安徽风雪网络安全测评有限公司
Anhui FengXue Cyber Security Evaluation Co., Ltd.

宁国人民医院
网络安全等级保护
评估及整改建议报告

编制时间： 2022 年 09 月

目录

1 评估分析背景介绍

随着全国各行各业电子信息工程化的实施和互联网络的迅猛发展及业务发展和市场竞争的需要，以信息公开化、电子化为核心的电子化信息系统已经成为企业发展业务、提高服务水平、加强管理和提升效益的必备手段，但是，紧随信息化发展而来的网络安全问题日渐突出，根据国家四部委联合下发的2007公通字43号文以及《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号）要求，规定的重要信息系统，必须实施等级保护建设。

同时以GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》为评价基础，以《信息系统等级保护安全设计技术要求》和《信息安全等级保护安全建设整改工作指南》为设计指导，并充分吸收近年来安全领域出现的信息系统安全保障理论模型和技术框架，提出以建立一个“安全物理环境”基础上的“一个中心”保障下的“三重防护体系”架构体系（一个中心是指安全管理中心，三层纵深防御体系则由安全计算环境、安全区域边界以及安全通信网络组成），能够有效地帮助解决日渐突出网络安全问题，保障其业务系统可靠、稳定的运行，从而有效满足当前及未来一段时期安全需求。

本报告针对宁国人民医院的网络环境以及当前的安全措施为基础，分析安全建设需求，结合国家等级保护的建设规范和技术要求而编制，一方面对宁国人民医院的信息安全建设起到指导作用；另一方面可形成宁国人民医院安全防护系统建设方案；通过将等级保护基本要求，在实际网络、应用环境中落地，形成多系统复杂环境的等级保护建设方法，指导宁国人民医院落实等级保护的制度和要求。

2 评估分析过程概述

本次对宁国人民医院与信息系统等级保护标准三级要求的评估分析，采用了现状访谈、文档评审、配置核查三种方式。

现状访谈是指与有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。

文档评审是指检查 GB/T 22239-2019 和 GB/T 28448-2019 中规定的必需具有的制度、策略、操作规程等等是否齐备；检查是否具有完整的制度执行情况记录，如机房验收文档及机房的使用登记记录等。

配置核查是指根据宁国人民医院相关软硬件的安全配置情况，评估其是否符合相关等级的安全要求。

3 评估依据标准

1.《中华人民共和国网络安全法》

2.《信息安全等级保护管理办法》（公通字[2007]43 号）

3.《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）

4.GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

5.GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

6.GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

7.GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

8.《网络安全等级保护测评高风险判定指引》

9.GB/T 36627-2018《信息安全技术 网络安全等级保护测试评估技术指南》

4 三级高风险项

4.1 安全物理环境

4.1.1 物理访问控制

对应要求：

机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

4.1.2 防盗窃和防破坏

对应要求：

应设置机房防盗报警系统或设置有专人值守的视频监控系统。

4.1.3 防火

对应要求：

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。

4.1.4 电力供应

对应要求：

应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

4.2 安全通信网络

4.2.1 网络架构

对应要求：

1、应保证网络设备的业务处理能力满足业务高峰期需要。

2、应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。

3、应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

4、应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

5、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。

4.2.2 通信传输

对应要求：

1、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。

2、应采用密码技术保证通信过程中数据的保密性。

4.3 安全区域边界

4.3.1 边界防护

对应要求：

应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

4.3.2 访问控制

对应要求：

应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。

4.3.3 入侵防范

对应要求：

1、应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。

2、应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

4.3.4 恶意代码和垃圾邮件防范

对应要求：

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。

4.3.5 安全审计

对应要求：

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。

4.4 安全计算环境

4.4.1 身份鉴别

对应要求：

1、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。

2、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。

3、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。

4、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。

4.4.2 访问控制

对应要求：

1、应重命名或删除默认账户，修改默认账户的默认口令。

2、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。

4.4.3 安全审计

应用要求：

1、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。

2、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。

4.4.4 入侵防范

对应要求：

1、应关闭不需要的系统服务、默认共享和高危端口。

2、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。

3、应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

4、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。

4.4.5 恶意代码防范

对应要求：

应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

4.4.6 数据完整性

对应要求：

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。

4.4.7 数据保密性

对应要求：

1、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。

2、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。

4.4.8 数据备份恢复

对应要求：

1、应提供重要数据的本地数据备份与恢复功能。

2、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。

3、应提供重要数据处理系统的热冗余，保证系统的高可用性。

4.4.9 剩余信息保护

对应要求：

1、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。

2、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。

4.4.10 个人信息保护

对应要求：

1、应仅采集和保存业务必需的用户个人信息。

2、应禁止未授权访问和非法使用用户个人信息。

4.5 安全管理中心

4.5.1 集中管控

对应要求：

1、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。

2、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。

3、应能对网络中发生的各类安全事件进行识别、报警和分析。

4.6 安全管理制度

4.6.1 管理制度

对应要求:

应对安全管理活动中的各类管理内容建立安全管理制度。

4.7 安全管理机构

4.7.1 岗位设置

对应要求：

应成立指导和管理网络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担任或授权。

4.8 安全管理人员

4.8.1 安全意识教育和培训

对应要求：

应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

4.8.2 外部人员访问管理

对应要求：

应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。

4.9 安全建设管理

4.9.1 产品采购和使用

对应要求：

应确保网络安全产品采购和使用符合国家的有关规定。

4.9.2 外包软件开发

对应要求：

应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

4.9.3 测试验收

对应要求：

应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

4.10 安全运维管理

4.10.1网络和系统安全管理

对应要求：

1、应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

2、应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

4.10.2恶意代码防范管理

对应要求：

应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。

4.10.3变更管理

对应要求：

应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、 审批后方可实施。

4.10.4备份与恢复管理

对应要求：

应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

4.10.5应急预案管理

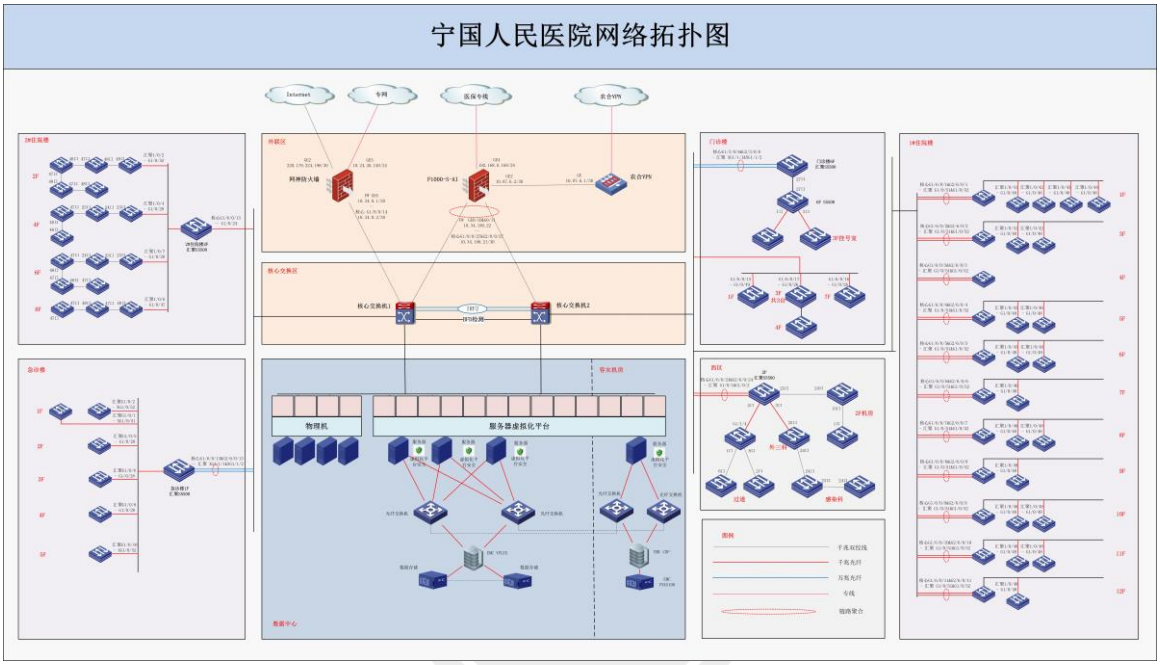
对应要求：

1、应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。

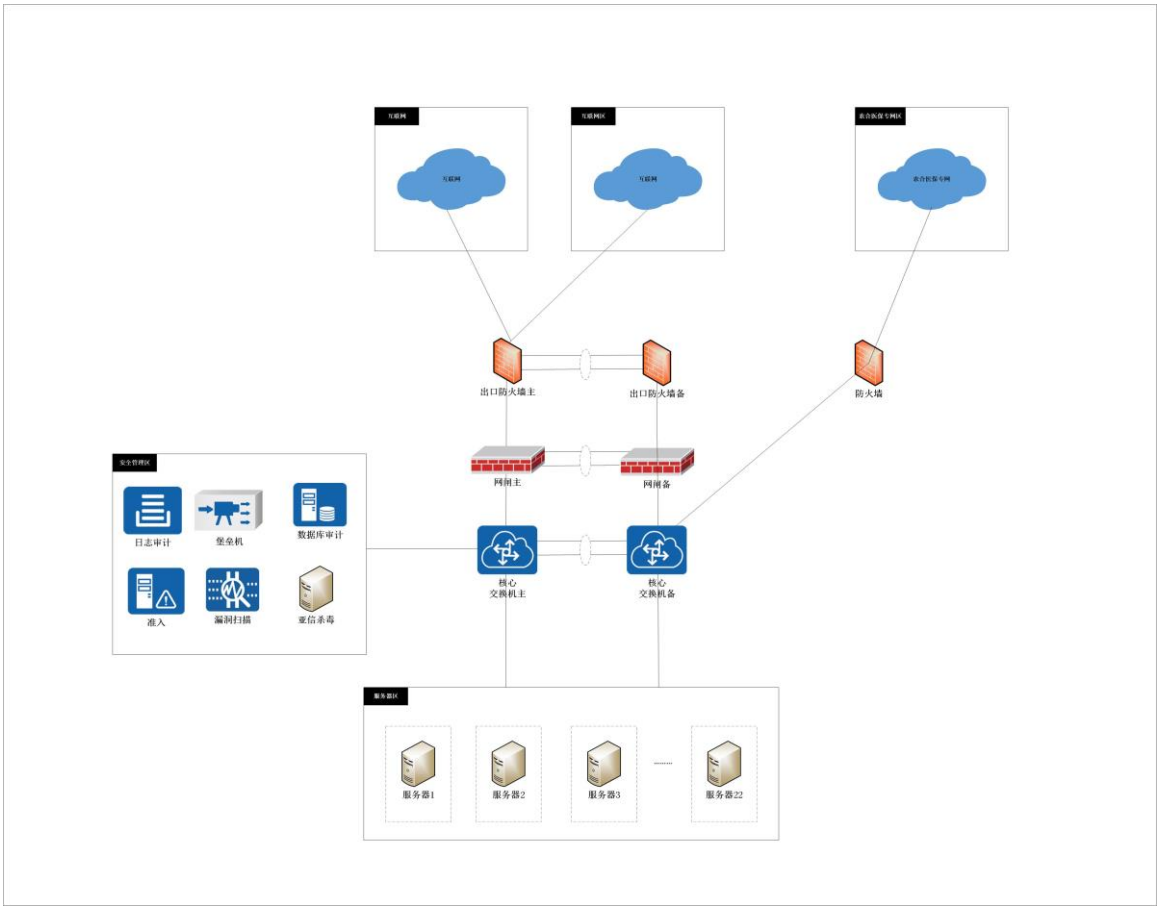
2、应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

5 拓扑图现状

5.1 现状拓扑



5.2 建议拓扑



6 系统安全整改建议和设备部署建议

按照国家《信息安全等级保护管理办法》的规定，结合 GB/T 22239-2019《信息安全技术 信息系统安全等级保护基本要求》，按照三级的要求，针对宁国人民医院前期测评，我们分别从安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面进行了分析，目前整理如下问题，并已给出相应整改建议，其中标记为高风险的为必须整改项。

6.1 安全整改建议

当前系统中存在的主要问题有：

6.1.1 安全区域边界层面

1、边界处访问控制设备（网神防火墙、H3C 防火墙）的策略不合理，建议依据实际业务情况，通过添加白名单的方式合理调整设备的访问控制策略，且默认拒绝所有通信。（高风险）

2、系统中安全设备均存在规则库过期以及部分设备存在设备过保的现象，建议联系设备维保人员对设备的规则库进行更新，对于过保设备进行续保或者更换新设备。（高风险）

3、系统中的堡垒机和日志审计未部署完毕，建议设备厂家尽快完成调试，关联系统中重要资产，通过堡垒机做到对设备的统一管控，通过日志审计做到对于设备审计记录的集中审计。（高风险）

6.1.2 安全计算环境层面

Linux 服务器

1、建议配置口令复杂度策略，如口令需由大小写字母、数字和特殊字符组成，且口令大于等于 8 位，配置口令定期更换策略，如 90 天更换一次。

2、建议配置登录失败策略，如登录失败次数大于 5 次时应账户锁定 15 分钟，配置登录超时策略，如登录后 30 分钟无操作自动退出，需重新输入用户名跟口令。

3、建议限制默认管理员账户的权限。

4、建议建立安全管理员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。

5、建议服务器开启安全增强型 Linux 子系统，SELinux 设置为 enforcing，对系统内重要主体和客体设置安全标记，并依据安全标记控制访问规则。

6、建议开启日志审计服务，并设置默认不能删除日志，对审计记录进行定期备份，日志留存时间满足六个月的要求。（高风险）

7、建议服务器安装防恶意代码软件，并确保病毒库为最新。（高风险）

8、建议采用加密算法和校验技术确保重要数据存储的保密性和安全性。（高风险）

Windows 服务器

1、建议配置口令复杂度策略，如口令需由大小写字母、数字和特殊字符组成，且口令大于等于 8 位，配置口令定期更换策略，如 90 天更换一次。

2、建议配置登录失败策略，如登录失败次数大于 5 次时应账户锁定 15 分钟，配置登录超时策略，如登录后 30 分钟无操作自动退出，需重新输入用户名跟口令。

3、建议限制默认管理员账户的权限。

4、建议建立安全管理员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。

5、建议开启远程会话连接加密，并将传输协议设置为 SSL 加密。（高风险）

6、建议开启日志审计服务，并设置默认不能删除日志，对审计记录进行定期备份，日志留存时间满足六个月的要求。（高风险）

7、建议服务器安装防恶意代码软件，并确保病毒库为最新。（高风险）

8、建议采用加密算法和校验技术确保重要数据存储的保密性和安全性。（高风险）

数据库

1、建议配置口令复杂度策略，如口令需由大小写字母、数字和特殊字符组成，且口令大于等于 8 位，配置口令定期更换策略，如 90 天更换一次。

2、建议配置登录失败策略，如登录失败次数大于 5 次时应账户锁定 15 分钟，配置登录超时策略，如登录后 30 分钟无操作自动退出，需重新输入用户名跟口令。

3、建议限制默认管理员账户的权限。

4、建议建立安全管理员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。

5、建议默认不能删除日志，已对审计记录进行定期备份，日志留存时间满足六个月的要求。（高风险）

6、建议采用加密算法和校验技术确保重要数据存储的保密性和安全性。（高风险）

业务系统

1、建议配置口令复杂度策略，如口令需由大小写字母、数字和特殊字符组成，且口令大于等于 8 位，配置口令定期更换策略，如 90 天更换一次。

2、建议配置登录失败策略，如登录失败次数大于 5 次时应账户锁定 15 分钟，配置登录超时策略，如登录后 30 分钟无操作自动退出，需重新输入用户名跟口令。

3、建议限制默认管理员账户的权限。

4、建议建立安全管理员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。

5、建议开启日志审计，对重要用户行为和重要安全事件进行审计。（高风险）

6、建议采用加密算法和校验技术确保重要数据传输的保密性和完整性。（高风险）

7、建议采用加密算法和校验技术确保重要数据存储的保密性和完整性。（高风险）

注：平台系统为 B/S 架构，可以安装 SSL 证书来实现数据的传输的保密性和完整性。

网络设备

1、建议设置交换机的 password-control 属性为 enable。（高风险）

2、建议禁用交换机的 TELNET 服务，仅使用较为安全的 SSH 方式进行远程管理。（高风险）

安全设备

1、建议配置口令复杂度策略，如口令需由大小写字母、数字和特殊字符组成，且口令大于等于 8 位，配置口令定期更换策略，如 90 天更换一次。

2、建议配置登录失败策略，如登录失败次数大于 5 次时应账户锁定 15 分钟，配置登录超时策略，如登录后 30 分钟无操作自动退出，需重新输入用户名跟口令。

3、建议限制默认管理员账户的权限。

4、建议建立安全管理员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。

6.2 设备部署建议

1、目前使用的防火墙和网闸存在单点故障，建议增加设备实现 HA。
2、建议部署新的防火墙（含 IPS 和防病毒功能）替换现有的 H3C 防火墙（停产过保、病毒库不能升级），并做好相应的安全策略。
3、建议部署态势感知平台设备，对未知安全威胁进行防范，防止网络被破坏等事件。
4、建议部署安全管理中心，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。
5、建议部署服务器杀毒软件，对现有未安装杀毒软件的 Linux 服务器进行病毒查杀。