**成都市温江区妇幼保健院**

**网络安全建设方案**

**2024年7月**

# 建设背景

2023年12月29日四川省卫生健康委员会印发《四川省互联网医院管理办法（试行）》，要求“互联网医院应具备满足互联网技术要求的设施设备、信息系统、技术人员以及信息安全系统”。

2021年11月1日《中华人民共和国个人信息保护法》正式实施，内容共8章74条，要求个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

2021年9月1日，《中华人民共和国数据安全法》正式实施。内容共7章55条，提出国家将对数据实行分级分类保护、开展数据活动必须履行数据安全保护义务承担社会责任等。

2019年12月1日开始实施等保2.0相关的《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》。

数字化转型是医疗行业发展的重要方向，而信息系统的网络安全是医疗数字化健康发展的基础。医疗信息系统涉及到患者的公民隐私、医疗数据、管理督导等多个方面，一旦遭受网络攻击或数据泄露，不仅会对患者的治疗和健康造成影响，还会对国家机构的声誉和公信力造成损害。成都市温江区妇幼保健院高度重视数字化转型中面临的网络安全威胁，为了提升医院网络安全防护能力、降低安全风险，成都市温江区妇幼保健院将针对医院终端和网络接入加强安全防护建设。

# 建设依据

## 相关政策文件及法律法规

* 《中华人民共和国网络安全法》
* 《中华人民共和国数据安全法》
* 《中华人民共和国密码法》
* 《中华人民共和国个人信息保护法》
* 《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）
* 《关于印发《信息安全等级保护管理办法》的通知》（公通字[2007]43号）
* 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429）
* 《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）
* 《卫生行业信息安全等级保护工作的指导意见》
* 《医疗卫生机构网络安全管理办法》

## 相关标准

* 《四川省智慧医院评审标准》
* 《信息安全技术网络安全等级保护基本要求》(GB/T 22239-2019)
* 《信息系统安全保护等级定级指南》（GB/T 22240-2008）
* 《计算机信息系统安全保护等级划分准则》（GB17859-1999）
* 《信息系统等级保护安全设计技术要求》
* 《信息安全等级保护实施指南》
* 《信息系统安全等级保护测评要求》
* GA/T671-2006《信息安全技术 终端计算机系统安全等级技术要求》
* GB/T22080-2008《信息技术 安全技术 信息安全管理体系要求》
* GA/T387－2002计算机信息系统安全等级保护网络技术要求
* GA/T388－2002计算机信息系统安全等级保护操作系统技术要求
* GA/T389－2002计算机信息系统安全等级保护数据库管理系统技术要求
* GA/T390－2002计算机信息系统安全等级保护通用技术要求
* GA/T391－2002计算机信息系统安全等级保护管理要求
* GB/T 35273-2020信息安全技术个人信息安全规范

# 风险分析

## 终端安全风险

1、成都市温江区妇幼保健院内网接入的终端类型日益丰富，除了PC、服务器、哑终端，还有各种智能终端；这些终端的产权归属是复杂的，可能属于医院，也可能属于医护人员、第三方供应商等；终端上的操作系统也是多样的，除了主流的，还有小众的，甚至老旧的（例如Win 7/XP等原厂不提供服务的），终端的复杂性导致网络的安全风险加剧。

2、终端操作系统和主流应用的高危漏洞越来越多，临时补救、补丁验证和修复缓不救急；医院终端与医院业务的交互频繁，落在终端上的数据和应用变得越来越多且杂乱，给黑客攻击提供了更多的通道；医院医护人员的安全意识参差不齐，导致医院电脑终端很容易被利用，成为黑客攻击的跳板或帮凶。

3、医院电脑终端未进行相关安全防护，终端可能受到病毒、木马、勒索软件等恶意软件的攻击，这些攻击可能导致数据丢失、系统瘫痪，甚至威胁到患者的生命安全。

4、医院未对终端红外、蓝牙、摄像头、手机/平板、移动数据网卡、MODEM设备、ISDN设备、ADSL设备、移动存储介质等进行管控，这些设备随意接入与使用，将带来病毒传播、数据泄露等风险。

5、医院医护人员可随意更改主机名、IP地址、MAC地址等信息，弱口令、弱密码屡见不鲜，终端壁纸不统一、不规范，随意设置共享端口，给医院资产管理、网络审计等方面造成不便。

6、有的医护人员为了工作方便，通常存在“一机多网”的情况，将终端同时连通医院内网和互联网，容易成为黑客攻击的途经，这将给医院内网带来极大的安全风险。

对于攻击者而言，终端既可以作为攻击目标，也可以作为攻击的跳板，因此终端的安全直接关系着成都市温江区妇幼保健院整体网络安全。由于医院终端时刻面临着病毒感染、网络入侵和漏洞利用等风险，因此加强终端的安全性和可对抗性，是保证业务安全和网络安全基础问题，也是核心问题。

同时，终端安全状况没有一个标准的基准线，对不安全的终端设备如果不能采取有效的隔离和修复措施，漏洞病毒的防护应对不到位，一旦发生病毒感染，往往扩散到全网络，令成都市温江区妇幼保健院网络陷于瘫痪状态，数据安全无法保证，医护人员工作也无法正常进行。

## 网络接入风险

1、缺乏内网接入身份验证机制，外来人员随意可接入到医院内部网络，给医院各业务系统带来风险。未经确认身份是否合法的终端即可接入到网络中，容易发生数据窃取、病毒传播等风险。

2、部分医务人员安全意识薄弱，终端存在较大的安全风险，比如未安装杀毒软件、不合规操作系统、未及时更新操作系统、终端使用弱密码等。不合规终端接入网络，给医院内网环境带来巨大威胁，比如导致勒索病毒在内网疯狂传播，严重的可能影响医院业务。

3、智慧医疗和移动医疗导致医院IoT物联网设备迅速增加，但是缺乏有效的安全管控机制，一旦被黑客利用，便可迅速进入医院内网，出现数据泄密、病毒扩散、系统破坏等风险。

4、医生办公终端、医疗手持终端、医疗器械、IoT终端等。这些终端设备未经可信认证就能随意接入医院内网或无线网络，并且这些终端本身可能存在一些安全隐患，给医院内网安全带来巨大隐患。

开放式的网络使得任何一个人都能够通过便携设备随意接入成都市温江区妇幼保健院网络中，能够访问医院各种网络资源，犹如没有门卫一样，任何人都可以随便进出，随意访问，不受到任何检查和限制。可以想象这样的开放式网络为恶意访问提供了入侵的便利条件，采用非常简单的攻击技术便可造成巨大的破坏，从而不但给成都市温江区妇幼保健院带来巨大的安全风险，更有可能造成医院的各种数据泄露。

## 网络攻击风险

* 医疗行业成为黑客攻击的重要目标

由于医院的特殊性，患者预约信息、检查检验信息、就诊信息、医学数据等医疗信息都是属于需要紧急使用的信息，一旦这些数据被加密勒索，就会造成很大的影响，这些具有较高商业价值的诊疗信息，长期受到黑色产业链的觊觎。

* 勒索病毒等攻击造成严重威胁

2017年以来，医疗行业已成为攻击者实施勒索的最主要目标，有29%的勒索软件的攻击目标是各类医疗相关机构。除勒索外，医疗业务资源被黑客滥用于挖矿，亦会破坏内部IT环境、数据中心的正常运行秩序以及关键应用的交付，同样使得业务连续性遭受极大安全威胁。勒索、挖矿已经成为影响医疗业务连续性的主要威胁。

* 医疗信息泄露问题

医疗数据泄露事件也呈逐年上升趋势，医院的网络与终端不加以管控，导致患者的就诊信息泄露，不仅会造成患者的安全威胁、面临患者的法律诉讼、医疗机构的声誉受损，严重的话还会导致社会安全感下降。

# 建设方案概述

## 建设总体原则



医院作为保障基础民生的重要基础设施，确保医疗服务的稳定是十分重要的。方案依据信息安全等级保护要求，以“纵深防御”为指导思想，以技术保障为基础、以管理运营为抓手、以监测预警为核心、以协同响应为目标，从技术、管理、服务等方面进行全面的安全设计和建设，有效提高信息系统的防护、检测、响应、恢复能力，以抵御不断出现的安全威胁与风险，保证系统长期稳定可靠的运行。

**计算环境方面：**

1、建设终端安全管理系统：对医院内网终端提供统一漏洞修复、病毒查杀、外设管理、进程防护、访问控制、勒索防御、挖矿防御等。

**安全管理方面：**

1、建设准入控制系统：实现医院核心业务的访问控制、实现用户和终端的实名制认证管理、终端接入的安全防护、终端入网的追溯分析。

## 终端安全管理系统建设

### 产品概述

终端安全管理系统注重实效的一体化终端安全解决方案，通过体系化防御、数字化运营方法，帮助医院准确识别、保护和监管终端，并确保这些终端在任何时候都能可信、安全、合规地访问数据和业务。系统集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，通过系统合规与加固、威胁防御与检测、运维管控与审计、统一管理与运营等功能，帮助医院构建持续有效的终端安全能力。

### 产品功能

* 终端恶意代码检测

恶意代码攻击常常利用社会工程学、零日漏洞、定制恶意软件等，传统的基于特征库的被动防御体系无法识别异常流量，存在严重的滞后性。终端安全管理系统提供先进的网络版防病毒功能，通过多种查杀引擎构建的多维智能检测体系，并配合主动防御，可对医院终端蠕虫病毒、恶意软件、APT、广告软件、勒索软件、引导区病毒等进行检测查杀。

终端安全管理系统具备多引擎病毒扫描与检测，包括但不限于：快速查杀、全盘查杀、自定义查杀、存储介质查杀方式，并可以设置多种查杀时机。

快速查杀：有效扫描随系统自启动运行的风险文件，扫描系统常被利用的位置，如系统关键目录、内存等。

全盘查杀：全面扫描计算机，包含快速扫描内容以及所有磁盘、内存、引导区等，更彻底清理木马病毒。

自定义查杀：按指定位置有选择性的扫描。

存储介质查杀：当U盘接入时，主动对U盘中的文件进行扫描，同时针对U盘传播恶意软件（如隐藏文件等）和常见的恶意修改操作进行修复。

多种查杀时机：具备开机时、进程启动时、账户登录时、以及每天、每周、每月等周期性的多种执行时机。

终端病毒文件被扫描清除后，具备在隔离区备份保存的功能，将病毒文件加密备份在系统硬盘上，可随时恢复到原始路径或提取至目标路径。当在隔离区执行删除操作后，该文件才彻底从硬盘上删掉。

* 终端漏洞修复

终端安全管理系统漏洞检查与修复功能可有效提升医院终端整体漏洞防护等级，终端安全管理系统具备三大类漏洞管理能力，分别是操作系统级Office高危漏洞、官网尚未修复的0day漏洞、软件更新以及功能性更新补丁。

操作系统及Office高危漏洞：此类补丁一般为微软发布的严重或重要级别漏洞补丁，漏洞级别由微软安全公告全球公开发布，涵盖有Windows系统级补丁、Office补丁以及Windows中各种组件的补丁（如Visual Studio、.Net Framework等）。

官网尚未修复的0day漏洞：0day漏洞一般为微软或其它流行软件被曝光的严重漏洞，在官方还来不及修复情况下已经遭到黑客利用，从而使造成非常广泛的恶劣影响。

软件更新：此类为第三方软件的严重漏洞。主要为比较流行软件中的漏洞（例如Adobe Flash Player、Acrobat Reader），而这些漏洞可能导致严重问题。

在日常的漏洞管理过程中，终端安全管理系统可对全网计算机终端进行漏洞扫描，并把计算机与漏洞进行多维关联，根据终端或漏洞进行分组管理，根据不同的计算机分组与操作系统类型将补丁错峰下发，在保障网络带宽的前提下可以有效提升整体终端漏洞防护等级。

* 终端办公安全防护

为保障医护人员的日常办公安全，终端安全管理系统对常用的办公工具和办公行为进行了重点防护，包括邮件防护、U盘安全防护、即时通讯工具（IM）防护、下载防护、局域网文件防护、网页安全防护、勒索软件防护、搜索安全防护、浏览器及首页防护等防护，以全面保障办公业务安全。

邮件防护：实时对邮件收发软件收取的电子邮件进行安全检测，防止邮件中内置的恶意程序利用操作系统的漏洞，对系统进行攻击或病毒植入。

U盘安全防护：实时检测系统接入U盘的行为，对U盘中关键位置的文件进行安全扫描，对发现的风险文件进行提示和清理，避免系统受到U盘中恶意文件的入侵。

即时通讯工具（IM）防护：实时对即时通讯工具（IM）下载的文件进行安全检测，对文件的风险进行提示和清理，防止从IM下载恶意程序。

下载防护：实时对下载软件、浏览器下载的文件进行安全检测，对文件的风险进行提示和清理，防止从网络应用下载恶意程序。

局域网文件防护：实时检测局域网网络共享文件的拷入、执行行为，当检测文件不安全时，进行提示和拦截，防止从局域网共享目录下载恶意程序。

网页安全防护：实时对浏览器中访问的URL和网页内容进行安全扫描，对发现的风险进行提示和拦截。

勒索软件防护：实时检测未知风险程序的篡改文件和勒索病毒相关特征行为，避免系统遭受勒索软件的加密等破坏行为。

搜索安全防护：搜索引擎有时会利用Cookies记录上网痕迹，然而这些Cookies很容易受到黑客利用，导致个人隐私泄露，同时会遭受个性化推荐广告或者其他弹窗骚扰，通过搜索引擎安全防护，将上网Cookies定期清理，保障个人隐私安全。

浏览器及首页防护：终端用户可以设置终端默认浏览器和首页，防止被恶意篡改，实现浏览器标准化管理。

* 终端系统安全防护

为防止终端系统被恶意程序侵害，终端安全管理系统提供进程防护、注册表防护、驱动防护、远程登录防护、网络入侵防护、僵尸网络攻击防护、网络攻击防护、ARP攻击防护、主机防火墙等安全机制，保障终端操作系统核心资源的运行安全。

进程防护：实时监测活跃进程的各种系统行为（如进程创建、系统注入与挂钩等），当判定为恶意行为时，进行提示和拦截，避免系统受到各种恶意行为的侵害。

注册表防护：实时监测系统关键注册表的创建、修改和删除行为，当判定为恶意行为时，进行提示和拦截，以阻止恶意程序试图开机启动、伴生启动或破坏系统的行为。

驱动防护：实时监测系统的驱动安装、加载、卸载等行为，当判定为恶意行为时，进行提示和拦截，以阻止恶意程序试图躲避安全软件的检测、破坏安全软件或破坏系统的行为。

远程登录防护：自动阻止远程登录行为，防止黑客远程爆破和拦截恶意的远程登录。

网络入侵防护：实时对流入本机的网络包数据和行为进行检测，在网络层拦截漏洞攻击、黑客入侵等威胁。

僵尸网络攻击防护：实时对流出本机的网络包数据和行为进行检测，在网络层拦截后门攻击、C2连接等威胁。

网络攻击防护：实时对流出本机的网络包数据和行为进行检测，在网络层拦截后门攻击、C2连接等威胁。

ARP攻击防护：实时检测和拦截局域网中的ARP欺骗攻击行为。

主机防火墙：基于网络五元组信息对终端主机网络的出入站流量进行控制，配置和管理防火墙放行或拦截规则，对终端的异常网络请求进行有效控制。

* 终端信息采集

帐号信息采集：实时采集终端的本地账户及域账户信息，包括账户名称、用户ID、所属用户组、是否启用、账户类型、账户主目录、是否为域账号等信息。

软件信息采集：实时采集终端的软件信息，包括软件名称、软件版本、软件开发厂商、软件运行路径、软件大小、软件安装时间等信息。

硬件信息采集：采集终端的硬件信息，包括显示器、光驱、系统信息、主板信息、显卡信息、音频、PC信息、内存信息、鼠标、键盘、处理器、硬盘信息、网卡等信息。

服务信息采集：实时采集终端的服务信息，包括服务名称、显示名称、服务版本号、服务程序开发商、服务运行路径、服务描述、服务启动类型、服务状态等信息。

启动项信息采集：采集终端的启动项信息，包含启动项类型有：系统的注册表启动项（包括各类系统插件、Run项、右键菜单）、应用层服务、驱动、计划任务、WMI等。采集启动项信息包括启动项名称、启动项类型、启动项状态、描述等。

资产盘点：按资产视角展示各类型资产，包括Web服务、Web框架、Web应用、数据库、软件应用、注册表、启动项、端口、进程、系统账户、系统安装包、Jar包、计划任务、环境变量、内核模块、Windows证书等资产类型。

* 终端违规外联控制

违规外联可在网络安全区域之间、内网与外网之间建立新的连接通道，使防火墙、控制网关等防护设备组成的信息安全保障防线变成了马奇诺防线。外部的黑客、病毒就能够绕过防火墙、控制网关等防护屏障，侵入违规外联的终端计算机，非法窃取敏感数据，甚至利用该终端作为跳板，进一步渗透内网的重要服务器，整个内部网络将面临被控制的重大风险。

为了更有效、更及时侦测内部终端是否存在非法连接外网或指定网络的行为，终端安全管理系统可通过其外联探测功能，定时对终端的访问进行循环检测，采用域名解析、PING地址探测、TCP链接检测等方式，发现终端的违规外联行为，在探测到互联网连接时执行断网、重启或锁屏等措施，保证医院终端网络安全。

* 终端外设控制

为细化外设的使用权限，减轻病毒传播、数据泄露等风险。系统具备外设管控措施，实现对终端串口、并口、USB接口管控，对内置光驱和外置光驱进行管控；对红外、蓝牙、摄像头、手机/平板、移动数据网卡、MODEM设备、ISDN设备、ADSL设备管控。针对移动存储介质按组划分不同的授权使用范围和读写权限，细化控制不同的读写权限，集中管控终端的移动存储介质使用规则，规避移动存储介质带来的安全风险。

* 终端网络管控

系统支持对终端网卡地址控制、热点创建控制、DNS地址设置（非地址绑定）、Wi-Fi连接控制，禁止终端同时连接多个无线信号（多无线网卡环境）。检测当前终端是否存在有线无线共用场景，如存在则自动断开无线连接，通过设置可信Wi-Fi列表控制终端能连接的无线SSID。基于IP、域名和端口等维度进行终端网络控制，阻止网络攻击。实现对终端的DNS地址进行统一配置，阻止通过指定的DNS进行攻击。

注：合同签订后终端安全管理系统产品所有权归采购方（含前三年授权）！