文件编号：SECPT-2020132-DJCP-ZGJY

**邯郸市生态环境局在线监测**

**信息系统安全等级保护**

**整 改 建 议**

**河北赛克普泰计算机咨询服务有限公司**

**2020年08月21日**

# 保密申明

本文件包含了来自于河北赛克普泰计算机咨询服务有限公司可靠、权威的信息，这些信息作为邯郸市生态环境局正在实施的等保测评项目专用。

接受本文件，表示同意对其内容保密，未经河北赛克普泰计算机咨询服务有限公司书面授权认可，不得复制、泄露或散布这份文件。如果您不是有意接受者，请注意，对这份文件内容的任何形式的泄露、复制或散布都是被禁止的。

# 文档信息表

|  |
| --- |
| **文档基本信息** |
| **项目名称** | 邯郸市生态环境局等保测评项目 |
| **文档名称** | 邯郸市生态环境局信息系统安全等级保护整改建议 |
| **文档版本** | V1.0 | **是否为正式交付件** | 是 |
| **文档创建日期** | 2020.8.17 | **当前修订日期** | 2020.8.21 |
| **保密级别** | 商密 | **文档审批要求** | 是 |
| **文档审阅信息** |
| **审阅人** | **项目角色** | **审阅时间** | **审阅意见** |
| 王蕴芳 | 项目经理 | 2020.8.21 | 正式提交客户审阅 |
| **文档批准信息** |
| **批准人** | **项目角色** | **批准时间** | **批准意见** |
| 陈志宾 | 质量监督 | 2020.8.21 | 批准 |
| **文档创建信息** |
| **版本** | **修正章节** | **日期** | **作者** | **变更记录** |
| V1.0 |  | 2020.8.21 | 翟羽佳、王蕴芳 | 创建文档 |
|  |  |  |  |  |
|  |  |  |  |  |
| **客户确认信息** |
| 客户签字 |  | 日期 |  |

**目 录**

[保密申明 I](#_Toc48920756)

[文档信息表 II](#_Toc48920757)

[内容简介 VI](#_Toc48920758)

[安全提示 VII](#_Toc48920759)

[1 现状及整改建议 8](#_Toc48920760)

[1.1 安全物理环境-机房 8](#_Toc48920761)

[1.2 安全通信网络 8](#_Toc48920762)

[1.3 安全区域边界 10](#_Toc48920763)

[1.4 安全计算环境 12](#_Toc48920764)

[1.4.1 网络设备和安全设备 12](#_Toc48920765)

[1.4.2 服务器和数据库 17](#_Toc48920766)

[1.4.3 应用系统 31](#_Toc48920767)

[1.5 安全管理中心 41](#_Toc48920768)

[1.6 安全管理制度 44](#_Toc48920769)

[1.7 安全管理机构 44](#_Toc48920770)

[1.8 人员安全管理 46](#_Toc48920771)

[1.9 系统建设管理 48](#_Toc48920772)

[1.10 系统运维管理 52](#_Toc48920773)

[2 技术修补 56](#_Toc48920774)

[2.1 设备整改采购清单 56](#_Toc48920775)

[附录一：安全加固参考 59](#_Toc48920776)

[一、 windows服务器 59](#_Toc48920777)

[1 <身份鉴别> 59](#_Toc48920778)

[1.1 配置密码策略 59](#_Toc48920779)

[1.2 配置账户锁定策略 60](#_Toc48920780)

[1.3 更改远程桌面管理端口号 61](#_Toc48920781)

[1.4 实现双因子身份认证 62](#_Toc48920782)

[2 <访问控制> 63](#_Toc48920783)

[2.1 修改系统默认账号 63](#_Toc48920784)

[2.2 审计账号配置 63](#_Toc48920785)

[3 <安全审计> 64](#_Toc48920786)

[3.1 审核策略设置 64](#_Toc48920787)

[3.2 配置日志审计系统 65](#_Toc48920788)

[3.3 部署网络/数据库安全审计系统 66](#_Toc48920789)

[4 <剩余信息保护> 66](#_Toc48920790)

[4.1 开机清除虚拟页面 66](#_Toc48920791)

[4.2 交互式登录不显示上次用户名 67](#_Toc48920792)

[5 <入侵防范> 67](#_Toc48920793)

[5.1 开启系统防火墙 67](#_Toc48920794)

[5.2 部署入侵检测系统(IDS） 68](#_Toc48920795)

[5.3 部署漏洞扫描系统 68](#_Toc48920796)

[5.4 系统补丁更新 68](#_Toc48920797)

[5.5 关闭默认共享 69](#_Toc48920798)

[5.6 关闭多余服务（可选） 70](#_Toc48920799)

[6 <恶意代码防范> 70](#_Toc48920800)

[6.1 安装杀毒软件 71](#_Toc48920801)

[7 <资源控制> 71](#_Toc48920802)

[7.1 监控服务器资源状态 71](#_Toc48920803)

[7.2 配置屏幕保护程序 71](#_Toc48920804)

[二、 CentOS7服务器 72](#_Toc48920805)

[1 <身份鉴别> 72](#_Toc48920806)

[1.1 配置账户密码策略 72](#_Toc48920807)

[1.2 配置登录失败处理策略 74](#_Toc48920808)

[1.3 实现双因子身份认证 76](#_Toc48920809)

[2 <访问控制> 76](#_Toc48920810)

[2.1 修改UMASK值 76](#_Toc48920811)

[2.2 设置关键目录的权限 77](#_Toc48920812)

[2.3 为不同的管理员分配不同的账号 77](#_Toc48920813)

[2.4 锁定系统无用账户 78](#_Toc48920814)

[3 <安全审计> 78](#_Toc48920815)

[3.1 配置日志审计功能 79](#_Toc48920816)

[3.2 记录设备相关安全事件 79](#_Toc48920817)

[3.3 配置日志服务器 82](#_Toc48920818)

[3.4 部署网络/数据库安全审计系统 82](#_Toc48920819)

[4 <入侵防范> 83](#_Toc48920820)

[4.1 配置防火墙 83](#_Toc48920821)

[4.2 部署入侵检测系统(IDS) 84](#_Toc48920822)

[4.3 部署漏洞扫描系统 84](#_Toc48920823)

[4.4 关闭无用服务 84](#_Toc48920824)

[4.5 系统补丁更新 86](#_Toc48920825)

[5 <恶意代码防范> 87](#_Toc48920826)

[5.1 安装杀毒软件 87](#_Toc48920827)

[6 <资源控制> 87](#_Toc48920828)

[6.1 设置访问控制列表 87](#_Toc48920829)

[6.2 设置登录超时时间 88](#_Toc48920830)

[6.3 限制用户对资源的访问 89](#_Toc48920831)

[三、 H3C设备-相关配置策略 90](#_Toc48920832)

[1 <访问控制> 90](#_Toc48920833)

[1.1 ARP绑定 90](#_Toc48920834)

[2 <安全审计> 92](#_Toc48920835)

[2.1 配置日志审计系统 92](#_Toc48920836)

[3 <网络设备防护> 94](#_Toc48920837)

[3.1 限制设备登录地址 94](#_Toc48920838)

[3.2 配置口令复杂度策略 95](#_Toc48920839)

[3.3 开启登录失败处理功能 96](#_Toc48920840)

[3.4 开启闲置超时时间 97](#_Toc48920841)

[3.5 远程管理防窃听 98](#_Toc48920842)

[3.6 权限分离控制 99](#_Toc48920843)

# 内容简介

我机构于2020年08月5日至2020年08月6日开展了邯郸市生态环境局在线监测系统等保测评项目现场测评工作，本文档为依照《信息安全技术信息系统安全等级保护基本要求》GB/T 22239-2019，对委托方信息系统进行现场访谈、检查与测试后整理而成。内容为与标准不符项的现状、符合程度及整改参考建议，其中包括配置加固及设备差距分析。

本文档目标读者为委托方信息安全相关的决策、规划、管理和执行人员。

# 安全提示

**由于安全加固实施过程中会涉及修改系统配置等操作，为避免安全加固实施过程中对业务系统产生影响，建议实施人员在加固操作前进行完善的系统备份工作，或者在模拟本单位实际生产环境的测试环境中测试安全加固建议的参考操作步骤是否适用于本单位实际环境。为保证业务系统正常运行，可仅进行适用于本单位实际情况的安全加固。**

# 现状及整改建议

## 安全物理环境-机房

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| **防火** | c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 | 机房未划分区域管理，未采取防火隔离措施。 | 不符合 | 建议按照不同等级系统的安全需求、功能和特性划分区域进行管理，区域与区域间采用物理方式隔断设置物理访问控制措施，并在重要区域前设置过渡区域，进行物品交付或设备安装前的存放等。 | * 是
* 否
 |  |
| **防水和防潮** | 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； | 机房配置了专用精密空调防止水蒸气结露。用水设备四周未设置挡水、排水设施。 | 部分符合 | 建议在空调设备及可能出现漏水隐患的区域周边增设防水堤，以降低因漏水、积水对信息设备造成的影响。 | * 是
* 否
 |  |
| **防静电** | b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 | 机房未配备静电消除器。 | 不符合 | 建议机房使用静电消除器、防静电手环等设施，避免机房中有静电隐患。 | * 是
* 否
 |  |
| **电力供应** | c)应设置冗余或并行的电力电缆线路为计算机系统供电。 | 机房采用单路市电进行电力供应。 | 不符合 | 建议为机房配备双路供电通道。 | * 是
* 否
 |  |
| **电磁****防护** | b）应对关键设备实施电磁屏蔽。 | 机房未配备电磁屏蔽装置。 | 不符合 | 建议关键设备和磁介质存放在具有电磁屏蔽的机柜内，防止电磁信号的泄漏，同时防止外界的电磁干扰导致设备的不正常运行或数据丢失，从而造成系统误算或死机现象。 | * 是
* 否
 |  |

## 安全通信网络

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| **网络架构** | e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。 | 经检查,关键网络设备、计算设备硬件、关键安全设备未实现硬件冗余。 | 不符合 | 建议关键网络设备、计算设备硬件、关键安全设备采用冗余架构设计。 | * 是
* 否
 |  |
| **通信传输** | a）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； | 1）主要网络设备、主要主机操作系统、主要数据库管理系统的管理数据和重要业务数据未采用密码技术实现传输完整性； 2）主要网络设备、主要主机操作系统、主要数据库管理系统、主要应用系统的鉴别数据采用SSH或HTTPS的方式实现传输完整性。 | 部分符合 | 建议对重要数据采用经国家密码主管部门认可的密码技术，保证其在通信过程中数据的完整性。 | * 是
* 否
 |  |
| b）应采用密码技术保证通信过程中数据的保密性。 | 1）主要网络设备、主要主机操作系统、主要数据库管理系统的管理数据和重要业务数据未采用加密或其他措施实现传输保密性；2）主要网络设备、主要主机操作系统、主要数据库管理系统、主要应用系统的鉴别数据采用SSH或HTTPS的方式实现传输保密性。 | 部分符合 | 建议对系统管理数据、鉴别信息及重要业务数据采用经国家密码主管部门认可的密码技术，保证其在通信过程中数据的保密性。 | * 是
* 否
 |  |
| **可信验证** | a) 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。 | 未部署可信验证设备。 | 不符合 | 建议部署可信验证设备，将关键系统、应用纳入可信验证体系，在通信设备的可信性遭到破坏时及时报警并将验证结果输送至安全管理中心。 | * 是
* 否
 |  |

## 安全区域边界

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| **边界防护** | b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 经检查，系统未部署准入系统，不可以对终端进行准入控制和行为检查。 | 不符合 | 建议采用技术手段和管理措施对非法接入行为进行检查，防止非授权设备私自联入网络，进行非法访问。常用的技术手段包括部署网络准入系统，在终端安装管理软件，对网络接入设备和客户端进行集中管理，对发现的非法接入设备进行阻断并可形成报告确定发生非法接入的接入设备。关闭网络设备未使用的端口且对使用中的端口进行IP/MAC地址绑定等。 | * 是
* 否
 |  |
| c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 经检查，系统未部署终端安全管理软件，不能够对内部用户非授权联到外部网络的行为进行检查和限制。 | 不符合 | 建议采用内网安全管理系统的非法外联监控功能或非法外联软件实现对非法外联设备接入其他网络的阻断，并可形成报表报告其终端位置。防止内部用户私自联接到外部非受控网络感染病毒木马导致敏感信息泄露。 | * 是
* 否
 |  |
| **入侵防范** | c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 未部署抗APT攻击/网络分析系统/网络回溯系统/威胁情报检测系统等。 | 不符合 | 建议在网络中部署抗APT攻击系统，实现对新型攻击行为的检测和防护。 | * 是
* 否
 |  |
| d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 1）经检查，相关具有入侵防范功能的设备日志记录了攻击源IP、攻击类型、攻击目标、攻击时间等信息；2）相关设备未开启报警功能。 | 部分符合 | 建议对防火墙、IPS等设备的配置和设备状态进行检查和调整，使其可以对网络入侵攻击行为进行检测记录并及时向管理员进行报警。(可使用短信猫、邮件、微信等方式报警) | * 是
* 否
 |  |
| **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； | 未部署网络审计系统，不能对系统中重要用户行为和重要安全事件进行审计。 | 不符合 | 建议部署网络审计系统，对系统中重要用户行为和重要安全事件进行审计。 | * 是
* 否
 |  |
| d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 1）未部署网络审计系统，不能够对远程访问的用户行为进行单独审计。2）已部署上网行为管理设备，可对访问互联网的用户行为进行单独审计。 | 部分符合 | 建议部署网络审计系统，对远程访问的用户行为进行单独审计。 | * 是
* 否
 |  |
| **恶意代码和垃圾邮件防范** | a)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。 | 网络边界处未部署防恶意代码产品。 | 不符合 | 建议在网络边界处部署防恶意代码产品。 | * 是
* 否
 |  |
| **可信验证** | a) 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。 | 经检查，未部署可信验证设备，无法实现系统、应用等程序的可信验证。 | 不符合 | 建议部署可信验证设备，将关键系统、应用纳入可信验证体系，在边界设备的可信性遭到破坏时及时报警并将验证结果输送至安全管理中心。 | * 是
* 否
 |  |

## 安全计算环境

### 网络设备和安全设备

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别** | 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； | 部分设备未使用HTTPS、SSH方式进行远程管理。（核心交换机、汇聚交换机、连省路由器） | 部分符合 | 建议网络设备和安全设备关闭Telnet、HTTP远程管理方式，采用SSH、HTTPS远程管理方式。 | * 是
* 否
 |  |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 网络设备和安全设备仅使用用户名＋口令的方式对用户进行身份鉴别，未采用两种或两种以上组合的鉴别技术。 | 不符合 | 建议网络设备和安全设备采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户身份进行鉴别。 | * 是
* 否
 |  |
| **访问控制** | b)应重命名或删除默认账户，修改默认账户的默认口令； | 未重命名或删除默认账户，但修改了默认账户的默认口令。 | 不符合 | 建议网络设备和安全设备删除默认账户，或重命名默认账户。 | * 是
* 否
 |  |
| 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； | 部分网络设备和安全设备未设不同权限的管理员账号，未实现特权用户的权限分离。（核心交换机、汇聚交换机、连省路由器、东软防火墙） | 部分符合 | 建议对网络设备和安全设备进行角色划分，划分为系统管理员，安全管理员、审计管理员等角色。 | * 是
* 否
 |  |
| **入侵防范** | b)应关闭不需要的系统服务、默认共享和高危端口； | 部分网络设备开启了无非必要的高危端口（http、telnet等）。（核心交换机、汇聚交换机、连省路由器） | 部分符合 | 建议根据实际网络环境关闭网络设备不必要的服务。执行如下命令关闭域名解析功能undo dns resolve CDP、DNS lookup、DHCP、finger、udp-small-server、tcp-small-server、http、bootp、IP源路由、PAD等服务视情况选择性关闭。 | * 是
* 否
 |  |
| 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； | 网络设备和安全设备未限制远程登陆的管理地址。 | 不符合 | 建议网络设备和安全设备对远程登陆主机IP进行限制。 | * 是
* 否
 |  |
| 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； | 未定期进行漏洞扫描，未定期进行版本升级。 | 不符合 | 建议网络设备和安全设备定期进行漏洞扫描并在经过充分测试评估后及时修补漏洞。 | * 是
* 否
 |  |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 1）经检查，相关具有入侵防范功能的设备日志记录了攻击源IP、攻击类型、攻击目标、攻击时间等信息； 2）相关设备不具有实时报警功能。 | 部分符合 | 建议对防火墙、IPS等设备的配置和设备状态进行检查和调整，使其可以对网络入侵攻击行为进行检测记录并及时向管理员进行报警。(可使用短信猫、邮件、微信等方式报警) | * 是
* 否
 |  |
| **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 | 未部署可信验证设备。 | 不符合 | 建议部署可信验证设备。 | * 是
* 否
 |  |
| **数据完整性** | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 1）经检查，未采用密码技术保证重要业务数据、审计数据在传输过程中的完整性；2）使用SSH、HTTPS协议保证了鉴别数据在传输过程中的完整性。 | 部分符合 | 建议采用校验技术或密码技术保证重要数据在传输过程中的完整性。 | * 是
* 否
 |  |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 1）经检查，未采用密码技术保证重要业务数据、审计数据在存储过程中的完整性；2）鉴别数据加密存储，保证了鉴别数据在存储过程中的完整性。 | 部分符合 | 建议采用校验技术或密码技术保证重要数据在存储过程中的完整性。 | * 是
* 否
 |  |
| **数据保密性** | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 1）经检查，未采用密码技术保证重要业务数据、审计数据在传输过程中的保密性。2）使用SSH、HTTPS协议保证了鉴别数据在传输过程中的保密性。 | 部分符合 | 建议采用校验技术或密码技术保证重要数据在传输过程中的保密性。 | * 是
* 否
 |  |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 1）经检查，未部署存储加密设备。不能保证重要业务数据、审计数据在存储过程中的保密性；2）鉴别数据使用密码技术加密存储。 | 部分符合 | 建议网络设备在存储过程中对鉴别数据、重要业务数据、审计数据、配置数据等采用密码技术进行加密。可使用密码机或其他方式实现。 | * 是
* 否
 |  |
| **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； | 网络设备和安全设备未定期对设备配置进行备份。 | 不符合 | 建议网络设备和安全设备定期对重要数据进行备份，并定期进行备份文件的恢复验证测试。 | * 是
* 否
 |  |
| 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； | 未建设异地容灾机房。 | 不符合 | 建议建设异地机房，并将网络设备的重要数据进行异地实时备份。 | * 是
* 否
 |  |
| c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 网络设备和安全设备未采取冗余部署方式，不可以保证数据的高可用性。 | 不符合 | 建议采用冗余的方式部署网络设备和安全设备。 | * 是
* 否
 |  |
| **建议管理员定期查看安全设备的授权或特征库升级情况，并在设备许可到期前及时购买设备许可证，防止安全设备无法正常使用造成安全事故。** |

### 服务器和数据库

#### 1）Linux系统

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| **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；【高风险】 | 1）经检查/etc/passwd/和/etc/shadow文件，root等用户为使用状态，表示用户可直接登录，身份标识具有唯一性；查看/etc/login.defs文件：1.密码最长有效期：PASS\_MAX\_DAYS 999992.密码最短存留期：PASS\_MIN\_DAYS 03.密码长度限制：PASS\_MIN\_LEN 54.密码到期前警告期限：PASS\_WARN\_AGE 7,未对密码的有效期限进行限制； 2）经检查，查看/etc/pam.d/system-auth文件： password requisite ，未设置密码复杂度策略并对密码进行定期更换。 | 部分符合 | 1）建议运维人员经过测试后，使Linux系统实现普通用户登录系统切换到root管理员用户；2）建议Linux系统在/etc/pam.d/system-auth和/etc/login.defs文件中设置密码周期，并定期更换口令（至少一季度更换一次）。 | * 是
* 否
 |  |
| 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；【高风险】 | 1）经检查，查看/etc/pam.d/system-auth文件，未启用登录失败功能。2）经检查，未在/etc/profile等文件设置TMOUT时间参数不具有登录超时锁定机制。 | 不符合 | 1）建议在/etc/pam.d/system-auth文件设置普通用户的登录失败处理功能，防止恶意用户对口令进行猜测。2）建议在/etc/profile文件设置tmout参数，防止用户在离开服务器后被恶意用户登录。 | * 是
* 否
 |  |
| d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 1）经检查，管理员采取用户名加密码的方式进行远程连接，未使用两种及两种以上组合鉴别方式对管理员身份进行鉴别。 | 不符合 | 建议在系统中配置USB Key、动态口令等，使用两种鉴别技术对系统管理员进行身份鉴别；建议在堡垒机中进行设置，配置相关策略，仅通过堡垒机进行运维。 | * 是
* 否
 |  |
| **访问控制** | b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）经检查，查看配置文件/etc/passwd，未对root用户进行重命名，Linux系统无法修改root用户但已修改root用户的默认口令；2）经检查，未限制root用户的远程登录。 | 部分符合 | 建议在/etc/ssh/sshd\_config进行配置，限制root用户的远程登录，实现普通用户登录后切换到root管理员用户进行相关的操作。 | * 是
* 否
 |  |
| 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； | 1）经检查，查看/etc/passwd文件，不存在多余的、默认的账户，系统具有操作系统管理员用户和运维管理员用户但未建立安全管理员连接系统的账户，存在人员共享账户的情况。 | 部分符合 | 建议Linux系统设置审计员账户，对审计日志进行操作，实现审计员和管理员用户的权限分离，防止单个用户权限过大导致无法实现权限制约。 | * 是
* 否
 |  |
| 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； | 1）经检查，系统具有操作系统管理员用户和运维账户，但未建立审计管理员用户；查看/etc/sudo.conf文件，超级管理员用户权限仅限制为root，超级管理员权限分配合理；2）经检查，设置umask值为0022，未对新建用户的默认权限进行合理限制。 | 部分符合 | 建议设置Linux系统的umask值为027，防止新建用户的权限过大导致越权，建立审计员用户，实现管理用户的权限的最小化。 | * 是
* 否
 |  |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 1）经检查，未设置专门安全管理员对配置策略进行配置；2）经检查，仅由root用户设置访问控制规则，其他用户不具有该权限。 | 部分符合 | 建议建立专门安全管理员进行配置策略，防止管理员用户非授权访问其他权限模块，造成权限不能分离的情况。 | * 是
* 否
 |  |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 1）经检查，输入sestatus和sestatus -b，SElinux 状态处于disabled并且未配置安全规则，无法对重要主体设置安全标记。 | 不符合 | 建议在与运维人员沟通后，对selinux进行开启，设置安全规则对系统的重要配置文件和资源，防止非授权人员访问系统的重要信息资源。 | * 是
* 否
 |  |
| **安全审计** | 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；【高风险】 | 1）经检查，已开启审计策略，未部署日志审计系统对审计日志进行保护；2）经检查，无法查看到6个月之前的日志信息。 | 部分符合 | 1）建议建立审计员用户，专门对审计日志进行操作，防止审计日志受到未预期的删除、覆盖等操作；2）建议部署日志审计系统，对系统的日志进行备份，保证可以查看到6个月之前的日志。 | * 是
* 否
 |  |
| **入侵防范** | b）应关闭不需要的系统服务、默认共享和高危端口；【高风险】 | 经检查，系统未开启不需要的系统服务，执行iptables -L，系统未开启防火墙功能并对多余端口进行限制。 | 不符合 | 建议在与运维人员沟通后，开启防火墙并设置相关安全策略，对高危端口135，445等高危端口在操作系统层面进行关闭。 | * 是
* 否
 |  |
| 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； | 1）经检查，系统定期进行漏洞扫描，但未对漏扫报告中的高风险问题进行及时的修复；2）经检查，运行rpm -qa | grep patch，系统未及时安装补丁程序。 | 不符合 | 建议定期对系统进行漏洞扫描工作（至少一个月扫描一次），并对漏扫报告进行评估，针对高危漏洞及时修复补丁程序。 | * 是
* 否
 |  |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 1）经检查， 运行/var/log/messages |grep refused，不存在入侵痕迹；2）经检查，iptables -L，未设置防火墙策略并放行所需端口；3）经检查，已安装主机入侵检测软件并且网络中部署有ips。 | 部分符合 | 建议运维人员定期查看日志审计信息，对入侵行为及时进行处理；建议开启防火墙策略并对业务所需端口和高危端口进行相关过滤。 | * 是
* 否
 |  |
| **可信验证** | a）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。 | 经检查，操作系统未实现系统程序的可信验证功能。 | 不符合 | 建议购买可信验证产品，对Linux系统的引导程序、系统参数进行保护。 | * 是
* 否
 |  |
| **数据完整性** | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 1）经检查，linux系统采取ssh加密协议进行远程管理，可以保证鉴别数据在传输过程中的完整性；2）其他数据未采用校验码技术或密码技术进行数据传输，未采取措施对数据完整性进行校验。 | 部分符合 | 建议采用密码技术或校验技术对报文进行加密，保证数据在传输过程中的完整性。 | * 是
* 否
 |  |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经检查，鉴别信息进行加密存储，其他信息未采取密码技术或校验技术，无法保证数据在存储过程中的完整性。 | 部分符合 | 建议系统的重要业务信息、重要审计数据、配置数据采用密码技术或校验技术对报文进行加密，保证数据在存储过程中的完整性。 | * 是
* 否
 |  |
| **数据保密性** | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 1）经检查，linux系统采取ssh加密协议进行远程管理，可以保证鉴别数据在传输过程中的保密性；2）经检查，未采用密码技术保证其他数据在传输过程中的保密性。 | 部分符合 | 建议Linux系统采用密码技术来保证鉴别数据、重要业务数据和重要个人信息在传输过程中的保密性。 | * 是
* 否
 |  |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经检查，Linux系统未采用密码技术保证数据在存储过程中的保密性。 | 不符合 | 建议Linux系统采用密码技术来保证鉴别数据、重要业务数据和重要个人信息在存储过程中的保密性。 | * 是
* 否
 |  |
| **数据备份与恢复** | 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； | 经检查，未提供异地数据备份功能，并进行实时备份。 | 不符合 | 建议部署异地机房或其他异地备份机制，利用通用网络实时备份重要数据到指定地点。 | * 是
* 否
 |  |

#### 2）Windows系统

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| **身份鉴别** | d）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。 | 1）经检查，管理员采取用户名加密码的方式进行远程连接，未使用两种及两种以上组合鉴别方式对管理员身份进行鉴别。 | 不符合 | 建议在系统中配置USB Key、动态口令等，使用两种鉴别技术对系统管理员进行身份鉴别；建议在堡垒机中进行设置，配置相关策略，仅通过堡垒机进行运维。 | * 是
* 否
 |  |
| **访问控制** | b）应重命名或删除默认账户，修改默认账户的默认口令； | 经检查，未重命名administrator用户但已修改默认账户的默认口令。 | 不符合 | 建议重命名系统默认administrator用户或者禁用，重新建立系统管理员用户，防止默认用户被不法分子猜测导致系统被入侵。 | * 是
* 否
 |  |
| 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； | 经检查，系统存在管理员，已为管理用户分配所需的最小权限，但未建立审计员用户实现管理用户的权限分离。 | 部分符合 | 建议建立专门审计员用户，对审计日志进行审计，为不同用户建立不同的用户名，实现管理员用户和审计员用户的权限分离。 | * 是
* 否
 |  |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 经检查，操作系统未设置安全员对操作系统访问控制策略进行设置，仅由管理员用户进行设置，访问控制策略分配合理。 | 部分符合 | 建议建立安全员用户，配置访问控制策略权限，防止超级管理员用户对访问控制策略进行操作，实现访问控制策略规则具有唯一性。 | * 是
* 否
 |  |
| **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；（终端设备） | 经检查[开始]->[控制面板] ->[管理工具]->[本地安全策略]->[本地策略]->[审核策略]，服务器仅开启审核登录和审核账户登录事件策略，未开启全部的审核策略。 | 不符合 | 建议开启操作系统的审核策略，对系统的操作事件进行审计，使审计范围覆盖到每个操作系统用户。 | * 是
* 否
 |  |
| 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；【高风险】 | 经检查，审计记录由管理员进行保护，未建立专门的审计员账户进行管理，审计记录会备份至本地但无法查看到6个月之前的日志信息。 | 部分符合 | 建议建立审计员用户，对审计日志进行审计；建议部署日志审计系统，对审计日志进行审计，防止审计日志受到未预期的删除、修改或覆盖等。 | * 是
* 否
 |  |
| **入侵防范** | b）应关闭不需要的系统服务、默认共享和高危端口；【高风险】 | 1）经检查，未关闭系统默认共享； 2）经检查，查看[控制面板]->[管理工具]->[服务]，未关闭打印服务等系统不必要的服务； 3）经检查，操作系统未关闭不必要的端口：135，139，445端口。 | 不符合 | 建议服务器操作系统关闭默认共享；建议操作系统开启防火墙策略，关闭不必要的高危端口：135，139，445等端口。 | * 是
* 否
 |  |
| 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； | 1）经检查，系统定期进行漏洞扫描，但未对漏扫报告中的高风险问题进行及时的修复。 | 不符合 | 建议系统通过漏扫设备，定期（建议每个月）对操作系统进行漏洞扫描，及时对操作系统的状态进行评估，防止系统漏洞被利用导致出现入侵事件。 | * 是
* 否
 |  |
| **可信验证** | a）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。 | 经检查，未实现可信验证功能。 | 不符合 | 建议配置可信验证产品，对计算设备的引导程序、应用程序、重要参数等进行可信验证。 | * 是
* 否
 |  |
| **数据完整性** | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 1）经检查，windows系统采取rdp加密协议进行远程管理，可以保证鉴别数据在传输过程中的完整性；2）其他数据未采用校验码技术或密码技术进行数据传输，未采取措施对数据完整性进行校验。 | 部分符合 | 建议应用系统采取校验码技术或密码技术，对应用系统在传输过程中的数据完整性进行校验。 | * 是
* 否
 |  |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经检查，鉴别信息进行加密存储，其他信息未采取密码技术或校验技术，无法保证数据在存储过程中的完整性。 | 部分符合 | 建议应用系统采取校验码技术或密码技术，对应用系统在存储过程中的数据完整性进行校验。 | * 是
* 否
 |  |
| **数据保密性** | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 1）经检查，windows系统采取rdp加密协议进行远程管理，可以保证鉴别数据在传输过程中的保密性；2）经检查，未采用密码技术保证其他数据在传输过程中的保密性。 | 部分符合 | 建议windows系统采用密码技术来保证鉴别数据、重要业务数据和重要个人信息在传输过程中的保密性。 | * 是
* 否
 |  |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经检查，windows系统未采用密码技术保证数据在存储过程中的保密性。 | 不符合 | 建议windows系统采用密码技术来保证鉴别数据、重要业务数据和重要个人信息在存储过程中的保密性。 | * 是
* 否
 |  |
| **数据备份与恢复** | 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； | 1）经检查，未提供异地数据备份功能，并进行实时备份。 | 不符合 | 建议部署异地机房或其他异地备份机制，利用通用网络实时备份重要数据到指定地点，防止本地机房出现问题后造成数据的丢失。 | * 是
* 否
 |  |
| **剩余信息保护** | a) 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； | 1）经检查，查看管理工具-本地安全策略-安全选项，不显示上次的用户名[未启用]，系统鉴别信息所在的存储空间被释放或重新分配前无法得到完全清除。 | 不符合 | 建议执行“Win+R->运行->secpol.msc”打开本地安全策略，选择“本地安全策略->安全设置->本地策略->安全选项”将[交互式登录：不显示上次的用户名]设置为已启用。 | * 是
* 否
 |  |
| b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除； | 1）经检查，查看[本地安全策略]->[本地策略]->[安全选项]->[关机：清除虚拟内存页面文件]已禁用，系统内重要信息资源所在存储空间重新分配前无法进行清除。 | 不符合 | 建议执行“Win+R->运行->secpol.msc”打开本地安全策略，选择“本地策略-安全选项”将[关机：清除虚拟内存页面文件] 设置为已启用。 | * 是
* 否
 |  |

#### 3）SQL Server数据库

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| **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； | 1）经检查，数据库采用windows与SQL SERVER 身份验证模式；2）经检查，打开Microsoft SQL Server Management Studio,对象资源管理中——安全性——登录名。右键各个用户——属性——常规，查看所有用户外均未勾选强制实施密码策略、强制密码过期策略；3）执行命令select \* from syslogins where password is null，查询存在空口令用户；4）经访谈和检查，密码复杂度符合要求但未定期更换。 | 部分符合 | 1）建议根据需要对系统用户口令设置复杂度限制。打开SQL Server Management Studio，对象资源管理中-安全性-登录名-用户右击属性-常规，勾选强制实施密码策略、强制实施过期策略。 | * 是
* 否
 |  |
| a）应对登录的用户分配账户和权限； | 1）经访谈和检查，当前数据库使用Windows账户登录；2）经访谈和检查，未建立账户权限表。 | 不符合 | 1）建议制定用户权限表，并根据权限表进行用户权限分配；在SQL Server Management Studio，对象资源管理器中，右键服务器-属性-权限中，选中每个登录用户，设置合理的用户权限。2）建议不使用Windows账户登录，可使用sa账户。 | * 是
* 否
 |  |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 1）经检查，打开Microsoft SQL Server Management Studio,对象资源管理中——安全性——登录名，查看未修改sa账户名称；2）经访谈和检查，已修改默认口令。 | 部分符合 | 1）建议重命名sa账户：先运行代码sp\_configure 'allow updates', 1goRECONFIGURE WITH OVERRIDEgo然后再运行以下代码：update sysxlogins set name='你要改成的名字' where sid=0x01update sysxlogins set sid=0xE765555BD44F054F89CD0076A06EA823 where name='你要改成的名字'接着：sp\_configure 'allow updates', 0goRECONFIGURE WITH OVERRIDEgo | * 是
* 否
 |  |
| **访问控制** | 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； | 1）经检查，打开Microsoft SQL Server Management Studio,对象资源管理中——安全性——登录名，查看存在多余的账户plan和zhichao；2）经访谈和检查，无共享账户。 | 部分符合 | 建议删除或禁用数据库多余帐户。 | * 是
* 否
 |  |
| 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； | 1）未由不同员工分别担任操作系统管理员与数据库管理员。 | 不符合 | 建议由不同员工分别担任操作系统管理员与数据库管理员。 | * 是
* 否
 |  |
| **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； | 1）经检查，打开Microsoft SQL Server Management Studio，对象资源管理器中，右键服务器——属性——安全性，查看登录审核为“仅限失败的登录”，未勾选“启用C2审核跟踪”，数据库开启部分审计功能。 | 部分符合 | 建议提供独立的日志审计功能，对设备的配置管理操作行为、重要的业务操作等行为进行审计。打开Microsoft SQL Server Management Studio，对象资源管理器中，右键服务器-属性-安全性，设置登录审核为“失败和成功的登录”，选择勾选“启用C2审核跟踪”。 | * 是
* 否
 |  |
| 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； | 1）经访谈和检查，未对审计记录定期备份；2）经访谈和检查，未部署第三方审计工具；3）经检查，查看日志文件查看器中日志的留存时间大于六个月。 | 部分符合 | 建议对审计记录进行保护，定期备份。 | * 是
* 否
 |  |
| **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； | 经访谈和检查，数据库未遵循最小安装的原则。 | 不符合 | 建议加强数据库的管理，卸载或禁用多余的组件或服务。 | * 是
* 否
 |  |
| 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。 | 1）经访谈和检查，对操作系统进行漏扫，但不是定期；2）经访谈和检查，未定期修补漏洞。 | 部分符合 | 建议定期对数据库系统进行漏扫，对于系统中存在的已知漏洞，在经过充分测试评估后更新系统补丁，避免遭受由系统漏洞带的风险。 | * 是
* 否
 |  |
| **可信验证** | a）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。 | 对系统引导程序、系统程序、重要配置参数和应用程序等未进行可信验证。 | 不符合 | 建议在应用程序的关键环节对系统调用的主体、客体、操作进行可信验证，并对终端、关键内存区域等执行资源进行可信验证，并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。 | * 是
* 否
 |  |
| **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； | 1）经访谈和检查，对重要数据每月全量备份；2）经访谈和检查，未进行恢复性测试演练。 | 部分符合 | 建议对数据定期对备份文件进行恢复测试，确保备份文件有效。 | * 是
* 否
 |  |
| 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； | 经检查，未提供异地数据备份功能。 | 不符合 | 建议提供异地实时备份功能。 | * 是
* 否
 |  |
| **剩余信息保护** | a）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； | 系统内鉴别信息所在的内存存储空间，被释放或再分配给其他使用人员前能够得到完全清除，但硬盘存储空间无法做到完全清除。 | 部分符合 | 建议采用存储介质消除工具，可以实现对硬盘数据的清除。 | * 是
* 否
 |  |

### 应用系统

#### 1）邯郸市环境保护局污染源自动监控系统

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 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； | 1）经检查，该系统采用B/S架构部署，具有专用的登录控制模块，登录模块输入账户+密码+滑块验证，验证其信息正确后登录系统；2）经检查，每个系统用户具有唯一用户名，系统增加用户时用户名唯一，可保证用户身份标识唯一；3）经检查，系统仅要求用户密码不小于8位，但无密码复杂度的限制，不能避免设置弱口令；4）经测试，未强制要求定期更换密码。  | 部分符合 | 1）建议系统对用户鉴别信息长度、组成复杂度和更换周期进行限制，要求密码长度8位以上，由数字、字母和特殊符号混合组成，并定期修改密码（修改周期一般为三个月）； | * 是
* 否
 |  |
| 身份鉴别 | 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； | 1）经抓包测试，系统未采用密码技术传输数据，用户鉴别信息明文传输，无法防止鉴别信息在网络传输过程中被窃听。 | 不符合 | 建议系统采用HTTPS、CA证书、VPN、国密算法等密码技术防止鉴别信息在传输过程中被窃听。 | * 是
* 否
 |  |
| 身份鉴别 | d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现； | 1）经检查，系统仅采用用户名+口令+滑块鉴别技术，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 | 建议对系统采用两种或两种以上组合的鉴别技术实现用户身份鉴别，如口令、数字证书、令牌、生物技术等，且其中一种鉴别技术至少应使用密码技术来实现。 | * 是
* 否
 |  |
| 访问控制 | b) 应重命名或删除默认账户，修改默认账户的默认口令； | 1）经检查，系统存在默认管理员账户admin或administrator等，并且未修改默认账户的默认口令。 | 不符合 | 建议重命名或删除默认账户admin（administrator、sysadmin等），并修改该账户的默认口令，口令满足复杂度要求，并定期修改。 | * 是
* 否
 |  |
| 访问控制 | 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。 | 1）经检查，系统中存在超级管理用户，具有系统所有权限，未设立安全员、审计员，未实现管理用户的权限分离。 | 不符合 | 建议系统授予管理用户为完成承担任务所需的最小权限，管理用户仅需具备管理相关功能权限，同时，管理用户应实现权限分离，管理用户分为管理员、安全员和审计员；管理员仅具有系统管理、用户创建与删除、角色创建与删除等功能权限，安全员具备安全参数配置、用户权限分配等功能权限，审计员具备日志查看等功能权限。 | * 是
* 否
 |  |
| 访问控制 | g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 1）经检查，系统未提供对重要主体和客体设置安全标记的功能。 | 不符合 | 建议对重要主体（系统中管理用户）和重要客体（系统中鉴别数据、重要业务数据、个人信息以及敏感数据等）设置安全级别，高安全级别的用户才能访问到高安全级别的数据，低安全级别的管理用户只能访问到同级别及低级别的数据。（比如管理用户和重要数据均划分为1、2、3三个安全级别，安全级别3为最高级别，3安全级别的用户能够访问到1、2、3级别的数据，2级别的用户仅能访问到1、2安全级别的数据）。 | * 是
* 否
 |  |
| 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； | 1）经检查，系统未提供安全审计功能，未对重要的用户行为和重要安全事件进行审计。 | 部分符合 | 建议系统提供并启用安全审计功能，对用户登录情况、管理用户的操作行为、关键的业务操作行为等重要用户行为和安全事件进行审计，审计范围覆盖到每个用户。 | * 是
* 否
 |  |
| 安全审计 | 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； | 1）经检查，审计记录内容不全，界面仅有最后登陆时间，在后台对最后登陆时间、登陆时长、重置密码、创建时间有记录；无法完整描述审计事件。 | 部分符合 | 建议审计记录包括事件的日期和时间、发起者信息（如用户名、IP地址等）、事件类型、事件是否成功及其他与审计相关的信息。 | * 是
* 否
 |  |
| 安全审计 | 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； | 1）经检查，未对审计日志进行定期备份。 | 不符合 | 建议定期对数据库进行全量备份，并且审计记录保存半年以上。 | * 是
* 否
 |  |
| 入侵防范 | 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； | 1）经检查，系统存在高风险，未定期对应用系统进行漏洞扫描，未及时修补漏洞。 | 不符合 | 建议定期对应用系统进行漏洞扫描，在发现高风险漏洞后，在经过充分测试评估后，及时对漏洞进行修补，保证系统中不存在高风险漏洞。 | * 是
* 否
 |  |
| 可信验证 | a）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。 | 1）未对应用程序进行可信验证。 | 不符合 | 建议对应用程序进行可信验证，并在应用程序的关键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。 | * 是
* 否
 |  |
| 数据完整性 | a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 1）经抓包测试，系统未采用校验技术或密码技术保证重要数据在传输过程中的完整性，重要数据明文传输。 | 不符合 | 建议系统采用HTTPS、数字签名、VPN、国密算法等密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性，防止数据在传输过程中被篡改、窃取或破坏。 | * 是
* 否
 |  |
| 数据完整性 | b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等 | 1）系统用户密码加密存储，其他数据明文存储，未采用密码技术实现其存储完整性。 | 不符合 | 建议采用数字签名等密码技术（采用SM2、SM4等国密算法）或数据库加密系统实现重要业务数据、重要审计数据、重要配置数据、重要个人信息等重要数据在存储过程中的完整性。 | * 是
* 否
 |  |
| 数据保密性 | a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 1）经抓包测试，系统鉴别数据、重要业务数据和重要个人信息明文传输，未采用密码技术保证其在传输过程中的保密性。 | 不符合 | 建议系统采用HTTPS、CA证书、VPN、国密算法等密码技术实现鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性。 | * 是
* 否
 |  |
| 数据保密性 | b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等 | 1）经检查，鉴别数据、重要业务数据和重要个人信息等重要数据在数据库中明文存储，未采用密码技术保证其存储保密性。 | 不符合 | 建议采用SM2、SM4等密码技术或数据库加密系统实现重要业务数据、重要审计数据、重要配置数据、重要个人信息在存储过程中的保密性。 | * 是
* 否
 |  |
| 数据备份和恢复 | a) 应提供重要数据的本地数据备份与恢复功能； | 1）经检查，未定期对备份数据进行恢复测试。 | 部分符合 | 建议定期对备份数据进行恢复测试，确保备份文件的有效性；同时，应对应用软件进行版本控制，备份最新版本软件。 | * 是
* 否
 |  |
| 数据备份和恢复 | 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。 | 1）经检查，未提供异地实时备份功能，未利用通信网络将重要数据实时备份至备份场地 | 不符合 | 建议建立异地灾备机房，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，保证当本地系统发生灾难性后果（如火灾）不可恢复时，利用异地保存的数据对系统数据能进行恢复。 | * 是
* 否
 |  |
| 个人信息保护 | b) 应禁止未授权访问和非法使用用户个人信息。 | 1）经检查，只有系统管理用户才有权限进行访问用户个人信息，其余用户无此权限。未建立个人信息保护制度 | 部分符合 | 建议制定用户个人信息管理制度和流程对用户个人信息访问进行严格管理。 | * 是
* 否
 |  |

#### 2）重点污染源自动监控与基础数据库系统

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 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； | 1）经检查，该系统采用B/S架构部署，具有专用的登录控制模块，登录模块输入用户名+密码，验证其信息正确后登录系统；2）经检查，每个系统用户具有唯一用户名，系统增加用户时用户名唯一，可保证用户身份标识唯一；3）经检查，系统仅要求用户密码不小于6位，但无密码复杂度的限制，不能避免设置弱口令；4）未强制定期更换。  | 部分符合 | 1）建议系统对用户鉴别信息长度、组成复杂度和更换周期进行限制，要求密码长度8位以上，由数字、字母和特殊符号混合组成，并定期修改密码（修改周期一般为三个月）；2）建议系统中的弱密码和空口令账户修改成满足密码复杂度的口令。 | * 是
* 否
 |  |
| 身份鉴别 | 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； | 1）经抓包测试，系统未采用密码技术传输数据，用户鉴别信息明文传输，无法防止鉴别信息在网络传输过程中被窃听。 | 不符合 | 建议系统采用HTTPS、CA证书、VPN、国密算法等密码技术防止鉴别信息在传输过程中被窃听。 | * 是
* 否
 |  |
| 身份鉴别 | d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现； | 1）经检查，系统仅采用用户名+口令一种鉴别技术，未采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。 | 不符合 | 建议对系统采用两种或两种以上组合的鉴别技术实现用户身份鉴别，如口令、数字证书、令牌、生物技术等，且其中一种鉴别技术至少应使用密码技术来实现。 | * 是
* 否
 |  |
| 访问控制 | 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。 | 1）经检查，系统未建立独立的审计管理员，并设置三者权限之间相互制约。  | 不符合 | 建议系统授予管理用户为完成承担任务所需的最小权限，管理用户仅需具备管理相关功能权限，同时，管理用户应实现权限分离，管理用户分为管理员、安全员和审计员；管理员仅具有系统管理、用户创建与删除、角色创建与删除等功能权限，安全员具备安全参数配置、用户权限分配等功能权限，审计员具备日志查看等功能权限。 | * 是
* 否
 |  |
| 访问控制 | g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 1）经检查，系统未提供对重要主体和客体设置安全标记的功能。 | 不符合 | 建议对重要主体（系统中管理用户）和重要客体（系统中鉴别数据、重要业务数据、个人信息以及敏感数据等）设置安全级别，高安全级别的用户才能访问到高安全级别的数据，低安全级别的管理用户只能访问到同级别及低级别的数据。（比如管理用户和重要数据均划分为1、2、3三个安全级别，安全级别3为最高级别，3安全级别的用户能够访问到1、2、3级别的数据，2级别的用户仅能访问到1、2安全级别的数据）。 | * 是
* 否
 |  |
| 入侵防范 | 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； | 1）经检查，系统存在高风险，未定期对应用系统进行漏洞扫描，未及时修补漏洞。 | 不符合 | 建议定期对应用系统进行漏洞扫描，在发现高风险漏洞后，在经过充分测试评估后，及时对漏洞进行修补，保证系统中不存在高风险漏洞。 | * 是
* 否
 |  |
| 可信验证 | a）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。 | 1）未对应用程序进行可信验证。 | 不符合 | 建议对应用程序进行可信验证，并在应用程序的关键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。 | * 是
* 否
 |  |
| 数据完整性 | a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 1）经抓包测试，系统未采用校验技术或密码技术保证重要数据在传输过程中的完整性，重要数据明文传输。 | 不符合 | 建议系统采用HTTPS、数字签名、VPN、国密算法等密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性，防止数据在传输过程中被篡改、窃取或破坏。 | * 是
* 否
 |  |
| 数据完整性 | b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等 | 1）系统用户密码加密存储，其他数据明文存储，未采用密码技术实现其存储完整性。 | 不符合 | 建议采用数字签名等密码技术（采用SM2、SM4等国密算法）或数据库加密系统实现重要业务数据、重要审计数据、重要配置数据、重要个人信息等重要数据在存储过程中的完整性。 | * 是
* 否
 |  |
| 数据保密性 | a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 1）经抓包测试，系统鉴别数据、重要业务数据和重要个人信息明文传输，未采用密码技术保证其在传输过程中的保密性。 | 不符合 | 建议系统采用HTTPS、CA证书、VPN、国密算法等密码技术实现鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性。 | * 是
* 否
 |  |
| 数据保密性 | b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等 | 1）经检查，鉴别数据、重要业务数据和重要个人信息等重要数据在数据库中明文存储，未采用密码技术保证其存储保密性。 | 不符合 | 建议采用SM2、SM4等密码技术或数据库加密系统实现重要业务数据、重要审计数据、重要配置数据、重要个人信息在存储过程中的保密性。 | * 是
* 否
 |  |

## 安全管理中心

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| **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； | 1）未部署堡垒机设备对系统中所有设备管理员的操作行为进行审计；2）未分配三权分立账号（系统管理员、审计管理员、安全管理员）。  | 不符合 | 建议使用堡垒机设备，收集所有网络设备和安全设备的资产信息，对所有设备进行集中审计与管理。 | * 是
* 否
 |  |
| 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。 | 1）未部署堡垒机设备对系统中所有设备管理员的操作行为进行审计；2）未分配三权分立账号（系统管理员、审计管理员、安全管理员）。  | 不符合 | 建议网络设备进行角色划分，划分为系统管理员，安全管理员、审计管理员等角色。系统管理员权限不同于审计管理员和安全管理员。 | * 是
* 否
 |  |
| **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； | 1）未部署堡垒机设备对系统中所有设备管理员的操作行为进行审计；2）未分配三权分立账号（系统管理员、审计管理员、安全管理员）。  | 不符合 | 建议使用堡垒机设备，收集所有网络设备和安全设备的资产信息，对所有设备进行集中审计与管理。 | * 是
* 否
 |  |
| 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。 | 1）未部署堡垒机设备对系统中所有设备管理员的操作行为进行审计；2）未分配三权分立账号（系统管理员、审计管理员、安全管理员）。  | 不符合 | 建议网络设备进行角色划分，划分为系统管理员，安全管理员、审计管理员等角色。审计管理员权限不同于系统管理员和安全管理员。 | * 是
* 否
 |  |
| **安全管理** | a）应对安全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管理操作，并对这些操作进行审计； | 1）未部署堡垒机设备对系统中所有设备管理员的操作行为进行审计；2）未分配三权分立账号（系统管理员、审计管理员、安全管理员）。  | 不符合 | 建议使用堡垒机设备，收集所有网络设备和安全设备的资产信息，对所有设备进行集中审计与管理。 | * 是
* 否
 |  |
| b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 | 1）未部署堡垒机设备对系统中所有设备管理员的操作行为进行审计；2）未分配三权分立账号（系统管理员、审计管理员、安全管理员）。  | 不符合 | 建议网络设备进行角色划分，划分为系统管理员，安全管理员、审计管理员等角色。安全管理员权限不同于审计管理员和系统管理员。 | * 是
* 否
 |  |
| **集中管控** | c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； | 未部署IT运维管理平台，对系统中网络链路、安全设备、服务器的运行状态进行集中管理。。 | 不符合 | 建议部署IT运维管理平台，实现对系统中网络链路、安全设备、服务器的运行状态进行集中管理。 | * 是
* 否
 |  |
| d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； | 未部署日志审计系统。 | 不符合 | 建议部署日志审计系统，统一收集和存储各设备日志并进行集中审计分析。 | * 是
* 否
 |  |
| e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； | 未部署统一策略管理平台和补丁管理平台。 | 不符合 | 建议建立安全管理中心，对设备状态、补丁升级、安全审计等安全相关事项进行集中管理。 | * 是
* 否
 |  |

## 安全管理制度

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 管理制度 | d）应形成由安全政策、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。 | 具有安全策略以及基本的 管理制度，但未形成全面的安全管理制度体系。 | 部分符合 | 建议建立《00信息安全策略》以及《01信息安全方针》；信息安全方针对信息安全的基本架构、信息安全的根本目标、原则进行描述。分项策略应从物理、网络、主机、数据、应用、建设和管理等层面分别阐述信息安全的目标和原则。完善由安全政策、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。一般情况下， 一套全面的安全管理制度体系最常见的为4层架构，即由网络安全工作的总体方针策略，各种安全管理活动的管理制度、日常操作行为的操作规程和安全配置规范和各类记录表单。 | * 是
* 否
 |  |

## 安全管理机构

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 人员配备 | a)配备一定数量的系统管理员、网络管理员、安全管理员等； | 不具有岗位与人员对应关系表，未明确各岗位具体人员。 | 不符合 | 建议制定《02 单位内部人员对应表》，明确机房管理员、系统管理员、网络管理员、安全管理员等重要岗位人员的信息。 | * 是
* 否
 |  |
| b)应配备专职安全管理员，不可兼任； | 未配备专职的安全管理员 | 不符合 | 建议配备专职安全管理员。 | * 是
* 否
 |  |
| 授权和审批 | 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； | 未定期对审批事项进行审查。 | 不符合 | 建议定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。需要形成审批事项列表，在该列表中明确审批事项、涉及的审批部门、批准人等，并要求定期对该列表进行更新维护，如部门职责或岗位职责改变则某-审批活动涉及的审批部门和批准人则会改变，活动的重要程度改变则该活动的审批流程也会改变等。 | * 是
* 否
 |  |
| d）应记录审批过程并保存审批文档。 | 经检查，具有部分活动的审批过程记录。 | 部分符合 | 建议保存关键活动的审批过程记录。 | * 是
* 否
 |  |
| 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。  | 不定期针对工作需要召开会议，不具有会议记录。 | 部分符合 | 建议1）信息化工作部门应定期召开部门内部工作会议，讨论存在的信息安全问题，部署安全工作；2）信息安全管理机构内部应定期召开一次安全工作会议部署安全工作的实施，并且根据信息系统运行使用情况，不定期召开协调会议，共同协调处理期间的信息安全问题，若发生重大信息安全事件时，应及时召开协调会议，对出现的信息安全问题进行处理；3）信息安全领导小组应至少每年召开一次例会；应保存上述1)—3)项中产生的《03 会议记录表》，详细记录会议内容、会议时间、参加人员和会议结果等内容。 | * 是
* 否
 |  |
| b)应加强与兄弟单位、公安机关、电信公司的合作与沟通； | 具有职责范围内的联系方式，未形成外联单位通讯录。 | 不符合 | 建议形成《04 外联单位通讯录》，对合作内容、合作方式、联系电话等形成纸质的记录文件。外联单位包括公安机关、电信公司和兄弟单位、信息安全产品供应商、信息安全服务提供商、信息安全等级保护专业机构等。 | * 是
* 否
 |  |

## 人员安全管理

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 人员录用 | c）应签署保密协议。 | 内部人员未签订保密协议。 | 部分符合 | 应与录用后的技术人员签订《05保密协议》，保密协议应包括保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容。 | * 是
* 否
 |  |
| 人员离岗 | a）应严格规范人员离岗过程，及时终止即将离岗员工的所有访问权限。 | 未形成人员离岗流程规范。 | 不符合 | 建议建立《06 人员安全管理制度》，对离岗人员办理严格的离岗手续，及时终止离岗人员的所有访问权限，至少包括物理访问权限、网络设备访问权限、操作系统访问权限、数据库访问权限、应用系统访问权限、用户终端访问权限等。 | * 是
* 否
 |  |
| 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。 | 未签署保密承诺。 | 不符合 | 建议关键岗位人员离岗须承诺调离后的保密义务，保存与调离人员签署的保密承诺书，详见《07 保密承诺书》。 |  |  |
| 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； | 经访谈和检查，未对各岗位的人员进行各类考核 | 不符合 | 应指定信息化工作部门负责技能考核工作，至少每年对各个岗位的人员进行一次安全技能、安全认知及信息安全等级保护相关内容的考核。考核记录中的考核人员应包括各个岗位的人员，考核内容应包含安全知识、安全技能等。记录日期应与考核周期是否一致。《08 考核记录登记表》、《09岗位意识考核试卷》、《10 基本技能考核记录表》 | * 是
* 否
 |  |
| 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。 | 经访谈和检查，未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。 | 不符合 | 建议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。 | * 是
* 否
 |  |
| c）应对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。 | 未制定培训计划。 | 不符合 | 建议制定《11 信息安全培训管理制度》，明确培训周期、培训方式、培训内容和考核方式等内容；每年针对不同岗位制订不同的《12 培训计划表（安全）》，明确培训方式、培训对象、培训内容、培训时间和地点等方面内容，培训内容至少包括信息安全基础知识、岗位操作规程、信息安全等级保护政策法规、信息安全等级保护技术知识等；信息安全基础知识、岗位操作规程、信息安全等级保护政策法规、信息安全等级保护技术知识的培训应至少每年一次。 | * 是
* 否
 |  |
| 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。 | 经访谈和检查，无培训记录。 | 不符合 | 建议对安全教育和培训的情况和结果进行记录并归档保存，保留《13 培训记录表》。 | * 是
* 否
 |  |

## 系统建设管理

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 安全方案设计 | 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。 | 经访谈和检查，目前未制定系统安全建设工作计划。 | 不符合 | 建议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，根据信息系统的等级划分情况，参考国家的法律法规、技术标准（如：《信息安全技术 信息系统安全等级保护实施指南》GB/T 25058—2010），遵循行业的相关规定，建立信息安全保障体系建设规划，明确信息化建设总体规划，并针对现阶段急迫和关键的安全问题，建立短期工作计划。 | * 是
* 否
 |  |
| 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。 | 经访谈和检查，未形成详细设计方案等配套文件。 | 不符合 | 建议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。 | * 是
* 否
 |  |
| 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。 | 经访谈和检查，未形成详细设计方案等配套文件，无相关审定活动。 | 不符合 | 建议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。 | * 是
* 否
 |  |
| 产品采购和使用 | 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。 | 《生态环境局采购管理办法》部门集中采购，是指纳入政府采购管理的单位，由本单位组织实施属于部门集中采购范围的采购项目的行为。单位在实行部门集中采购时，其采购方式及委托的采购代理机构等审批手续，均由各单位按本办法的规定进行办理 | 部分符合 | 建议采购产品前应预先对产品进行选型测试确定产品的候选范围，保存产品选型测试结果记录；至少每年对候选产品名单进行审定和更新，保存候选产品名单的审定记录和更新后的候选产品名单。 | * 是
* 否
 |  |
| 外包软件开发 | a)应根据开发需求检测软件质量； | 不具有软件测试报告 | 不符合 | 应在软件交付前，根据合同或是设计说明书的要求对软件的质量进行检测，并保留测试报告。 | * 是
* 否
 |  |
| b）应在软件安装之前检测软件包中可能存在的恶意代码。 | 经访谈和检查，软件安装之前未使用第三方的检测工具检测软件包中可能存在的恶意代码。 | 不符合 | 建议应要求开发单位提供软件源代码文档，并指定专门部门负责保管；根据软件源代码对软件中可能存在的后门进行审查，或者可以委托第三方检测机构进行,保存软件源代码审查记录，详细记录对可能存在后门的审查结果；若未能提供软件源代码，则应要求开发单位提供第三方机构出具的软件源代码审查报告。 | * 是
* 否
 |  |
| c）应要求开发单位提供软件设计的相关文档和使用指南； | 文档内容不完善 | 不符合 | 应要求开发单位提供需求分析说明书、软件设计说明书、软件操作手册等软件开发文档和使用指南，并指定专门部门负责保管。 | * 是
* 否
 |  |
| 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。 | 经访谈和检查，开发单位未提供软件源代码，未经过审查明确不存在后门。 | 不符合 | 建议开发单位提供软件源代码。 | * 是
* 否
 |  |
| 工程实施 | 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； | 不具有工程实施方案 | 不符合 | 建议制订工程实施方案，明确工程时间限制、进度控制和质量控制等方面内容；按照工程实施方案的要求对工程实施过程进行进度和质量控制，保存按照实施方案形成的阶段性工程报告等文档。 | * 是
* 否
 |  |
| c）应通过第三方工程监理控制项目的实施过程。 | 未聘请监理公司 | 不符合 | 一般来讲，对于外包实施项目，需要第三方工程监理的参与，来控制项目的实施过程，对工程进展，时间计划、控制措施、工程质量等进行把关。 | * 是
* 否
 |  |
| 测试验收 | 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； | 未形成测试验收方案以及测试验收记录。 | 不符合 | 建议根据设计方案或合同要求等制订测试验收方案，明确参与测试的部门、人员、测试验收的内容、现场操作过程等方面内容；应保存测试验收记录，详细记录测试时间、人员、现场操作过程和测试验收结果等内容；应保存系统测试验收报告，详细描述整体测试验收过程以及测试验收结果，必要时，提出存在的问题及改进意见等内容。 | * 是
* 否
 |  |
| 系统交付 | 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； | 过程文档不全面 | 部分符合 | 建议保存系统建设过程中的所有文档、指导用户进行系统维护的文档和系统培训手册等；项目实施计划、概要设计说明书、详细设计说明书、开发计划、系统测试报告、用户手册、源代码及数据库、系统维护手册、验收报告等文档。 | * 是
* 否
 |  |

## 系统运维管理

| **控制点** | **要求项** | **测评结果** | **符合程度** | **整改建议** | **整改情况** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 环境管理 | 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。 | 经访谈和检查，未对办公环境人员行为进行明确。 | 不符合 | 建议形成《14 办公环境安全管理制度》，加强对办公环境的保密性管理，明确工作人员离开座位时退出登录状态、桌面没有敏感信息文件、不在办公区接待来访人员等方面内容；按照人员离岗要求和调离手续要求，人员调离办公室时应立即收回钥匙。 | * 是
* 否
 |  |
| 资产管理 | 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。 | 经访谈和检查，未对信息分类与标识方法作出规定。 | 不符合 | 建议建立《15 信息资产的分类和标识管理办法》其内容应规定分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）。 | * 是
* 否
 |  |
| 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。 | 经访谈和检查，未建立介质安全管理制度。 | 不符合 | 建议建立《16 移动介质安全管理规范》，对介质的存放环境、使用、维护、销毁、介质物理传输过程中的对人员选择、打包、交付等方面作出规定。 | * 是
* 否
 |  |
| 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。 | 经访谈和检查，未实行存储环境专人管理。 | 不符合 | 建议对介质的存放环境采取有效的保护措施，防止介质被盗、被毁、介质内存储信息被授权修改以及非法泄漏等，并指定专人负责管理介质的存储环境，避免由于高温、潮湿等自然因素对介质造成物理破坏。 | * 是
* 否
 |  |
| 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。 | 经访谈和检查，未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。 | 不符合 | 1）建议建立介质的目录清单，并根据该清单至少每季度对介质的使用现状进行检查，对介质的完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏）进行检查；2）应在《16 移动介质安全管理规范》中明确介质在物理传输过程中的控制措施，至少包括选择可靠的传输人员、严格介质的打包、选择安全的物理传输途径、双方在场交付等；3）应保存介质管理记录，详细记录介质的存储、归档、查询和借用等情况；详见《17 备份介质登记表》、《18 备份介质借用登记表》、《19 介质销毁登记表》、《20 存储介质携带外出审批表》。 | * 是
* 否
 |  |
| 恶意代码防范管理 | 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； | 此制度内容不完善 | 不符合 | 建议制订《21 防病毒管理办法》，明确防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面内容。 | * 是
* 否
 |  |
| 备份与恢复管理 | 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，备份策略应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。 | 经访谈和检查，未建立完善的备份管理制度 | 不符合 | 建议建立《22 数据备份管理规范》，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；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。 | * 是
* 否
 |  |
| 应急预案管理 | a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。 | 经访谈和检查，此制度内容不完善。 | 部分符合 | 建议建立《23 信息系统紧急预案》应急预案框架一般为单位总体应急预案管理的顶层文件，明确应急组织构成员职责、应急预案启动条件、响应、后期处置、预案日常管理、资源保障等内容，与各类网络安全事件专项应急预案共同构成整个应急预案体系。 | * 是
* 否
 |  |
| 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； | 不定期进行应急预案演练。 | 部分符合 | 至少每年对应急预案进行一次演练，保存《24 应急预案培训、演练、评审记录》。 | * 是
* 否
 |  |

# 技术修补

## 设备整改采购清单

针对以上整改建议，落实到具体实施中分三部分，即设备采购、配置加固、管理体系，设备采购具体内容如下表所示：

| **序号** | **类别** | **设备/措施** | **数量** | **具体整改措施** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1 | 机房改造 | 双路市电 | 1 | 建议为机房配备双路供电通道。 | 风险：低根据实际情况选择性整改 |
| 电磁干扰器、屏蔽机房或屏蔽机柜 | 1 | 建议机房采用电磁屏蔽装置或电磁干扰器，防止因电磁波泄露导致信息泄露事件。 | 风险：低根据实际情况选择性整改 |
| 2 | 安全设备 | 终端安全管理设备(含准入系统) | 1 | 在系统中增加终端安全管理设备，实现非授权接入和违法外联行为的检测和管控。 | 风险：高建议及时进行整改 |
| 日志审计系统 | 1 | 对网络设备、服务器等设备产生的日志集中存储、审计、分析，保证日志信息存储6个月以上，定期生成审计报表。 | 风险：高建议及时进行整改 |
| 防毒墙 | 1 | 建议在系统外网边界或区域边界部署防毒墙设备，配置安全防护策略，实现网络入口病毒检测、查杀（可集成到下一代防火墙模块中）。 | 风险：高建议及时进行整改 |
| IT运维管理系统 | 1 | 建议系统中部署IT运维管理系统，实现对网络设备的状态监控，以及线路流量的监测。 | 风险：高建议及时进行整改 |
| 双因素身份认证系统 | 1 | 建议系统中部署双因子认证系统，实现系统中设备、操作系统的双因子身份认证。 | 风险：中根据在条件允许情况下整改 |
| 抗APT攻击系统 | 1 | 建议外网与内网中部署APT攻击监测设备，对系统中可能存在的未知威胁检测攻击进行监测和阻断。 | 风险：中根据在条件允许情况下整改 |
| 网络审计系统 | 1 | 外网与内网部署网络/数据库安全审计系统，对人员访问系统的行为进行解析、分析、记录、汇报，以帮助用户事前规划预防、事中实时监视、违规行为响应、事后合规报告、事故追踪溯源，加强内外部网络行为监管、促进核心资产（数据库、服务器、网络设备等）的正常运营。 | 风险：中根据在条件允许情况下整改 |
| 漏洞扫描设备 | 1 | 建议系统中部署漏洞扫描设备，实现对终端和服务器存在的漏洞进行扫描，并对漏洞补丁及时弥补。 | 风险：中根据在条件允许情况下整改 |
| 可信验证设备 | 1 | 建议外网与内网中部署可信验证设备，将关键系统、应用纳入可信验证体系，在通信设备、网络设备、安全设备的可信性遭到破坏时及时报警并将验证结果输送至安全管理中心。 | 风险：中根据在条件允许情况下整改 |

# 附录一：安全加固参考

1. windows服务器
2. **<身份鉴别>**
	1. 配置密码策略

**参考配置操作：**

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”。

|  |  |  |
| --- | --- | --- |
| **策略** | **默认设置** | **推荐设置** |
| 密码必须符合复杂性要求 | 已禁用 | 已启用 |
| 密码长度最小值 | 0个字符 | 8个字符 |
| 密码最短使用期限 | 0天 | 2天 |
| 密码最长使用期限 | 42天 | 90天 |
| 强制执行密码历史 | 0个记住的密码 | 5个记住的密码 |
| 用可还原的加密来储存密码 | 已禁用 | 已禁用 |

* 1. 配置账户锁定策略

**系统当前状态：**

账户锁定时间：不适用

账户锁定阀值：0次无效登录

重置账户锁定计数器：不适用

**参考配置操作：**

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->账户锁定策略”。设置如下策略：

|  |  |  |
| --- | --- | --- |
| **策略** | **默认设置** | **推荐设置** |
| 复位账户锁定计数器 | 不适用 | 30 分钟 |
| 账户锁定时间 | 不适用 | 30 分钟 |
| 账户锁定阈值 | 0 | 5 次无效登录 |

* 1. 更改远程桌面管理端口号

**系统当前状态：**

当前使用远程桌面对服务器进行远程管理，未更改远程桌面管理端口号。

**参考配置操作：**

1）打开注册表

开始---运行---"regedit"---确定

或者 "win+R"---"CMD"---确定

2）定位的注册表

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp

3）修改右边PortNamber的值，其默认值是3389，修改成所希望的端口即可。

PS：基数为十进制

4）定位的注册表

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStations\RDP-Tcp

5）修改右边PortNamber的值，其默认值是3389，修改为上一步所设置的端口号。

6）设置完毕，重新启动后生效，

使用远程桌面连接时，需要在计算机名或者IP地址后加“：”和已修改的端口号。

* 1. 实现双因子身份认证

**系统当前状态：**

当前管理员仅使用用户名+密码方式对服务器进行管理，未使用两种及两种以上组合鉴别方式对管理员身份进行鉴别。

**参考配置操作：**

建议为在系统中配置堡垒机、USB Key、动态口令等，使用两种鉴别技术对系统管理员进行身份鉴别。

1. **<访问控制>**
	1. 修改系统默认账号

**参考配置操作：**

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”。

Administrator－>属性－> 更改名称（如有业务影响，请慎行）

Guest帐号->属性－> 已停用

* 1. 审计账号配置

**参考配置操作：**

1、新建audit用户名和audits用户组，并将audit用户划归到audits；

2、用进入“控制面板->管理工具->本地安全策略->安全设置-本地策略->用户权限分配，右键点击策略“管理审核和安全日志”点属性，修改为只有audits审计用户组或用户：点击“添加用户和组”，然后点击“对象类型”，在“对象类型”框中选中【组】，然后点击“高级”，出现搜索结果下拉框后，点击“立即查找”，在“搜索结果”下拉框中选中audits组，最后确定。

1. **<安全审计>**
	1. 审核策略设置

**参考配置操作：**

开始->运行-> 执行“控制面板->管理工具->本地安全策略->审核策略”

|  |  |  |
| --- | --- | --- |
| **策略** | **默认设置** | **推荐设置** |
| 审核策略更改 | 无审核 | 成功、失败 |
| 审核登录事件 | 无审核 | 成功、失败 |
| 审核对象访问 | 无审核 | 成功、失败 |
| 审核过程跟踪 | 无审核 | 失败 |
| 审核目录服务访问 | 无审核 | 无审核 |
| 审核特权使用 | 无审核 | 成功、失败 |
| 审核系统事件 | 无审核 | 成功、失败 |
| 审核帐户登录事件 | 无审核 | 成功、失败 |
| 审核账户管理 | 无审核 | 成功、失败 |

* 1. 配置日志审计系统

建议在网络上部署日志审计系统，采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，并出具丰富的审计报表。

通过类似SNARE for Windows常见Windows日志转SYSLOG工具，将日志转化为syslog格式后，统一发送到日志审计系统。

* 1. 部署网络/数据库安全审计系统

在网络中部署网络/数据库安全审计系统，通过对人员访问系统的行为进行解析、分析、记录、汇报，以帮助用户事前规划预防、事中实时监视、违规行为响应、事后合规报告、事故追踪溯源，加强内外部网络行为监管、促进核心资产（数据库、服务器、网络设备等）的正常运营。

1. **<剩余信息保护>**
	1. 开机清除虚拟页面

**参考配置操作：**

在本地安全策略-安全设置-本地策略-安全选项：

|  |  |  |
| --- | --- | --- |
| **策略** | **默认设置** | **推荐设置** |
| 关机：清除虚拟内存页面文件 | 已禁用 | 已启用 |

* 1. 交互式登录不显示上次用户名

**参考配置操作：**

在本地安全策略-安全设置-本地策略-安全选项：

|  |  |  |
| --- | --- | --- |
| **策略** | **默认设置** | **推荐设置** |
| 双击交互式登录：不显示上次的用户名 | 已禁用 | 已启用 |

1. **<入侵防范>**
	1. 开启系统防火墙

**参考配置操作：**

系统管理员出示业务所需端口列表，根据列表只开放系统与业务所需端口，具体步骤为：进入“控制面板－>网络连接－>本地连接”，在高级选项的设置中：启用Windows防火墙，在“例外”中配置允许业务所需的程序接入网络，在“例外->编辑->更改范围”编辑允许接入的网络地址范围。

* 1. 部署入侵检测系统(IDS）

**参考配置操作：**

准确分析、报告网络中正在发生的各种异常事件和攻击行为，实现对网络的“全面检测”，并通过实时的报警信息和多种格式报表，为用户提供翔实、可操作的安全建议，帮助用户完善安全保障措施。

* 1. 部署漏洞扫描系统

**参考配置操作：**

实现对网络设备、操作系统、应用系统进行全面安全漏洞检测，清晰定性安全风险，给出修复建议和预防措施，及时的发现和修补漏洞隐患。

* 1. 系统补丁更新

**系统当前状态：**

系统未开启Windows update自动更新，无法及时更新最新补丁和漏洞。

**参考配置操作：**

1）在【自动更新】处开启其“自动”更新的功能。

2）若系统运行在内网，需建立内网补丁服务器或由管理员手工将补丁安装到操作系统中。

注：补丁安装应当先在测试机上完成。补丁安装可能导致系统或某些服务无法工作正常。在下载补丁包时，一定要对签名进行核实，防止执行特洛伊木马。

* 1. 关闭默认共享

**系统当前状态：**

当前系统开启了默认的共享策略，对整个系统存储的数据带来了安全隐患，例如：

C:\WINDOWS\system32>net share

共享名 资源 注解

-------------------------------------------------------------------------------

C$ C:\ 默认共享

E$ E:\ 默认共享

IPC$ 远程 IPC

ADMIN$ C:\Windows 远程管理

命令成功完成。

**参考配置操作：**

“开始”→“运行”输入“regedit”确定后，打开注册表编辑器，找到“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters”项，双击右侧窗口中的“AutoShareServer”项将键值由1改为0，这样就能关闭硬盘各分区的共享。如果没有AutoShareServer项，可自己新建REG\_DWORD类型的AutoShareServer 键，值为 0。然后还是在这一窗口下再找到“AutoShareWks”项，也把键值由1改为0，关闭admin$共享。最后到“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa”项处找到“restrictanonymous”，将键值设为1，关闭IPC$共享。

注意：本法必须重启机器，但一经改动就会永远停止共享。

* 1. 关闭多余服务（可选）

**参考配置操作：**

进入“控制面板->管理工具->计算机管理”，进入“服务和应用程序”：查看所有服务，不必要的服务需关闭。

1. **<恶意代码防范>**
	1. 安装杀毒软件

**系统当前状态：**

当前系统未安装杀毒软件，无法防止病毒对内部网络进行感染。

**参考配置操作：**

在服务器和终端设备上安装网络版杀毒软件，配置防病毒服务器，实现下发病毒扫描策略、更新病毒库、统计报警信息等，便于管理人员对整个网络中的病毒防护状况进行管理。

1. **<资源控制>**
	1. 监控服务器资源状态

**参考配置操作：**

在网络中配置资源监控系统，对服务器的cpu、内存等资源进行实时监控，且应具有报警功能。管理员可以及时了解网络上各种设备的运行状况，可以及时发现并处理设备资源使用率过高、服务器宕机等异常状况。

* 1. 配置屏幕保护程序

**参考配置操作：**

进入“控制面板－>显示－>屏幕保护程序”：

启用屏幕保护程序，设置等待时间为“5 分钟”，启用“在恢复时使用密码保护”。

1. CentOS7服务器
2. **<身份鉴别>**
	1. 配置账户密码策略

**参考配置操作：**

1）#vi /etc/login.defs

修改下列参数为建议值

PASS\_MAX\_DAYS 90 #密码有效期为90天

PASS\_MIN\_DAYS 1 #密码最短修改时间为1天

PASS\_MIN\_LEN 8 #密码最小长度为8位

PASS\_WARN\_AGE 7 #密码过期提前7天提示修改

2）配置密码策略

authconfig --passminlen=8 --update #密码最短长度为8位

authconfig --enablereqlower --update #至少需要一个小写字符。

authconfig --enablerequpper --update #至少需要一个小写字符。

authconfig --enablerequpper --update #至少需要一个大写字符

authconfig --enablereqdigit --update #至少需要一个数字

authconfig --enablereqother --update #至少一个特殊字符

检查方法：cat /etc/security/pwquality.conf

minlen 最小密码长度

ucredit 最少大写字母

lcredit 最少小写字母

dcredit 最少数字

ocredit 最少特殊符号

3）口令至少5次内不能重复

# vi /etc/pam.d/system-auth

将password sufficient pam\_unix.so sha512 shadow nullok try\_first\_pass use\_authtok 行后添加参数： remember=5

 remember=5 更新的口令至少5次内不能重复

* 1. 配置登录失败处理策略

**参考配置操作：**

1）限制本地登录次数

# vi /etc/pam.d/login

在第二行增加如下内容：

auth required pam\_tally2.so deny=3 unlock\_time=1800 even\_deny\_root root\_unlock\_time=1800

2）限制ssh登录次数

# vi /etc/pam.d/sshd

在第二行增加如下内容：

auth required pam\_tally2.so deny=3 unlock\_time=1800 even\_deny\_root root\_unlock\_time=1800

3）查看用户登录失败的次数（以root为例）

# pam\_tally2 --user root

4）解锁指定用户（以root为例）

# pam\_tally2 -r -u root

5）各参数解释

even\_deny\_root 也限制root用户；

deny 设置普通用户和root用户连续错误登陆的最大次数，超过最大次数，则锁定该用户

unlock\_time 设定普通用户锁定后，自动解锁时间，单位是秒；

root\_unlock\_time 设定root用户锁定后，自动解锁时间，单位是秒；

**注：**在#%PAM-1.0的下面，即第二行，添加内容，一定要写在前面。如果写在后面，虽然用户被锁定，但是只要用户输入正确的密码，还是可以登录的。

此处使用的是 pam\_tally2 模块，如果不支持 pam\_tally2 可以使用 pam\_tally 模块。另外，不同的pam版本，设置可能有所不同，具体使用方法，可以参照相关模块的使用规则。

* 1. 实现双因子身份认证

**系统当前状态：**

当前管理员仅使用用户名+密码方式对服务器进行管理，未使用两种及两种以上组合鉴别方式对管理员身份进行鉴别。

**参考配置操作：**

建议在系统中配置USB Key、动态口令等，使用两种或两种以上鉴别技术对系统管理员进行身份鉴别。

1. **<访问控制>**
	1. 修改UMASK值

**参考配置操作：**

1）编辑/etc/profile文件，设置umask值：

#vi /etc/profile

在末尾增加 umask 027。

2）补充说明

umask 的默认设置一般为 022，这给新创建的文件默认权限755（ 777-022=755），这会给文件所有者读、写权限，但只给组成员和其他用户读权限。

umask 的计算：

umask 是使用八进制数据代码设置的，对于目录，该值等于八进制数据代码 777 减去需要的默认权限对应的八进制数据代码值；对于文件，该值等于八进制数据代码 666 减去需要的默认权限对应的八进制数据代码值。

* 1. 设置关键目录的权限

**参考配置操作：**

1）对系统中重要文件配置权限：

chmod 600 /etc/security

* 1. 为不同的管理员分配不同的账号

**参考配置操作：**

1）为每个操作系统管理员创建账号：

#useradd username #创建账号

#passwd username #设置密码

2）根据管理员职责，为每个账户分配不同权限。

* 1. 锁定系统无用账户

**参考配置操作：**

通过cat /etc/shadow查看当前帐户列表，以下用户(lp|sync|halt|news|uucp|operator|games|gopher|smmsp|nfsnobody|nobody)密码字段列不是以\*或者!!开头的，需要禁用或删除

命令：passwd -l username

注解：禁用无关帐户

1. **<安全审计>**
	1. 配置日志审计功能

**系统当前状态：**

 系统未配置audit功能，没有使用aureport生成审计报告可以生成分析报表。

**参考配置操作：**

1）安装audit软件包

yum install audit

2）开始audit 服务

service auditd start

3）根据实际情况，在 /etc/audit/auditd.conf 文件中配置对audit审计工具进行配置。

4）根据实际情况，在/etc/audit/audit.rules 文件中配置审核规则。

* 1. 记录设备相关安全事件

**参考配置操作**

1）修改配置文件 vi /etc/syslog.conf，

配置如下类似语句：

\*.err;kern.debug;daemon.notice; /var/adm/messages

定义为需要保存的设备相关安全事件。

2）更改日所有志文件属性，使文件只可追加不可修改：

chattr +a /var/log/messages #如果不存在则忽略

chattr +a /var/log/secure

chattr +a /var/log/maillog

chattr +a /var/log/cron

3）参数含义：

kern 由kernel产生的信息；

user 由用户进程产生的信息。对那些由程序或不在此列出的工具产生的信息，其缺省类型都是“user”;

mail 邮件系统产生的信息；

daemon 系统守护进程的信息，如in.ftpd、telnetd；

auth 由login, su, getty等进行身份认证时产生的信息；

syslog 由syslogd自己内部产生的信息；

lpr 行打印spooling系统的信息；

news USENET 网络新闻系统的信息；

uucp UUCP系统信息；

cron cron和at工具信息；

local0-7 保留为local使用；

mark syslogd内部产生的时间戳信息；

\* 除mark之外的所有其它类型（此符号不可用以代表所有级别）。

保留字段中的“级别”代表信息的重要性，可以是：

emerg 紧急，处于Panic状态。通常应广播到所有用户；

alert 告警，当前状态必须立即进行纠正。例如，系统数据库崩溃；

crit 关键状态的警告。例如，硬件故障；

err 其它错误；

warning 警告；

notice 注意；非错误状态的报告，但应特别处理；

info 通报信息；

debug 调试程序时的信息；

none 通常调试程序时用，指示带有none级别的类型产生的信息无需送出。如\*.debug;mail.none表示调试时除邮件信息外其它信息都送出。

* 1. 配置日志服务器

建议在网络上部署日志服务器，采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，并出具丰富的审计报表。

1）vim /etc/syslog.conf将\*.info;mail.none;authpriv.none;cron.none /var/log/messages中的/var/log/messages修改为： @（日志服务器IP）

2）重新读取配置文件：service syslog reload

* 1. 部署网络/数据库安全审计系统

在网络中部署网络/数据库安全审计系统，通过对人员访问系统的行为进行解析、分析、记录、汇报，以帮助用户事前规划预防、事中实时监视、违规行为响应、事后合规报告、事故追踪溯源，加强内外部网络行为监管、促进核心资产（数据库、服务器、网络设备等）的正常运营。

1. **<入侵防范>**
	1. 配置防火墙

**参考配置操作：**

1）启动iptables：

# service iptables start

2）开放端口（根据实际业务需求进行配置）：

修改/etc/sysconfig/iptables文件，增加如下一行：

-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT

3）重启防火墙：

# service iptables restart

4）检查防火墙策略：

#iptables -L

* 1. 部署入侵检测系统(IDS)

准确分析、报告网络中正在发生的各种异常事件和攻击行为，实现对网络的“全面检测”，并通过实时的报警信息和多种格式报表，为用户提供翔实、可操作的安全建议，帮助用户完善安全保障措施。

* 1. 部署漏洞扫描系统

实现对网络设备、操作系统、应用系统进行全面安全漏洞检测，清晰定性安全风险，给出修复建议和预防措施，及时的发现和修补漏洞隐患。

* 1. 关闭无用服务

**系统当前状态：**

系统中服务开启均为系统安装时默认状态。

**参考配置操作：**

取消所有不需要的服务，编辑“ /etc/inetd.conf”文件，通过注释取消所有你不需要的服务（在该服务项目之前加一个“ #”）。

1）更改“ /etc/inetd.conf”权限为 600，只允许 root 来读写该文件。

# chmod 600 /etc/inetd.conf

2）确定“ /etc/inetd.conf”文件所有者为 root。

# chown root /etc/inetd.conf

3）编辑 /etc/inetd.conf 文件（ vi /etc/inetd.conf），取消不需要的服务，如： ftp, telnet, shell, login, exec, talk, ntalk,imap, pop-2, pop-3, finger, auth 等等。把不需要的服务关闭可以使系统的危险性降低很多。

4）给 inetd 进程发送一个 HUP 信号：

# killall -HUP inetd

5）用 chattr 命令把/ec/inetd.conf 文件设为不可修改。

# chattr +i /etc/inetd.conf

注：/etc/inetd.conf 文件中只开放需要的服务。对于启用的网络服务，使用 TCP Wrapper 增强访问控制和日志审计功能。建议使用 xinetd 代替 inetd，前者在访问控制和日志审计方面有较大的增强。这样可以防止对inetd.conf的任何修改（以外或其他原因）。唯一可以取消这个属性的只有root。如果要修改inetd.conf文件，首先要取消不可修改属性：# chattr -i /etc/inetd.conf

portmap（如果启动使用 nfs 等需要 rpc 的服务，建议关闭portmap 服务）

cups 服务（ Common Unix Printing Service，用于打印，建议关闭）

named 服务（除非主机是 dns 服务器，否则关闭 named 服务）

apache（ http）服务

xfs（ X Font Service）服务

vsftpd

lpd

linuxconf

identd

smb

* 1. 系统补丁更新

建立补丁服务器或由管理员手工将补丁安装到操作系统中。

注：补丁安装应当先在测试机上完成。补丁安装可能导致系统或某些服务无法工作正常。在下载补丁包时，一定要对签名进行核实，防止执行特洛伊木马。

1. **<恶意代码防范>**
	1. 安装杀毒软件

**系统当前状态：**

当前系统未安装杀毒软件，无法防止病毒对内部网络进行感染。

**参考配置操作：**

在服务器和终端设备上安装网络版杀毒软件，配置防病毒服务器，实现下发病毒扫描策略、更新病毒库、统计报警信息等，便于管理人员对整个网络中的病毒防护状况进行管理。

1. **<资源控制>**
	1. 设置访问控制列表

**系统当前状态：**

 系统未设置访问控制列表。

**参考配置操作：**

1）编辑 hosts.deny文件，加入(ALL:ALL)：

#vi /etc/hosts.deny

sshd: ALL #拒绝一切SSH远程访问，配合文件hosts.allow使用

2）编辑 hosts.allow 文件，加入允许访问的主机列表，比如：

#vi /etc/hosts.allow

sshd:192.168.59.1:allow #允许192.168.59.1访问SSH服务进程

* 1. 设置登录超时时间

**参考配置操作：**

通过修改账户中“ TMOUT”参数，可以实现此功能。编辑/etc/profile文件，在“ HISTFILESIZE=”后面加入TMOUT值：

#vi /etc/profile

TMOUT=300 #表示300秒

export TMOUT #设置为全局变量

# source /etc/profile #使配置生效

这样，若系统中登录的用户在 5分钟内无动作，系统会自动注销该账户。

* 1. 限制用户对资源的访问

**参考配置操作：**

1）编辑 /etc/security/limits.conf文件，根据实际使用情况配置参数，限制用户对系统资源的使用限度。

core - 限制内核文件的大小

　　date - 最大数据大小

　　fsize - 最大文件大小

　　memlock - 最大锁定内存地址空间

　　nofile - 打开文件的最大数目

　　rss - 最大持久设置大小

　　stack - 最大栈大小

　　cpu - 以分钟为单位的最多 CPU 时间

　　noproc - 进程的最大数目

　　as - 地址空间限制

　　maxlogins - 此用户允许登录的最大数目

2）编辑/etc/pam.d/login文件，在其末端添加如下语句

session required /lib/security/pam\_limits.so

3）编辑/etc/security/limits.conf文件，在其中添加如下语句

\* hard rss sizeofmem

\* hard nproc maxNumberOfProcesses

\* hard as sizeofvirtualmem

#其中sizeofmem和sizeofvirtualmem为数值，其单位为KB；maxNumberOfProcesses也为数值，其单位为个

4）重启服务

/etc/init.d/sshd restart

1. H3C设备-相关配置策略
2. **<访问控制>**
	1. ARP绑定

**参考配置操作：**

1.1.1、建议关闭交换机闲置端口，参考命令如下：

<H3C> system-view

[H3C] interface Ethernet 0/0/1

[H3C- Ethernet 1/0/1] shutdown

1.1.2、建议在交换机上进行IP和MAC的绑定，参考命令如下：

<H3C> system-view

[H3C] interface *interface-type interface-number* #进入接口视图

[H3C] ip verify source { ip-address | ip-address mac-address | mac-address } #配置IPv4接口绑定功能

【相关参数说明】：

|  |  |  |
| --- | --- | --- |
| **参数** | **参数说明** | **取值** |
| **ip-address** *ip-address* | IP地址。 | X.X.X.X点分十进制形式。 |
| **ipv6-address** *ipv6-address* | IPv6地址。 | 格式为 X:X::X:X。 |
| **mac-address** *mac-address* | MAC地址。 | H-H-H十六进制形式。 |

1. **<安全审计>**
	1. 配置日志审计系统

建议部署日志审计系统，并将相关设备的日志以syslog方式远程存放到日志服务器中，参考命令如下：

**参考配置操作：**

[H3C] system-view

[H3C]info-center channel *channel-number* name *channel-name*  #为指定编号的信息通道命名

[H3C]info-center source { *module-name* | default }channel { *channel-number* | *channel-name* } [ debug { level *severity* | state *state* }\* | log{ level *severity* | state *state* }\* | trap { level *severity* | state *state* }\* ]\* #配置系统信息的输出规则

[H3C]info-center loghost [ vpn-instance *vpn-instance-name* ] { *host-ipv4-address* | ipv6 *host-ipv6-address* } [ port *port-number* ] [ channel { *channel-number* | *channel-name* } | facility *local-number* ] \* #指定日志主机地址并设置相关输出参数

[H3C]info-center timestamp loghost { date | iso | no-year-date | none } #设置发往日志主机的系统信息的时间戳输出格式，缺省情况下，发往日志主机的系统信息的时间戳输出格式为date格式

[H3C]save

【相关参数说明】：

|  |  |  |
| --- | --- | --- |
| **参数** | **参数说明** | **取值** |
| *module-name* | 指定模块名。 | 字符串形式，不支持空格，长度范围是1～24。 |
| **default** | 指定信息模块为缺省模块。 | - |
| *channel-number* | 指定信息通道号。 | 整数形式，取值范围是0～9。 |
| *channel-name* | 指定信息通道名。 | 字符串形式，不支持空格，不区分大小写，不支持“-”、“/”和“\”等字符，长度范围是1～30。 |
| **log** | 指定日志信息。 | - |
| **state** | 指定信息的发送状态。 | - |
| **trap** | 指定告警信息。 | - |

1. **<网络设备防护>**
	1. 限制设备登录地址

**参考配置操作：**

防止出现越权和滥用的情况，从而造成数据被窃取篡改的情况，用访问控制列表对管理员的登录地址进行限制，达到保护网络设备的作用，参考命令如下：

<H3C> system-view

[H3C]acl [ number ] *acl-number* #要创建基本ACL，acl-number的取值范围是2000～2999；要创建用户自定义ACL，acl-number的取值范围是5000～5999

[H3C]description *text*  #配置ACL描述信息，ACL的描述信息可以用来表示该ACL的用途，长度不能超过127个字符

[H3C] rule [*rule-id*] { deny | permit } [ fragment | logging | source { *source-address source-wildcard* | any } | time-range *time-name* ]\* #配置ACL规则

[H3C] quit

**【相关参数说明】：**

| **参数** | **参数说明** | **取值** |
| --- | --- | --- |
| *acl-number* | 指定ACL访问控制列表的序号。地址访问控制列表号分为两种：* 基本访问控制列表号。
* 高级访问控制列表号。
 | 整数形式，取值范围是2000～3999。* 基本访问控制列表序号的取值范围是2000～2999。
* 高级访问控制列表序号的取值范围是3000～3999。
 |

* 1. 配置口令复杂度策略

缺省情况下，设备不对用户密码进行复杂度检查。

**参考配置操作：**

[H3C] system-view

[H3C]password-control enable #使能全局密码管理功能

[H3C]password-control length 12 #配置密码长度最短不少于12位

[H3C]password-control composition type-number *type-number* [ type-length *type-length* ] #配置用户密码的组合策略

[H3C]password-control complexity { same-character | user-name } check #配置用户密码的复杂度检查策略，缺省情况下，不对用户密码进行复杂度检查。

* 1. 开启登录失败处理功能

缺省情况下（默认使能），用户登录尝试次数为3次；如果用户登录失败，则1分钟后再允许该用户重新登录。

**参考配置操作：**

<H3C> system-view

[H3C]password-control login-attempt *login-times* [ exceed { lock | lock-time *time* | unlock } ] #配置用户登录尝试次数以及登录尝试失败后的行为。

【相关参数说明】：

|  |  |
| --- | --- |
| **参数** | **参数说明** |
| *lockout-time* | 锁定时间（单位：分钟），取值范围1~2147483647。 |

* 1. 开启闲置超时时间

缺省情况下（默认使能），所有的用户界面的超时时间为10分钟。

**参考配置操作：**

<H3C> system-view

[H3C] user-interface console 0

[H3C] idle-timeout *minutes* [ *seconds* ] # 配置登录闲置超时时间：该命令只有在用户登录不需要AAA认证时才会生效。

//如果用户配置了登录时进行AAA认证，用户界面断连的超时时间需按照

[H3C] user-interface vty 0 4

[H3C]idle-timeout *minutes* [ *seconds* ] #设置VTY 用户界面的超时时间。

【相关参数说明】：

|  |  |  |
| --- | --- | --- |
| **参数** | **参数说明** | **取值** |
| *minutes* | 指定用户界面断连的超时时间的分钟数。 | 整数形式，取值范围是0～35791，单位是分钟。 |
| *seconds* | 指定用户界面断连的超时时间的秒数。 | 整数形式，取值范围是0～59，单位是秒。 |

* 1. 远程管理防窃听

建议在进行远程维护管理设备时，设备应配置采用SSH等加密协议，禁用Telnet或HTTP明文登录方式，避免出现传输数据被窃取和修改的可能。

**参考配置操作：**

[H3C] system-view

[H3C]public-key local create { dsa | rsa | ecdsa } [ name *key-name* ] #生成本地密钥对

[H3C]ssh server enable #使能SSH服务器功能

[H3C]ssh user username service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign publickey *keyname* } #建立SSH用户，并指定SSH用户的认证方式

[H3C] user-interface vty 0 4

[H3C]protocol inbound ssh #只允许通过SSH协议远程访问

[H3C] save

* 1. 权限分离控制

建议根据用户的业务需求，配置其所需的最小权限，从而分离超级管理员账户的权限。

**参考配置操作：**

[H3C] system-view

[H3C] local-user *user-name* [ class { manage | network } #添加本地用户，并进入本地用户视图

[H3C] password { cipher | simple } *password* #设置本地用户的密码

[H3C] service-type ssh

[H3C] authorization-attribute { level *level* | user-role security-audit } \* #缺省情况下，未设置本地用户的任何授权属性，对于ssh、terminal用户，仅授权属性level有效。

【相关参数说明】：

| **参数** | **参数说明** | **取值** |
| --- | --- | --- |
| *user-name* | 用户名。如果用户名中带域名分隔符，如@，则认为@前面的部分是用户名，后面部分是域名。如果没有@，则整个字符串为用户名，域为默认域。 | 字符串形式，不支持空格，不区分大小写，长度范围是1～64。格式“user@domain”。 |
| *password* | 用户口令。 | 字符串形式，不支持空格、单引号和问号，区分大小写，长度范围是1～16。若为密文形式用户口令，长度是32。 |