家庭医生健康云平台

安全体系说明

# 系统架构

## 总体设计原则

### 前瞻性、先进性原则

系统的设计和所采用的技术必须具备足够的前瞻性 和先进性，充分考虑到由于医院业务发展所带来的海量数据处理，确保未来 5 年内可以满足医院业务运作对整个系统的需求。

### 实时性原则

临床信息系统业务处理频繁、信息交换量较大的信息系统， 业务处理的速度直接关系到医院正常运作和经济效益，以及客户对医院的评价。 在正常情况下，系统必须在大业务量的情况下同时保持快速的实时响应能力，以 保证整个业务系统的通畅运行。

### 扩充性、开放性原则

为适应不断飞速发展的医院业务，系统要具备良好的扩展性、开放性和移植性，能随着业务规模的增长和业务种类的增加，能方便地增加新的硬件以提高处理能力，增加或修改软件功能以适应新业务的开展。整个系统采用结构化、模块化设计，对外提供清晰、完整的资料和控制接口，支持业界通用的标准平台和协议，提供标准接口，以便进行系统集成和系统资料交换。

### 安全性原则

医院业务系统关系到救护病人的生命，系统的安全性属于优先考虑的指标之一。在系统设计、实施阶段必须从多个方面充分考虑整个系统的安全性，另外系统中所有的重要操作留有痕迹，以规范管理。按照每个用户所在 的岗位和所需完成的业务，由系统管理员分配权限，每个用户只能看到本人所允许和应该看到的信息。

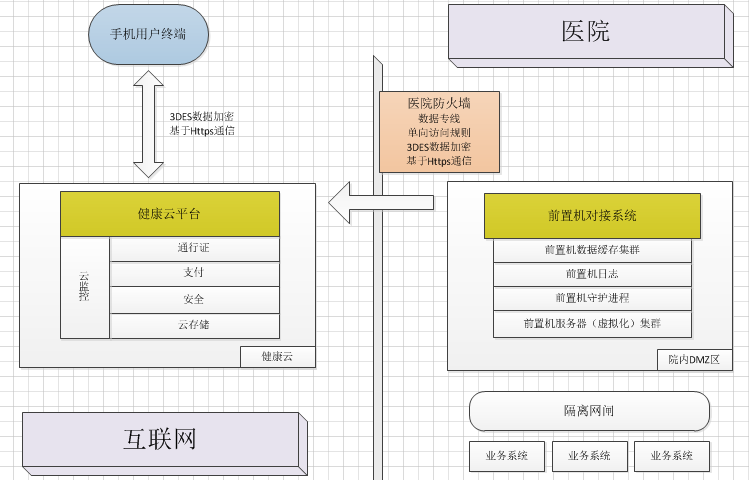
### 操作性原则

快速查询患者资料是临床信息系统必须具备的重要功能之一，要求人机界面友好、直观、清楚、统一，通过收集和整理医护人员提出的专业意见，达到既简化操作，提高软件的可用性，同时又保证资料的一致性。

## 系统架构图

为了不影响医院内部信息系统的运行速度和减少用户的等待时间，本应用系统以当前主流的Java EE平台进行开发，平台系统采用 B/S 模式下多层 MVC 结构设计，界面处理、业务逻辑、数据运算分离，采用院内多台前置机集群，平台服务集群与负载均衡的方式为用户提供数据访问。

健康云系统整体系统架构图



1. 医院前置机与健康云平台采用专线方式进行连接，传输数据使用3DES进行加密处理；
2. 前置机上面部署健康云对接服务系统（JAVA WEB）与医院数据缓存服务（redis），其中接口采用webservice与restFul标准服务，数据格式使用标准的XML与JSON对象，参考【医院前置机】；
3. 医院内部资源基于业务系统进行管理，例如挂号：健康云系统仅仅是转发了用户的请求到HIS系统，HIS系统根据实际情况控制挂号成功与否，在这里可以HIS系统可以控制时间、日期、人数等等。

### 综合展现层

系统用户通过B/S 结构的浏览器界面进行业务管理。应用展现层通过 CMS 技术实现后台对医院各 类常规栏目的管理和发布等，通过 PORTAL 技术实现各类常规栏目的展现。同时，统一的 PORTAL 将支持未来 EAI 系统集成整合功能，支持 AD 单点登陆实现用户一次登录全部访问所有有权限的业务数据的功能。同时为运维人员和领导提供更加直观清晰报表查询、数据分析的综合展现方式。

### 业务应用层

包括主要的门户网站常用功能、支持未来业务系统的集成、接口系统等多种功能。以 ESB 企业服务总线的模式构建统一的系统集成平台，为所有的应用系统提供技术支撑，包括未来的新开发业务系统。

### 业务支撑层

实现各管理功能的业务逻辑，包括系统各类任务管理、工作流管理、用户信息、用户功能权限、用户登录日志和系统操作日志的管理。

### 系统支撑层

包括网络、主机、备份、存储、数据库和中间件等系统集成的支撑，构成系统的各软件模块进程、数据库、计算机设备等的监控和管理；数据备份等功能。

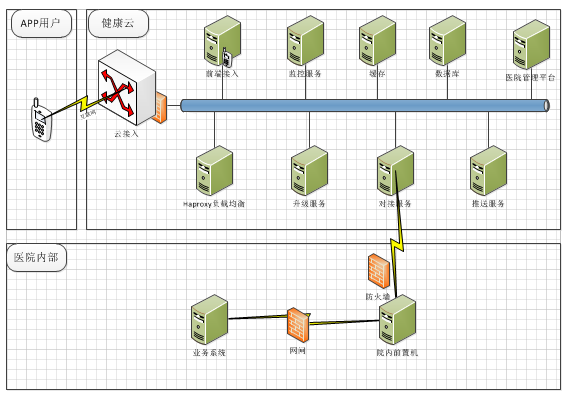
### 并发响应保证

为了加速请求响应速度，院内架设数据缓存服务，用于缓存手机用户请求的业务系统数据，提高用户体验。

院内前置机承担了主要的业务转发处理工作，为了满足互联网大并发的要求，因此使用集群模式处理业务。

## 物理拓扑图

### 手机平台物理拓扑图



### 网闸隔离模式

系统用户通过B/S 结构的浏览器界面进行业务管理。应用展现层通过 CMS 技术实现后台对医院各 类常规栏目的管理和发布等，通过 PORTAL 技术实现各类常规栏目的展现。同时，统一的 PORTAL 将支持未来 EAI 系统集成整合功能，支持 AD 单点登陆实现用户一次健康云服务平台充分考虑卫生专网隔离要求,将整个网络划分为外部终端、互联网、边界检查区、公众医疗服务区、隔离交换区、医院信息系统。

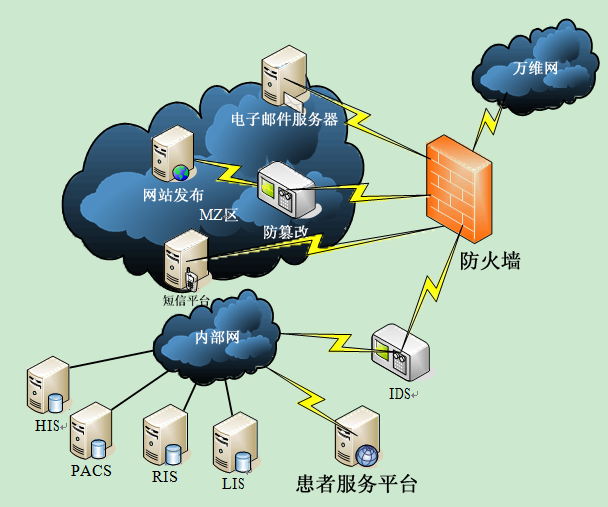
医院信息系统处于医院内网，应用服务区通过隔离网闸获取外网医疗信息请求，核实身份合法性后，查询专网内相关医疗信息（如挂号、排队、检验结果等医疗信息），再将查询结果通过隔离网闸推送至公众医疗服务区;如果是预约类请求，根据医院信息化程度做实时或预处理，并存储近期与个人医疗相关的信息，以提高系统的查询效率。

隔离交换区负责阻隔卫生系统专网与互联网之间的通路，二者间的数据通过数据摆渡方式进行，在摆渡时需要进行安全性检查。

边界检查区负责保障内部网络安全平稳运行，包括防火墙、入侵检测和入侵防御、漏洞扫描、证书服务、身份认证、网络集中管理等。

健康云承载业务系统运行，包括各类应用服务器、数据库服务器、中间件服务器和数据存储设备,以及核心业务数据的远程灾备等。

### 网站平台物理拓扑图

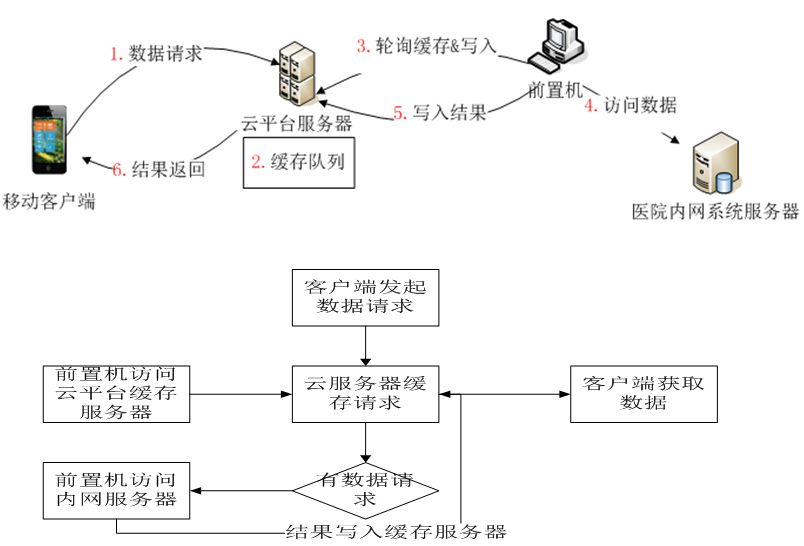


基于防火墙与负载均衡技术构建的患者服务平台，服务为了提高响应能力使用专用的数据读取层（基于现有业务的镜像数据库或者其他技术）来平衡数据访问压力。平台可以通过接口与其他业务系统对接。

患者平台建设需要参考标准WEB网站搭建，采用集群服务与页面缓存技术。

## 数据流转图

健康云产品从设计上将传统的被动服务（你找我，我服务）为主动服务（我找你，我服务）,以我为主的提供必要服务内容。基于这种设计理念，在数据空间流转上分为6步进行。如下图：



第一步：用户通过移动客户端向云平台服务器发送数据请求。

第二步：云平台服务器接收到用户请求后，暂存在云平台的缓存队列中。

第三步：医院前置机通过轮询云平台缓存队列，获取用户请求。

第四步：前置机通过隔离网闸向医院内网信息系统将用户请求的数据获取。

第五步：前置机将获取的用户数据写入至云平台缓存队列。

第六步：云平台服务最后将由前置机写入的用户数据，转发至移动客户端。

## 医院前置机

### 基本说明

医院前置机承担了医院内部业务系统与健康云平台之间的对接任务，主要负责数据的转发与缓存的使用，前置机采用流行的XML与JSON数据格式，通过标准的webservice与restful接口与医院内部业务系统和健康云进行数据对接，其中前置机位于医院内部隔离网闸一侧，保证的业务网络的独立性。

### 数据交换规则

医院前置机与医院内部业务系统采用以下方式进行对接

A)、WebService

医院业务系统开放WebService供前置机调用，前置机通过POST方式提交相关参数，业务系统将处理结果回传给前置机。

B)、数据库视图

医院业务系统开放数据库访问（只读）权限给前置机，并提供对应业务的数据视图访问模式，由前置机对接系统直接操作数据库获得内容。

C)、医院数据服务总线

在医院已经建立医院数据服务总线（HSB）的场合下，前置机可以直接连接到服务总线上，访问业务系统

D)、HL7 卫生信息交换标准

根据医院业务系统实行标准，前置机可以直接对接HL7数据规范完成业务系统对接。

### 性能与安全

医院前置机对接系统承担了健康云系统用户业务数据请求转发工作。

医院管理人员通过云平台配置相关的参数，来动态控制系统处理数据处理能力。

医院管理人员也可以通过云平台配置相关的参数，来动态修改数据加密密钥与状态。

单台前置机最低并发处理能力在1500左右，虚拟机的场合最低并发处理能力在500左右，对接系统通过配置前置机集群模式来提高数据处理能力。

## 手机支付

### 多方式提醒

考虑目前黑客与木马存在的多样性，在手机支付的各个环境进行多步提醒，主要通过微信、支付宝窗、短信与APP内部通知方式来警示用户操作行为。

### 健康卡支付验证码

用户在支付的过程中，需要输入验证码来完成支付动作，以此来明确用户行为。

验证码通过手机短信、APP通知方式来下发。

如果用户没有正常收到通知，那么可以手动进行【超时重发】操作。

# 安全控制

基于单向访问请求规则下面的手机APP系统架构，**按照安全等保二级标准，在本项目中各层面的安全保障措施如下：**

|  |  |  |
| --- | --- | --- |
| **安全层级** | **安全管控要求** | **健康云应用平台管控措施** |
| 数据安全 | 数据访问控制  重要数据加密传输  核心数据加密存储  数据库定期备份 | 1、数据库严格管理规范，限定用户读写操作，并记录用户访问日志；  2、业务系统间数据传输过程使用加密处理保证安全；  3、用户账户基本信息和登录密码、对接密码以及交易密码等采用相关的加密算法进行保存；  4、数据库采用双机热备，每天凌晨进行差分备份，每星期进行一次完整备份。 |
| 应用安全 | 用户注册，应用注册  用户策略(口令强度,认证策略等)  应用策略(应用摘要，应用版本等)  身份认证和权限控制 | 1、手机用户自由注册、医院运维管理人员由管理员开通；  2、用户密码采用MD5加密；  3、运维人员由管理员分配管理权限；  4、运维人员登录时候，根据需要使用USB Key与IP地址绑定限制，配合手机短信验证码进行认证管理。 |
| 主机安全 | 主机资源访问控制  IP过滤控制  主机操作系统和应用补丁管理  主机负载互为热备 | 1、医院前置机在内网里面指定HIS系统IP地址访问，其他系统访问需要添加到IP地址规则列表  2、前置机系统由医院管理，参考内部管理规范；  3、前置机使用双机机器集群服务，保证稳定性。 |
| 通信安全 | SSL传输协议  数字签名机制 | 1、前置机与健康云采用https连接；  2、前置机对接系统内置Token令牌机制，Token由本机设备信息产生与云端对接采用。 |
| 网络安全 | 内网无线安全接入控制  外网无线安全接入控制 | 1、前置机采用专线与健康云平台对接；  2、前置机通过网闸与医院内业务系统对接。 |
| 终端安全 | 设备注册  设备策略(密码策略、访问限制)  本地数据加密存储  锁屏/解锁/远程关机/禁用  应用擦除，数据擦除 | 1、手机用户注册时候进行设备绑定，使用Token令牌记录设备信息并保存到本地作为APP证书使用；  2、用户可以设定手势密码， |

## 移动设备安全方面

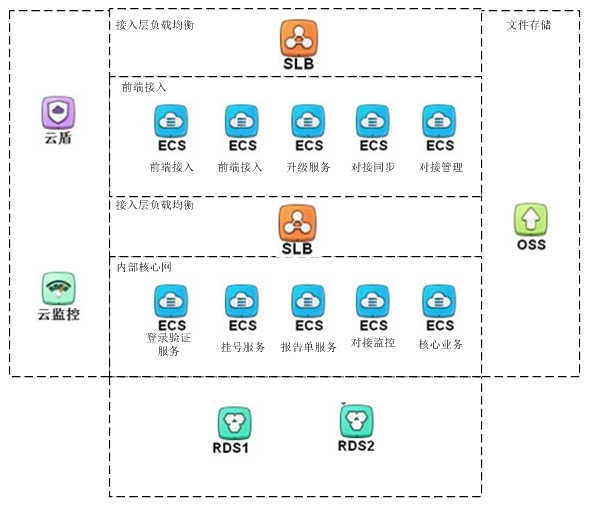
为了防止App在安装后被恶意篡改，我们的App在安装后会扫描自身文件的正确性与合法性，一旦出现问题，APP内部会出现警示，提示用于App版本存在问题。

在APP内部支付过程中，用户会跳转到外部应用，对应的支付软件（支付宝）提供相应的安全保证机制。

如果用户发生了移动设备遗失的状况，只需要通过我们的客服热线电话选择冻结当前账户，然后使用新的手机重新绑定账户，操作成功后，遗失设备里面的APP账户将不能正常登录。当遗失设备重新登录的时候，健康云APP会强制清空历史缓存。

## 网络安全方面

为了防止服务端被攻击，我们的接入层服务器部署在阿里云中，并开启了云盾、云盾DDoS和云监控。使用云盾、云盾DDoS产品进行系统保护，能够实现DDos防护、主机入侵防护，以及漏洞检测、木马检测等防护功能。使用了云监控之后，一旦系统出现问题，管理员就可以收到短信、邮件的方式的告警信息。



为了防止云盾被攻破，我们在云端使用了分层部署和双SLB架构。(参见云端架构图)SLB在提供负载均衡的同时，能够对网络进行有效的隔断。即使云盾出现问题，恶意攻击者也只能侵入接入层。第二层SLB隔断之下的业务处理层，仍然是安全的。这为管理的干预和处理提供了时间。

为了防止医院的防火墙和前置机被攻击，我们采用了单向访问的部署方案。此种部署方案的特点是医院的防火墙不需要打开侦听端口，从而完全杜绝了被攻击的可能。系统不记录任何院方接入地址信息，由院方主动询问健康云业务请求状态。

## 数据传输方面

为了防止数据在传输过程中被篡改和伪装。我们的App使用带证书的Https通信方式与接入服务器之间进行交互。

在院内前置机与健康云平台之间使用基于Https链路的医疗专线网络连接保证数据通信安全。

## 信息安全层面

为了防止数据在交互过程中被窃取。我们的App对交互过程中的数据进行了加密，目前使用的加密算法是3DES。

加密公钥与私钥有医院自行生成，医院通过管理平台上传到云端保存，开启加密设定后，全系统数据在网络传输过程中将通过该算法与密钥进行数据加密处理。

其中数据加密的范围包括App数据到健康云端、健康云端到医院前置机过程。

整个加密过程也可以通过配置进行动态开关，也医院可以定期更换密钥设定。

业务请求在10秒内响应成功后，数据自动从消息队列内删除；如果超时队列内数据强制从消息队列内删除。

## 交易安全层面

为了保护关键交易流程的执行安全。我们的App在开发时针对用户注册、用户信息修改、挂号等关键交易流程，增加了混淆令牌保护。即便数据包被完整抓取和重发，也是不会成功执行。

为了保证业务系统的公平性，防止恶意使用。我们的App在用户信息修改(特别是设备绑定信息)或者挂号等步骤，还会追加短信验证码等技术。

为了防止登录后的遗留环境被利用。数据敏感的查询业务和交易业务都会纳入会话机制的管理。一旦App后台化或者交互中断达到有效期上限，登录会话就会失效。用户在执行相应操作时，就需要重新登录。会话机制的开关和会话有效期都可以通过服务端进行控制。

基于挂号支付业务下面的交易处理，APP自动跳转到第三方支付APP业务完成，保证交易安全。

## 系统行为日志

为了确保系统在运行过程中的安全，全系统记录业务相应日志到日志系统内，该系统由院方管理，并且制定加密钥匙，健康云只是负责记录，院方定期下载该业务日志进行解密后分析处理。

### 前置机业务响应日志

主要包括以下日志

1. 手机用户信息
2. 业务请求与响应信息
3. 数据同步处理信息

前置机业务系统会记录对应操作相关的日志文件里面，运维人员可以直接查看相应的日志记录信息。

### 健康云后台管理日志

主要包括以下日志

1. 管理人员登录日志
2. 运维人员操作日志
3. 财务人员审计日志

管理人员通过日志下载功能即可查看本医院所有管理人员的操作日志记录。

## 用户隐私保证

### 用户、手机设备与患者相互关系

**A、用户注册**

用户的管理周期开始于注册流程，原则上没有终结。设备和患者的管理都是基于用户的管理来实现的。

用户在注册过程中通过手机号码完成注册流程，注册成功后即拥有用户健康通行证，该通行证保证用户在多设备之间切换的安全性。

**B、用户登录**

用户在登录后获得系统下发的请求令牌，该令牌可以确保用户在登陆后操作的基本合法性。

用户在APP内设定手势密码后，当APP进入后台等待，在切换回前台显示的时候强制验证该手势密码。

**C、设备切换**

用户和设备之间的存在绑定关系，这个关系在用户注册和登录时建立。一个用户允许有多台绑定设备，而一个设备只允许绑定一个用户。这里有一个主设备的概念，那就是用户最后使用的设备。一旦用户交替使用设备，系统会提示主设备变更，并向用户确认是否放弃使用前一个设备。综上，设备管理的周期开始于用户注册或登录流程，结束于用户放弃使用该设备。

如果用户发生了设备遗失状况，只需要通过我们的热线电话选择冻结当前账户，然后使用新的手机重新绑定账户。通过上述操作，遗失手机里面的APP账户将不能正常登录。

注：当前安全机制中使用的手机号只能确定用户。设备标识只能识别设备和用户无关。

**D、患者绑定**

用户和患者之间并不是一一对应的，他们是多对多的绑定关系。这个关系在添加患者时建立。系统可以配置一个用户允许添加的患者人数。

在绑定过程中，我们同时校验了患者信息的正确性。

### 系统流程保证

* 1. 用户敏感信息

包括通讯录、短信记录、照片、位置信息等其他SD卡内容，健康云绝对不会私自获取信息，根据必要性系统会提示用户明确知道目前的访问情况，保证得到用户授权。

* 1. 用户诊疗信息

目前经过我们系统的患者数据：患者姓名、手机、身份证、就诊卡号。这些数据可以不在手机、云端上保存，系统架构可以证明。

* 1. 用户登录信息

目前获取的信息包含：手机号、设备标识码、昵称、头像、性别等在个人信息中维护的信息保存于云端，此信息只用于用户登录、支付等必要的身份识别场景，健康云确保用户信息安全。

* 1. 以上所有的患者数据、设备信息传递中都会使用...链路安全，加密算法，令牌，短信验证码等方式进行处理，并且及时销毁。

## DMZ区域安全层面

主要采用以下策略：

1.内网可以访问DMZ

此策略是为了方便内网用户使用和管理DMZ中的服务器。

2.外网不能访问内网

数据不允许外网的用户进行访问，采用防火墙单向访问策略，只允许DMZ区域服务器通过专线访问健康云。

3.DMZ访问内网有限制

很明显，如果违背此策略，则当入侵者攻陷DMZ时，就可以进一步进攻到内网的重要数据。

4.DMZ服务器使用虚拟机方式进行集群管理，有效防止内网系统免于侵害。

# 机房环境

### 应用服务器

|  |  |  |  |
| --- | --- | --- | --- |
| 服务器说明 | 配置要求 | 数目 | 说明 |
| 医院前置机 | 处理器1U 内存4GB RAM 存储300GB | 2 | 集群配置，用于响应用户请求 |
| 缓存服务器 | 处理器1U 内存4GB RAM 存储300GB | 2 | 集群配置，用于缓存数据 |
| 交换机防火墙 | H3C(千兆光纤) | 1 | 提供单向对外数据请求访问 |
| 内网隔离网闸 |  | 1 |  |

其中服务器可以采用虚拟机模式进行使用。

# 运维管理

## 专业技术团队

健康云提供专职的技术研发与支持团队，做到24小时故障解决，通知配备专人维护网络、服务器设备与软件系统，提供7\*24小时电话报修热线。

## 应急预案

### 机房长时间停电应急预案

⑴ 接到长时间停电通知后，应及时通过OA发布或电话通知停电通告，要求用户在停电前停止业务、保存数据。

⑵ 打电话询问供电部门询问停电原因及具体停电时间。

### 通信网络故障应急预案

1. 发生通信网络故障后，计算机操作员应及时将信息告知网络安全领导小组。
2. 网络安全领导小组及时查清通信网络故障位置，或告知相关通信网络运营商，请求协助查清原因。

⑶相关责任人负责写出故障分析报告，上报网络安全领导小组备查。

### 不良信息和网络病毒事件应急预案

⑴ 当发现不良信息或网络病毒时，网络管理员应立即断开网线，终止不良信息或网络病毒传播，并告知信息网络事件应急小组。

⑵ 接到报告后，网络安全领导小组应立即通告局域网内所有计算机用户防病毒方法，隔离网络，指导各计算机操作人员进行杀毒处理，直至网络处于安全状态。

⑶ 对不良信息要进一步追查来源，对未经相关领导同意，擅自发布信息，造成不良影响且触犯法律者，移交执法部门追究法律责任。

### 计算机软件系统故障应急预案

1. 发生计算机软件系统故障后，计算机操作人员立即保存数据，并停止该计算机使用应用。
2. 由部门负责人将情况报告网络安全领导小组，不得擅自进行处理。
3. 网络安全领导小组迅速派出技术人员进行处理，必要情况下，应对硬盘进行备份。
4. 在保持原始数据安全的情况下，对计算机系统进行修复；修复系统成功，则检查数据丢失情况，利用备份数据恢复；若修复失败，立即联系相关厂商请求支援。

### 黑客攻击事件应急预案

⑴ 当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告网络安全领导小组。

⑵ 接到报告后，网络安全领导小组应立即关闭网络，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。

⑶ 及时清理系统、恢复数据、程序，尽力将系统和网络恢复正常。

### 机房设备硬件故障应急预案

⑴ 发生机房设备硬件故障后，网络安全领导小组应立即确定故障设备及故障原因，并进行先期处置。

⑵ 若故障设备在短时间内无法修复，应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

1. 故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关厂商与市局信息中心，并认真填写设备故障报告单备查。