**容灾机房（信息科机房）**

**目 录**

[1. 项目简介 1](#_Toc176101051)

[1.1. 项目名称 1](#_Toc176101052)

[1.2. 项目建设单位 1](#_Toc176101053)

[1.3. 项目建议书编制依据 1](#_Toc176101054)

[1.4. 项目概况 1](#_Toc176101055)

[1.5. 主要结论和建议 1](#_Toc176101056)

[2. 项目建设单位概况 2](#_Toc176101057)

[2.1. 项目建设单位与职能 2](#_Toc176101058)

[2.2. 项目实施机构与职责 3](#_Toc176101059)

[3. 项目建设的必要性 4](#_Toc176101060)

[3.1. 项目背景和依据 4](#_Toc176101061)

[3.2. 容灾机房（信息科机房）建设标准 5](#_Toc176101062)

[3.3. 现有容灾机房（信息科机房）信息化应用状况 6](#_Toc176101063)

[3.4. 项目建设的意义和必要性 7](#_Toc176101064)

[4. 需求分析 9](#_Toc176101065)

[4.1. 安全保密与自主可控 9](#_Toc176101066)

[4.2. 系统需求分析 12](#_Toc176101067)

[5. 建设方案 17](#_Toc176101068)

[5.1. 建设原则和策略 17](#_Toc176101069)

[5.2. 项目建设目标 17](#_Toc176101070)

[5.3. 国内外医院容灾机房技术对比 17](#_Toc176101071)

[5.4. 技术方案 18](#_Toc176101072)

[6. 环保、消防、职业安全、职业卫生和节能 27](#_Toc176101073)

[6.1. 环境影响和环保措施 27](#_Toc176101074)

[6.2. 消防措施 27](#_Toc176101075)

[6.3. 职业安全和卫生措施 27](#_Toc176101076)

[6.4. 节能目标及措施 28](#_Toc176101077)

[7. 项目组织机构和人员 29](#_Toc176101078)

[7.1. 领导和管理机构 29](#_Toc176101079)

[7.2. 项目实施及运行维护机构 29](#_Toc176101080)

[7.3. 技术力量和人员配置 29](#_Toc176101081)

[7.4. 培训目的 30](#_Toc176101082)

[7.5. 培训目标及对象 30](#_Toc176101083)

[7.6. 培训方式 30](#_Toc176101084)

[7.7. 培训内容 32](#_Toc176101085)

[8. 项目实施进度 33](#_Toc176101086)

[9. 项目风险分析 34](#_Toc176101087)

[9.1. 协调风险及控制 34](#_Toc176101088)

[9.2. 项目技术风险控制 34](#_Toc176101089)

[9.3. 社会影响风险及控制 34](#_Toc176101090)

[附表1：项目软件配置清单及预算 36](#_Toc176101091)

[附表2：项目详细配置清单 37](#_Toc176101092)

# 项目简介

## 项目建议书编制依据

1、通过中讯邮电咨询设计院有限公司现场调查收集的资料，分别包括了信息科和相关科室人员的建议。

2、2024版电子病历系统应用水平分级评价标准中电子病历基础要求：



## 项目概况

医院容灾机房项目的背景主要源于对数据安全性和业务连续性的高度需求。随着信息化时代的快速发展，医院对数据的依赖程度越来越高，容灾机房作为医院重要的信息存储和处理枢纽，其可靠性和稳定性对于保障业务连续运行至关重要。然而，自然灾害、人为因素或技术故障等可能导致容灾机房发生灾难性故障，给医院正常开展业务带来较大风险。因此，医院考虑建设容灾机房项目，实现数据的实时备份和快速切换，以保障医院业务的正常和连续性，同时有效防止网络数据泄露或被窃取、篡改。

## 主要结论和建议

结论：随着信息化建设的普及与发展，医院数据中心所面临的风险和威胁也越来越大，由于计划外系统中断造成的停机会给医院带来的经济与信誉等诸多方面的损失。在以往的信息化建设过程中，由于管理的需要，IT 资源往往走过一个从分散到集中的道路，当前信息化通常都是一个资源高度整合的系统。正是因为高度集中，一旦发生意外事故，势必造成医院业务中断，后果不堪设想。为保证 7×24 全天候运行，需要一个全面的业务连续性计划，可以提供业务高可用性、数据高可靠的双重保障。此次项目建设需要对医院进行数据中心容灾建设，构建统一、完善的数据中心容灾体系，为各类应用业务提供高可用性基础保障，保障数据的一致性和完整性。

建议：为有利于该项目的顺利开展，建议及时组织相关信息化技术人员成立医院信息化项目工作小组，继续完善项目建设方案，加快项目推进步伐。并建议落实项目建设资金，继续本项目的工程设计及概算编制、招标文件编制及相关招投标工作，争取2024年底竣工验收，2025年初试运营。

# 项目建设单位概况

## 项目实施机构与职责

### 信息科

1、制定计算机管理规程：负责计算机房的管理及计算机统一操作规程和规范的制定；

2、组织实施硬件升级：关注计算机科学和技术的发展，提出软件和硬件升级的建议和计划，并在批准后组织实施；

3、调试和维护配置：负责网络工作站的硬件配置、安装和维护，负责网络计算机的正常运行；

4、负责安全系统：负责用户软件的分配、授权、严格的密码安全系统；

5、掌握计算机原理并定期检查：掌握常用计算机部件的原理和维修方法，指导技术人员维护全院通用计算机的硬件，定期检查和维修，并回答用户的询问；

6、协助管理设备信息：协助电脑网络中心秘书管理设备信息，包括登记、分类、储存、备份和抄录。

# 项目建设的必要性

## 项目背景和依据

医院是一所集医疗、教学、科研、预防保健、卫勤保障为一体的大型综合性正规甲等医院。医院门诊量和住院人数持续上升，进一步加重了医院的负担，但凭借着医院信息人员的专业能力和内部信息化多年的建设，目前具备一定规模,随着医疗行业信息化建设多样化的背景下,各项不同种类的IT应用系统不断的加入到医院信息化建设的队伍中来，目前医院正在进行部分的国产化建设，以体检系统等业务系统为试点进行国产化的改造工作。

单位现有环境采用的是物理服务器方式，数量有10台服务器，用来运行单位所有的业务系统，现状规划的是一台服务器运行一套业务系统。 主要运行HIS、LIS等核心的业务系统，其余还有PACS等业务系统，对于医院来说，这些业务系统和数据尤为重要；根据梳理，医院目前对于数据备份保护的现状，面临如下需求：

(1) 数据中心数据备份保护刚性需求：高可用、多负载、虚拟化等技术无法保障由逻辑错误、勒索病毒、病毒、误删除造成的业务系统中断，所以在保障业务系统连续性的同时，数据安全也更为重要。

(2) 解决自然灾害或突发事件风险需求：如地震、火灾、水灾、雷击等，发生概率低，一旦发生就是彻底灾难事故，对于数据和应用造成毁灭性的破坏，在主机房整体故障的极端情况下，需要保障数据安全。

(3) 响应国家国产化建设需求：信息化应用创新发展是当前的国家战略，国产化是大势所趋，在进行信息系统环境进行国产化建设的同时，备份容灾平台也需要进行全面国产化。

(4)制定应急制度及措施需求：缺乏对数据安全备份、恢复、应急事件处理等工作的规范和规章制度，紧急事件应急响应预案缺乏演练，面对紧急事件时缺乏经验；。功能性能指标达到预定目标要求情况。

容灾能力建设是《中华人民共和国网络安全法》下应急预案制度的重要组成部分。容灾能力建设是《中华人民共和国数据安全法》下数据处理者的法定义务。容灾能力建设是最大程度减轻勒索病毒攻击造成损失的重要手段。

## 容灾机房（信息科机房）建设标准

本项目的设备选型及设计规划按照以下标准执行：

《电子计算机房设计规范》 GB50174-93

《智能建筑设计标准》 GB/T50314-2000

《民用建筑电气设计规范》 JGJ/T16-92

《电子计算机房设计规范》 GB50174-93

《民用闭路监视电视系统工程技术规范》 GB50198-94

《有线电视系统工程技术规范》 GB50200-94

《火灾自动报警系统施工和验收规范》 GB50166-92

《火灾自动报警系统设计规范》 GBJ50116-98

《大楼通信综合布线系统》 YD/T926.1-1997

《建筑与建筑群综合布线系统工程设计规范》 GB50311-2000

《建筑与建筑群综合布线系统工程验收规范》 GB50312-2000

《安全防范工程程序与要求》 GA/T75-94

《安全防范系统通用图形符号》 GA/T74-94

《物业管理IS09002》 GB/T19002-1994；

《电气装置安装工程电缆线路施工及验收规范》 GB50168-92；

《电气装置安装工程接地装置施工及验收规范》 GB50169-92；

《电气装置安装工程盘、柜及二次回路结线施工及验收规范》 GB50171-92；

《电气装置安装工程蓄电池施工及验收规范》 GB50172-92；

《电气装置安装工程电气照明装置施工及验收规范》 GB50259-92；

《低压成套开关设备验收规范》 CECS49：93；

《套接紧定式钢导管电线管路施工及验收规范》 CECS120：2000；

《计算站场地技术要求》 GB2887-89

《计算站场地安全要求》 GB9361-88

《计算机房活动地板技术条件》 GB6650

《通风与空调工程施工与验收规范》 GB50243-97

《电气装置安装施工及验收规范》 GBJ232-9092

《低压配电设计规范》 GB50054-95

《建筑物防雷设计规范》 GB50057-94（2000年版）

《高层民用建筑设计防火规范》 GB50045-95（2001年版）

《建筑内部装修设计防火规范》 GB50222-95（公告22.29）

《建筑设计防火规范》 GB16-87（2001年版）

《电子计算机机房施工及验收规范》 SJ/T30003-93

《涉及国家秘密的计算机信息系统安全保密方案设计指南》其他相关规范 。

## 现有容灾机房（信息科机房）信息化应用状况

‌容灾机房应用现状体现了医院在保障业务连续性和数据安全方面的努力，但同时也暴露出一些挑战和改进空间。

容灾机房，作为IT系统高可用性技术的一部分，通过在相隔较远的异地建立两套或多套功能相同的IT系统，实现健康状态监视和功能切换，确保在主系统因灾难停止工作时，整个应用系统可以切换到备用系统，保持功能正常运行。这种技术强调处理外界环境对系统的影响，特别是灾难性事件对整个IT节点的影响，提供节点级别的系统恢复功能‌。

然而，尽管医院对容灾的认识和投入在增加，业务连续性这一难题仍未得到彻底有效的解决。例如，国内某云服务商的云服务异常事件，暴露出即使在医院安全意识和保障技术持续优化的背景下，业务连续性问题的解决仍然面临挑战。此外，医院信息化容灾建设的概况显示，大部分医院采用了同楼容灾方式，而采用异楼容灾方式的医院比例较低，显示出容灾建设的总体比例仍然偏低，且存在较大的提升空间‌。

在国际比较中，我国的综合容灾覆盖率与欧美等国相比存在较大差距。例如，我国的综合容灾覆盖率为34%左右，而欧美超过80%‌2。这表明，尽管国家层面在推进现代化产业体系和提升数据要素及安全的重要性，但容灾系统的建设和运维运营仍然面临诸多挑战，需要进一步的技术创新和政策支持来提升容灾覆盖率和技术水平‌。

综上所述，容灾机房的应用现状体现了医院在保障业务连续性和数据安全方面的努力，但同时也暴露出一些挑战和改进空间。未来的发展需要更多的技术创新和政策支持，以提高容灾系统的覆盖率和有效性，确保无论何时何地都能提供最佳的业务连续性体验‌。

## 项目建设的意义和必要性

容灾机房建设的意义在于确保数据安全、保护业务连续性、提高恢复速度，以及提升医院信誉度和竞争力。

容灾机房的建设对于现代医院而言至关重要，它通过定期备份和保护数据，确保资料的安全性和可恢复性，即使在灾难发生时，医院仍能及时恢复业务。这种机制不仅有助于防止数据丢失和业务中断，还能减少医院面对的风险和损失。通过建设异地容灾中心，医院可以确保在灾难发生时能够维持关键业务的持续运行，因为数据和基础设施的复制已经完成，业务可以在另一地点恢复。此外，容灾机房的建设还能大大加快业务恢复的速度，这对于降低系统停机时间以及保持客户满意度至关重要。

容灾机房的建设还带来了其他益处，包括防止数据丢失和业务中断、减少风险和损失、提升医院信誉度等。具备强大的异地容灾能力，能够增加医院的信誉度和客户信任，为医院带来更多业务机会。在数字化时代，数据存储和容灾已经成为了医院级云计算中至关重要的一环，确保医院数据的安全和可靠性，避免数据丢失、应用程序中断等问题，从而保障业务正常运行。

容灾机房的建设对于医院而言，不仅是保障数据安全和医院运营连续性的重要手段，也是提升医院竞争力和信誉度的关键因素。

合理分布工作空间及各类设备安装场所，缩短工艺流程，降低劳动强度，提高工作效率，确保电子计算机系统稳定可靠运行，保障机房工作人员良好的工作环境,并且以国家有关标准及规范为依据。

根据医院提出的要求与现场实际情况以及计算机系统实际操作运行等情况进行设计，力求在设计、选材中做到整体布局的合理化和科学化。

机房各项功能完整配套，达到专业规范、技术先进、经济合理、安全适用、质量优良、管理方便之目的。

在经济实用的前提下，选择优质机房专用装修材料，主体装修材料宜选用吸音效果好、不易变形、变色、易清洁、防火性好，且高度耐用的材料，达到最佳装修效果。

室内控制设备、电器设备、布线系统的选材我们注重其可靠性，全部采用符合国家标准的优质产品，以确保系统投入运行后故障率为最低。

机房设计应具有考虑现有设备的利旧（包括UPS、精密空调），同时够满足今后发展的需要。。

# 需求分析

## 安全保密与自主可控

### 安全保密配套设施建设

安全保密，门禁控制，使用门禁系统，采用人脸、指纹身份等验证方式。只有授权人员才能进入机房，且系统会记录人员的进出时间和身份信息。监控，安装全方位的视频监控系统，覆盖机房的各个角落，实时预览监控机房内的情况。通过录像，以便后续查看和分析。环境安全，确保机房的温度、湿度等环境因素处于合适的范围，以保障设备的正常运行。同时，要防止火灾、水灾等灾害对机房的破坏。安装火灾自动报警和灭火系统，如烟雾探测器、气体灭火装置等，以及防水浸的传感器。当机房内的烟雾探测器检测到烟雾时，会立即触发气体灭火装置，迅速扑灭火源，保护设备和数据的安全。人员安全管理背景审查与培训，对所有可能接触到容灾机房的人员，包括工作人员、维护人员和供应商等，进行严格的背景审查。确保他们没有不良记录和潜在的安全风险。同时，定期对相关人员进行安全培训，包括安全意识教育、保密制度培训、应急响应流程等。

自主控制，积极采用国产的硬件产品设备。国内一些企业在硬件研发方面取得了显著进展，其产品在性能、可靠性等方面逐渐能够满足容灾机房的需求。

### 监管体系的融入

系统整个架构的可靠性设计，这是容灾容错的一个基础。这个基础之上，我们还要有对于服务的可用性控制，即有了这个基础之后，还有一定的发现、定位、处置能力的一个控制能力，结合在一起，才能真正的达到容灾容错实战的能力要求。

容灾机房的架构与技术主服务器处理业务，从服务器进行数据备份。当主服务器出现故障时，从服务器可以接管业务。主从架构两个数据中心同时处理业务，互为备份。当一个数据中心出现故障时，另一个可以继续提供服务。双活架构在两个地理位置不同的数据中心同时进行数据备份，并设置一个离线备份中心。故障切换当主服务器出现故障时，自动将业务切换到备用服务器上。高可用技术通过专用的硬件设备进行负载均衡，性能较高但成本也较高。硬件负载均衡通过安装软件在服务器上实现负载均衡，成本较低但性能可能不如硬件负载均衡。软件负载均衡通过在地理位置分散的节点上缓存内容，减少用户访问延迟，提高系统性能和可用性。

### 内控安全设计

数据分区隔离，不同业务系统、不同应用之间的数据和配置信息等具备严格的安全隔离措施，可采用不同的存储资源池和访问策略，防止重要数据或配置信息被同一存储空间上其他业务系统的操作、维护人员或管理员非法访问。

数据传输加密，为了保证系统数据传输的完整性、机密性、不可抵赖性，保证信息传输的过程中不被恶意篡改或窃听，以保证通过黑客工具对这些业务数据进行分析破解甚至篡改，而使系统所到攻击产生严重的后果，系统采用https方式进行数据通信，支持客户端证书和服务端证书双向认证，实现对传输数据的加密，从而保证数据信息的安全性、机密性。

数据存储加密，对于本地需要存储的数据信息，支持加密后再进行数据存储，提高数据的安全性，即使数据被盗取，也无法识别数据的原型。

### 安全保密检测评估改

安全传输与存储备份数据的方法在容灾系统中扮演着至关重要的角色。为了确保备份数据的完整性、保密性和可用性，需要采取一系列的安全措施来实现安全传输和存储。本章将详细介绍安全传输与存储备份数据的方法。

安全保密检测数据的方法，加密传输，在备份数据传输过程中，使用加密算法对数据进行加密是保证数据安全性的关键。常用的加密算法包括对称加密算法和非对称加密算法。对称加密算法使用相同的密钥进行加密和解密，适用于大量数据的传输:非对称加密算法使用公钥和私钥进行加密和解密，适用于安全性要求较高的场景。可以选择合适的加密算法和密钥长度，确保数据传输过程中的机密性。传输层安全协议:使用传输层安全协议(TLS，TransportLayerSecurity)来保护备份数据的传输。TLS提供了身份验证、数据完整性和数据加密等功能，能够有效防止数据在传输过程中被篡改、窃听和伪造。备份数据传输过程中使用TLS协议，可以确保数据传输的安全性。

跨网络隔离，跨不同网络进行备份数据的传输时，应确保备份数据不被未经授权的网络访问。可以通过构建虚拟专用网络(VPN，VirtualPrivate Network)来实现网络隔离，建立加密的通信隧道保证备份数据只在授权的网络环境中传输。安全认证与访问控制:在备份数据传输过程中，进行安全认证和访问控制是确保数据传输安全的重要手段。使用身份验证机制，只允许授权用户进行备份数据的传输。可以采用基于令牌的身份验证、数字证书等方式，对用户进行身份验证和授权。

### 国产自主可控要求的落实

本次建设采用的硬件及软件均采用自主可控的CPU、操作系统以及国产软件品牌，同时提供系统安全架构设计、等级保护要求落实、安全保密检测评估及发现问题整改，以及落实国产自主可控要求情况。

平台内置分布式防火墙、虚拟机沙箱、平台集成WAF等安全机制，有效提高平台安全级别；整体安全按照等保要求进行规划，在物理，网络，通信，应用，数据以及云平台安全进行了统一的安全建设，全方位实现纵深安全防御。

应用安全层面，平台深度集成了下一代防火墙、无代理杀毒软件、数据库审计等安全模块，构建了4-7层网络和应用安全防护能力。

虚拟机和租户之间的安全保护，利用创新云安全资源池，同时实现东西向租户安全隔离和南北向业务安全保护；并遵从等保合规的要求。

### 进度管控和保密管理

容灾机房基础建设进度管控和保密管理至关重要，以下是对此的概述：

进度管控，需制定详细的建设方案，包括机房选址、布局规划、基础设施建设等，确保各环节有序进行。在实施过程中，要定期检查建设进度，确保按时完成各项任务。对于出现的问题和延误，要及时调整计划，确保整体建设进度不受影响。

保密管理，容灾机房建设涉及敏感数据和设备，必须实施严格的保密措施。设立门禁系统，限制无关人员进入机房区域。对参与建设的人员进行保密培训，确保他们了解并遵守保密规定。定期检查保密措施的执行情况，及时发现并纠正潜在的安全隐患。

## 系统需求分析

### 环境适配

地理位置与选址适配，地质与自然灾害因素考虑，容灾机房的选址应尽量避开地震带、洪水易发区、山体滑坡等地质灾害高发区域。在地震频发地区建设容灾机房，需要对建筑结构进行特殊的抗震设计，采用加固的地基和抗震框架等措施，以确保在地震发生时，机房建筑及内部设备的安全。如果容灾机房建在靠近河流等易受洪水威胁的区域，就需要建设完善的防洪设施，如防水堤坝、排水系统等，防止洪水侵入机房。

电力与网络资源的接近性，容灾机房是电力消耗大户，应靠近可靠的电力供应源，如变电站等。这样可以减少电力传输过程中的损耗，并且在电力供应出现问题时能够更快速地与电力公司进行沟通和解决。

此外，良好的网络连接也是关键。选址应靠近主要的网络节点和通信枢纽，以便能够快速接入高速网络，降低网络延迟。

室内环境适配，温度与湿度控制，容灾机房内的设备对环境温度和湿度有严格的要求。温度过高会影响设备的性能和寿命，甚至导致设备故障；湿度过高可能引起设备腐蚀，湿度过低则容易产生静电。一般来说，容灾机房的温度应保持在 20-25 摄氏度之间，相对湿度在 40%-60%之间。

为了实现精确的温湿度控制，需要安装专业的空调系统。精密空调能够根据机房内的实际温度和湿度情况进行自动调节，确保环境参数始终处于合适的范围内。

电力适配，电力供应系统设计，容灾机房的电力供应系统需要具备高可靠性。应配备大容量的不间断电源（UPS）。UPS 可以在市电中断时立即提供电力支持，保证机柜内设备的持续运行，其容量要根据容灾机房的设备负载和停电时间要求进行合理设计。

消防与安防适配，消防系统配置，容灾机房需要配备完善的消防系统，以应对可能发生的火灾。火灾自动报警系统应能够及时检测到火灾的发生，并发出警报。采用感烟探测器、感温探测器等多种探测器相结合的方式，提高火灾检测的准确性。在机房顶部安装感烟探测器。

灭火系统方面，由于容灾机房内有大量的电子设备，不能采用传统的水喷淋灭火方式，而是采用气体灭火系统。

安防系统建设，容灾机房的安防系统包括门禁系统、视频监控系统等。门禁系统要严格控制人员的进出，采用人脸身份验证方式，视频监控系统要覆盖机房的各个角落，并且具备高清画质和录像存储功能，以便在发生安全事件时能够进行调查和追溯。

### 效能

可靠性与稳定性效能，电力供应保障，容灾机房配备了不间断电源（UPS），UPS 能够在市电出现短暂波动或中断时，立即提供稳定的电力，确保服务器等关键设备不会因瞬间断电而出现故障或数据丢失。当市电突然出现几毫秒的电压下降时，UPS 能够迅速补充电力，维持服务器的正常运行。而备用发电机则在市电长时间中断的情况下启动，为容灾机房提供持续的电力支持。这样的电力保障措施大大提高了容灾机房的可靠性，保证业务的连续性。

制冷与散热系统效能，高效的制冷和散热系统对于容灾机房至关重要。容灾机房内的大量服务器和设备在运行过程中会产生大量的热量，如果不能及时散热，会导致设备温度过高，影响性能甚至损坏设备。先进的制冷系统，如精密空调，能够精确控制机房内的温度和湿度，保持设备在适宜的工作环境中。将机房温度控制在 22-24 摄氏度，相对湿度控制在 40%-60%的范围内，确保服务器等设备能够稳定运行。

安全性与防护效能，物理安全防护，容灾机房通常具有严格的物理安全措施。只有经过授权的人员才能进入机房区域，防止未经许可的人员进入破坏设备或窃取数据。

机房内部的设备布局也考虑了物理安全因素，机房配备了消防系统，包括烟雾探测器、自动灭火装置等，一旦发生火灾能够及时进行灭火，保护设备和数据的安全。

### 完善体系

选址与布局，选择交通便利、地质稳定、气候适宜、电力供应稳定、网络条件良好且安全保障措施完善的地区进行机房建设。合理规划机房布局，充分考虑设备类型、数量、尺寸等因素。

基础设施建设，建设稳定可靠的供配电系统，包括高压配电、低压配电、UPS不间断电源等。设计合理的制冷系统，确保机房内部环境的恒温恒湿。配置完善的消防设施，确保机房安全。

设备选型与配置，根据业务需求和技术架构，选择高性能、高可靠性的服务器、存储设备和网络设备。

安全防护设计，实施物理安全措施，确保机房内部设备的安全。

### 提升能力

容灾机房提升能力主要涉及冷却效率、电源管理、空间优化、安全性以及资源可视化等方面。

提高冷却效率，通过优化空调回路管理，提高冷却单元的返回温度，以增强容量和效率。电源管理，部署UPS，确保电源中断时的连续运作，同时提高电源利用效率。空间优化，重新规划机房布局，提升空间利用率，以应对设备增加带来的空间挑战。增强安全性，安装物理设备，如监控摄像头、门禁系统确保机房运行安全。资源可视化，构建容灾机房可视化平台，实现环境方面的全面监控和管理，提高资源使用效率和管理便捷性。。

### 引领发展与成果共享

容灾机房基础建设在引领医院高质量发展中扮演着重要角色。它不仅为医院提供了强大的数据存储和处理能力，还通过数据统计和分析，为绩效管理提供了坚实的数据支撑，助力医院实现科学化、规范化、精细化的运营管理。容灾机房是医院信息化建设的核心：它整合了医疗、教学、科研等业务系统和资源系统，为医院运营管理决策提供了全面的数据支持。数据统计工作对绩效管理至关重要：通过信息收集、科学研究和辅助管理决策，容灾机房能够挖掘医院运行的深层规律，主动牵引医院绩效高质量发展。容灾机房的建设还推动了智慧医院的发展：通过提供超宽、极简、融合、智维的全光网络，为医院的高质量发展提供了坚实的基础

容灾机房作为医院信息化、数字化发展的重要保障，其建设成果显著，主要体现在以下几个方面：

提升了医院运营效率，通过优化机房布局、增强冷却效率、提高电源管理等方式，确保了容灾机房的高效运行，进而提升了医院整体的运营效率和服务质量。增强了数据安全性：机房建设严格遵循相关国家标准和规范，实施了物理措施，如监控摄像头、门禁系统等，确保了医院设备的安全性。支撑了智慧医院建设，容灾机房机房的建设不仅满足了当前的业务需求，还为智慧医院的可持续发展提供了支撑，如通过人才培养体系解决了医信专业人才缺失的问题。

### 转化应用

医疗信息化支持，医院容灾机房容灾机房为业务系统提供稳定的运行环境。通过高速的网络连接和可靠的服务器存储，确保医生能够准确、及时地记录患者的病历信息，为患者提供连贯的医疗服务。

医疗设备运行保障，医疗设备网络连接，现代医疗设备如监护仪、心电图机等很多都具备网络连接功能，医院容灾机房为这些设备提供了网络接入点和数据传输通道。

设备远程监控与维护，医院容灾机房可以作为医疗设备远程监控和维护的中心。一些高端医疗设备制造商可以通过网络连接到医院容灾机房，对设备的运行状态进行实时监测，提前发现潜在的故障隐患，并进行远程诊断和修复。

科研与教学支持，医学数据存储与分析，医院容灾机房为医学科研提供了大量的数据存储和分析能力。医院在日常医疗活动中积累了丰富的患者临床数据，这些数据存储在机房的服务器中。科研人员可以通过医院内部网络访问这些数据，进行疾病研究工作。

远程教学与培训，医院容灾机房可以支持远程教学和培训活动。通过网络视频会议等技术，医院可以邀请国内专家进行学术讲座和手术演示，医护人员可以在医院内部的会议室或通过个人电脑观看学习。。

### 成本控制与管理

容灾机房基础建设经费开支的合理性与规范性，经费开支与项目需求的匹配性，容灾机房建设经费的开支应与项目的实际需求相匹配，包括机房装修、电气系统、UPS系统、空调系统等各项基础设施的建设和集成。预算安排的遵循情况，经费开支应严格遵循预算安排，确保资金的有效利用，避免超支和浪费。投资效益的评估，应对机房基础建设的投资效益进行评估，确保经费开支能够带来相应的回报，提高医院的整体运营效率和服务质量。容灾机房基础建设经费开支应合理、规范，并与规划投资和预算安排相符合，以确保项目的顺利实施和医院的长期发展。

容灾机房基础建设推广复用的成本是否合理，需综合考虑多个因素，包括建设规模、设备费用、机房类型等。在评估价格优势时，应与国内外其他同类项目进行比较，分析在建设成本、运营效率以及长期维护成本等方面的差异。建设成本，包括机房装修、机电设备、消防设施等费用，需根据具体需求和配置进行预算。运营效率，高效的机房设计和管理可以降低运营成本，提高价格优势。长期维护成本，机房的维护成本也是评估价格优势的重要因素。评估容灾机房基础建设推广复用的成本及价格优势需全面考虑，并与国内外同类项目进行对比分析

### 建设内容优化调整

容灾机房建设的调整内容合理性与程序合规性对功能性能、质量效益等方面具有重要影响。功能性能提升，合理的调整内容能够确保机房建设满足当前及未来的业务需求，提升数据处理和业务运行的能力，确保系统的高效运行。质量效益保障，合规的程序能够确保机房建设的质量，减少因建设过程中的疏漏导致的后期运维成本，提高整体的投资效益。长期可持续发展，合理的调整内容与合规的程序共同确保机房建设的可持续性，为医院的长期发展提供稳定、可靠的技术支持。

# 建设方案

## 建设原则和策略

本次容灾机房位于1号楼，面积约为18平米，标准要达到《电子计算机机房设计规范》中的C级标准。

按照国际标准 TIA-942（Telecommunications Infrastructure Standard for Data Centers）、国内标准 GB 50174-2017《灾备机房设计规范》等。明确标准中对于机房选址、布局、环境要求、设备配置等方面的具体规定。根据标准，容灾机房不应选择在易受洪水、地震等自然灾害影响的区域，并且要考虑到电力供应的稳定性和网络接入的便利性。

## 项目建设目标

可用性指标，正常运行时间，预定目标可能是全年 99.99%的可用性。全年停机时间不能超过约 52.6分钟（计算方式：365天×24小时×60分钟×(1-0.9999)=52.6分钟）。主干网络冗余，预定有2条冗余的网络链路，当一条链路出现故障时，流量能够自动切换到其他链路而不影响业务。

性能指标，机房的温度目标可能设定在 22℃±2℃，湿度目标可能在 40%-60%之间。通过安装在机房内不同位置的温湿度传感器采集数据。

安全性指标，门禁系统的目标可能是只有授权人员能够进入机房，并且有详细的进出记录。消防系统目标是在火灾发生时能够及时报警并有效灭火。

## 国内外医院容灾机房技术对比

‌国内外医院容灾机房技术在设计理念、技术应用、实施细节等方面存在差异，但共同目标是确保医院信息系统的安全、稳定运行。

设计理念，国内外医院容灾机房设计的核心目标都是确保医院信息系统的数据安全、业务连续性以及在灾难发生时能够迅速恢复服务。国内医院容灾机房设计强调从实际需求出发，明确灾备系统的恢复时间目标（RTO）和恢复点目标（RPO），确保在灾难发生时能够迅速切换到备用系统，保持业务连续运行‌。

技术应用‌，国内外医院容灾机房技术均采用多种技术手段，包括但不限于远程镜像技术、快照技术、互连技术等，以实现数据的远程备份和快速恢复。国内医院容灾机房技术还特别关注服务器虚拟化设计，通过研究服务器设计、存储设备设计和服务器虚拟化管理设计，提高资源利用率和系统灵活性‌。

实施细节‌，在实施细节上，国内外医院容灾机房建设均注重通信链路的设计和选择，考虑到距离支持、带宽能力等因素，以确保数据传输的可靠性和效率。国内医院容灾机房建设还强调数据全生命周期的安全管理，包括数据的收集、存储、传输、处理、使用、交换和销毁，采取备份、加密等措施加强数据的存储安全‌。

案例分析‌，例如，TiDB技术提供了同城两中心容灾方案，通过自适应同步模式（Data Replication Auto Synchronous，简称DR Auto-Sync）实现核心业务系统的同城两中心灾备部署，确保了数据的一致性和系统的可用性‌。

国内外医院容灾机房技术在设计理念、技术应用和实施细节上各有侧重，但共同目的是确保医院信息系统的安全、稳定运行，以及在灾难发生时能够迅速恢复服务。随着技术的发展和医院信息化建设的不断深入，这些技术将不断完善和优化，以适应日益增长的数据安全和业务连续性需求。

## 技术方案

### 系统架构

容灾机房设备布局图：



容灾机房设备布局图：



### 系统流程



### 运行环境要求

环境条件：温度和湿度，机房应保持适宜的温度和湿度，通常建议温度在18°C至27°C之间，湿度在35%至65%之间，以防止设备过热或静电问题。清洁度，机房应保持较高的清洁度，避免灰尘和污染物对设备的影响。

电力供应：不间断电源（UPS），应配备UPS以确保在电力中断时关键系统的持续运行。备用电源，如柴油发电机，用于长时间的电力供应保障。电源分配，合理设计电源分配系统，包括双路电源输入和冗余配置，以提高供电的可靠性。

冷却系统：空调系统，应安装高效、可靠的精密空调系统，确保机房内的温度和湿度稳定。热通道和冷通道，通过热通道和冷通道的设计，优化气流，提高冷却效率。

防火和安全：防火系统，包括烟雾探测器、灭火系统和防火门等，确保在火灾发生时能迅速响应。物理安全，如门禁系统、监控摄像头和入侵检测系统，保护机房免受未经授权的访问。

网络和通信：冗余网络，设计冗余的网络架构，包括冗余的网络设备和通信链路，以确保网络的高可用性。

电缆管理：合理规划电缆布线，使用高质量的电缆和连接器，确保网络传输的稳定性和安全性。

灾难恢复：备份和恢复策略，制定数据备份和灾难恢复计划，确保在数据丢失或设备故障时能迅速恢复业务。异地备份，考虑异地备份解决方案，以应对可能的自然灾害或其他无法预测的事件。

合规性：遵守相关法规和行业标准，如HIPAA（美国健康保险流通与责任法案）、ISO 27001信息安全管理体系等，确保机房设计符合数据保护和隐私法规的要求。

可扩展性和灵活性：考虑未来可能的扩展需求，包括设备的增加和网络带宽的提升。

### 系统功能介绍

一、机房装修工程

吊顶工程，吊顶采用，利旧原有铝合金微孔吊顶板，规格600\*600\*0.8mm。

地面工程，地面采用钢质抗静电活动地板，无框，规格600\*600\*32mm。地板的作用：管线敷设、静电泄漏。地板架空高度：300-350mm。地面防尘处理：采用环保防尘漆刷2遍。地面保温处理：采用20mm 橡塑保温棉板B1级，表层贴0.3mm镀锌铁皮。

墙面工程，铲除原有墙面的腻子、乳胶漆；重新刮腻子（二遍）、重新刷乳胶漆（二遍）。

门窗工程，灾备机房机房门应保证最大设备能进出：选用甲级钢制防火门，规格1200\*2200mm、900\*2200mm。

机房承重，UPS电池、机柜等设备应做承重处理、采用50以上角钢焊接散力支架，以满足机房承重要求。

二、防雷接地及配电系统

防雷系统：一级防雷—— 输出动力电至灾备机房的动力配电柜。

二级防雷—— 灾备机房配电箱市电输入,安装电源二级浪涌保护器：40KA。

三级防雷—— 灾备机房配电箱UPS输出，安装电源二级浪涌保护器：20KA。

接地系统，采用30\*3mm紫铜排做接地铜排，采用50mm²接地线接至新建地网，机房内的地板脚、墙面龙骨、顶面龙骨、机柜等设备应进行等电位联结。

UPS不间断电源，利旧1台UPS，蓄电池满载后备时间不小于60分钟。

照明设计，灯具选择，高效节能LED平板灯，主机房600\*600，其他区域600\*600，灯具分区分组控制。

配电系统设计，灾备机房机房总电源由专业强电单位引入专用电缆至配电间市电配电柜 ，再进行二次供电分配设计。整个配电系统采用放射式配电，各用电设备不同类别采用分路控制，整个配电系统参数如下：

（1） 配电系统频率：50Hz；

（2） 电压：380V/220V；

（3） 线制：三相五线制/单相三线制。

（4） 配电方式：所有机柜均采用独立的双路UPS供电回路，分路独立控制，两路互为备份。

供电回路分类如下：

（1） UPS供电总回路分为

 网络列头机柜专用回路、备用回路；

 服务器机柜专用回路、备用回路；

 网络交换机柜专用回路、备用回路；

 机房备用照明专用回路；

 消防、门禁、监控、环控等设备供电

（2） 动力供电总回路分为

 机房空调专用回路；

 市电照明专用回路；

 机房市电维修回路；

配电线路，强电电缆采用地板下走线方式，采用单独回路直接配至各用电设备，每个回路采用独立的电缆。

（1） 机柜线缆采用阻燃电缆。

（2） 市电维修及空调线缆采用阻燃电线。

（3） 照明线路采用阻燃电线。

系统插座，机柜负载配电线路按国标并留有余量，机房内所有计算机和网络设备的电源采用工业连接器连接，墙面维修插座选用五孔带接地插座。

（1） PDU管理器：安装10口16A。

（2） 维修插座：采用10A五孔带接地插座。

（3） 精密空调电源：精密空调采用阻燃电缆直接连接至端子。

（4） 普通空调电源：采用10A五孔带接地插座。

三、气体灭火控制系统

主要对灾备机房进行七氟丙烷气体自动灭火系统无管网设计。

气体报警控制部分，采用气体灭火控制器配智能光电感烟（温）探测器、紧急启停按钮、声光报警器、放气指示灯、控制模块等，实现火灾自动报警及气体灭火联动控制功能。

气体灭火控制部分，主机房、配电间灭火装置选用七氟丙烷无管网气体灭火装置，吊顶内分别设置感烟（温）探测器。

四、环境监控系统

实现对机房设备环境的集中监控，机房所监控的智能设备或子系统主要包括：精密空调监控、UPS监控、供配电、机房的温湿度监测、漏水监测、视频监控、门禁等。系统建立可以扩充的整体平台，能够实现子系统之间的联动，实现手机短信等报警时。

五、信息网络及网络安全系统

防火墙：主要在于及时发现并处理网络运行时可能存在的安全风险、数据传输等问题，其中处理措施包括隔离与保护，同时可对计算机网络安全当中的各项操作实施记录与检测，以确保计算机网络运行的安全性，保障资料与信息的完整性

核心交换机电路保护系统：主机电路安全防护系统，适用于保护各行各业的220V电子电气设备。产品采用三级EMI滤波电路设计，具有智能防雷和浪涌保护功能，可以实时监测输入电流、电压、频率、功率，监测所连接用电设备的漏电状态，监测接地通断、防雷器状态、防雷器寿命以及环境温湿度、烟感、水浸等。并且支持设备漏电、过载、过欠压、接地失效、防雷器失效、环境超标等联动保护功能。同时，产品可以滤除电路中的杂波噪声和高频干扰，降低电磁辐射，提高信号的传输质量，避免信号受到干扰而导致数据传输出错、输出音质和画面质量下降，以及抑制电源高频电压浸入从而稳定电压，保障设备良好稳定运行，并延长用电设备的使用寿命。智能物联网安全感知与管理平台，可以实时接收告警信息，可以远程实时监控、管理、在线运维、数据存储备份、数据分析、GIS地图定位、大屏展示、故障报修等，实现智能化运维管理。实时监测与保护用电设备，事前防患于未然。避免因为雷击、浪涌、电流电压不稳、环境超标、杂波噪声和高频干扰等问题造成用电设备损坏、干扰、过早老化、寿命缩短、质量下降，以及设备漏电造成人身安全、电气火灾等风险隐患。保障工作和生产，保障人身安全，增加用电设备的在线时间和使用寿命，减少损失。提升管理效率，节省运维成本。

备用核心交换机：主要承载灾备机房备用网络的数据传输，保证在应急情况下能够持续提供网络不中断服务。

服务器交换机：主要承载服务器数据传输。

六、数据及应用备份系统

备份一体机（含备份软件）：机架式标准2U12盘位设备，配2颗国产X86架构2.5GHz 16core CPU，配 128GB 内存，标配 2\*480G SSD 盘做系统盘，配4个千兆网络端口和2个万兆光口，配置12块4TB企业及磁盘；存储备份系统为专用基于Linux的64位嵌入式系统非ESXi、Openstack和Windows等虚拟化架构，保证备份系统底层安全和性能；本次配置不低于20TB数据保护容量授权，包含不限制数量的定时备份代理、实时备份代理，实时复制代理。支持对Oracle、DB2、MySQL、MariaDB、Sybase、PostgreSQL、MongoDB、SQL Server、Cache等主流数据库进行在线备份保护，备份任务配置过程全部图形化向导指引完成，可在图形化界面选择相应数据库，无需编写脚本。支持达梦、人大金仓、神舟通用、南大通用、瀚高和优炫等国产化数据库备份，支持阿里云RDS、TDSQL、OpenGuass、MongDB等；支持Windows和Linux平台下的文件系统的卷级备份功能，以整卷为单位进行数据备份，提升海量小文件环境下的备份效率。支持整卷恢复和单文件目录级别的细粒度恢复。持密钥加密和密钥更新，避免密钥外泄引起数据泄露，提高系统和数据安全性，提升传输过程以及存储的安全性。支持对备份数据进行加密传输和存储，支持AES256和SM4两种加密算法，提升传输过程以及存储的安全性；数据传输支持Open-SSL 的TLS 双向认证和加密，认证证书不低于2048位。支持永久增量备份，在首次完全备份后，后续所有的备份均为增量级别的备份。每次的增量备份均与上次备份后的原生格式副本数据进行合并，形成一份全新的原生格式的生产数据副本。不仅能够提高备份和恢复效率，而且支持删除任意中间完全备份时间点，不会影响后续的时间点恢复，提高数据安全性。提供防勒索病毒的能力，通过不可变存储功能避免病毒篡改、删除存储数据，支持强制数据保留策略，通过root/administrator 账号无法访问、浏览、删除这些数据所在的 RAID、LVM、文件系统和磁盘，从而达到抵御勒索病毒攻击的目的。支持并行重复数据删除，通过在多个不同的节点上构建指纹池，并将指纹并行分布于多个节点，有效解决单点性能和存储空间压力问题。备份系统在对Oracle备份时（含OracleRAC），可通过web界面进行备份通道数、FilePerSet、备份跳过数据文件坏块、BLKsize、Maxopenfile等多样化参数配置，兼容各种生产环境和备份需求。为保证核心系统的数据丢失量最低，备份系统配置Oracle和MySQL的持续日志实时备份保护，保证尽可能近的数据恢复时间点。支持系统管理员、审计管理员、安全管理员、租户、操作员和巡检员六类角色，通过分权管理，提升备份系统的管理安全性。支持设置数据复制窗口，在非数据复制窗口期，复制设备之间网络物理隔离。避免非数据复制时间段，灾备设备服务对外暴露而产生的安全风险。具备数据一致性校验功能，针对备份对象支持手工选择一致性校验算法，至少包含MD5、CRC32等。具备备份数据的安全管理机制，在通过其他备份系统进行数据恢复时需要得到现有备份系统的本地授权许可后，才可以浏览、恢复本地传输过去的备份数据，最大限度避免备份数据的泄密可能。提供独立部署的备份统一管理平台，实现对灾备节点运维管理，提升灾备系统可用、灾备资源可用、可恢复能力，帮助医院灾备扩容决策、灾难恢复能力评估、可视化展示灾备成效等。支持对管理员提供灾备平台全局运行情况概览（资源用量、灾备机房拓扑等）。通过统一管理平台实现对系统管理员、安全管理员、审计管理员、租户、普通用户等用户日志查看和分析，支持设置日志保留策略。通过统一管理平台支持以邮件告警的方式，针对于灾备系统的平台运行异常情况、硬件故障、软件故障等等信息及时通知管理员。

应用服务器：承载HIS等业务系统应用级备份部署。

七、综合布线系统

主干网络采用双核心、双汇聚、万兆至接入层，其中核心交换机在数据中心机房与灾备机房进行异地部署；双核心、双汇聚采用虚拟化做堆叠，各汇聚层双链路万兆链接至双核心，接入层交换机双链路接至双汇聚。其中中心机房至灾备机房采用2根48芯单模光缆，各楼宇汇聚点通过24芯光纤接入灾备机房。

# 环保、消防、职业安全、职业卫生和节能

## 环境影响和环保措施

本项目建设不对环境造成影响，不产生污染。但要保证所选设备和机房局部空间无污染，符合消防安全要求，选用绿色电脑、外设和绿色节能照明光源。机房建设工程遵循国家机房设计标准规范的要求。

项目场地建设遵循建设部颁布的《民用建筑工程室内环境污染控制规定》（GB50352），国家质量监督检验检疫总局颁布的《室内装饰装修材料有害物质限量》等国家标准。

场地建设后，系统运行过程中不产生有害废气、废水、废渣等物质，不会污染环境。而空调、风机等硬件基本选用低噪声设备，并采取双层玻璃、隔离屏蔽等有效的消声措施。电磁辐射完全符合国际标准，对人体健康并不造成较大威胁。

## 消防措施

在项目建设中严格按照国家消防规范《建筑内部装修设计防火规范》（GB50222）、《中华人民共和国消防法》等国家法律和规定。在各个区域内都装自动喷淋系统和报警装置，配置七氟丙烷灭火器，以及适量手提式二氧化碳气体灭火器。

## 职业安全和卫生措施

项目建设根据有关国家和部门标准规范，采取的主要安全卫生措施有：

1）所有用电设备的金属外壳、金属底座、电缆金属铠装层、电缆保护管以及所有金属支架均与接地装置连接，设有安全接地，配电系统设有短路保护、过电流保护装置，以保证操作人员的安全和设备安全；

2）建筑内设计足够的人行通道和运输通道，设置疏散标志，以保证通行安全。在主要通道和出入口均设置应急照明；

3）办公环境配有空调、空气净化等装置，为工作人员提供舒适的工作环境；

4）对消防、电磁干扰满足工作人员的卫生环境要求；

5）场地设有值班室、货物间、男女洗手间等辅助用房。

## 节能目标及措施

项目建场地建设遵循《公共建筑节能设计标准》、《建筑节能工程施工质量验收规范》等国家规定，场地建设后，系统运行过程中主要是使用计算机设备、网络设备和检测设备，运行能耗较小。在项目实施中，仍将严格遵守国家有关规定，控制能耗。根据有关国家和部门标准规范，采取的主要节能措施有：

1）引进国内先进的关键计算机设备、网络设备和检测设备，要求能耗低、可靠性高；

2）国内生产与办公设备选用优质节能产品；

3）设计中选用的各类配套设备，均选用优质节能系列产品；

4）各种管道应采取保温、隔热等措施；

5）建筑墙面、吊顶作保温层或双层隔离，减少能量损耗。

# 项目组织机构和人员

## 领导和管理机构

为了保证项目顺利实施和正常运行，确保工程质量并达到预期目标，工程建设成立本项目建设领导小组，统一组织、协调本项目的建设工作。在领导小组的领导下，成立项目建设管理办公室（简称办公室）作为项目建设的执行机构。

项目建设组织机构的设立应本着“统一领导、分工明确、职责清晰、协调配合”的原则。

项目的组织管理与职责分工如下：

1、项目领导小组：是项目建设的决策和协调机构，明确建设目标、建设内容及项目建设的组织方式，同时还负责跨部门跨地区重大问题的协调。

2、项目建设专家委员会：在重庆市专家库抽取专家，负责为本项目的设计与实施提供咨询和建议，协助审核各阶段的计划、实施方案。

## 项目实施及运行维护机构

综合组：负责组织编写项目建设方案，组织项目方案论证会。

工程组：制订工程实施方案和进度计划，组织工程实施和质量管理，负责项目协调和工程验收移交。

技术组：负责工程技术方案、工程设计书、工程建设计划、设备采购标书等工程技术文件的编写、审核，配合工程组做好技术把关和测试验收工作。

安全组：负责项目信息安全目标的实现，协助工程组管理项目安全子系统的建设，完成安全系统测试、验收工作。提出各单位建立网络与信息安全应急处理机制意见，制定应急预案和备份方案，处理网络与信息安全事件，并根据安全事件的性质及时向安全部门报告。

财务组：负责项目资金管理。

标准组：负责组织研究、制定本项目的标准规范体系并监督执行。

## 技术力量和人员配置

技术力量和人员配置，应该在保证工程建设质量和进度、保障外网的安全与正常运维的要求下进行设置。随着业务的不断发展，根据需要动态调整人员的配置。

项目建设专家委员会，应该由不少于3人构成，成员的组成应该充分体现广泛的代表性。人员的遴选由项目领导小组讨论决定。

在建设阶段，可以临时设立综合组、工程组、技术组、安全组、财务组和标准组。初期，技术力量的配置，本着“干练、精简、高效”的原则。人员培训方案

## 培训目的

培训的目的是使用户熟悉并掌握种业务系统的使用。

## 培训目标及对象

为了确保各系统建设的顺利运行和系统投入使用后的稳定，通过对用户方工作人员进行相应的专业技术和应用技术培训，达到提高工作效率、发挥各系统应用效率的预期目标。

通过培训工作的开展，要达到如下目标：

1. 用户方了解各系统建设背景、基本理论和方法；
2. 用户方掌握各系统的使用方法；
3. 用户方熟悉各类硬件、软件系统的使用操作；
4. 用户方掌握网络系统的安装、调试和日常维护等操作；
5. 用户方掌握网络安全基本知识，建立网络安全意识；
6. 用户方掌握数据库基本知识，能够进行安装、调试和日常维护；

培训对象包括：各专业单位人员、各科室使用人员、系统维护人员、相关领导等。

## 培训方式

### 统一培训

为保证工程实施的顺利进行，便于项目实施过程中甲乙双方的沟通和配合，在系统建设实施以前，用户方技术人员以及客户代表必须具备一定的技术水平和项目管理知识。

在实施系统服务过程结束时，为使客户能顺利接手该系统，用户方技术人员必须掌握所安装的各种产品、系统的有关安装、设置、管理、使用和客户化等方面的技术。

因此，在项目实施之前以及在项目实施完毕后各进行一次集中培训，分别称之为基础培训和移交培训。

基础培训：在系统实施服务开始前，承建单位将为客户提供有关系统体系结构、产品类别和选择、产品体系结构、产品功能以及项目管理等方面的培训。

移交培训：在系统实施服务过程结束时，承建单位将为客户提供针对所安装的各种产品、系统的有关安装、设置、管理、使用和客户化等方面的现场培训，目的是使客户能顺利接手该系统。

### 现场培训

现场培训是项目实施过程中重要组成部分。现场培训将在用户指定设备安装地点进行，具体内容包括：

结合系统实施现场的实际情况，介绍设备安装、调试的方法；

在承建单位专业工程人员的指导下，用户方可以直接参与设备安装和调试工作；

现场问题处理培训。

### 网络培训

项目实施中进行的集中和现场培训，旨在使用户迅速具备系统的操作、调试和维护的基本能力。对技术队伍的培训和技术人员之间的交流日常化、随时化，使技术人员随时保持对新技术的跟踪和认知能力，不断在培训中和交流中更新、强化和深化自身技术能力。

由于成本和时间原因，在日常工作中，采用传统的培训方式保持对技术人员日常化、随时化的培训和交流是难以实现的。为解决这一问题，建议承建单位通过网络化的培训来解决问题。将把集中培训和现场培训中的内容等制作成多媒体课件形式。用户方技术人员人可以通过网络随时、随地通过课件进行学习。

### 培训考核

为保证最终的学习效果，建议为每一期培训班布置考试题目，以验收学员的学习成果，保证培训质量。

## 培训内容

培训的内容应包括对项目相关业务应用系统的管理、操作、运维，主要侧重于对业务应用系统使用及系统的基本维护、常见问题及解决办法等，并提供实践性的操作，旨在使受训者熟悉平台系统设计的思路，掌握平台的操作和维护等。

按培训的目的和对象不同，本项目中主要包括的培训，可分为两个类别的培训，依次为：系统操作及管理培训、系统技术及管理培训。

系统操作及管理培训：对管理人员、系统应用人员的培训，主要包括分功能、分步骤地完成本系统的全部管理、应用的培训，使相关人员能独立、熟练地操作系统完成相关业务。

系统技术及管理培训：对管理人员、系统维护人员的培训，主要包括各业务系统的安装调试、配置、升级、使用系统的初始化和操作应用、人员角色基础信息的录入和功能权限配置、系统监控分析优化、系统日常运维、系统紧急故障处理和系统容灾及恢复、系统接口交互等。

表 7-1**人员培训计划表**

| **序号** | **培训项目** | **培训内容** | **培训对象** | **培训方式** | **培训效果** |
| --- | --- | --- | --- | --- | --- |
| 1 | 系统操作及管理培训 | 系统功能操作、系统应用 | 管理人员、系统业务人员、系统使用人员 | 培训教材+授课+练习考核 | 使相关人员能独立、熟练地操作系统完成相关业务。 |
| 2 | 系统技术及管理培训 | 系统的的安装调试、配置、升级、使用系统的初始化和操作应用、人员角色基础信息的录入和功能权限配置、系统监控分析优化、系统日常运维、系统紧急故障处理等 | 管理人员、系统维护人员 | 培训教材+授课+练习考核 | 掌握常规的系统技术，能调试、配置等运行维护，能处理系统日常的故障和维护 |

# 项目实施进度

本次信息化建设项目建设的实施分为以下三个阶段：

第一阶段：项目建设的准备阶段

项目建设的准备阶段，主要是一系列前期准备工作的完成。包括全省、市、区同类项目考察、资料的收集和调研、项目建议书和可研报告的拟定、各项信息系统需求的确定、专家评审、项目建设经费的来源以及项目建设期限的确立等。

第二阶段：项目建设的确立

本阶段的工作内容主要包括项目建设方案设计、项目招标、承建单位等。

第三阶段：项目的实施

本阶段为项目建设的实施阶段，工作内容包括了项目建设合同和监理合同的签署，信息系统分批建设、验收申请及竣工交付使用等。

第四阶段：项目的验收审计

本阶段为项目建设的验收审计阶段，要点涉及是否按规定程序和要求组织验收，检查有关手续是否齐全，以及是否按要求开展各子项专业验收。需审查合同履行是否全面、真实，有无违约行为等。

# 项目风险分析

## 协调风险及控制

由于医院信息化建设项目涉及到门诊科、信息科、医务科、护理科等科室之间的业务协同，且它们分布在不同的业务部门，因此处理各自的工作时出现不统一的工作节奏，因此要建设统一模式，需要协调各个相关部门，统一认识。

医院信息化建设项目是为重庆市市民提供健康、医疗服务的，要求动员和依靠医管局及兄弟单位方方面面的力量来共同完成。因此领导必须重视，规章制度要健全。由于工作牵涉的单位多、部门杂，实现统一集中运作，需要各联动单位积极响应，希望用户单位牵头召开有关会议，进行组织协调工作，在技术集群、人员集中、集成管理等方面统一思想，形成共识，为实现“通过医疗信息化建设，加强监管能力、提高决策水平和管理效能；优化医疗服务流程、降低运行成本、提高医疗服务质量、减轻市民就诊及医药费用负担；加强公共卫生应急处理能力。”的构想提供有力的思想和组织保障。

## 项目技术风险控制

医院信息化建设项目是一个跨学科、跨专业的综合系统工程，这一系统工程是以计算机网络系统、物联网平台为基础，以通信系统、云计算技术为纽带，以集成数据采集与交换、全数字化医疗临床信息应用和医院综合运营管理服务系统为技术支撑的技术综合体，因此技术发展给项目的建设带来一定的风险，避免系统投入使用，技术已落后的可能。由于不同地区、部门系统的设计理念及技术规范的不同，系统和硬件设计的不同，因此没有经过实际运行的技术，是可能存在技术风险。但我们在整体设计中尽可能使用较为成熟的技术，并部分开展物联网及虚拟化技术的应用，同时利用先进的ITSM技术运维管理系统的支持，是能够把握“稳中快跑、适度超前”的建设思路的，总体在技术风险上是可控、可规避的。

## 社会影响风险及控制

项目的参与单位对项目系统重要性认识不到位、服务意识不强、业务人员技术问题、网络发展不平衡，项目建设阶段的问题，都可能使医院智能化建设项目在社会各阶层造成不好的影响。

可以通过各种途径提高医院信息化建设项目在重庆市的认知率，为本项目工作创造良好的舆论氛围，项目相关单位成员结合本单位的实际情况，加强基本硬件建设，同时通过培训提高内部人员的实际工作能力。联动单位加强内部沟通，防止出现互相推倭，扯皮现象，这样才能提高联动系统在社会的影响力。

# 附表1：项目软件配置清单及预算

系统软件配置：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名 称 | 数量 | 预算 |
| 1 | 机房装修工程 | 1套 | 3.5万元 |
| 2 | 机房防雷接地及配电系统 | 1套 | 3万元 |
| 3 | 机房气体灭火控制系统 | 1套 | 2.5万元 |
| 4 | 机房动环系统 | 1套 | 3万元 |
| 5 | 机房信息网络及网络安全系统 | 1套 | 10万元 |
| 6 | 机房数据及应用备份系统 | 1套 | 23万元 |
| 7 | 机房综合布线系统 | 1套 | 5万元 |

# 附表2：项目详细配置清单

| **序号** | **设备名称** | **技术要求及设备参数** | **单位** | **数量** | **备注** |
| --- | --- | --- | --- | --- | --- |
| **一、机房装修工程** |
| **（一）地面工程** |
| 1  | 地板漆 | 1.颜色：绿色2.技术要求：刷两遍地板漆 | KG | 20 |  |
| 2  | 地面保温 | 1.规格：20mm2.等级：橡塑保温棉板B1级 | ㎡ | 18 |  |
| 3  | 镀锌铁皮 | 1.规格：0.3mm镀锌铁皮2.尺寸：2000\*1000\*0.3mm | ㎡ | 18 |  |
| 4  | 硫酸钙防静电地板 | 1.名称：全钢无边防静电地板2.配件：含支架3.规格：600\*600\*32mm | ㎡ | 18 |  |
| 5  | 地板吸盘 | 1.吸盘形状：圆形产品2.种类：单杯吸盘3.产品吸力：水平吸力50kg4.垂直吸力:35kg | 个 | 1 |  |
| 6  | 设备支架 | 1.名称：50\*5角钢2.规格：现场定制 | 台 | 3 |  |
| 7  | 空调挡水坝 | 1.技术要求：防水3遍2.规格：现场定制 | 台 | 1 |  |
| **（二）墙面工程** |
| 1  | 原始墙面铲除 | 1.墙面乳胶漆铲除2.腻子铲除 | 项 | 1 |  |
| 2  | 墙刮腻子 | 1.挂网2.刮腻子两遍 | ㎡ | 54 |  |
| 3  | 墙乳胶漆 | 1.刮乳胶漆两遍 | ㎡ | 54 |  |
| 4  | 金属踢脚线 | 1.规格：100mm高 | 米 | 18 |  |
| 5  | 甲级钢制防火门 | 1.尺寸：1200\*2200mm2.材质：钢制2.配件：含锁具、含闭门器 | 套 | 1 |  |
| 6  | 甲级钢制防火门 | 1.尺寸：900\*2200mm2.材质：钢制2.配件：含锁具、含闭门器 | 套 | 1 |  |
| 7  | 墙面开槽及恢复 | 1.包含应急照明、开关、插座、消防设备开槽2.含水泥河沙 | 项 | 1 |  |
| **二、防雷接地及配电系统** |
| **（一）防雷接地** |
| 1  | 铜排均压环 | 1.规格：30\*3紫铜排 | 米 | 25  |  |
| 2  | 绝缘柱 | 1.特性：氧化铝陶瓷2.功能：绝缘装置陶瓷 | 个 | 50  |  |
| 3  | 等电位联结端子箱 | 1.名称：等电位连接端子箱 | 个 | 1  |  |
| 4  | 电源二级浪涌保护器 | 技术参数：1.额定电压Un 220V2.大持续运行电压Uc 385V3.标称放电电流In(8/20μs)\ 20kA4.大放电电流Imax(8/20μs) 40kA5.保护水平Up(8/20μs) <1.8kV6.串接过流保护装置 32A/10kA7.响应时间 25ns8.尺寸 2mods,DIN438809.失效指示 绿色:正常 红色:失效10.安装导线截面积 10-35mm211.安装方式 35mm标准导轨(EN50022/DIN46277-3)12.工作环境温度 -40/85℃13.外壳材料 热塑材料，符合UL94 V-014.外壳保护等级 IP20 | 个 | 1  |  |
| 5  | 电源三级浪涌保护器 | 技术参数：1.SPD端口：一端口2.SPD类别：组合型3.电源：TT-TN-IT4.额定电压： Un 220V5.大持续运行电压：Uc 385V6.标称放电电流：In(8/20μs) 10kA7.大放电电流：Imax(8/20μs) 20kA8.保护水平：UP(8/20μs) <1.5kV9.串接过流保护装置：16A/6kA10.响应时间：≤25ns11.尺寸：2mods,DIN43880 | 个 | 1  |  |
| 6  | 接地主干线 | 1.规格：BVR-50mm²（双色）2.技术要求：国标 | 米 | 5  |  |
| 7  | 地板支架接地线 | 1.规格：BVR-6mm²（双色）2.技术要求：国标 | 米 | 50  |  |
| 8  | 防雷接地制作 | 1.规格：现场定制2.技术要求：接入大楼引下主体 | 项 | 1  |  |
| 9  | 防雷接地测试 | 1.标准：地阻小于4欧姆2.出具防雷接地测试报告 | 项 | 1  |  |
| **（二）配电系统** |
| 1  | UPS系统 | 利旧 | 台 | 1 |  |
| 4  | LED一体化面板灯 | 1.名称：LED一体化面板灯1.规格：600\*600 | 套 | 4  |  |
| 5  | 应急装置 | 1.名称：应急装置 | 支 | 2  |  |
| 6  | 安全出口标志灯 | 1.名称：安全出口标志灯2.配件：带电池 | 套 | 2  |  |
| 7  | 单联单控开关 | 1.名称：单联单控开关1.规格：暗装86型 | 套 | 1  |  |
| 8  | 机柜PDU | 1.规格：10位16A2.含工业连接器 | 个 | 4  |  |
| 9  | 照明线 | 1.规格：ZR-BV-2.5mm22.技术要求：国标 | 米 | 380  |  |
| 10  | 插座线 | 1.规格：ZR-BV-4mm22.技术要求：国标 | 米 | 200  |  |
| 11  | UPS输入线缆 | 1.规格：WDZA-YJV3\*10mm22.技术要求：国标 | 米 | 15 |  |
| 12  | 机柜线缆 | 1.规格：WDZA-YJV3\*4mm22.技术要求：国标 | 米 | 40 |  |
| 13  | 桥架 | 1.规格：200\*100\*1.02.材质：喷塑 | 米 | 12 |  |
| 14  | 镀锌线管 | 1.规格：镀锌线管 φ202.厚度：1.0 | 米 | 62.5 |  |
| 15  | 镀锌线管吊件 | 1.镀锌线管配套2.含直接、弯头、吊件 | 项 | 1 |  |
| **三、气体灭火控制系统** |
| 1 | 柜式七氟丙烷灭火装置 | 1.配件：包括钢瓶、容器阀、柜体、信号反馈 装置、连接软管、单喷嘴（不含灭火剂）；2.规格：每瓶充装70公斤灭火剂 | 台 | 1 |  |
| 2 | 七氟丙烷灭火剂 | 1.名称：七氟丙烷灭火剂2.类型：HFC-227ea | kg | 40 |
| 3 | 防护区自动泄压装置 | 1.技术要求：有效泄压面积约:0.1㎡ | 台 | 1 |
| 4 | 气体灭火控制器 | 1.技术要求：可实现2个防区的气体灭火控制 | 台 | 1 |
| 5 | 点型光电感烟火灾探测器 | 技术参数：1.双光电感烟探测器；2.采用专用嵌入式MCU技术的分布智能型产品；3.电子编码，具有污染补偿功能；4.与LD10G底座配套使用。 | 只 | 1 |  |
| 6 | 点型光电感温火灾探测器 | 技术参数：1.智能型2.电子编码3.具有定温特性（A2S）4.内置单片机5.与LD10G底座配套使用。 | 只 | 1 |  |
| 7 | 编码通用底座 | 1.技术要求：配合G系列编码探测器使用。 | 只 | 2 |  |
| 8 | 火灾声光警报器 | 技术参数：1.编码型2.占联动点3.与E/EN系列控制器配合使用。 | 只 | 2 |  |
| 9 | 放气指示灯 | 技术参数：1.编码型2.占用一个地址点3.与气体灭火控制器配套使用。 | 只 | 2 |  |
| 10 | 警铃 | 技术参数：1.工作电压：DC20v—DC30v 2.工作电流：25mA | 只 | 2 |  |
| 11 | 紧急启/停按钮 | 技术参数：1.编码型2.配合新一代气体灭火一体机LD5507EN、LD5509EN使用3.实现现场紧急启动和紧急停止以及现场手动/自动切换控制。 | 只 | 2 |  |
| 12 | 镀锌线管 | 1.规格：镀锌线管 φ202.厚度：1.0 | 米 | 50 |  |
| 13 | 镀锌线管吊件 | 1.镀锌线管配套2.含直接、弯头、吊件 | 项 | 1 |  |
| 14 | 阻燃电线 | 1.规格：ZR-RVS2\*1.52.技术要求：国标 | 米 | 200 |  |
| **四、动环系统** |
| 1 | 嵌入式数据采集主机 | 技术参数：1.RS485输入≥8路；2.TCP/IP信号接入网络，支持TCP/IP,ModbusRTU等通用协议； | 台 | 1 | 接入数据中心机房动环平台 |
| 2 | UPS监控 | 1.技术要求：需监测UPS参数如：输入电压、输入频率、输入电流、输出电压、输出频率、输出电流、输出功率、机箱温度、电池电压、电池充电程度(后备时间)等 | 套 | 1 |  |
| 3 | 精密空调监控 | 1.技术要求：对精密空调进行远程遥控、遥信、参数监测、故障诊断，监控空调各部件(压缩机、风机、加热器、加湿器、去湿器、滤网等)的运行状态与参数 | 套 | 1 |  |
| 4 | 温湿度传感器 | 技术参数：1.12VDC供电2.测量范围:温度：-20℃~70℃ ，精度±0.5 ℃湿度：0～100%rh，精度±3%rh | 个 | 2 |  |
| 5 | 烟雾传感器 | 技术参数：1.工作电压：DC 12 V2.静态电流：≤5mA3.报警电流：≤80mA4.工作温度：－10℃ to +50℃5.环境湿度：≤95%RH6.安装方式：吸顶7.监测面积：20平方米8.指示灯：30秒闪一次9.报警输出：继电器常开／常闭 | 个 | 1 |  |
| 6 | 区域式漏水传感器 | 1.技术要求：多路干接点输出信号 (漏水1路、断线1路)声音设置灵活：声音有/无，声音锁定/不锁定丰富的指示灯内容，闪动代表有未确认警报,兼容多种感应线可调节灵敏度,响应时间5s | 套 | 1 |  |
| 7 | 门禁人脸一体机 | 技术参数：1.用户数:不低于500人 2.指纹容量：不低于500枚3.人脸容量：不低于500张4.记录容量：不低于10万条5.通讯方式：TCP/IP、RS485/2326.包含门禁卡：不低于20张 | 台 | 2 |  |
| 8 | 出门按钮 | 技术参数：1.最大静态直线拉力：280kg；2.使用范围：木门、防火门、金属门、玻璃门等3.安全类型：通电上锁、断电开锁 | 个 | 2 |  |
| 9 | 双门磁力锁 | 技术参数：1.50万次机械使用寿命；2.适合标准86电器接线暗盒使用3.PC防火材料 | 把 | 2 |  |
| 10 | 门禁专用电源 | 1.名称：门禁电源箱2.规格：12V5A | 台 | 2 |  |
| 11 | 门禁远程监控接口 | 技术参数：1.集成门禁数据2.实时显示门禁状态以及进出门记录 | 套 | 1 |  |
| 12 | 网络半球 | 技术参数：1.≥1080P分辨率2.支持Smart265编码3.POE供电4. ≥30米红外夜视 | 台 | 2 |  |
| 13 | 硬盘录像机 | 1.规格：通用型1盘位录像机6路1080P解码(可增强至8路1080P) | 满接4MP | 最大支持8TB | 台 | 1 |  |
| 14 | 监控硬盘 | 1.规格：8TB监控专用硬盘2.技术要求：存储时间6个月 | 块 | 1 |  |
| 15 | 视频远程监控接口 | 1.技术要求：动环系统内嵌入视频监控画面，可浏览实时监控画面，以及回放录像。 | 套 | 1 |  |
| 16 | 24口POE交换机 | 技术参数：1.24个10/100/1000Mbps自适应电口+2个10/100/1000Mbps上联光口，其中24个口支持PoE/PoE+供电2.最大PoE功率≥370W3.交换机容量≥52Gbps4.包转发率≥38.69Mpps5.非网管型交换机，机架式。 | 台 | 1 |  |
| 17 | 网线 | 技术参数：1.导体：实心无氧铜（铜芯线径≥0.57mm）2.绝缘层：高密度聚乙烯（HDPE）3.外护套：聚氯乙烯（PVC）厚度：0.55mm4.线缆结构：4对8芯双绞线,每对之间采用十字骨架隔离,每芯均有颜色区分,外皮印有厂商标识及电缆编码，有撕裂绳，线缆外径≥6.3mm5.标准：传输性能参数满足ISO/IEC 11801 E类标准和TIA/EIA 568.2-D六类标准；性能指标优于现行六类线缆250MHz，支持1G Base-T, 622M ATM 等高带宽应用6.运行温度：-25至60°C7.最大电容：≤5.6nF/100m8.特性阻抗：(f：1-155MHz)100±15Ω质量保证：1.提供原厂三年质保服务。2.提供技术参数及功能的证明材料3.质量标准：提供符合GB/T 18380.12标准阻燃检测报告、提供泰尔实验室出具的单体性能检测报告、提供具有CMA、CNAS、ilac-MRA认可的检测机构检测的信道测试报告和链路测试报告 | 箱 | 1 |  |
| 18 | 电源线 | 1.规格：RVV2\*12.技术要求：国标 | 米 | 15 |  |
| 19 | 管材 | 1.规格：PVC20，PVC25，PVC32等各种管件 | 批 | 1 |  |
| 20 | 安装调试费 | 技术要求：1.动环设备安装、监控设备安装、门禁设备安装2.布线 | 项 | 1 |  |
| **五、信息网络及网络安全系统** |
| 1 | 防火墙主机 | 1. 千兆电口数量≥8个，千兆光口数量≥2个，万兆光口数量≥4个，业务扩展插槽≥2个（可扩展4万兆光口、4千兆光4千兆电接口卡），最大支持≥16个千兆电口，最大支持≥10个千兆光口或12个万兆光口。2.硬盘插槽≥1个，配置可插拔1T企业级硬盘≥1个，支持并配置模块化电源≥2个（1+1电源冗余）。3.三层网络吞吐≥3Gbps ，IPS吞吐量≥1.5Gbps，每秒新建连接≥3万。支持通过软件授权，灵活扩展网络吞吐量性能，提供生产厂家官网链接及截图；网络吞吐性能通过扩充可达到≥10Gbps。4.支持路由模式、透明模式、混合模式，支持快速上线向导功能，指导配置人员完成快速入网、模式选择、网络配置、连通性检查、授权导入等必要上线步骤；5.IPS规则数量≥5500条，可针对具体的规则条目设置启用和禁用，具有IPS入侵检测预定义模板，用户可设置新的签名过滤器，来自定义新的IPS入侵检测防御模板，支持SYN、UDP、ICMP等洪水型DoS/DDoS攻击防护，支持TearDrop、Smurf、LAND、Winnuke、Fraggle等基于数据包的攻击防护，支持带源路由选项IP报文控制功能、支持带路由选项IP报文控制功能；支持ARP欺骗防御功能，支持自定义设置网关MAC广播间隔时间。6.支持自动扫描用户网内资产，自动识别资产端口和服务启用情况，结合用户资产信息生成推荐的安全防护策略，提供产品功能界面截图。7.支持基于流量学习的方式对网内资产的互访关系进行梳理，可视化展示目标资产的端口的访问关系，包括：访问源IP、命中策略、阻断次数、最近一次阻断时间等信息，提供产品功能界面截图。8.精确识别网络应用，包括但不限于HTTP协议、IP网络电话、网络游戏软件、网络购物、P2P应用软件、互联网金融、即时通讯、远程控制等，具备完善的应用库，应用数量≥3400种。9.支持策略配置向导功能，运维人员可通过向导流程完成地址对象创建、策略创建、策略模拟运行、策略执行等必要配置步骤，提供产品功能界面截图。10.支持策略模拟功能，可提供一个虚拟的策略空间来对运行创建的模拟策略，模拟策略不会对真实业务流量产生影响 ，但可以把模拟策略的执行结果与现有的真实策略的不同的处置动作进行对比展现，方便用户判断模拟策略是否会对重要业务产生不良影响，如模拟策略符合用户需求，可一键转化为真实策略，提供产品功能界面截图。11.具备策略优化能力，支持对配置的策略进行梳理，能够识别策略问题，问题类型包括但不限于一般问题、严重问题、建议优化等。分析维度包括但不限于从未匹配、7天未匹配、30天未匹配、90天未匹配、冲突策略、组合策略、归纳策略、影子策略等，对问题策略支持列表展示，并提供优化建议。12.支持策略的全生命周期展现，包括策略的变更时间、变更类型、变更账号、变更策略、变更内容等；支持通过颜色区分策略的变更项、删除、新增等；支持策略项变更前后的对比展示，提供产品功能界面截图。13.支持策略进入模拟空间，可对无把握的安全策略先在策略模拟空间进行试运行，看看对应流量是否有符合预期。（提供生产厂家官网链接及截图）14.支持整体呈现内对内、内对外、外对内的攻击统计，图示化呈现攻击的方向和区域，可选级别、刷新频率、周期、攻击类型；TOP攻击源、被攻击主机、新增攻击源、新增攻击端口、攻击趋势图等。15.支持系统日志、安全日志（攻击防护日志）、操作日志（登录、策略变更等）等不同分类日志的留存，可查询和导出日志；支持根据源地址、目的地址、源端口、目的端口、日志类型、严重性、动作等条件进行日志查询，支持呈现各个接口流量趋势图，支持实时、最近1天，最近1周的查看范围；呈现各接口的流量详细信息，支持报表导出，支持自定义外发系统日志、安全日志等，支持同时将日志发给多个syslog服务器，支持CPU、内存使用趋势监控，可选择实时、最近1天、最近1周的显示周期。16.支持自定义设置登录端口、登录超时时间、登录错误允许次数、锁定时间，开启、关闭验证码功能，支持恢复默认配置，支持一键收集本机上所有信息，并提供打包下载，用于故障定位，提供产品功能界面截图。17.支持通过手动输入和扫描二维码两种方式将设备添加到云平台进行管理，可实现把防火墙的系统状态在云平台进行监控和展示，用户可通过登录各自的云平台账号后对纳管的防火墙进行远程策略下发，策略查看和安全事件分析等，基于首页设备图示，实现鼠标移动到相应接口，即可显示接口的加电状态、接口类型、接口IP和上下行速率等，提供产品功能界面截图。18.可实现对策略进行增、删、改的操作，可在模拟空间中，匹配真实流量，分析策略调整前后流量匹配命中的差异，并据此调整策略直至满意，保证业务不中断也能调策略，降低策略调整的风险，并能实现精细化策略调整。（提供生产厂家官网链接及截图）19.配置要求：配置提供病毒库升级功能授权≥3年、入侵防御特征库升级功能≥3年、 URL特征库升级功能≥3年、应用识别特征库升级功能≥3年、威胁情报特征库升级功能授权≥3年。质量保证：1.提供原厂三年质保服务

2.提供技术参数及功能的证明材料 | 台 | 1 |  |
| 2 | 防火墙硬盘 | 块 | 1 |  |
| 3 | 防火墙授权 | 年 | 3 |  |
| 4 | 核心交换机电路保护系统 | 1. 采用高性能微控制器主控芯片；2. 设备结构为多功能软硬件集成一体机。19寸标准机架式安装、占用机柜高度≤1.5U、挂耳可拆卸；3. 设备配置网络通讯接口至少包括RJ45、4G，网络防雷接口≧2路、漏电监测接口≧2路、电源输出接口≧2路国标插座；4. 支持防雷击防浪涌功能，最大放电电流Imax(8/20μs)≧40kA，电压保护水平Up≦1.7kV；支持监测诊断功能至少包含：电压、电流、功率、雷击浪涌次数、防雷器状态、防雷器温度、防雷器寿命、接地通断、断电、漏电监测，漏电流、雷电峰值电流、雷击时长、雷击总时长、雷击强度、雷电波形、接地电阻、温度、湿度、水浸；5. 设备标配≧2.0寸触摸显示屏，可显示监测指标信息，屏显内容包括：电压、电流、频率、功率、雷击浪涌次数、防雷器状态、防雷器温度、防雷器寿命、接地通断、漏电监测、温湿度、烟雾、水浸、安装单位、联系人、联系电话；通过手机扫描设备屏显的电子二维码进行关注，手机微信端和管理平台端均可进行查询、故障报修、图片上传、设备绑定授权、管理工单；6. 设备内置告警扬声器≧1个，具有系统、网络、入网状态指示灯，告警方式支持本机扬声器告警、手机微信告警、管理平台告警；7. 支持供电BYPASS功能，本机系统出现问题或者系统重启也不影响正常输出供电；8. 管理方式支持Web管理；质量保证：1.提供原厂三年质保服务

2.提供技术参数及功能的证明材料 | 台 | 1 |  |
| 5 | 核心交换机 | 1.灾备机房部署备用核心交换机一台（设备由业主提供）2.设备上架，部署网络环境3.与数据中心机房主用核心交换机进行虚拟化部署 | 台 | 1 |  |
| 6 | 三层交换机 | 1. 提供≥24个10/100/1000Base-T以太网端口，≥4个万兆SFP+端口，实配1+1冗余电源。2、交换容量≥670Gbps，包转发率≥150Mpps。3、采用国产CPU、国产交换芯片。4、设备MAC表项≥48K，ARP表项≥8K，IPv4路由表项≥12K，IPv6路由表项≥4K，ACL容量≥3.5K，产品端口浪涌抗扰度≥10KV（即具备10KV的防雷能力）。5、支持Openflow 1.3相关SDN协议，提供准入管控功能。6、支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议；支持SAVI功能，可防止地址解析欺骗。7、支持专门基础网络保护机制，支持多种类型的防护，如ARP防护，当ARP速率超过攻击水线，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行。8、支持生成树协议，保证网络的稳定运行和链路的负载均衡，合理使用网络通道，提供冗余链路利用率，支持虚拟路由器冗余协议，支持快速链路检测协议，可快速检测链路的通断和光纤链路的单向性，并支持端口下的环路检测功能，防止端口下因私接Hub等设备形成的环路而导致网络故障的现象。9、支持SNMP、CLI(Telnet/Console)、RMON、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web。10、为保证IPv6的可部署性和应用性，需通过IPv6 Ready Phase2认证测试。质量保证：1.提供原厂三年质保服务

2.提供技术参数及功能的证明材料 | 台 | 1 |  |
| 7 | 交换机电源 | 个 | 2 |  |
| 8 | 万兆光模块 | 1.万兆单模光纤模块（10km，1310nm）。 | 块 | 6 |  |
| 9 | 千兆光模块 | 1.1000BASE-LX mini GBIC转换模块（1310nm），10km，单模。 | 块 | 4 |  |
| 10 | 服务器机柜 | 1. 采用整体式框架结构设计，方便运输、安装灵活。2.环境条件1）工作温度：-5℃到 +40℃；2）相对温度：≦85%RH （25℃±5℃时）；3）海拔高度：≦1000m；4）垂直倾斜度：≦5%。3.外观与形象1）外观高贵典雅，工艺精湛，尺寸精密。2）凸显优质工程，彰显高贵品质。3）机柜外形尺寸：服务器机柜：600mm\*1000mm\*1200mm4）颜色及表面处理：黑色（色标号RAL9005）、静电粉末喷涂工艺，机柜表面颜色、质感要高雅、防腐、耐脏、不易产生划痕；机柜表面要求进行脱脂、酸洗、防锈磷化、纯水清洗等预处理；表层外观应表面光洁、色泽均匀、无露底、无流积、无起泡、无裂纹、金属件无毛刺和锈蚀。4.结构与材料1）柜体选用优质冷轧钢板制作,推荐采用框架结构。2）钢板厚度：总体板厚为1.2～2.0mm，前、后门、侧门、框架≥1.2mm，立柱≥2.0mm，连接件、承重板≥1.5mm。3）柜门的形式：机柜前后网孔门结构，配置安全锁。前后门为整体单开门结构，高级旋把门锁，门开启角度130°；选用优质冷轧钢板，钢板厚度≧1.2mm，前后门安装后，无倾斜、凹陷、凸起或局部歪、扭现象存在；4）侧板：选用优质冷轧钢板，钢板厚度≧1.2mm，可速装速卸；5）机械活动部位转动灵活、插拔适度、锁定可靠、施工安装和维护方便。6）配置：每台机柜需配置四个风扇、一块台板、一个10A6位PDU电源、机柜螺丝不低于20套；地脚螺钉4颗。7）产品通过24h的中性盐雾试验。5.承重1）安装角轨厚度≧2.0mm2）立柱和安装角轨≧4折3）承重板选用优质冷轧钢板，钢板厚度≧1.5mm，承板深度≧350mm，承重≧100Kg。4）产品通过72h的静载荷800KG的承重试验；质量保证：1.提供原厂三年质保服务

2.提供技术参数及功能的证明材料 | 台 | 2 |  |
| **六、数据及应用备份系统** |
| 1 | 备份一体机（含备份软件） | 1.机架式标准2U12盘位设备，配≧2颗国产X86架构2.5GHz 16core CPU，配≧ 128GB 内存，标配≧ 2\*480G SSD 盘做系统盘，配≧4个千兆网络端口和≧2个万兆光口，配置≧12块4TB企业级磁盘； 2. 提供基于磁盘数据块复制技术的整机备份，无需了解主机业务系统类型、部署方法、业务系统间的数据交互机制、数据结构/逻辑关系和数据库的品牌/版本，本次提供≧20TB数据保护容量授权。3. 提供对任意品牌技术的X86、C86、ARM服务器的统一灾备保护功能，提供对非国产Windows/Linux操作系统的灾备保护功能，满足对32/64位系统平台及应用支持，具体如下：Windows Sever 2003以上版本；WindowsXP/7/8/10；Redhat /Centos/Oracle Linux 5.x及其之后；Suse 10 sp1~sp4/11sp1~sp4/12 sp1~sp4；Ubuntu12 -~Ubuntu16；Debian8 ~ Debian9；提供对国产操作系统中标麒麟、银河麒麟、统信、中科方德等的灾备保护。4. 支持对X86、C86、ARM架构下的物理主机、虚拟化主机、超融合主机、云主机提供CDP持续数据保护，实时备份磁盘任意时刻的状态，备份时间粒度最小可达秒级实现RPO趋近于0。 5. 支持针对X86架构下集群业务系统类似于Oracle RAC等整机集群CDP持续数据保护，保障核心应用系统数据完整性。6. 支持X86架构下重要业务如HANA数据库实时数据库等核心应用的CDP持续数据保护功能；7. 支持基于Vmware虚拟化平台主机定时备份保护功能，无需在虚拟机中安装任何客户端代理;8. 支持完整备份和增量备份，第一次备份时使用完整备份保留整机应用的完整状态，后续采用增量备份，大幅减少备份的数据量。9. 支持对WindowsXP/7/8/10操作系统办公终端提供整机备份保护，按照策略实现历史时间点的整机回滚，保障重要办公终端数据安全；10. 支持备份时通过备份与恢复系统进行网络带宽占用限速、磁盘读写占用限速，以确保备份时对生产的影响小并且在可控范围内。11. 可将选定的备份点加载为CIFS文件共享和网络共享路径可直接在WEB浏览器中直接URL访问，管理员可快速确认需被验证的备份点文件是否是符合预期，备份点是否可用、可靠；12. 针对X86和C86生产环境，可自建隔离私有虚拟化验证环境，无论备份任务是否停止，可同时选一个备份任务的多个备份点执行虚拟化验证备份数据的一致性和可靠性，在灾难发生时采用二分法快速定位出最佳数据恢复的备份历史点（提供截图和证明材料）；13. 可同时启动多个虚拟机对集群业务系统、Oracle RAC等共享存储的集群数据库和应用提供快速整机虚拟化验证。14. 演练时，演练目标机无需预置任何演练环境（目标机无操作系统、目标机和原机操作系统不一致、目标机无应用系统、目标机无数据库等）可即时开展对指定业务模拟故障后的演练重建功能。15. 用户日常运维过程中丢失单个文件/文件夹，备份系统支持将任意时间的备份点加载为网络共享路径或在WEB浏览器中直接URL访问的方式，管理员可轻松找到该文件并复制出来；支持采用文件的直接恢复的方式，可指定恢复单个文件或文件夹到原机某个目录下；16. 支持整机全场景恢复，无需部署配置操作系统、应用和数据库等系统环境，实现全场景带业务逻辑的整机灾难重建，无需人工手动安装驱动、更改注册表信息、应用配置信息等，极大降低灾难重建恢复难度和效率。17. 针对X86和C86生产环境，支持应急接管时无需另配置恢复主机，备份系统可自建应急接管虚拟主机，无需集成/配置第三方虚拟化平台，降低因虚拟化平台兼容性而导致的恢复风险；18. 支持可基于同一个备份点同时启动多个不同IP地址、不同个数CPU、不同大小内存等配置虚拟机对外提供服务，以应对副本使用、系统故障应急等不同功能、性能需求。 19. 支持应急接管时，可即刻开始对接管主机提供秒级CDP增量备份保护，且应急接管期间新增的数据会形成备份点可用于数据恢复，防止接管期间的误删除、误操作、逻辑错误等导致数据丢失。 20. 支持应急接管时，可同时配置将接管主机整机回迁至原生产环境的相关参数，应急接管期间整机包含新增数据的无缝回迁至生产环境主机，应急接管结束后择机可恢复至生产环境。21. 备份系统的专用嵌入式操作系统维护后台采用动态口令机制，动态口令由设备管理员和原厂口令组成，原厂口令随着设备管理员的改密码操作而变化，确保系统后台密码都是唯一的，减少被攻破的可能性。22. 备份系统网络可配置“网卡关闭/开启策略”，还可将除备份数据传输端口外的SSH、网络访问等网络端口全部关闭，杜绝除传输备份数据流之外一切网络访问的可能，降低备份系统被攻击的概率。23. 支持以图形或WEB方式进行批量操作管理，包括在管理范围内设备的状态和性能信息、各种数据保护参数、各种备份作业的设置信息、各种备份/恢复作业的执行状态统计信息、各种备份业务数据的相关信息等。全面支持简体中文的界面操作。质量保证：1.提供原厂三年质保服务2.提供技术参数及功能的证明材料 | 台 | 1 | 数据实时备份 |
| 2 | 应用服务器 | 1.搭建服务器（设备由甲方提供）2.满足医院使用要求3.用于HIS等备用业务系统 | 台 | 2 | 服务器业主提供 |
| 3 | 数据备份服务 | 1.技术要求：每季度至少巡检一次并提供原厂巡检报告。巡检内容：包含但不限于整体运行情况、容灾备份情况、备份恢复演练等。 | 年 | 3 |  |
| 4 | 应用备份技术服务 | 1.设备上架2.网络环境部署 | 项 | 1 |  |
| **七、综合布线系统** |
| 1 | 24芯室外单模光纤 | 技术参数：1.采用扎纹钢带铠装护套和钢丝加强件，抗拉、抗压，具有良好的机械性能2.外护套采用聚乙烯PE料，添加UV防晒材料，具有抗UV、耐高低温、不易老化3.管内间隙填充特种油膏保护光纤同时有效防水。内套和护套之间的间隙填充复合物连续填充特种防水化合物。4.允许拉伸力（N）：长期500，短期10005.压扁力（N/100mm）：长期300，短期10006.弯曲半径：长期30D，短期15D7.储存、使用温度：－40℃～70℃8.光纤衰减: OS2: 1310nm≤ 0.36 dB/km,1550≤0.23 dB/kmOM1：852nm≤3.0 dB/km，1300nm≤ 1.0 dB/kmOM2：852nm≤3.0 dB/km，1300nm≤ 1.0 dB/km OM3：852nm≤3.0 dB/km，1300nm≤ 1.0 dB/km质量保证：1.提供原厂三年质保服务2.提供技术参数及功能的证明材料3.质量标准：提供具有CMA、CNAS、ilac-MRA认可的检测机构的检测光缆链路测试报告（24芯单模）、提供具有CMA、CNAS、ilac-MRA认可的检测机构的符合ITU-T G.657、ITU-T G.652标准的测试报告（24芯单模） | 米 | 2000 |  |
| 2 | 24口光纤ODF架 | 技术参数：1.外观：灰白色（烤漆）；磨砂；2.材质：优质冷轧板3.抽屉式结构4.内置熔纤盘5.标准19英寸机架式，24口6.工作温度：-40~+85℃7.执行标准：TIA-568C.3-2008(光缆布线组件标准）8.适用接口：SC/LC/FC/ST等光纤连接器 | 台 | 2 |  |
| 3 | 48口光纤ODF架 | 技术参数：1.外观：灰白色（烤漆）；磨砂；2.材质：优质冷轧板3.抽屉式结构4.内置熔纤盘5.标准19英寸机架式，48口6.工作温度：-40~+85℃7.执行标准：TIA-568C.3-2008(光缆布线组件标准）8.适用接口：SC/LC/FC/ST等光纤连接器 | 台 | 1 |  |
| 4 | 48芯室外单模光纤 | 技术参数：1.采用扎纹钢带铠装护套和钢丝加强件，抗拉、抗压，具有良好的机械性能2.外护套采用聚乙烯PE料，添加UV防晒材料，具有抗UV、耐高低温、不易老化3.管内间隙填充特种油膏保护光纤同时有效防水。内套和护套之间的间隙填充复合物连续填充特种防水化合物。4.允许拉伸力（N）：长期500，短期10005.压扁力（N/100mm）：长期300，短期10006.弯曲半径：长期30D，短期15D7.储存、使用温度：－40℃～70℃8.光纤衰减: OS2: 1310nm≤ 0.36 dB/km,1550≤0.23 dB/kmOM1：852nm≤3.0 dB/km，1300nm≤ 1.0 dB/kmOM2：852nm≤3.0 dB/km，1300nm≤ 1.0 dB/km OM3：852nm≤3.0 dB/km，1300nm≤ 1.0 dB/km质量保证：1.提供原厂三年质保服务2.提供技术参数及功能的证明材料3.质量标准：提供具有CMA、CNAS、ilac-MRA认可的检测机构的检测光缆链路测试报告（48芯单模）、提供具有CMA、CNAS、ilac-MRA认可的检测机构的符合ITU-T G.657、ITU-T G.652标准的测试报告（48芯单模） | 米 | 1200 |  |
| 5 | 48口光纤ODF架 | 技术参数：1.外观：灰白色（烤漆）；磨砂；2.材质：优质冷轧板3.抽屉式结构4.内置熔纤盘5.标准19英寸机架式，48口6.工作温度：-40~+85℃7.执行标准：TIA-568C.3-2008(光缆布线组件标准）8.适用接口：SC/LC/FC/ST等光纤连接器 | 台 | 4 |  |
| 6 | 光纤跳纤 | 技术参数：1.接头类型包括ST、SC 、LC、FC, MPO等跳线及混合跳线等；2.接头材料：陶瓷套管3.重复插拔：≤0.2dB，每500次插拔4.插入损耗：SM≤0.3dB，MM≤0.3dB5.回波损耗：≥50dB6.线缆结构由原来的基础上增加了导光光纤，内置导光光纤，在两端线身上留有光源输入口，无需拔插可通过任意的可见光照明装置快速定位线缆两端的关系（提供产品画册或者产品演示）质量保证：1.提供原厂三年质保服务2.提供技术参数及功能的证明材料3.重要功能：具备一键巡线功能，提供具有CMA、CNAS、ilac-MRA认可的检测机构检测的寻线功能测试报告4.质量标准：提供具有CMA、CNAS、ilac-MRA认可的检测机构检测的链路测试报告 | 批 | 1 |  |
| 7 | 辅材 | 1.配件：各种接头、扎带、膨胀、胶布、自攻螺丝、穿线器等 | 批 | 1 |  |
| 8 | 通信光缆施工 | 光纤部署：1.灾备机房-数据中心机房（2条48芯光纤）2.24芯光纤部署：灾备机房-1号楼；灾备机房-2号楼（完成割接）；灾备机房-3号楼（完成割接）；灾备机房-四合院（完成割接）；灾备机房-科教楼；灾备机房-机关楼。3.技术要求：暗敷 | 项 | 1 |  |
| 9 | 部署要求 | 1.主干网络采用双核心、双汇聚、万兆至接入层，其中核心交换机在数据中心机房与灾备机房进行异地部署；双核心、双汇聚采用虚拟化做堆叠，各汇聚层双链路万兆链接至双核心，接入层交换机双链路接至双汇聚，完成网络割接2.原有数据机房做为灾备机房，配合完成原数据机房内服务器、超融合、存储、医院各业务系统、网络设备、网络安全设备搬迁；3.根据原数据机房情况，编制详细割接及实施方案，并经过甲方评审。 4.按照用户要求的时间及时对网络、网络安全系统、医院业务系统进行割接并及时恢复，部署相关数据备份和应用备份。 | 项 | 1 |  |