| b)应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； | 未自行开发软件； | 不适用 |
| c)应制定代码编写安全规范，要求开发人员参照规范编写代码； | 未自行开发软件； | 不适用 |
| d)应确保提供软件设计的相关文档和使用指南，并由专人负责保管； | 未自行开发软件； | 不适用 |
| e)应确保对程序资源库的修改、更新、发布进行授权和批准。 | 未自行开发软件。 | 不适用 |
| 外包软件开发 | a)应根据开发需求检测软件质量； | 软件开发协议或相关文档中包含技术验收指标并按照该指标实施验收，有相关检测记录或报告； | 符合(5分) |
| b)应在软件安装之前检测软件包中可能存在的恶意代码； | 安装之前检测软件包中存在的恶意代码； | 符合(5分) |
| c)应要求开发单位提供软件设计的相关文档和使用指南； | 开发单位提供软件设计文档及使用指南； | 符合(5分) |
| d)应要求开发单位提供软件源代码，并审查软件中可能存在的后门。 | 开发单位未提供软件源代码，未对源代码进行审查。 | 部分符合(3分) |
| 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； | 由四川监狱管理局网络信息处负责工程的总体实施，相关部门的人员负责具体工作； | 符合(5分) |
| b)应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程； | 工程合同均制定详细的工程实施方案； | 符合(5分) |
| c)应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。 | 制定工程实施的管理制度以及对实施人员的行为规范。 | 符合(5分) |
| 测试验收 | a)应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告； | 未委托公正的第三方测试单位对系统进行安全性测试，公司自行对系统进行安全测评； | 不符合 |
| b)在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告； | 根据设计方案制定了测试验收方案； | 符合(5分) |
| c)应对系统测试验收的控制方法和人员行为准则进行书面规定； | 制定了系统测试验收的管理规范，明确控制方法和人员行为准则； | 符合(5分) |
| d)应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作； | 有专门的部门负责系统测试验收管理； | 符合(5分) |
| e)应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。 | 相关部门和人员对系统测试验收报告进行审定和签字。 | 符合(5分) |
| 系统交付 | a)应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； | 系统交付时制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； | 符合(5分) |
| b)应对负责系统运行维护的技术人员进行相应的技能培训； | 开发厂商对维护人员进行产品运维培训，并有培训记录； | 符合(5分) |
| c)应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档； | 硬件产品商和系统开发商提供相关安全手册、操作和维护手册等； | 符合(5分) |
| d)应对系统交付的控制方法和人员行为准则进行书面规定； | 制定了系统支付的管理制度； | 符合(5分) |
| e)应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。 | 有专门部门负责系统交付的管理，系统交付按照相关规定进行。 | 符合(5分) |
| 系统备案 | a)应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用； | 有专门的部门负责管理系统定级的相关材料，并有使用控制记录； | 符合(5分) |
| b)应将系统等级及相关材料报系统主管部门备案； | 无明确系统主管部门； | 不适用 |
| c)应将系统等级及其他要求的备案材料报相应公安机关备案。 | 未将系统等级及其他备案材料报公安机关备案。 | 不符合 |
| 等级测评 | a)在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改； | 该系统第一次进行等保测评； | 不适用 |
| b)应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改； | 该系统第一次进行等保测评； | 不适用 |
| c)应选择具有国家相关技术资质和安全资质的测评单位进行等级测评； | 选择的测评单位具有国家相关技术资质和安全资格； | 符合(5分) |
| d)应指定或授权专门的部门或人员负责等级测评的管理。 | 有专门的部门负责等级测评管理。 | 符合(5分) |
| 安全服务商选择 | a)应确保安全服务商的选择符合国家的有关规定； | 在服务商选择时，合同中明确要求相关服务商要有国家的相关资质； | 符合(5分) |
| b)应与选定的安全服务商签订与安全相关的协议，明确约定相关责任； | 与选定的安全服务商签订与安全相关的协议，明确约定相关责任； | 符合(5分) |
| c)应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。 | 选定的安全服务商提供技术培训和服务承诺。 | 符合(5分) |

## **A.10 系统运维管理**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 系统运维管理 | 环境管理 | a)应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理； | 指定专人对机房供配电、空调、温湿度控制等设施进行不定期维护管理； | 符合(5分) |
| b)应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理； | 指定人员负责机房安全，有机房安全管理员，有机房出入登记； | 符合(5分) |
| c)应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定； | 已建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定； | 符合(5分) |
| d)应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。 | 加强了对办公环境的保密性管理，规范了办公环境人员行为。 | 符合(5分) |
| 资产管理 | a)应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； | 编制并保存与信息系统相关的资产清单，包括重要程度和所处位置等内容； | 符合(5分) |
| b)应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为； | 已建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门,并规范资产管理和使用的行为； | 符合(5分) |
| c)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； | 对重要资产进行赋值和标识管理，不同类别产品采取不同的管理措施； | 符合(5分) |
| d)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。 | 建立信息分类文档，规定了分类标识的原则。 | 符合(5分) |
| 介质管理 | a)应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定； | 已建立介质安全管理制度，并对介质的存放环境、使用、维护和销毁作出规定； | 符合(5分) |
| b)应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理； | 对各类介质进行控制和保护，介质的存储环境有专人管理； | 符合(5分) |
| c)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，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点； | 介质的归档和查询没有记录，归档的介质没有做定期清点； | 不符合 |
| d)应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁； | 对存储介质的送出维修作了保密处理； | 符合(5分) |
| e)应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同； | 目前没有需要异地存储的介质； | 符合(5分) |
| f)应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。 | 介质进行分类和标识管理，对重要介质中的数据和软件采取加密存储。 | 符合(5分) |
| 设备管理 | a)应对信息系统相关的各种设备（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； | 由开发厂家负责设备的定期维护； | 符合(5分) |
| b)应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理； | 对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理； | 符合(5分) |
| c)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、涉外维修和服务的审批、维修过程的监督控制等； | 建立配套设施、软硬件维护方面的管理制度； | 符合(5分) |
| d)应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备)的启动/停止、加电/断电等操作； | 具备关键设备的操作指南； | 符合(5分) |
| e)应确保信息处理设备必须经过审批才能带离机房或办公地点。 | 信息处理设备必须经过审批才能带离机房或办公地点。 | 符合(5分) |
| 监控管理和安全管理中心 | a)应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存； | 对通信线路、主机、网络设备和应用软件的运行情况、网络流量等形成记录并保存； | 符合(5分) |
| b)应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施； | 未定期对检测和报警记录进行分析、评审，并形成分析报告； | 不符合 |
| c)应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。 | 有安全管理中心，能进行集中管理。 | 符合(5分) |
| 网络安全管理 | a)应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作； | 有专人对维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作进行管理； | 符合(5分) |
| b)应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定； | 建立了网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定； | 符合(5分) |
| c)应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份； | 网络设备进行过升级并在更新前对现有的重要文件进行备份； | 符合(5分) |
| d)应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补； | 未安排专人定期对网络设备进行漏洞扫描； | 不符合 |
| e)应实现设备的最小服务配置，并对配置文件进行定期离线备份； | 设备实现最小服务配置，定期对配置进行备份； | 符合(5分) |
| f)应保证所有与外部系统的连接均得到授权和批准； | 和外部系统的连接需得到主管领导的授权和批准； | 符合(5分) |
| g)应依据安全策略允许或者拒绝便携式和移动式设备的网络接入； | 有关于便携式和移动设备网络接入的相关策略，并根据策略进行控制； | 符合(5分) |
| h)应定期检查违反规定拨号上网或其他违反网络安全策略的行为。 | 未定期检查违反规定拨号上网或其他违反网络安全策略的行为。 | 不符合 |
| 系统安全管理 | a)应根据业务需求和系统安全分析确定系统的访问控制策略； | 根据业务需求和系统安全分析确定系统的访问控制策略； | 符合(5分) |
| b)应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补； | 未定期对系统进行漏洞扫描，并及时进行漏洞修补； | 不符合 |
| c)应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装； | 安装系统时更新了最新的补丁程序，后续未及时更新最新补丁，安装补丁前进行测试； | 不符合 |
| d)应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定； | 已建立系统安全管理制度，其内容符合要求描述； | 符合(5分) |
| e)应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则； | 有专门的系统管理员对系统进行管理，划分系统管理员角色，明确角色的权限和职责； | 符合(5分) |
| f)应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作； | 具有系统操作手册，详细记录操作日志； | 符合(5分) |
| g)应定期对运行日志和审计数据进行分析，以便及时发现异常行为。 | 未定期运行日志和审计数据进行分析。 | 不符合 |
| 恶意代码防范管理 | a)应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查； | 对所有员工进行防病毒意识和知识的培训； | 符合(5分) |
| b)应指定专人对网络和主机进行恶意代码检测并保存检测记录； | 未指定专人对恶意代码进行检测，并保存记录； | 部分符合(3分) |
| c)应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定； | 有恶意代码防范管理制度，内容符合要求； | 符合(5分) |
| d)应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。 | 未定期检查信息系统内恶意代码库的升级情况，没有记录。 | 不符合 |
| 密码管理 | a)应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。 | 已建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。 | 符合(5分) |
| 变更管理 | a)应确认系统中要发生的变更，并制定变更方案； | 对系统重大变更，制定了变更方案； | 符合(5分) |
| b)应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告； | 已建立变更管理制度，重要系统变更前，应向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告； | 符合(5分) |
| c)应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录； | 建立变更控制的申报和审批程序文件，文件内容覆盖全面，记录并保存； | 符合(5分) |
| d)应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。 | 有变更失败后的恢复程序文件，恢复过程经过演练。 | 符合(5分) |
| 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； | 定期备份的重要业务信息、系统数据、软件系统的相关数据； | 符合(5分) |
| b)应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范； | 已建立备份与恢复管理相关的安全管理制度，但未对备份信息的备份方式、备份频度、存储介质和保存期等进行规范； | 部分符合(3分) |
| 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，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法； | 技术核查结果系统数据定期进行备份，但未定期进行恢复测试； | 部分符合(3分) |
| d)应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存； | 有控制数据备份和恢复过程的程序文件，记录备份过程，文件保存； | 符合(5分) |
| e)应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。 | 定期测试备份介质的有效性，未定期执行恢复过程。 | 不符合 |
| 安全事件处置 | a)应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点； | 已告知用户在发现安全弱点和可疑事件时应及时报告； | 符合(5分) |
| b)应制定安全事件报告和处置管理制度，明确安全事件的类型，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； | 已制定安全事件报告和处置管理制度，明确安全事件的类型，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； | 符合(5分) |
| c)应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分； | 已根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分； | 符合(5分) |
| d)应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等； | 暂未发现引发安全事件的系统弱点； | 符合(5分) |
| e)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，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存； | 记录并保存引发安全事件的原因，记录处理过程并进行分析鉴定，制定防止再次发生的补救措施； | 符合(5分) |
| f)对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。 | 对造成系统中断和造成信息泄密的安全事件采用不同的处理程序和报告程序。 | 符合(5分) |
| 应急预案管理 | a)应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； | 在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； | 符合(5分) |
| b)应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障； | 有足够的资源支持应急预案的执行； | 符合(5分) |
| c)应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次； | 未定期对系统相关的人员进行应急预案培训； | 不符合 |
| d)应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期； | 未定期对应急预案进行演练； | 部分符合(3分) |
| e)应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。 | 对应急预案进行定期审查更新，并保留其审查记录。 | 符合(5分) |

# 二、二级系统

## **A.1物理安全**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 双流棠湖中学网络中心机房 | 物理位置的选择 | a)机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。 | 机房和办公场地满足基本的防震、防风和防雨要求。 | 符合(5分) |
| 物理访问控制 | a)机房出入口应安排专人值守，控制、鉴别和记录进入的人员； | 制定了机房管理制度；出入口未安排专人对进入人员进行身份鉴别和登记，但是有门禁系统；机房无专人值守，没有值守记录；有两个出入口； | 不符合 |
| b)需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。 | 外来人员进入机房有审批流程和相应的审批记录，对外部人员的活动范围进行限制。 | 符合(5分) |
| 防盗窃和防破坏 | a)应将主要设备放置在机房内； | 主要设备放在机房内； | 符合(5分) |
| b)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记； | 设备在机房位置固定，且进行设备标签标注，标识不易去除； | 符合(5分) |
| c)应将通信线缆铺设在隐蔽处，可铺设在地下或管道中； | 通信线缆铺设在地下走线架中； | 符合(5分) |
| d)应对介质分类标识，存储在介质库或档案室中； | 介质没有分类标识存储在档案室； | 不符合 |
| e)主机房应安装必要的防盗报警设施。 | 机房重要区域有视频监控设施，设施运行正常，有运维记录。 | 符合(5分) |
| 防雷击 | a)机房建筑应设置避雷装置； | 机房大楼有避雷针，有建筑防雷设计； | 符合(5分) |
| b)机房应设置交流电源地线。 | 有交流电源地线，并且有交流电源地线的说明。 | 符合(5分) |
| 防火 | a)机房应设置灭火设备和火灾自动报警系统。 | 机房摆放灭火器，安装火灾喷淋系统。 | 符合(5分) |
| 防水和防潮 | a)水管安装，不得穿过机房屋顶和活动地板下； | 屋顶和活动地板下无水管穿过； | 符合(5分) |
| b)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 屋顶和墙壁未出现漏水、渗透和返潮的现象； | 符合(5分) |
| c)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。 | 机房设置了挡水和排水设施。 | 符合(5分) |
| 防静电 | a)关键设备应采用必要的接地防静电措施。 | 主要设备采用了接地防静电措施。 | 符合(5分) |
| 温湿度控制 | a)机房应设置温、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。 | 一台中央空调和三台单体空调调控温度，温度和湿度满足电子信息设备的使用要求。 | 符合(5分) |
| 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； | 机房采用双电源供电； | 符合(5分) |
| b)应提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求。 | 设置了短期备用电源（UPS）且运行正常。 | 符合(5分) |
| 电磁防护 | a)电源线和通信线缆应隔离铺设，避免互相干扰。 | 机房电源线和通信线缆隔离铺设。 | 符合(5分) |

## **A.2网络安全**

### A.2.1 交换机

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 核心交换机 | 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 开启相应安全审计策略，对网络设备的运行状况、网络流量、用户行为等进行日志记录； | 符合(5分) |
| 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。 | 开启日志审计，审计记录包括事件的时间、日期、用户、事件类型和事件是否成功，能够进行溯源。 | 符合(5分) |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 口令不为空； | 符合(5分) |
| b)应对网络设备的管理员登录地址进行限制； | 指定IP和mac绑定的pc进行远程管理访问控制； | 符合(5分) |
| c)网络设备用户的标识应唯一； | 只有一个管理员账户，不在多个用户使用同一个账号情况； | 符合(5分) |
| d)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令长度至少8位，采用字符、数字和特殊字符组合，一个月定期修改； | 符合(5分) |
| e)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 登录超时时间没有限制，连续登录失败多次没有相关处置措施； | 不符合 |
| f)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 | telnet关闭，只能通过console口登录。 | 符合(5分) |

### A.2.2 网络结构

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络结构 | 结构安全 | a)应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要； | 未发现设备存在性能瓶颈，主要网络设备业务处理能力基本满足需求； | 符合(5分) |
| b)应保证接入网络和核心网络的带宽满足业务高峰期需要； | 未发现接入网络和核心网络存在瓶颈，系统采用足够的带宽和流量控制措施保证高峰期业务运行需要； | 符合(5分) |
| c)应绘制与当前运行情况相符的网络拓扑结构图； | 已绘制与当前网络结构相符的网络拓扑图，能客观反映实际网络现状的规则； | 符合(5分) |
| d)应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。 | 已根据各部门的工作职能划分了网段，包括：门户网站网段、教学楼网段、图书综合楼网段等。 | 符合(5分) |
| 访问控制 | a)应在网络边界部署访问控制设备，启用访问控制功能； | 在网络边界处部署访问控制设备（防火墙），启用访问控制功能； | 符合(5分) |
| b)应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级； | 边界处访问控制设备的访问控制规则有明确的源IP、目的IP、协议及端口，边界处的网络设备关闭了不必要的服务； | 符合(5分) |
| c)应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户； | 对VPN等拨号用户接入网络情况，对每个用户的网络访问范围进行了控制； | 符合(5分) |
| d)应限制具有拨号访问权限的用户数量。 | 对VPN等拨号用户数量进行了限制。 | 符合(5分) |
| 边界完整性检查 | a)应能够对内部网络用户私自联到外部网络的行为进行检查。 | 没有采取任何技术手段或管理措施对非法外联行为进行检查、定位和检查。 | 不符合 |
| 入侵防范 | a)应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。 | 网络边界处没有安装入侵检测设备。 | 不符合 |

## **A.3 主机安全**

### A.3.1 linux主机

### A.3.2 windows主机

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 门户网站服务器 | 身份鉴别 | a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别； | 勾选“要使用本机，用户必须输入用户名和密码”； | 符合(5分) |
| b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 密码必须符合复杂性要求已禁用，密码长度最小值6个字符，密码最短使用期限0天，密码最长使用期限0天，0个记住密码，没有勾选密码永不过期，勾选用户下次登录时必须更改密码，administrator没有勾选密码永不过期，sqlmanager 勾选密码永不过期； | 不符合 |
| c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | 账户锁定时间不适用，账户锁定阈值0次无效登录，重置账户锁定计数器不适用，采用3389远程登录； | 不符合 |
| d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 禁用telnet服务，采用3389远程登录； | 符合(5分) |
| e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。 | 不存在多个用户使用同一账户情况。 | 符合(5分) |
| 访问控制 | a)应启用访问控制功能，依据安全策略控制用户对资源的访问； | 只有一个网络管理员，未制定用户权限表； | 不符合 |
| b)应实现操作系统和数据库系统特权用户的权限分离； | 数据库和操作系统管理员为同一个人，操作系统和数据库使用不同账户登录； | 不符合 |
| c)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； | 没有重命名管理员账号Administrator，禁用了Guest账户； | 不符合 |
| d)应及时删除多余的、过期的帐户，避免共享帐户的存在。 | 删除多余过期账户。 | 符合(5分) |
| 安全审计 | a)审计范围应覆盖到服务器上的每个操作系统用户和数据库用户； | 仅开启了审核登录事件，安全设置成功、失败； | 符合(5分) |
| b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； | 仅开启了审核登录事件，安全设置成功、失败； | 部分符合(1分) |
| c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | 仅开启了审核登录事件，安全设置成功、失败； | 符合(5分) |
| d)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 仅管理员有管理审核和安全日志权限，RestrictGuestAcces键值为1。 | 符合(5分) |
| 入侵防范 | a)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。 | 安装SP2，仅开启必须服务端口，未关闭默认共享，系统安全补丁最新一次更新时间为：2018/06/28 最近检查更新时间：从未 安装更新时间：从未。 | 不符合 |
| 恶意代码防范 | a)应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库； | 安装免费版360杀毒软件； | 符合(5分) |
| b)应支持防恶意代码软件的统一管理。 | 免费版360杀毒软件不支持统一管理。 | 不符合 |
| 资源控制 | a)应通过设定终端接入方式、网络地址范围等条件限制终端登录； | 通过开启主机防火墙限制； | 符合(5分) |
| b)应根据安全策略设置登录终端的操作超时锁定； | 启用屏幕保护，未开启会话空闲时间； | 不符合 |
| c)应限制单个用户对系统资源的最大或最小使用限度。 | 未对主机cpu、内存、硬盘等状态采取监控措施，仅通过人工定期查看资源的使用情况。 | 部分符合(1分) |

### A.3.3 SQL数据库

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 门户网站数据库 | 身份鉴别 | a)应对登录操作系统和数据库系统的用户进行身份标识和鉴别； | 数据库系统对登录用户进行身份标识和鉴别； | 符合(5分) |
| b)操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | sa用户已经禁用，有TANGHU\Administrator和TZWDATASERVER\sqlmanager，勾选windows身份验证，没有勾选强制实施密码策略和强制密码过期,密码必须符合复杂性要求已禁用，密码长度最小值6个字符，密码最短使用期限0天，密码最长使用期限0天，0个记住密码； | 不符合 |
| c)应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | 登录用户没有勾选“强制实施密码策略”，账户锁定阈值0次无效登录，账户锁定时间不适用，重置账户锁定计数器不适用 | 不符合 |
| d)当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 使用默认客户端对服务器进行远程管理； | 符合(5分) |
| e)应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。 | 数据库只有一个管理人员进行登录使用，不存在多个用户使用同一个账户情况。 | 符合(5分) |
| 访问控制 | a)应启用访问控制功能，依据安全策略控制用户对资源的访问； | 启用访问控制功能，依据安全策略控制用户对资源的访问； | 符合(5分) |
| b)应实现操作系统和数据库系统特权用户的权限分离； | 系统管理员与数据库管理员是同一个人； | 不符合 |
| c)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令； | sa已经禁用； | 符合(5分) |
| d)应及时删除多余的、过期的帐户，避免共享帐户的存在。 | 删除多余账户。 | 符合(5分) |
| 安全审计 | a)审计范围应覆盖到服务器上的每个操作系统用户和数据库用户； | 登录审核中勾选了仅限失败的登录，没有勾选失败和成功的登录，选项中没有勾选启用C2审核跟踪； | 不符合 |
| b)审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； | 登录审核中勾选了仅限失败的登录，没有勾选失败和成功的登录，选项中没有勾选启用C2审核跟踪； | 不符合 |
| c)审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | 登录审核中勾选了仅限失败的登录，没有勾选失败和成功的登录，选项中没有勾选启用C2审核跟踪； | 不符合 |
| d)应保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 用户的服务器角色包括：public、sysadmin，对审计日志进行了保护。 | 符合(5分) |
| 入侵防范 | a)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。 | 系统安全补丁最新一次更新时间为：2018/06/28，安装补丁进行了测试。 | 符合(5分) |
| 资源控制 | a)应通过设定终端接入方式、网络地址范围等条件限制终端登录； | 最大并发连接数为0，允许远程连接到此服务器，仅允许管理网段用户登录数据库； | 符合(5分) |
| b)应根据安全策略设置登录终端的操作超时锁定； | 远程查询超时值600秒； | 符合(5分) |
| c)应限制单个用户对系统资源的最大或最小使用限度。 | 内存：（最小服务器内存：0，最大服务器内存：2147483647 创建索引占用的内存：0，每次查询占用的最小内存：1024）。 | 符合(5分) |

## **A.4 应用安全**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 四川省双流棠湖中学门户网站 | 身份鉴别 | a)应提供专用的登录控制模块对登录用户进行身份标识和鉴别； | 系统对登录用户进行身份标识和鉴别； | 符合(5分) |
| b)应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用； | 由管理员统一创建用户名，不能创建同名用户，密码长短至少8位，由字母且必须大小写、数字、特殊字符组合； | 符合(5分) |
| c)应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施； | 连续登录3次失败，系统提示失败，并退出系统登录页面； | 符合(5分) |
| d)应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。 | 启用身份鉴别，用户身份标识唯一性检查，具有登录失败处理功能。 | 符合(5分) |
| 访问控制 | a)应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问； | 系统权限分离功能有效，不登录系统不可以访问功能页面url，不登录系统，直接输入下载文件的url不可以下载，（在url中ID元素加入自己算法进行验证，避免无权限下载）； | 符合(5分) |
| b)访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作； | 系统访问控制功能正常，覆盖范围包括与资源访问相关的主体、客体及他们之间的操作； | 符合(5分) |
| c)应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限； | 由专门管理员进行用户权限管理，无法越权； | 符合(5分) |
| d)应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。 | 维护不同管理员角色，特权用户权限分离，用户按照最小原则授权。 | 符合(5分) |
| 安全审计 | a)应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计； | 没有专门审计功能模块，通过调用数据库记录可以查看系统登录信息； | 部分符合(1分) |
| b)应保证无法删除、修改或覆盖审计记录； | 审计记录不能删除，修改、覆盖。记录至少保存6个月，最早记录2011年04月09日； | 符合(5分) |
| c)审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。 | 审计记录包括：ip和时间，审计内容不完整。 | 部分符合(1分) |
| 通信完整性 | a)应采用校验码技术保证通信过程中数据的完整性。 | 网站系统不适用。 | 不适用 |
| 通信保密性 | a)在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证； | 使用http建立会话； | 不符合 |
| b)应对通信过程中的敏感信息字段进行加密。 | 系统对通信过程中整个报文或会话过程进行加密。 | 符合(5分) |
| 软件容错 | a)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数据格式或长度符合系统设定要求； | 输入界面提供数据有效性检验，不能创建1=1用户，没有采取有效的SQL注入、网页防篡改等措施； | 不符合 |
| b)在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施。 | 系统未提供对输入数据进行保护功能。 | 不符合 |
| 资源控制 | a)当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话； | 系统具有超时会话功能，时间设置为15分钟； | 符合(5分) |
| b)应能够对应用系统的最大并发会话连接数进行限制； | 系统通过插件IIS设置最大连接数为1000个； | 符合(5分) |
| c)应能够对单个帐户的多重并发会话进行限制。 | 系统未限制单个用户多重并发会话数。 | 不符合 |

## **A.5 数据安全及备份恢复**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 数据安全及备份恢复 | 数据完整性 | a)应能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。 | 主要的主机操作系统、网络设备操作系统、数据库管理系统、应用系统数据在传输过程中采取了完整性保护措施，并通过MD5加密算法和公司内部算法进行完整性保护。 | 符合(5分) |
| 数据保密性 | a)应采用加密或其他保护措施实现鉴别信息的存储保密性。 | 主要网络设备、主机操作系统、数据库管理系统和应用系统的管理数据、鉴别信息和重要业务数据采取加密措施实现存储保密性。 | 符合(5分) |
| 备份和恢复 | a)应能够对重要信息进行备份和恢复； | 棠湖中学第二机房进行异地备份，数据库每天进行备份，且同步备份； | 符合(5分) |
| b)应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。 | 关键的网络设备和服务器没有采取硬件冗余。 | 不符合 |

## **A.6 安全管理制度**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 安全管理制度 | 管理制度 | a)应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等； | 已制定信息安全工作的总体方针和安全策略。明确了机构安全工作的总体目标、范围、原则和安全框架等； | 符合(5分) |
| b)应对安全管理活动中重要的管理内容建立安全管理制度； | 已对安全管理活动中的各类管理内容建立安全管理制度； | 符合(5分) |
| c)应对安全管理人员或操作人员执行的重要管理操作建立操作规程。 | 对安全管理人员执行的日常管理操作建立操作流程。 | 符合(5分) |
| 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； | 已指定四川省双流棠湖中学信息中心负责安全管理制度的制定； | 符合(5分) |
| b)应组织相关人员对制定的安全管理制度进行论证和审定； | 相关安全管理制度均会在制度评审会中进行论证和审定； | 符合(5分) |
| c)应将安全管理制度以某种方式发布到相关人员手中。 | 制度正式发布，有专门的发布方式。 | 符合(5分) |
| 评审和修订 | a)应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。 | 四川省双流棠湖中学信息中心负责组织，相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，每年评审一次，没有保留评审记录。 | 部分符合(2分) |

## **A.7 安全管理机构**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 安全管理机构 | 岗位设置 | a)应设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； | 已设立四川省双流棠湖中学信息中心负责信息安全管理工作，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； | 符合(5分) |
| b)应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。 | 目前设立了系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责。 | 符合(5分) |
| 人员配备 | a)应配备一定数量的系统管理员、网络管理员、安全管理员等； | 配备有系统管理员、网络管理员和安全管理员； | 符合(5分) |
| b)安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。 | 未配备专职的安全管理员。 | 不符合 |
| 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部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批； | 已制定审批事项表，明确审批部门和审批人，并对关键活动进行审批； | 符合(5分) |
| b)应针对关键活动建立审批流程，并由批准人签字确认。 | 对系统变更、重要操作、物理访问和系统接入等事项已建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。 | 符合(5分) |
| 沟通和合作 | a)应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通； | 内部机构之间以及信息安全职能部门未定期召开信息安全协调会议； | 不符合 |
| b)应加强与兄弟单位、公安机关、电信公司的合作与沟通。 | 在日常工作中经常同电信，移动，联通，公安机关等保持合作沟通。 | 符合(5分) |
| 审核和检查 | a)安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 | 安全管理员未定期进行系统安全检查，检查内容覆盖系统运行相关管理活动，没有保存记录文档。 | 不符合 |

## **A.8 人员安全管理**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 人员安全管理 | 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； | 已设立专门的人事部门负责人员录用； | 符合(5分) |
| b)应规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核； | 严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核； | 符合(5分) |
| c)应签署保密协议。 | 相关人员均签署了保密协议。 | 符合(5分) |
| 人员离岗 | a)应规范人员离岗过程，及时终止离岗员工的所有访问权限； | 人员离职办理离职手续时将终止所有访问权限； | 符合(5分) |
| b)应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； | 人员离岗时收回了身份证件、钥匙、徽章等以及机构提供的软硬件设备； | 符合(5分) |
| c)应办理严格的调离手续。 | 人员离岗需办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。 | 符合(5分) |
| 人员考核 | a)应定期对各个岗位的人员进行安全技能及安全认知的考核。 | 没有定期安全技能和知识的考核。 | 不符合 |
| 安全意识教育和培训 | a)应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训； | 对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，没有培训记录； | 部分符合(2分) |
| b)应告知人员相关的安全责任和惩戒措施， 并对违反违背安全策略和规定的人员进行惩戒； | 制定了对违反违背安全策略和规定的人员进行惩戒措施； | 符合(5分) |
| c)应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训。 | 未定期对信息安全基础知识、岗位操作规程等进行培训，未制定了书面的培训文档，未记录。 | 部分符合(2分) |
| 外部人员访问管理 | a)应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。 | 外部人员访问受控区域前需进行书面申请，有专人陪同，方可进入受控区；机房有进出记录。 | 符合(5分) |

## **A.9 系统建设管理**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 系统建设管理 | 系统定级 | a)应明确信息系统的边界和安全保护等级； | 已经完成定级工作，定级报告已明确系统边界和安全保护等级； | 符合(5分) |
| b)应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由； | 在定级报告中明确了信息系统为某个安全保护等级的方法和理由； | 符合(5分) |
| c)应确保信息系统的定级结果经过相关部门的批准。 | 定级结果无上级主管部门的批准盖章，有学校安全主管的批准。 | 符合(5分) |
| 安全方案设计 | a)应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施； | 目前正在实施信息安全等级保护测评，安全措施会在下一步的整改阶段中进行完善； | 部分符合(2分) |
| b)应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案； | 目前正在实施信息安全等级保护测评，安全方案会在下一步的整改阶段中进行完善； | 部分符合(2分) |
| c)应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案； | 目前正在实施信息安全等级保护测评，安全建设和产品采购在下一步的整改阶段中进行完善； | 部分符合(2分) |
| d)应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。 | 有相关部门和测评专家对相关配套文件进行论证和审定，并出具了评审意见。 | 符合(5分) |
| 产品采购和使用 | a)应确保安全产品采购和使用符合国家的有关规定； | 由四川省双流棠湖中学信息中心负责采购，在采购合同有明确安全产品采购和使用符合国家的有关要求，防火墙不具备销售许可资质； | 不符合 |
| b)应确保密码产品采购和使用符合国家密码主管部门的要求； | 由四川省双流棠湖中学信息中心负责采购，在采购合同中明确密码产品采购和使用需符合国家密码主管部门的要求； | 符合(5分) |
| c)应指定或授权专门的部门负责产品的采购。 | 由四川省双流棠湖中学信息中心负责采购。 | 符合(5分) |
| 自行软件开发 | a)应确保开发环境与实际运行环境物理分开； | 软件开发和系统运行环境隔离，开发人员和测试人员分开，测试数据得到保护； | 符合(5分) |
| b)应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； | 制定软件开发制度，制度内容完善； | 符合(5分) |
| c)应确保提供软件设计的相关文档和使用指南，并由专人负责保管。 | 有软件设计文档和使用指南。 | 符合(5分) |
| 外包软件开发 | a)应根据开发要求检测软件质量； | 自行软件开发 | 不适用 |
| b)应确保提供软件设计的相关文档和使用指南； | 自行软件开发 | 不适用 |
| c)应在软件安装之前检测软件包中可能存在的恶意代码； | 自行软件开发 | 不适用 |
| d)应要求开发单位提供软件源代码，并审查软件中可能存在的后门。 | 自行软件开发 | 不适用 |
| 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； | 由四川省双流棠湖中学信息中心负责工程的总体实施，相关部门的人员负责具体工作； | 符合(5分) |
| b)应制定详细的工程实施方案，控制工程实施过程。 | 工程合同均制定详细的工程实施方案。 | 符合(5分) |
| 测试验收 | a)应对系统进行安全性测试验收； | 未委托公正的第三方测试单位对系统进行安全性测试； | 不符合 |
| b)在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告； | 根据设计需求制定了测试验收方案； | 符合(5分) |
| c)应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。 | 有专门的部门负责系统测试验收管理。 | 符合(5分) |
| 系统交付 | a)应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； | 系统交付时制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； | 符合(5分) |
| b)应对负责系统运行维护的技术人员进行相应的技能培训； | 学校对维护人员进行产品运维培训，并有培训记录； | 符合(5分) |
| c)应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。 | 硬件产品商和系统开发商提供相关安全手册、操作和维护手册等。 | 符合(5分) |
| 安全服务商选择 | a)应确保安全服务商的选择符合国家的有关规定； | 在服务商选择时，合同中明确要求相关服务商要有国家的相关资质； | 符合(5分) |
| b)应与选定的安全服务商签订与安全相关的协议，明确约定相关责任； | 与选定的安全服务商签订与安全相关的协议，明确约定相关责任； | 符合(5分) |
| c)应确保选定的安全服务商提供技术支持和服务承诺，必要的与其签订服务合同。 | 选定的安全服务商提供技术培训和服务承诺。 | 符合(5分) |

## **A.10 系统运维管理**

| **测评对象** | **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- | --- |
| 系统运维管理 | 环境管理 | a)应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理； | 指定专人对机房供配电、空调、温湿度控制等设施进行不定期维护管理； | 符合(5分) |
| b)应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理； | 没有配备机房安全管理员； | 不符合 |
| c)应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定； | 建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定； | 符合(5分) |
| d)应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。 | 加强了对办公环境的保密性管理，规范了办公环境人员行为。 | 符合(5分) |
| 资产管理 | a)应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； | 编制并保存与信息系统相关的资产清单，包括重要程度和所处位置等内容； | 符合(5分) |
| b)应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。 | 已建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。 | 符合(5分) |
| 介质管理 | a)应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理； | 对各类介质进行控制和保护，介质的存储环境有专人管理； | 符合(5分) |
| b)应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点； | 介质的归档和借出有记录，存档介质做定期盘点； | 符合(5分) |
| c)应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏； | 对存储介质的送出维修作了保密处理。 | 符合(5分) |
| d)应根据所承载数据和软件的重要程度对介质进行分类和标识管理。 | 介质进行分类和标识管理，对重要介质中的数据和软件采取加密存储。 | 符合(5分) |
| 设备管理 | a)应对信息系统相关的各种设备（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； | 由开发厂家负责设备的定期维护； | 符合(5分) |
| b)应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理； | 对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理； | 符合(5分) |
| c)应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备)的启动/停止、加电/断电等操作； | 具备关键设备的操作指南； | 符合(5分) |
| d)应确保信息处理设备必须经过审批才能带离机房或办公地点。 | 信息处理设备必须经过审批才能带离机房或办公地点。 | 符合(5分) |
| 网络安全管理 | a)应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作； | 有专人对维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作进行管理； | 符合(5分) |
| b)应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定； | 建立了网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定； | 符合(5分) |
| c)应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份； | 网络设备进行过升级并在更新前对现有的重要文件进行备份； | 符合(5分) |
| d)应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补； | 未安排专人定期对网络设备进行漏洞扫描； | 不符合 |
| e)应对网络设备的配置文件进行定期备份； | 设备实现最小服务配置，定期对配置进行备份； | 符合(5分) |
| f)应保证所有与外部系统的连接均得到授权和批准。 | 和外部系统的连接需得到主管领导的授权和批准。 | 符合(5分) |
| 系统安全管理 | a)应根据业务需求和系统安全分析确定系统的访问控制策略； | 根据业务需求和系统安全分析确定系统的访问控制策略； | 符合(5分) |
| b)应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补； | 未定期对系统进行漏洞扫描，并及时进行漏洞修补 | 不符合 |
| c)应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装； | 安装系统时更新了最新的补丁程序，后续未及时更新最新补丁，安装补丁前进行测试； | 符合(5分) |
| d)应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定； | 已建立系统安全管理制度，其内容符合要求描述； | 符合(5分) |
| e)应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作； | 具有系统操作手册，详细记录操作日志； | 符合(5分) |
| f)应定期对运行日志和审计数据进行分析，以便及时发现异常行为。 | 未定期对运行日志和审计数据进行分析。 | 不符合 |
| 恶意代码防范管理 | a)应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查； | 没有对所有员工进行防病毒意识和知识的培训； | 不符合 |
| b)应指定专人对网络和主机进行恶意代码检测并保存检测记录； | 未指定专人对恶意代码进行检测； | 不符合 |
| c)应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。 | 依据规定进行对防恶意代码软件的授权使用、恶意代码库升级，但未定期汇报。 | 不符合 |
| 密码管理 | a)应使用符合国家密码管理规定的密码技术和产品。 | 已建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。 | 符合(5分) |
| 变更管理 | a)应确认系统中要发生的重要变更，并制定相应的变更方案； | 对系统重大变更，制定了变更方案； | 符合(5分) |
| b)系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。 | 系统变更需主管领导审批。 | 符合(5分) |
| 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； | 定期备份的重要业务信息、系统数据、软件系统的相关数据； | 符合(5分) |
| 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； | 已建立备份与恢复管理相关的安全管理制度，但未对备份信息的备份方式、备份频度、存储介质和保存期等进行规范； | 部分符合(2分) |
| c)应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。 | 技术核查结果系统数据定期进行备份，但未定期进行恢复测试。 | 部分符合(2分) |
| 安全事件处置 | a)应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点； | 已告知用户在发现安全弱点和可疑事件时应及时报告； | 符合(5分) |
| b)应制定安全事件报告和处置管理制度，明确安全事件类型，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； | 已制定安全事件报告和处置管理制度，明确安全事件的类型，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； | 符合(5分) |
| c)应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分； | 已根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分； | 符合(5分) |
| d)应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。 | 记录并保存引发安全事件的原因，记录处理过程并进行分析鉴定，制定防止再次发生的补救措施。 | 符合(5分) |
| 应急预案管理 | a)应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； | 在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容； | 符合(5分) |
| b)应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。 | 未定期对系统相关的人员进行应急预案培训。 | 不符合 |