武汉市江汉区卫计委信息系统
等级保护整改

项目建议书

武汉众一网诺科技有限公司

2019 年 06 月 23 日

目录

第1章　项目综述

1.1　前言

2016 年 11 月国务院办公厅印发《关于全面推进政务公开工作的意见》实施细则的通知，要求各省、自治区、直辖市人民政府，国务院各部委、各直属机构“对政府网站的开办、建设、定级、备案、运维、等级保护测评、服务、互动、安全和关停等进行监管”，武汉市政府积极推动、落实各政府部门的等级保护建设工作。

1.2　等级保护概述

为了进一步提高信息安全的保障能力和防护水平，1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。

2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

2004 年 9 月发布的《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）进一步强调了开展信息安全等级保护工作的重要意义，规定了实施信息安全等级保护制度的原则、内容、职责分工、基本要求和实施计划，部署了实施信息安全等级保护工作的操作办法。

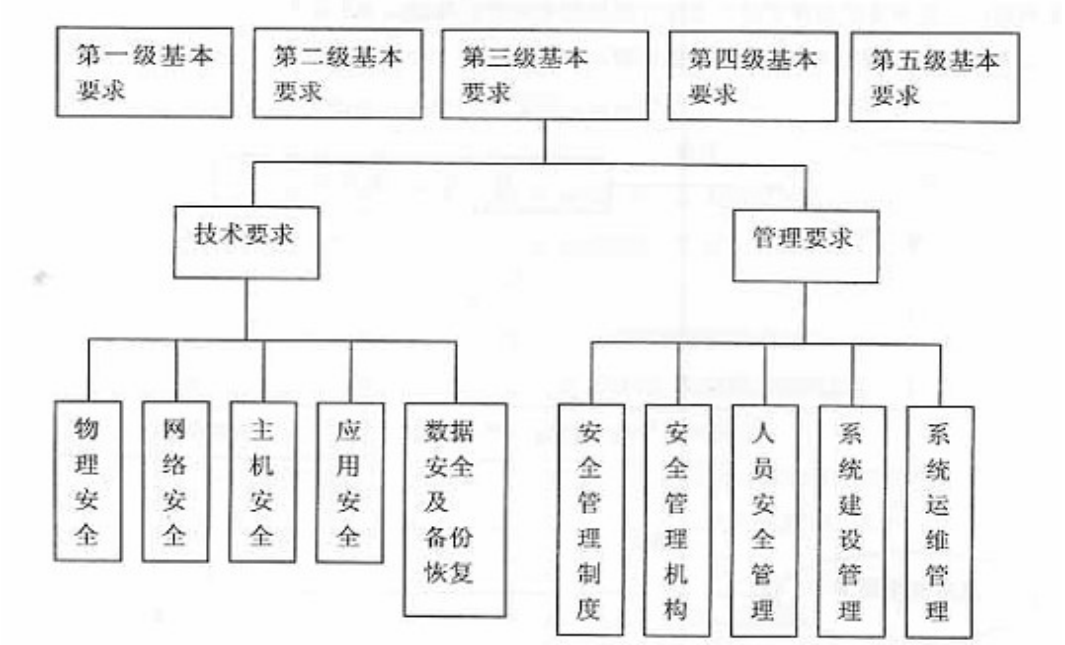
2007 年 6 月公安部会同国家保密局、国家密码管理局和国务院信息化工作办公室联合下发了《信息安全等级保护管理办法》（公通字[2007]43 号）。

2016 年 11 月 7 日由全国人民代表大会常务委员会发布《中华人民共和国网络安全法》，要求为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定。

2011 年 12 月，卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知（卫办发〔2011〕85 号），要求全国卫生系统做好信息安全等级保护工作，对促进卫生信息化健康发展，保障医药卫生体制改革，维护公共利益、社会秩序和国家安全具有重要意义。

在这些政策规范及法律的指引下，为推动我国信息安全等级保护工作的开展，近十年来，在公安部领导和支持下，在国内有关专家、企业的共同努力下，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制订了信息安全等级保护工作需要的一系列标准，形成了比较完整的信息安全等级保护标准体系，开展信息安全等级保护工作已成为信息化建设的重点内容，也是政府部门实现自身核心业务安全稳定运行的关键。《中华人民共和国网络安全法》标志着信息安全等级保护工作已经上升到国家战略层面，成为关系国计民生的重要任务。

根据《信息系统安全等级保护基本要求》，分为技术和管理两大类要求，具体如下图所示：

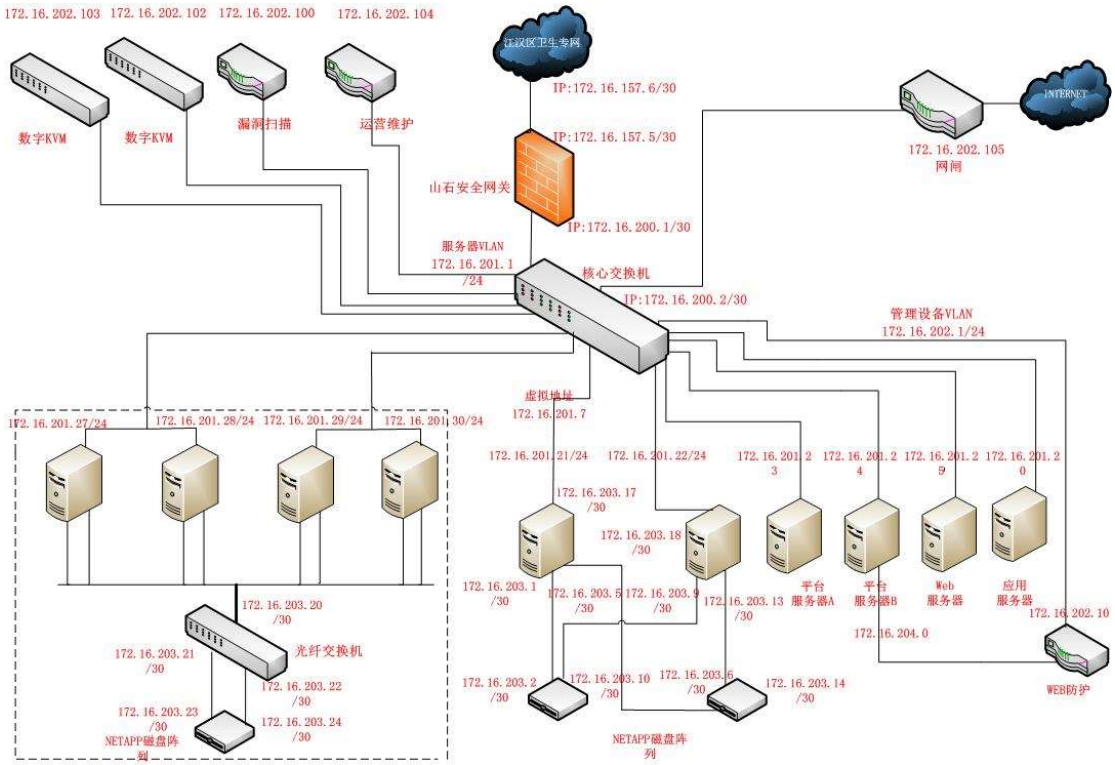


本方案通过对武汉市江汉区卫计委的重要信息系统，从技术层面及管理层面的全面评估和了解，整理出高风险的安全需求，并结合用户的实际业务要求，对武汉市江汉区卫计委整体信息系统的安全工作进行规划和设计，并逐步完成安全建设，以满足武汉市江汉区卫计委的信息安全目标及国家相关政策和标准的要求，同时为全面提高信息安全管理水平和控制能力打下坚实的基础。

第2章　项目现状与需求分析

2.1　项目现状

武汉市江汉区卫计委的网络拓扑如下图所示：



通过现场调研和网络拓扑图可了解到，当前系统承载于业务专网，机房内配备防火墙、绿盟 RSAS（漏洞评估系统）、上网行为管理、WAF，被部署有网闸，初步判断仍存在以下主要安全问题。

一、核心网络设备、边界山石防火墙均采用单机部署，存在物理设备硬件故障而影响整体系统服务，造成系统中断。

二、网络内部署有 WAF，但未启用，WAF 可提供应用层攻击防护、攻击行为检测、负载等功能。

三、网络内未部署安全运维审计系统（堡垒机），无法对网络内所有资产如防火墙、操作系统等统一管理，攻击者可能通过某一边界直接攻击内部服务器，等保 2.0 要求须建立可信的安全管理路径。

四、当前网络无边界完整性管理设备，即无法及时对内部用户的非法外联行为进行检测和阻断，从而会使得内部用户绕过边界访问控制，增大了受到外部攻击机病毒感染的风险；同时也无法对外部用户非法连接到内部行为进行检测和阻

断。

五、网络内缺乏威胁检测系统（等级保护 2.0 要求），传统 IDS、漏洞扫描设备已无法满足防护需求，无法对数据流量进行分析，准确发现各类新一代威胁和网络异常现象。新一代威胁往往使用多态、变形等高级逃避技术，无疑使发现攻击所需要的时间大大增加，并很难持续有效，新一代威胁具有极强的目标性，往往面对特定的组织目标进行定制化的攻击，在不知情的状态下，悄悄的达成了攻击目的。

六、网络设备、安全设备基础配置不完善，缺乏必要的安全访问控制策略；设备自身安全防护措施不足，如设备的登录地址限制、远程管理方式、鉴别方式和安全审计等。

2.2 存在问题

2.2.1 网络系统架构单一、网络边界划分不清

整个网络系统架构单一，具体表现单核心，一旦核心交换机出现故障。整个网络便瘫痪；网络边界模糊，部分应用防范措施不严格，互联网的安全隐患巨大，部分从互联网访问内部系统未通过安全的方式接入内网，各个应用系统之间的数据交互没有有效的安全控制策略。

2.2.2 安全防护薄弱

信息系统安全主要还是集中在网络安全设备上，主要是的防火墙，说明整体信息系统安全工作还处于网络层防护层面。网络边界防护手段严重不足；其他安全设备及防护措施严重不足；数据安全系统如容灾备份类薄弱。

2.2.3 数据缺乏体系化防护策略

在数据的产生、加工、传输、存储各环节缺少相应安全级别的针对性防护策略，缺乏体系防护策略，存在发生敏感数据泄露、丢失风险，而且数据泄露后难以溯源。

2.2.4 机房硬件设施较薄弱

1）、根据国家三级等保要求，机房应该具备防雷、防电、防火等要求；

2）、机房应设置监控报警系统，如摄像头监控、门禁等

3）、机房堆放较多的杂物，成为一个储物库，人员进入随意，缺乏必要的人员进出登记制度

2.2.5 管理制度缺失

按照国家三级等保要求，被测评单位应具备一定的安全管理制度，如：《安全事件报告和处置管理制度》、《机房安全管理制度》、《系统运行维护管理制度》等。针对相关制度，需将相关制度、流程张贴在机房内。

2.2.6 等保测评不足

目前武汉市江汉区卫计委重要信息系统未完成登记、定级、备案、测评和整改，存在隐患与漏洞，风险较高，一旦出现安全问题，将会造成较为严重的影响。

第3章　整改加固建议

3.1　整改加固目标

此次方案的目标是：落实 GB 22239-2019 对三级系统的安全保护要求，按国家等级保护三级系统防护能力构建一个安全的网络传输平台，把好网络核心节点出入口大门，控制无权用户的非法进入，防止从网络传输平台引入的攻击和破坏造成的安全威胁，保证网络只有授权的用户才能使用授权服务，确保各种信息在内网中传输的安全性和保密性。在保证该系统运行效率和投资收益比例恰当的前提下，通过技术和管理手段，最大程度地降低该系统的信息安全风险，确保该系统信息安全目标的实现。

通过为满足物理安全、网络安全、主机安全、应用安全、数据安全五个方面基本技术要求进行技术体系建设；为满足安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理五个方面基本管理要求进行管理体系建设。使得武汉市江汉区卫计委重要信息系统的等级保护建设方案最终既可以满足等级保护的相关要求，又能够全方面提供立体、纵深的安全保障防御体系，保证信息系统整体的安全保护能力。

3.2　整改加固依据

政策法规

- 《中华人民共和国计算机信息系统安全保护条例》（国务院[1994] 147 号）
- 《国家信息化领导小组关于加强信息安全保障工作的意见》（申发办[2003] 127 号）
- 《信息安全等级保护管理
- 办法》（公通字[2007] 43 号）

标准规范

- 《GB/T 22239-2019　信息安全技术信息系统安全等级保护基本要求》
- 《GB/T 22240-2008　信息安全技术信息系统安全等级保护定级指南》
- 其他参考标准：
- 《GB/T 20269-2006　信息安全技术信息系统安全管理要求》
- 《GB/T 20270-2006　信息安全技术网络基础安全技术要求》

- 《GB/T 20271-2006　信息安全技术信息系统通用安全技术要求》
- 《GB/T 20272-2006　信息安全技术操作系统安全技术要求》
- 《GB/T 20273-2006　信息安全技术数据库管理系统安全技术要求》

第4章　整改加固后网络系统拓扑图

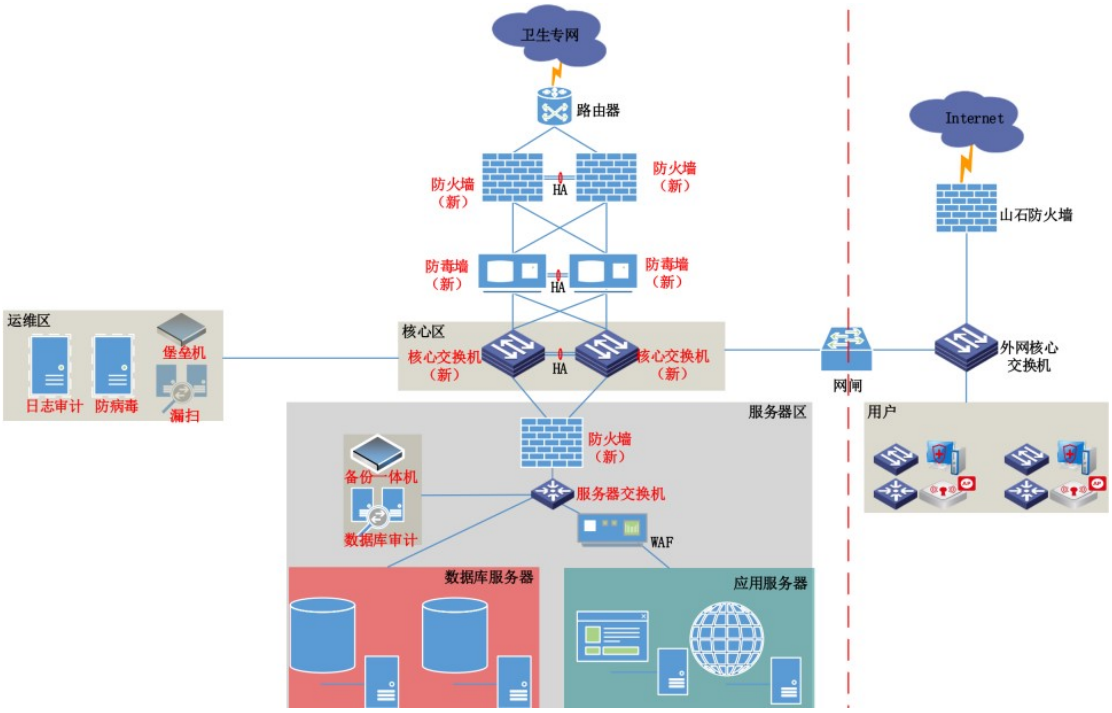


图 三级等保网络安全加固图

如图所示，按照国家信息安全等级保护三级要求实现网络边界隔离。

4.1 安全技术建设方案

4.1.1 设计目标

武汉市江汉区卫计委重要信息系统等级保护的设计目标是落实《信息系统安全等级保护基本要求》（GB/T 22239-2019）对第三级系统的安全保护要求：

（1）实现系统的自主访问控制，使系统用户对其所属客体具有自我保护的能力；

（2）增加系统安全审计、客体重用等安全功能，并实施以用户为基本粒度的自主访问控制，使系统具有更强的自主安全保护能力；

（3）通过实现基于安全策略模型和标记的强制访问控制以及增强系统的审计机制，使系统具有在统一安全策略管控下，保护敏感资源的能力。

4.1.2 物理安全

物理安全建设需要考虑物理环境安全评估、机房安全设施补足、物理安全管理咨询等相关工作。

4.1.2.1物理访问控制

1）、机房应设置专人值守，进出人员必须要进出登记

2）、机房应划分区域管理，区域与区域之间物理隔离，不得在机房内堆放杂物

3）、重要区域应配置电子门禁系统，机房进入必须授权方可进入

4.1.2.2防雷击

机房内应安装避雷装置

4.1.2.3防盗窃和防破坏

1）、机房各主要部件应该有清晰的、不易剔除的标记

4.1.2.4电磁防护

1）、应采用接地方式防止外界电磁干扰

2）、电源线和通信线缆应隔离敷设，避免互相干扰

4.1.3 网络安全

4.1.3.1 访问控制设计

网络访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够连入内部网络，那些用户能够通过哪种方式登录到服务器并获取网络资源。网络的访问权限控制是针对网络非法操作所提出的一种安全保护措施。控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。

在互联网区域**建议部署防火墙，**通过策略部署实现业务系统安全访问控制。

- 对业务系统提供边界防护和访问控制；
- 允许下属机构和网络公众用户通过穿过该防火墙，以 HTTP/HTTPS 的方式访问对外服务区域的服务器；
- 允许办公区域所有终端通过该防火墙的内部接口访问互联网；
- 允许安全管理区域的设备使用特定端口通过该防火墙的连接互联网的升级行为；
- 其他访问均被禁止。

4.1.3.2 网络入侵防御设计

要实现对边界处入侵和攻击行为的检测，同时能够有效防护互联网进来的攻击行为，因此在互联网区域建议部署**网络入侵防御系统**。

部署入侵防御系统，应完善入侵检测策略，动态地监测网络活动并做出及时的响应。

- 防范网络攻击事件：入侵防御系统采用细粒度检测技术，协议分析技术，误用检测技术，协议异常检测，可有效防止各种攻击和欺骗。针对端口扫描类、木马后门、缓冲区溢出、IP 碎片攻击等，入侵防御系统可在网络边界处进行监控和阻断。
- 防范拒绝服务攻击：入侵防御系统在防火墙进行边界防范的基础上，工作在网络的关键环节，能够应付各种 SNA 类型和应用层的强力攻击行为，包括消耗目的端的各种资源如网络带宽、系统性能等攻击，主要防范的攻击类型有 TCP Flood，UDP Flood，SYN Flood，Ping Abuse 等；
- 审计、查询：入侵研发系统能够完整记录多种应用协议（HTTP、FTP、

SMTP、POP3、TELNET 等）的内容。记录内容包括，攻击源 IP、攻击类型、攻击目标、攻击时间等信息，并按照相应的协议格式进行回放，清楚再现入侵者的攻击过程，重现内部网络资源滥用时泄漏的保密信息内容。同时必须对重要安全事件提供多种报警机制。

- 网络检测：在检测过程中入侵防御系统综合运用多种检测手段，在检测的各个部分使用合适的检测方式，采取基于特征和基于行为的检测，对数据包的特征进行分析，有效发现网络中异常的访问行为和数据包；
- 监控管理：入侵防御系统提供人性化的控制台，提供初次安装探测器向导、探测器高级配置向导、报表定制向导等，易于用户使用。一站式管理结构，简化了配置流程。强大的日志报表功能，用户可定制查询和报表。
- 异常报警：入侵防御系统通过报警类型的制定，明确哪类事件，通过什么样的方式，进行报警，可以选择的包括声音、电子邮件、消息。
- 阻断：由于入侵防御系统串联在保护区域的边界上，系统在检测到攻击行为后，能够主动进行阻断，将攻击来源阻断在安全区域之外，有效保障各类业务应用的正常开展，这里包括数据采集业务和信息发布业务；
- 在线升级：入侵防御系统内置的检测库是决定系统检测能力的关键因素，因此应定期进行在线升级，确保入侵检测库的完整性和有效性。

4.1.3.3 网络防病毒设计

应用系统服务器中建议部署**防病毒软件系统**，应完善防病毒策略，对进出网络的流量进行检测并在检测到病毒时及时的进行隔离或清除。防病毒软件系统在网络层实现对病毒的查杀，产品运行在区域边界上，分析不同安全区域之间的数据包，对其中的恶意代码进行查杀，防止病毒在网络中的传播。

1) 防病毒软件系统采用多引擎对进出网络的 HTTP、HTTPS、FTP、SMTP、POP3 协议流量进行依次的扫描过滤，最大程度的确保检测的准确性，减少漏查和误报。具体功能点如下：

- 分析检测并阻止 HTTP、HTTPS、FTP、SMTP、POP3 流量中的病毒、木马、间谍软件、蠕虫、后门、防钓鱼等网络威胁；
- 间谍软件回传阻止；
- 应对零日攻击；

- 快速定位内部威胁终端；
- 过滤阻断 Botnet Web 服务器；

4.1.4 主机安全

4.1.4.1 主机审计

安全审计有助于对入侵进行评估，是提高安全性的重要工具。审计信息对于确定是否有网络攻击的情况发生，以及确定问题和攻击源都非常重要。通过对安全事件的不断收集与积累并且加以分析，可以为发现可能的破坏性行为提供有力的证据。

安全审计可以利用数据库、操作系统、安全保密产品和应用软件的审计功能。对于重要的涉密系统应采用专用设备进行安全审计。

目前，操作系统、数据库系统、网络设备、应用系统等均提供了日志记录和审计功能，开启这些审计功能并定期进行审计，对于及时发现网络攻击行为，追踪和确定攻击来源具有很大的帮助。但由于设备分散，分布式的独立审计不能满足对各种网络攻击行为的审计要求，同时对网络攻击来说，有很大一部分威胁不是以网络入侵的形式进行的，而是由于内部合法用户的误操作或恶意操作，仅靠网络入侵检测也不能满足对网络的监控审计要求，本次针对数据库建议部署**数据库审计系统。**

为加强对内部人员网络行为安全监控与审计，防止滥用网络资源和非授权访问极为重要。因此，需要在系统中建议部署**堡垒机**，来实现对内部网络访问行为、主机操作行为等的采集、分析和识别，实时监视网络系统的运行状态，记录网络事件，发现安全隐患，并对网络活动的相关信息进行分析。

通过对网络数据的审计，对网络传输信息进行记录，监控来自网络内部和外部的用户活动，侦察系统中存在的现有的安全威胁和违规行为，就能够测试安全策略是否充足，证实安全策略的一致性，建议安全策略的改变，并协助分析攻击，收集证据，用于事后追踪起诉。

4.1.4.2 恶意病毒防范

系统中重要服务器主机上也应部署**防病毒软件系统**。全系统的病毒库更新可以采用集中管理。

- 在服务器上安装服务器版的防病毒软件，可以捍卫服务器免受病毒、特

洛伊木马和其它恶意程序的侵袭，不让其有机会透过文件及数据的分享进而散布到整个用户的网络环境，提供完整的病毒扫描防护功能；

- 文件系统对象的实时保护：防病毒系统通过对文件系统所有需要的模块进行分析，以及阻止恶意代码的执行，为服务器和终端中的文件系统提供实时保护。具体包括：
  - 监听对文件系统的访问；
  - 使用反病毒引擎对可疑对象和染毒对象进行探测；
  - 当检测到染毒或可疑对象时执行预设：
    - i. 阻止染毒或可疑对象；
    - ii. 在为染毒对象清除病毒之前将他们的副本存储在备份区；
    - iii. 启动反病毒引擎以清除或删除染毒对象；
    - iv. 将可疑对象放置在隔离区或将它们删除；
  - 在程序运行过程中向用户和本地管理员通报所发生的与其有关的事情；
  - 收集被检查过的对象的数据
- 隔离可疑对象：服务器防病毒系统隔离与备份组件隔离任何可疑对象，为了使防病毒厂商对其进行进一步的分析，该组件对恶意代码进行安全隔离。这个组件也可以使恶意代码的安全检测和清除方法的到发展。
- 隔离和备份组件执行下列任务：
  - 保存检测到的可疑对象；
  - 按要求保存疑对象；
  - 按要求发送可疑对象到防病毒厂商用于分析，同时允许发展其检测及清除病毒的安全方法；
  - 在接收防病毒厂商针对病毒的更新后，重新检测存储在隔离区的对象，用于确定对象的状态及清除病毒的必要性；
  - 按要求恢复隔离区中的对象
- 通过集中隔离工具，可以将感染病毒档案集中隔离到一台服务器；
- 通过病毒追踪工具，当有病毒通过网络共享扩散时，可以侦测到感染病毒的机器；
- 软件安装时可对病毒进行预处理，安装后不需要重新启动；

- 实现强大、完善的日志管理策略；
- 实现病毒库的自动升级：在安全管理区域部署防病毒系统的集中控管服务器，自动到互联网上升级厂商发布的病毒库更新代码，然后自动将更新代码下发到保护的服务器的终端上。

4.1.4.3 系统漏洞管理

应严格完善安全补丁管理流程，定期在应用服务器上发布经过测试的操作系统补丁包，由维护管理人员定期下载和安装操作系统补丁。

- 定期的网络安全自我检测、评估

建议配备**漏洞扫描系统**，网络管理人员定期进行网络安全检测服务，最大可能的消除安全隐患，尽可能早地发现安全漏洞并进行修补，有效的利用已有系统，优化资源，提高网络的运行效率。

- 安装新软件、启动新服务后的检查

由于漏洞和安全隐患的形式多种多样，安装新软件和启动新服务都有可能使原来隐藏的漏洞暴露出来，因此进行这些操作之后应该重新扫描系统，才能使安全得到保障。

4.1.5 应用安全

4.1.5.1 日志管理跟踪

日志管理跟踪记录用户登录系统的信息，操作的业务模块以及操作的重要库表的信息，包括用户名称、操作的模块，对重要库表的操作类型（增、删、改）、字段操作前和操作后的数值等。通过日志管理，在发生误操作时可以方便的进行回退处理，而且也可以跟踪一些业务操作员的违规操作。本次建议部署**日志审计系统。**

4.1.6 数据安全

按照业务系统的相关部署，在系统安全防护体系的整体框架下，依据系统的安全风险评估、战略规划等相关信息，结合网络和业务自身的实际情况，分析各相关系统不同等级的安全需求，平衡效益与成本，制定备份及恢复策略，在此基础上实现备份技术方案，构建并执行恢复预案，以便于提高系统抵御灾难的能力，尽可能减小因灾难引起的各种损失，从而增强系统的安全防护能力和持续作业能

力，保证全省业务系统持续不间断运转。

容灾中心作为异地数据容灾中心，借助容灾技术实现数据容灾。并通过安全体系建设保障备份数据的安全性。生产中心与灾备中心之间通过专线连接，实现备份数据远程复制，当生产中心故障时，业务数据可通过容灾中心数据对生产中心进行恢复，保障核心信息系统业务数据不丢失。实现数据备份、数据容灾、数据零丢失。

建议配置数据备份系统和数据容灾系统，并通过相应的技术手段将本地备份的数据保存至灾备机房。

4.2 安全管理建设方案

针对武汉市江汉区卫计委重要信系统，按照高级别（三级）的管理要求建设，主要是依据《信息系统安全等级保护基本要求》；通过安全咨询及安全规划，实现包括安全管理机构、安全管理制度、人员安全、系统建设管理和系统运维管理等安全管理体系，最终达到符合等级保护的管理要求。

4.2.1 安全管理制度

根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

制定严格的制定与发布流程，方式，范围等，制度需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。

信息安全领导小组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，定期或不定期对安全管理制度进行评审和修订，修订不足及进行改进。

4.2.2 安全管理机构

根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；

设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；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；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。

建立授权与审批制度；

建立内外部沟通合作渠道；

定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

4.2.3 人员安全管理

根据基本要求制定人员录用，离岗、考核、培训几个方面的规定，并严格执行；规定外部人员访问流程，并严格执行。

4.2.4 系统建设管理

根据基本要求制定系统建设管理制度，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级评测、安全服务商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。

4.2.5 系统运维管理

根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，包括：环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应等级安全状态中。

江汉区卫计委信息机房等保测评设备清单

序号	设备/软件名称	配置	数量	单价	合计	说明
1	核心交换机	机箱式路由交换机主机（4 个业务插槽，前两个业务插槽可插管理引擎模块，交流电源 1+1 冗余），标配 1 个 MRS-PWR-AC-B 交流电源,满配风扇盘，不含管理引擎模块 MRS-PWR-AC-B 交流电源模块（220V，500W） 强管理引擎模块，（24 个千兆 SFP 光接口+16 个复用的千兆以太网电口（RJ45）	1	65,000.00	65,000.00	
2	防火墙	2U 配置 6 个千兆电口，2 个 SFP 光口，吞吐率 20Gbps，并发 500W；含 IPS 模块	3	91,440.00	274,320.00	
3	防病毒过滤网关	2U 机箱 最大配置为 26 个接口，默认包括 2 个可插拔的扩展槽，2 个 10/100/1000BASE-T 接口（作为 HA 口和管理口），4 个 SFP 插槽和 4 个 10/100/1000BASE-T 接口 标配模块化双冗余电源，默认电口具有两组 BYPASS 接口 默认含企业版查杀病毒功能 整机吞吐率：3Gbps 最大并发连接数：220W 病毒检测吞吐率：800Mbps	2	91,800.00	183,600.00	
4	日志审计系统	含日志收集、存储、查询、关联分析、统计分析、告警响应等功能，综合处理性能:20000EPS 综合处理峰值：30000EPS，含 50 个日志源 license，需提供安装服务器	1	45,000.00	45,000.00	含 50 个日志源，需提供服务器
5	漏洞扫描系统	1U 配置 4 个千兆电口,1 个扩展槽，任务不限制 IP 数量 最大允许并发扫描 60 个 IP 地址	1	58,860.00	58,860.00	
6	企业版杀毒软件	防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS 病毒等进行查杀,提供主动防御系统防护等功能，含 50 个主机许可 license，以及 5 台服务器	1	10,980.00	10,980.00	含 50 个 PC 点授权，5 个服务器授权，需要提供服务器
7	堡垒机	1U 配置 4 个千兆电口,1 个扩展槽，1T 存储,含 50 个设备许可 license	1	97,200.00	97,200.00	
8	容灾备份一体机	2U 机架式存储设备；DDR3 内存 16Gx4 （ECC）；6 个热插拔盘位；510W 冗余供电；双路多核处理器；4 口千兆网卡，36T 容灾备份授权 license	1	136,000.00	136,000.00	

9	数据库审计	2U 配置 4 个千兆电口,500G 存储空间，吞吐率 500Mbps 记录事件 35000 条/秒 总记录事件 260 亿条	1	63,000.00	63,000.00	
10	24 口汇聚交换机	背板带宽：598Gbps 包转发率:216Mpps/222Mpps 接口类型:24 个 10/100/1000TX，4 个 SFP 接口数目:24 口 传输速率:10M/100M/1000Mbps 管理端口:1 个 Console 口	1	8,500.00	8,500.00	
11	机柜	600*1000*2000	1	4,500.00	4,500.00	
12	PDU	220V/16A	2	300.00	600.00	
13	理线工程	国标	1	5,400.00	5,400.00	
14	系统等保三级测评	国标	1	120,000.00	120,000.00	
江汉区卫计委信息机房设备合计（税费 13%）：				**1,072,960.00**		

第5章 设备清单及预算