# 1安全保密方案

## 保密措施方案

为做好本项目的保密工作，我公司根据该项目的具体情况结合保密原则进行了预估，特制定了相应的保密方案，在项目的实施过程中将严格按照保密方案做好保密工作。

### 方案目的

为维护项目双方的自身利益，保守国家秘密，工作秘密和商业秘密，依据《中华人民共和国保守国家秘密法》，特预先根据评估制定本保密方案。

### 适用范围

本方案根据客户需求预估制定，暂适用于本次项目。

### 保密措施

（1）对于项目中涉及国家秘密的事项的保密措施。

涉及国家秘密的传递，使用，存储，销毁等流程严格遵守《中华人民共和国保守国家秘密法》和甲方的相关保密规定。严禁非涉密人员和非项目涉密岗位人员接触知悉相关秘密事项，具体措施有以下几点：

涉及国家秘密的事项传递必须通过公司保密办指定的保密员进行传递，不允许通过邮政或快递等非机要渠道传递。

涉及国家秘密的信息处理必须在公司保密机要室内的涉密计算机上进行，由公司保密办进行涉密计算机的管理，严格限定知悉范围和使用范围，知悉人员由公司保密工作领导小组依据秘密事项范围要求确定。

对参与项目的技术研发人员，由公司保密办定期进行技术检查，杜绝泄密。

对相关涉密载体的管理，由公司保密办严格按照《中华人民共和国保守国家秘密法》和甲方的中对涉密载体的管理规定进行管理。项目部涉密人员严禁在保密机要室以外的范围使用涉密载体。

对项目部相关涉密和非涉密人员的保密教育由公司保密办分别以涉密人员每周一次和非涉密人员每周2次的频度进行保密教育。通过教育和谈话掌握相关人员的思想状态，防范可能产生的泄密情况，对思想状态不佳的项目部成员，由公司保密办报公司保密领导小组同意后调离相关岗位。

（2）对于项目中产生的内部秘密的保密措施

凡属于项目部内部秘密，项目部按照相关保密措施，指定专人具体负责落实，严格注意防止外企业或他人以“洽谈业务、开发合作、学习参观”等名义从中获取内部秘密。

涉及内部秘密部门不允许无关人员接触或外界参观，如必须参观的，需经甲方和公司保密办主任审批，由公司保密办负责预先做好保密措施。

内部会议或处理公务提供、发放文件、资料、图纸时，由项目部项目经理审批，统一编写受控号，严格按照文件发放范围登记发放，并向发放对象提出保密要求，事后要指定专人负责收回。

凡向外提供的各类学术交流论文、资料等，涉及到项目内部秘密的，应事先经项目部项目经理和公司保密办审查批准，并做好保密技术处理。

凡属项目内部秘密，但不需存档的文件、资料、图纸、刊物等，均应集中由公司保密办统一监销。

项目部工作人员不得擅自将企业内部秘密事项进行对外报导，不得用公用电话或无线电话谈论内部秘密事项。

### 责任与奖惩

在保守、保护项目说涉及的国家秘密和内部秘密以及改进保密技术措施等方面成绩显著的项目部成员，公司保密领导小组将给予现金和通报奖励。

凡违反规定，泄露国家、内部秘密、不够刑事处罚的，可视情节严重程度给予通报批评、警告等处分。

对有意向外界泄露、出卖内部秘密的人员，将根据危害程度追究经济赔偿或依法起诉。

凡发生泄露涉及国家秘密案件的，将根据《中华人民共和国保守国家秘密法》和《刑法》中有关规定移送国家司法机关依法追究刑事责任。

### 保密管理制度

#### 保密总则

为确保项目的绝对安全，维护本项目参与方的合法利益，保障本项目顺利，促进项目的顺利进展，特制定本管理制度。

本项目关系到各方的权利和利益，依照特定的程序确定，在一定时间内只限一定范围人员知悉的事项。

本项目现场所有人员都有保守项目秘密之义务。

对保守、保护秘密及改进保密技术、措施等方面成绩显著的现场人员实施奖励。

本制度由涉密项目部负责维护。

#### 保密等级划分

保密等级可分为“绝密”、“机密”、“秘密”三级。

本项目中的等级设定应由甲方在项目开工前确认。

按之前的项目经验，可临时按如下进行划分：

项目维护中，直接影响采购人权益的重要文件资料为绝密：

项目的规划、图纸设计、技术参数、统计资料、重要会议纪要等视为机密级。

项目档案资料、合同、协议等为秘密级。

#### 保密守则

全体人员均自觉地遵守下列保密守则：

不该说的项目涉密资料，绝对不说；

不该问的项目涉密资料，绝对不问；

不该看的项目涉密资料，绝对不看；

不该记录的项目涉密资料，绝对不记录；

不在私人通信中涉及项目涉密资料；

不在公共场所和家属、子女、亲友面前谈论项目相关资料；

不在不利于保密的地方存放涉密文件、资料；

不携带涉密材料游览、参观、探亲、访友和出入公共场所；

不将内部文件、资料、刊物作废纸出售；

不得擅自翻印、复印、全抄、录音秘密以上文件、资料、刊物；

不得因工作便利调取、泄露项目相关监控点视频内容。

档案室管理制度：

档案室应当设在有利于安全保密的地方，安装各项保密设施。

项目涉密文件、资料，由档案室的管理人员负责收发。

对发出、收进的涉密文件、资料，应当逐件进行登记、编号、办好收发手续。

传递涉密文件、资料，应当按照资料规定的阅读范围阅，不得擅自扩大传阅范围。

对涉密文件、资料，应当定期清查、清退，定期进行清查、清退一次。

#### 保密制度

本项目工作人员经常性接触项目机密材料，必须以身作则，模范遵守各项保密法规和制度。

严格执行文件管理制度。坚持在办公室阅办秘密文、电资料，特殊情况需在家阅办时，应采取必要的安全保密措施，阅办后及时向档案室清退。

禁止携带秘密文件、资料出入公共场所。

严禁擅自决定复制秘密文件、资料，确需复制时，应履行审批手续。涉及项目机密及其它党和国家机密，经本项目相关管理人员同意，可以翻印；其它秘密文件、资料的复制，必须征求发文机关同意。

召开重要和有保密内容的会议，要采取安全防范措施，并对与会人员进行保密教育。

用户的办公室、机要室、档案室、文印室、收发室等属办公重点保密场所，未经许可，外来人员不准擅自入内。

禁止在无保密措施的有线、无线通信中传递本项目秘密；不准通过普通邮政传递秘密文件、资料。

严禁在公共场所和家属及其他无关人员面前谈论项目机密。

全体员工应当做到不该说的不说，不该问的不问，不该看的不看，不该听的不听，不该记的不记。相互监督，共同负责，逐步实现保密工作经常化、制度化、规范化。

发现项目秘密、公司秘密已经泄露或者可能泄露时，应当立即采取补救措施，并迅速报告有关部门及时处理。

文件的管理规定：

文件一律由指定保管人签收、拆封、登记、清点。

文件只能在办公室阅读，不准外带。确因工作需要必须把文件带出时，须经领导批准，办理借阅手续，用后及时退还。借阅人不准把文件转借他人。

文件要由保密员专人保管，存放文件要有专柜、专室。不准将文件放置在无专人管理、无严密加锁的箱柜内。下班时不准将文件放在办公桌上。发现下落不明(丢失)文件要及时报告，并认真查找、处理。

#### 现场保密措施

项目维护人员务必增强保密意识，不该问的不问，不该说的不说，不该看的不看。每天开工和收工时，对现场维护人员进行安全检查，防止摄像器材进入现场。

秘密文件、资料和其他物品的制作、收发、传递、使用、复制、摘抄保存和销毁，由现场项目经理或委托专人执行。

对于密级文件、资料或其他物品，采取如下保密措施：

不经现场项目经理签批，不得复制和摘抄。

收发、传递和外出携带由指定人担任，并采取必要的安全措施。

所有资料在设备完善的保险装置中保存。

在对外交往合作中，需要提供保密事项的要事先报请现场项目经理签批。

项目维护过程中属于保密内容的会议，要选择具备保密措施的场所，限定参会人员的范围，依据保密规定使用会议设备和管理会议文件，确定会议是否传达及传达范围。

现场实维护作人员发现秘密泄露或者可能泄露时，要采取补救措施并及时报现场项目经理，项目经理要及时做出处理。

计算机信息系统使用管理规定：

不得在与网络联网的计算机信息系统中存储、处理、传递项目秘密信息。任何人不得在公众网上发布、存储、处理、传递、转发、抄送涉及项目秘密信息。

对秘密数据、资料载体如：磁盘、磁带、光盘等视同“三密”文件，履行借阅、使用、复制、传递、携带、移交、保存、销毁等登记手续。

存储过项目秘密信息的计算机媒体(包括软盘和硬盘)不能降低密级使用，维修时应保证所存储的项目秘密信息不被泄露，不再使用的应及时销毁。

#### 涉密人员的培训管理

保密办公室负责保密法规知识的宣传教育工作。要充分利用邮件、公告、板报宣传保密法规普及保密知识，提高全体员工的保密意识。

保密宣传教育工作，由公司保密办负责计划、安排，并组织实施。保密办小组每年至少安排一次对全体涉密人员的保密宣传教育，一年至少安排两次涉密人员培训，使涉密人员熟悉基本的保密法规，知悉其必须承担的保密责任和义务以及应当享有的权利。

新调入或新任用涉密岗位人员，必须先由人事行政部负责进行保密制度培训并考试合格后方可上岗工作。各部门负责人有责任教育调离涉密岗位的人员离岗后自觉遵守保密纪律，承担保密义务，不泄露本项目秘密。

保密办公室负责对因公、因私调离本项目岗位的涉密人员进行保密教育，使其了解保密范围，明确保密责任，掌握处理保密问题的方法。

保密培训工作由保密办公室拟定《年度培训计划》，纳入部门职工培训教育计划，由人事行政部负责组织，保密办公室参与实施，培训人员按规定在《培训签到表》签到。

#### 保密协议的签订

所有参与本项目的项目组成员树立保密意识，遵守保密规定，与采购人签订保密协议，因利用工作便利调取、泄露视频内容的，按国家相关法律处理，承担相应的法律责任。

我方保证对在讨论、签订、执行本协议过程中所获悉的属于对方的且无法自公开渠道获得的文件及资料（包括机构秘密、单位计划、技术信息、采购信息及其他秘密）予以保密。未经该资料和文件的原提供方同意，另一方不得向任何第三方泄露该秘密的全部或部分内容。但法律、法规另有规定或双方另有约定的除外。

具备以下主要条款：

保密的内容和范围；

保密合同双方的权利和义务；

保密协议的期限；

违约责任。

在保密合同有效期限内，员工应履行下列义务：

严格遵守本项目保密制度，防止泄漏项目秘密；

不得向他人泄漏项目秘密；

非经书面同意，不得利用该项目秘密进行生产与经营活动，不得利用项目秘密进行新的研究和开发。

## 安全架构设计

### 安全设计目标

安全设计总体目标是：结合安全保护要求，通过安全技术体系、安全管理体系和安全服务体系建设，在平台形成有效的安全防护能力、隐患发现能力、应急响应能力和系统恢复能力，为各级单位信息系统的运行提供安全保障，化担忧为行动，保证业务系统长期安全、稳定和高效运行，并能够不断完善和发展，实现以安全保应用，用安全促应用，以适应不断扩展的业务应用和管理需求。

根据国家信息安要求，建设完善安全体系，满足物理、网络、主机/虚拟化、数据、应用等安全技术和安全管理的需要，并达到以下具体目标：

1.通过安全规划和安全实施后，安全体系能够达到国家相关安全保障要求。

2.拥有一个支持各类安全服务，如访问控制、身份认证等的安全基础设施，保证网络系统和应用系统中各种安全服务实现能够获得有效支持，同时为今后使用新的安全措施或加强和完善原有安全措施提供扎实的基础。

3.平台对外边界出口清晰明确，配置的网络边界防护设备给予系统内部有效的保护，可以防止和抵抗来自外部对信息系统的攻击。

4.网络结构合理，根据实际业务的重要性有效地划分出级别不同的安全区域，安全区域之间的访问控制措施能有效地防止非授权访问现象以及防御外部可能的攻击行为。

### 安全设计原则

根据国家信息安全保障政策法规和技术标准要求，同时参照相关行业规定，综合考虑可实施性、可管理性、可扩展性、综合完备性、系统均衡性等方面。

#### 符合信息安全法规要求

安全保障体系遵从信息安要求，从产品、解决方案、咨询服务等方面打造可靠、高效、稳定的安全环境，确保业务的连续性和机密性。

#### 分域防护、综合防范原则

任何安全措施都不是绝对安全的，都可能被攻破。为预防攻破一层或一类保护的攻击行为无法破坏整个信息系统，需要合理划分安全域和综合采用多种有效措施，进行多层和多重保护。

#### 需求、风险、代价平衡原则

对任何类型网络，绝对安全难以达到，也不一定是必须的，需正确处理需求、风险与代价的关系，等级保护，适度防护，做到安全性与可用性相容，做到技术上可实现，经济上可执行。

#### 数据安全为核心原则

由于的核心业务数据涉及到个人信息、资金数据等，这些数据对于安全性较高，需要确保数据不被泄露、损坏、篡改或丢失，同时需要确保数据的完整性。

#### 技术与管理相结合原则

信息安全涉及人、技术、操作等各方面要素，单靠技术或单靠管理都不可能实现。因此在考虑信息系统信息安全时，必须将各种安全技术与运行管理机制、人员思想教育、技术培训、安全规章制度建设相结合。

#### 动态发展和可扩展原则

随着网络攻防技术的进一步发展，安全需求会不断变化，以及环境、条件、时间的限制，安全防护一步到位，一劳永逸地解决信息安全问题是不现实的。信息安全保障建设可先保证基本的、必须的安全性和良好的安全可扩展性，今后随着应用和网络安全技术的发展，不断调整安全策略，加强安全防护力度，以适应新的网络安全环境，满足新的信息安全需求。

### 安全技术方案设计

#### 安全技术体系框架

从物理安全、网络安全、主机安全、虚拟化安全、应用安全、数据安全等6个方面，对本项目的安全技术体系进行了分析，并在此基础上，对云平台的安全技术环境提出了建设性建议。

#### 物理安全

具体的物理安全防护措施有：

1. 所在建筑物具备防震、防雷、防风、防雨和防水等能力；

2. 安装并加强门禁系统、监视系统、接地及防雷设备等建设；

3. 设置有火灾报警系统及灭火设备，并定期检查消防安全隐患；

4. 采用双电源线路供电。

5. 有必要的空调和湿度调节设备，机房温、湿度能够满足设备正常运行需求；

6. 对进入来访人员经过申请和审批流程，限制和监控其活动范围，严格操作登记制度并妥善保存以备查等。

#### 网络安全

##### 边界访问控制

区域边界访问控制的主要任务是保证网络资源不被非法使用和非授权访问。网络访问控制策略是建立在安全域划分的基础上实现的。

由于同一安全域内保护对象拥有相同的访问控制策略，可以认为同一安全域之内是相互信任的，而安全风险主要是来自与安全域之间相互访问所带来的，因此，对于安全域的防护主要是对安全域边界的安全防护。

##### 网络入侵检测

在各区域边界，防火墙起到了协议过滤的主要作用，根据安全策略在偏重在网络层判断数据包的合法流动。但面对越来越广泛的基于应用层内容的攻击行为，防火墙并不擅长处理应用层数据。

入侵防护/检测系统（IPS/IDS）需要通过先进的硬件架构、软件架构和处理引擎对处理能力进行充分保证。

实时监测网络入侵行为，并将入侵行为跟踪分析，本方案通过采用基于网络的入侵检测系统，来实现来针对于服务器的恶意或非法的访问请求的探测。

##### 网络入侵防护

各安全域边界部署防火墙除具有区域边界访问控制功能外，还可进行网络入侵防护，提供主动的、实时的防护，其目标旨在准确监测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是简单地在监测到恶意流量的同时或之后才发出告警，第一时间将安全威胁阻隔在网络外部。

##### 网络流量控制

网络流量控制是利用软件方式来实现对网络数据流量进行控制的一种措施。从而优化带宽管理、管控网络应用、防范信息泄露、过滤不良信息、提升上网安全。

##### 网络分流管理

采集网链路流量进行复制、汇聚、分流、过滤等方式自由导向输出，以满足各类流量监控设备的部署需求。

##### 网络结构安全

1.网络设备冗余：接入到中环骨干网的交换机采用双机互备模式，规避单点故障风险，保障网络服务的连续性；

2.防火墙冗余：所有计算环境边界的防火墙采用双机冗余方式，规避单点故障风险，加强访问控制的持续性保护；

3.服务器冗余：所有计算环境内的关键应用系统采用主机冗余备份机制，规避单点故障，提高业务连续性。

4.根据安全域划分原则，将建设项目局域网划分为多个VLAN，其中：服务器VLAN，客户端VLAN，管理域VLAN等等。

5.使用ACL技术控制VLAN间的通信

##### 异常流量管理

通过在网络平台中互联网出口区安全边界最外侧部署异常流量管理系统，实时的发现并阻断异常流量，为正常的互联网访问请求提供高可靠环境。异常流量管理系统部署在互联网服务区安全边界最外层，直接面向互联网，阻断来自互联网的攻击，阻断病毒的自动探测和传播。

异常流量系统必须具备智能的流量分析能力、特征识别能力，具备大流量入侵时足够的性能处理能力。异常流量系统之后部署的即是边界防火墙设备。

##### 网络设备防护

为提高网络设备的自身安全性，保障各种网络应用的正常运行，对网络设备需要进行密码、漏洞等加固措施。

#### 数据安全

##### 数据传输安全

数据在传输过程中可能遇到被中断、复制、篡改、伪造、窃听和监视等威胁，为保障信息在网络传输过程的完整性、保密性和可用性，可通过IPSec的方式。

##### 数据访问控制

用户和虚拟机镜像间的权限控制；用户挂接卷进行权限确认；对象存储（OBS）用户对象的访问控制对数据访问的安全防护。

##### 用户数据隔离

通过虚拟化层实现虚拟机间存储访问隔离，严格隔离用户数据。

##### 剩余信息保护

存储资源重分配给VM之前进行完整的数据擦除

存储的用户文件/对象删除后，对应的存储区进行完整的数据擦除或标识为只写（只能被新的数据覆写），保证不被非法恢复

##### 数据备份与恢复

依托机房的集中数据存储和备份存储实业务系统的本地数据存储、备份与恢复。

### 安全管理方案设计

信息安全管理制度是信息安全领域各种规则的制度化的体现，在信息化相关活动中起着统一目标、规范流程、保障信息安全实施效果的重要作用。通过对信息安全制度规范的决策，首先从高层确保信息安全工作“有法可依”，推动信息安全制度建设工作，营造一个积极的信息安全控制环境。

#### 安全管理制度

参考国家信息安全等级保护标准要求，结合系统实际管理需要，建立行之有效的安全管理制度。

##### 管理制度

本项内容包括：

制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

对安全管理活动中的各类管理内容建立安全管理制度；

对要求管理人员或操作人员执行的日常管理操作建立操作规程；

形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

##### 制定和发布

本项内容包括：

应指定或授权专门的部门或人员负责安全管理制度的制定；

安全管理制度具有统一的格式，并进行版本控制；

组织相关人员对制定的安全管理制度进行论证和审定；

安全管理制度通过正式、有效的方式发布；

安全管理制度注明发布范围，并对收发文进行登记。

##### 评审和修订

本项内容包括：

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检查和审定，对存在不足或需要改进的安全管理制度进行修订。

#### 安全管理机构

信息安全管理机构是确保信息安全决策落实、支持信息安全工作开展的基础。信息安全等级保护建设过程中，安全管理制度规范的建立、日常安全管理、具体控制措施的贯彻执行以及对安全管理方针贯彻落实情况的监督等工作的开展都需要一个完善有效的信息安全组织架构来支撑。安全管理机构建设的目的主要是通过构建和完善信息安全组织架构，明确不同安全组织、不同安全角色的定位、职责以及相互关系，强化信息安全的专业化管理，实现对安全风险的有效控制。

#### 人员安全管理

对于系统工作的内部人员和到访的外部人员，涉及了人力资源管理，按照等级保护基本要求对人员安全管理的要求，在这部分规范和管理制定过程中，要结合人力资源管理的实际制度、规定和流程，以保证人员管理的可操作性。

#### 系统建设管理

对于在建、拟建的信息系统，应遵循等级保护系统建设管理要求，对于从系统初始立项开始，就应该严格按照系统定级、系统备案、安全方案设计、产品采购和使用、自行软件开发、外包开发、工程实施、测试验收、系统交付、等级测评等各个环节和流程进行管理，确定相应的安全服务商，并制定相应的管理制度和规定。

#### 系统运维管理

对于已运行的所有信息系统，遵循等级保护系统建设管理基本要求，对于系统运行的环境、资产、介质、设备、网络安全、系统安全、恶意代码防范、密码、变更、备份与恢复、安全事件处置、应急预案进行管理，并制定相应的管理制度和规定。

在安全管理区通过部署安全管理平台，实现对物理设备和云计算设备的监控、管理，统一通过安全管理平台实现全网的日志收集、分析、整合，并实现统一安全策略的下发和管理。

## 系统信息安全设计

本安全方案的目标是支撑和保障智慧教室系统和业务的安全稳定运行，防止信息网络瘫痪、防止应用系统破坏、防止业务数据丢失、防止卫监信息泄密、防止终端病毒感染、防止有害信息传播、防止恶意渗透攻击，以确保信息系统安全稳定运行，确保业务数据安全。

### 信息安全体系结构

#### 安全参考标准

《信息安全等级保护管理办法》和《信息安全技术——终端计算机系统安全等级要求》（GA/T 671-2006）、

《信息技术——系统安全工程——能力成熟度模型》（GB/T 20261-2006）、

《信息安全技术——信息系统安全管理要求》（GB/T 20269-2006）、

《信息安全技术——网络基础安全技术要求》（GB/T 20270-2006）、

《信息安全技术——信息系统通用安全技术要求》（GB/T 20271-2006）、

《信息安全技术——操作系统安全技术要求》（GB/T 20272-2006）、

《信息安全技术——数据库管理系统安全技术要求》（GB/T 20273-2006）、

《信息安全技术——信息系统安全工程管理要求》（GB/T 20282-2006）等信息安全技术相关标准。

#### 安全建设内容

本项目的安全和保密体系主要从物理安全保密、网络安全保密、系统安全保密、应用安全保密和信息安全保密等方面综合考虑，达到安全等保三级标准。



信息安全体系结构

##### 物理级安全

最底层的是物理级安全，其包括计算机安全，硬件安全等

物理安全是网络安全基础平台的一部分，物理安全是对计算机网络设备、设施及相关的数据存储介质提供的安全保护，使其免受各类自然灾害（地震、水灾、火灾等）以及人为操作失误或错误甚至计算机犯罪行为的破坏。物理安全防范是系统整体安全架构的基础，对系统的正常运行具有重要的作用。物理级安全主要包括环境安全、设备安全及存储介质安全等。

##### 网络级安全

第二层是网络级安全，主要包括链路冗余，防火墙等

现有网络是一个开放的系统，连接不同的节点和接入单位，这些不同的网络属于不同的安全域。网络安全需要考虑的是来自不可信任网段的攻击或网络错误导致对本网段的安全造成安全风险。

针对网络安全采用的具体安全措施主要有网络防火墙、安全准入、网络入侵检测、网络流量监控及网络漏洞扫描等。

##### 系统级安全

第三层是系统级安全包括数据灾备，病毒防范等

系统级的安全主要是从操作系统的角度考虑系统安全措施，防止不法分子利用操作系统的一些BUG、后门取得对系统的非法操作权限。系统级安全管理的主要内容包括：

（1）主机设备使用安全：配置操作系统，使其达到尽可能高的安全级别。

（2）系统安全扫描：及时检测、发现操作系统存在的安全漏洞，对发现的操作系统安全漏洞做出及时、正确的处理。

（3）病毒防杀。

##### 应用级安全

第四层是应用级安全包括统一身份认证，统一权限管理等，贯穿整个体系的是安全管理制度和安全标准，以实现非法用户进不来，无权用户看不到，重要内容改不了，数据操作赖不掉。在信息系统应用中要重点加强应用安全管理，包括统一身份认证、采用PKI加密、数字签名、隐私与权限管理等。

应用安全体系以密码技术为基础，建立一个应用级的安全平台，针对系统内各类具体的应用系统统一提供相应的应用级安全保护，包括数据资源的保护和应用系统处理过程的保护。应用级安全主要包括应用系统安全、主页防篡改、传输加密、数据库安全机制、单点登录、访问控制、用户管理、统一授权及应用审计等措施。

##### 管理级安全

构建完善的系统监控体系，实现对网络、应用系统的实时监控，检测系统安全漏洞。系统监控内容包括：

（1）网络监控：监控重要网络设备如路由器、交换机的硬件运行状态，线路的连通状况，主要关心的是设备整机以及模块是否能够正常工作。

（2）应用监控：对于主要业务应用服务的可用性监控，监控主要的性能参数。

另外制定网络信息安全管理规范，并在此基础上制订具体的信息安全管理制度，对各部门的安全管理工作做出指导，以明确权责，加强实施，从而提高电子政务系统的总体安全水平，相关安全管理制度可包括以下内容：

（1）场地与设施安全管理制度

根据国家安全生产与保卫的要求，并参照国家《计算机场地安全要求》、《计算机场地技术条件》和ISO17799等标准，对系统的网络设备与设施进行安全等级划分，并分别采取相应的安全防护措施，执行相应的安全保卫管理办法。

（2）人员安全管理制度

应制订人员安全管理制度，或在有关的人员管理制度中明确与信息安全有关的规定，主要包括关键岗位人选、人员考核、人员调离、人员培训等几方面的内容。

（3）设备安全管理制度

设备安全管理制度应对设备在选型、购置、使用、维护和定期保养、仓储管理过程中涉及到的安全问题进行规定。

（4）软件安全管理制度

应用软件安全管理制度的管理范围包括操作系统、应用软件、数据库、安全软件和工具软件等。软件安全管理制度对软件在采购、安装、使用、升级、更新、维护等过程中涉及的安全问题进行规定。

（5）网络安全管理制度

网络安全管理制度应对网络方案设计和网络运行管理过程中涉及的安全问题进行规定。

（6）技术文档安全管理制度

应制定技术文档的管理制度，对文档的登记、借用、复制、销毁等做出明确规定。

（7）应急管理制度

为保证关键业务在灾难发生的情况下仍然维持运转，应制定网络系统的应急管理制度，根据可能出现的紧急情况制定相应的应急计划，并对应急事件的处理、应急计划的实施条件、应急计划人员的管理等做出规定。

（8）审计管理制度

制订审计管理制度，对系统网络设备、主机系统和安全措施的日常运行日志数据进行审查、分析，为处理安全隐患和发生的安全事件提供依据。审计管理制度应对审计内容、日志分析、报警及处理措施等方面做出规定。

#### 安全体系设计依据

##### 国家等保三级建设

（1）三级安全保护能力定义

应具有能够对抗来自大型的、有组织的团体（如一个商业情报组织或犯罪组织等），拥有较为丰富资源（包括人员能力、计算能力等）的威胁源发起的恶意攻击、较为严重的自然灾难（灾难发生的强度较大、持续时间较长、覆盖范围较广（地区性）等）以及其他相当危害程度（内部人员的恶意威胁、设备的较严重故障等）威胁的能力，并在威胁发生后，能够较快恢复绝大部分功能。

（2）具体要求

O3-1. 应具有对抗中等强度地震、台风等自然灾难造成破坏的能力

O3-2. 应具有防止雷击事件导致大面积设备被破坏的能力

O3-3. 应具有防水和防潮的能力

O3-4. 应具有对水患检测和报警的能力

O3-5. 应具有自动灭火的能力

O3-6. 应具有检测火灾和报警的能力

O3-7. 应具有防止火灾蔓延的能力

O3-8. 应具有温湿度自动检测和控制的能力

O3-9. 应具有防止电压波动的能力

O3-10. 应具有对抗较长时间断电的能力

O3-11. 应具有防止静电导致大面积设备被破坏的能力

O3-12. 应具有对重要设备和介质进行电磁屏蔽的能力

O3-13. 应具有防止强电磁场、强震动源和强噪声源等污染影响系统正常运行的能力

O3-14. 应具有监测通信线路传输状况的能力

O3-15. 应具有及时恢复正常通信的能力

O3-16. 应具有对传输和存储数据进行完整性检测和纠错的能力

O3-17. 应具有系统软件、应用软件容错的能力

O3-18. 应具有软件故障分析的能力

O3-19. 应具有软件状态监测和报警的能力

O3-20. 应具有自动保护当前工作状态的能力

O3-21. 应具有合理使用和控制系统资源的能力

O3-22. 应具有按优先级自动分配系统资源的能力

O3-23. 应具有对软件缺陷进行检查的能力

O3-24. 应具有记录用户操作行为和分析记录结果的能力

O3-25. 应具有对用户的误操作行为进行检测、报警和恢复的能力

O3-26. 应具有严格控制机房进出的能力

O3-27. 应具有防止设备、介质等丢失的能力

O3-28. 应具有严格控制机房内人员活动的能力

O3-29. 应具有实时监控机房内部活动的能力

O3-30. 应具有对物理入侵事件进行报警的能力

O3-31. 应具有控制接触重要设备、介质的能力

O3-32. 应具有对通信线路进行物理保护的能力

O3-33. 应具有使重要通信线路及时恢复的能力

O3-34. 应具有限制网络、操作系统和应用系统资源使用的能力

O3-35. 应具有合理分配、控制网络、操作系统和应用系统资源的能力

O3-36. 应具有能够检测、分析、响应对网络和重要主机的各种攻击的能力

O3-37. 应具有发现所有已知漏洞并及时修补的能力

O3-38. 应具有对网络、系统和应用的访问进行严格控制的能力

O3-39. 应具有对数据、文件或其他资源的访问进行严格控制的能力

O3-40. 应具有对资源访问的行为进行记录、分析并响应的能力

O3-41. 应具有对恶意代码的检测、阻止和清除能力

O3-42. 应具有防止恶意代码等在网络中扩散的能力

O3-43. 应具有对恶意代码库和搜索引擎及时更新的能力

O3-44. 应具有保证鉴别数据传输和存储保密性的能力

O3-45. 应具有对用户进行唯一标识的能力

O3-46. 应具有对同一个用户产生多重鉴别信息并进行多重鉴别的能力

O3-47. 应具有对硬件设备进行唯一标识的能力

O3-48. 应具有对硬件设备进行合法身份确定的能力

O3-49. 应具有检测非法接入设备的能力

O3-50. 应具有对存储介质中的残余信息进行删除的能力

O3-51. 应具有对传输和存储中的信息进行保密性保护的能力

O3-52. 应具有防止加密数据被破解的能力

O3-53. 应具有路由选择和控制的能力

O3-54. 应具有信息源发的鉴别能力

O3-55. 应具有通信数据完整性检测和纠错能力

O3-56. 应具有对关键区域进行电磁屏蔽的能力

O3-57. 应具有持续非活动状态一段时间后自动切断连接的能力

O3-58. 应具有基于密码技术的抗抵赖能力

O3-59. 应具有防止未授权下载、拷贝软件或者文件的能力

O3-60. 应具有网络边界完整性检测能力

O3-61. 应具有切断非法连接的能力

O3-62. 应具有重要数据和程序进行完整性检测和纠错能力

O3-63. 应具有对敏感信息进行标识的能力

O3-64. 应具有对敏感信息的流向进行控制的能力

O3-65. 应具有及时恢复重要数据的能力

O3-66. 应具有保证重要业务系统及时恢复运行的能力

##### 安全管理规范化

为了避免网络、应用系统和数据资源遭受来自系统内外各类主动或被动式的攻击，保障各级系统稳定、有效地运行，本项目建设中必须建立完善的安全保密保障体系。具体内容主要包括：信息系统安全等级保护通用技术规范、信息系统安全管理规范、信息系统网络安全规范、数据库系统安全使用技术规范、操作系统安全使用技术规范、访问控制管理规范等。

信息安全标准体系中重点建设的标准具体包括：

（1）信息系统安全等级保护通用技术规范

我国已围绕《计算机信息系统安全保护等级划分准则》（GB 17859-1999）制定了一系列信息安全等级保护标准，为使本项目的安全建设符合国家信息安全等级保护工作要求，需制定适用于信息系统的通用技术规范。

（2）信息系统安全管理规范

信息安全等级保护标准体系，从与信息系统安全相关的管理层面、物理层面、网络层面、系统层面、应用层面对信息系统的运行和资源实施保护。包括：信息系统网络安全技术规范、操作系统安全使用技术规范、数据库系统安全使用技术规范。

（3）安全管理制度规范

按照平台实现的应用流程以及机构的设置，严格划分所有用户的角色，并据此设定不同的权限，确保用户只能访问权限许可范围内的资源。

制定各项访问控制措施，包括对网络、主机、数据库等的访问。对所有路由器、交换机的密码及配置应由网络管理员掌握，统一进行配置；对各类主机的管理和对用户以及文件系统的分配、访问权限设置等工作统一由主机管理员执行；对所有数据库的管理和对表、视图、记录和域的授权工作统一由数据库管理员执行。

禁止在生产系统中使用未经批准的应用程序，禁止在生产系统上加载无关软件，严禁擅自修改系统的有关参数。

用于开发、测试的系统必须与生产系统严格分开。

监视系统运行记录，及时审查日志文件，认真分析告警信息，及时掌握运行状况，对系统可能发生的故障做好应急方案。

软件程序的修改或增加功能时，须提出修改理由、方案、实施时间，报上级主管部门批准；程序修改后，须在测试系统上进行调试，确认无误经批准后方可投入生产应用。

软件修改、升级前后的程序版本须存档备查，软件修改、升级时须有应急补救方案。

### 系统安全设计原则

 在进行等级保护系统解决方案设计时将遵循以下设计原则：

 清晰定义模型的原则：在设计信息安全保障体系时，首先要对信息系统进行模型抽象，这样既能相对准确地描述信息体系的各个方面的内容及其安全现状，又能代表绝大多数地区和各种类型的信息系统。把信息系统各个内容属性中与安全相关的属性抽取出来，参照IATF（美国信息安全保障技术框架），建立“保护对象框架”、“安全措施框架”、“整体保障框架”等安全框架模型，从而相对准确地描述信息系统的安全属性和等级保护的逻辑思维。

分域防护、综合防范的原则：任何安全措施都不是绝对安全的，都可能被攻破。为预防攻破一层或一类保护的攻击行为无法破坏整个信息系统，需要合理划分安全域和综合采用多种有效措施，进行多层和多重保护。

需求、风险、代价平衡的原则：对任何类型网络，绝对安全难以达到，也不一定是必须的，需正确处理需求、风险与代价的关系，等级保护，适度防护，做到安全性与可用性相容，做到技术上可实现，经济上可执行。

技术与管理相结合原则：信息安全涉及人、技术、操作等各方面要素，单靠技术或单靠管理都不可能实现。因此在考虑信息系统信息安全时，必须将各种安全技术与运行管理机制、人员思想教育、技术培训、安全规章制度建设相结合。

动态发展和可扩展原则：随着网络攻防技术的进一步发展，网络安全需求会不断变化，以及环境、条件、时间的限制，安全防护一步到位，一劳永逸地解决信息安全问题是不现实的。信息安全保障建设可先保证基本的、必须的安全性和良好的安全可扩展性，今后随着应用和网络安全技术的发展，不断调整安全策略，加强安全防护力度，以适应新的网络安全环境，满足新的信息安全需求。



图 1 系统安全保护对象框架

### 系统安全设计思路

#### 保护对象框架

 保护对象是对信息系统从安全角度抽象后的描述方法，是信息系统内具有相似安全保护需求的一组信息资产的组合。

依据信息系统的功能特性、安全价值以及面临威胁的相似性，信息系统保护对象可分为计算区域、区域边界、网络基础设施、安全措施四类。具体内容略。

建立了各层的保护对象之后，应按照保护对象所属信息系统或子系统的安全等级，对每一个保护对象明确保护要求、部署适用的保护措施。

#### 整体保障框架

就安全保障技术而言，在体系框架层次进行有效的组织，理清保护范围、保护等级和安全措施的关系，建立合理的整体框架结构，是对制定具体等级保护方案的重要指导。
 根据中办发[2003]27号文件，“坚持积极防御、综合防范的方针，全面提高提高信息安全防护能力”是国家信息保障工作的总体要求之一。“积极防御、综合防范” 是指导等级保护整体保障的战略方针。



图 2 信息安全整体保障框架

信息安全保障涉及技术和管理两个相互紧密关联的要素。信息安全不仅仅取决于信息安全技术，技术只是一个基础，安全管理是使安全技术有效发挥作用，从而达到安全保障目标的重要保证。

安全保障不是单个环节、单一层面上问题的解决，必须是全方位地、多层次地从技术、管理等方面进行全面的安全设计和建设，积极防御、综合防范”战略要求信息系统整体保障综合采用覆盖安全保障各个环节的防护、检测、响应和恢复等多种安全措施和手段，对系统进行动态的、综合的保护，在攻击者成功地破坏了某个保护措施的情况下，其它保护措施仍然能够有效地对系统进行保护，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。

整体保障框架的建设应在国家和地方、行业相关的安全政策、法规、标准、要求的指导下，制订可具体操作的安全策略，并在充分利用信息安全基础设施的基础上，构建信息系统的安全技术体系、安全管理体系，形成集防护、检测、响应、恢复于一体的安全保障体系，从而实现物理安全、网络安全、系统安全、数据安全、应用安全和管理安全，以满足信息系统全方位的安全保护需求。同时，由于安全的动态性，还需要建立安全风险评估机制，在安全风险评估的基础上，调整和完善安全策略，改进安全措施，以适应新的安全需求，满足安全等级保护的要求，保证长期、稳定、可靠运行。

#### 安全措施框架

安全措施框架是按照结构化原理描述的安全措施的组合。本方案的安全措施框架是依据“积极防御、综合防范”的方针，以及“管理与技术并重”的原则进行设计的。

安全措施框架包括安全技术措施、安全管理措施两大部分。安全技术措施包括安全防护系统（物理防护、边界防护、监控检测、安全审计和应急恢复等子系统）和安全支撑系统（安全运营平台、网络管理系统和网络信任系统）。

安全技术措施、安全管理措施各部分之间的关系是人（安全机构和人员），按照规则（安全管理制度），使用技术工具（安全技术）进行操作（系统建设和系统运维）。

#### 安全区域划分

不同的信息系统的业务特性、安全需求和等级、使用的对象、面对的威胁和风险各不相同。如何保证系统的安全性是一个巨大的挑战，对信息系统划分安全区域，进行层次化、有重点的保护是有保证系统和信息安全的有效手段。

按数据分类分区域分等级保护，就是按数据分类进行分级，按数据分布进行区域划分，根据区域中数据的分类确定该区域的安全风险等级。目的是把一个大规模复杂系统的安全问题，分解为更小区域的安全保护问题。这是实现大规模复杂信息的系统安全等级保护的有效方法。



图 3 安全措施框架

随着安全区域方法的发展，发现力图用一种大一统的方法和结构去描述一个复杂的网络环境是非常困难的，即使描述出来其可操作性也值得怀疑。因此，提出了“同构性简化的方法”，其基本思路是认为一个复杂的网络应当是由一些相通的网络结构元所组成，这些网络结构元进行拼接、递归等方式构造出一个大的网络。可以说，结构性简化好像将网络分析成一种单一大分子组成的系统，而同构性简化就是将网络看成一个由几种小分子组成的系统。“3+1同构性简化”的安全域方法就是一个非常典型的例子，此方法是用一种3+1小分子构造来分析网络系统。（注：除了3+1构造之外，还存在其他形式的构造。）具体来说信息系统按照其维护的数据类可以分为安全服务域、安全接入域、安全互联域以及安全管理域四类。在此基础上确定不同区域的信息系统安全保护等级。同一区域内的资产实施统一的保护，如进出信息保护机制，访问控制，物理安全特性等。

信息系统可以划分为以下四个大的安全域（3+1同构法）：

安全接入域：由访问同类数据的用户终端构成安全接入域，安全接入域的划分应以用户所能访问的安全服务域中的数据类和用户计算机所处的物理位置来确定。安全接入域的安全等级与其所能访问的安全服务域的安全等级有关。当一个安全接入域中的终端能访问多个安全服务域时，该安全接入域的安全等级应与这些安全服务域的最高安全等级相同。安全接入域应有明确的边界，以便于进行保护。

安全互联域：连接传输共同数据的安全服务域和安全接入域组成的互联基础设施构成了安全互联域。主要包括其他域之间的互连设备，域间的边界、域与外界的接口都在此域。安全互联域的安全等级的确定与网络所连接的安全接入域和安全服务域的安全等级有关。

安全服务域：在局域范围内存储，传输、处理同类数据，具有相同安全等级保护的单一计算机（主机/服务器）或多个计算机组成了安全服务域，不同数据在计算机的上分布情况，是确定安全服务域的基本依据。根据数据分布，可以有以下安全服务域：单一计算机单一安全级别服务域，多计算机单一安全级别服务域，单一计算机多安全级别综合服务域，多计算机多安全级别综合服务域。



图 4 信息系统安全措施选择

安全管理域：安全系统的监控管理平台都放置在这个区域，为整个IT架构提供集中的安全服务，进行集中的安全管理和监控以及响应。具体来说可能包括如下内容：病毒监控中心、认证中心、安全运营中心等。

#### 安全措施选择

 27号文件指出，实行信息安全等级保护时“要重视信息安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理”。由此可见，信息系统等级保护可视为一个有参照系的风险管理过程。等级保护是以等级化的保护对象、不同安全要求对应的等级化的安全措施为参照，以风险管理过程为主线，建立并实施等级保护体系的过程。

安全措施的选择首先应依据我国信息系统安全等级划分的要求，设计五个等级的安全措施等级要求（安全措施等级要求是针对五个等级信息系统的基本要求）。不同等级的信息系统在相应级别安全措施等级要求的基础上，进行安全措施的调整、定制和增强，并按照一定的划分方法组成相应的安全措施框架，得到适用于该系统的安全措施。安全措施的调整主要依据综合平衡系统安全要求、系统所面临风险和实施安全保护措施的成本来进行。

#### 安全技术体系设计

##### 物理安全设计

物理环境安全策略的目的是保护网络中计算机网络通信有一个良好的电磁兼容工作环境，并防止非法用户进入计算机控制室和各种偷窃、破坏活动的发生。

1）机房选址

机房和办公场地选择在具有防震、防风和防雨等能力的建筑内。机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

2）机房管理

机房出入口安排专人值守，控制、鉴别和记录进入的人员；

需进入机房的来访人员须经过申请和审批流程，并限制和监控其活动范围。

对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；

重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

3）机房环境

合理规划设备安装位置，应预留足够的空间作安装、维护及操作之用。房间装修必需使用阻燃材料，耐火等级符合国家相关标准规定。机房门大小应满足系统设备安装时运输需要。机房墙壁及天花板应进行表面处理，防止尘埃脱落，机房应安装防静电活动地板。

机房安装防雷和接地线，设置防雷保安器，防止感应雷，要求防雷接地和机房接地分别安装，且相隔一定的距离；机房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；机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。配备空调系统，以保持房间恒湿、恒温的工作环境；在机房供电线路上配置稳压器和过电压防护设备；提供短期的备用电力供应，满足关键设备在断电情况下的正常运行要求。设置冗余或并行的电力电缆线路为计算机系统供电；建立备用供电系统。铺设线缆要求电源线和通信线缆隔离铺设，避免互相干扰。对关键设备和磁介质实施电磁屏蔽。

4）设备与介质管理

为了防止无关人员和不法分子非法接近网络并使用网络中的主机盗取信息、破坏网络和主机系统、破坏网络中的数据的完整性和可用性，必须采用有效的区域监控、防盗报警系统，阻止非法用户的各种临近攻击。此外，必须制定严格的出入管理制度和环境监控制度，以保障区域监控系统和环境监控系统的有效运行。

##### 计算环境安全设计

1）身份鉴别

身份鉴别可分为主机身份鉴别和应用身份鉴别两个方面：

主机身份鉴别

为提高主机系统安全性，保障各种应用的正常运行，对主机系统需要进行一系列的加固措施，包括：

对登录操作系统和数据库系统的用户进行身份标识和鉴别，且保证用户名的唯一性。

根据基本要求配置用户名/口令；口令必须具备采用3种以上字符、长度不少于8位并定期更换；

启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。

远程管理时应启用SSH等管理方式，加密管理数据，防止被网络窃听。

对主机管理员登录进行双因素认证方式，采用USB key+密码进行身份鉴别

应用身份鉴别

为提高应用系统系统安全性应用系统需要进行一系列的加固措施，包括：

对登录用户进行身份标识和鉴别，且保证用户名的唯一性。

根据基本要求配置用户名/口令，必须具备一定的复杂度；口令必须具备采用3种以上字符、长度不少于8位并定期更换；

启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。

应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

对于三级系统，要求对用户进行两种或两种以上组合的鉴别技术，因此可采用双因素认证（USB key+密码）或者构建PKI体系，采用CA证书的方式进行身份鉴别。

2）访问控制

三级系统一个重要要求是实现自主访问控制和强制访问控制。自主访问控制实现：在安全策略控制范围内，使用户对自己创建的客体具有各种访问操作权限，并能将这些权限的部分或全部授予其他用户；自主访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级；自主访问操作应包括对客体的创建、读、写、修改和删除等。 强制访问控制实现：在对安全管理员进行严格的身份鉴别和权限控制基础上，由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制；强制访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级。

由此主要控制的是对应用系统的文件、数据库等资源的访问，避免越权非法使用。采用的措施主要包括：

启用访问控制功能：制定严格的访问控制安全策略，根据策略控制用户对应用系统的访问，特别是文件操作、数据库访问等，控制粒度主体为用户级、客体为文件或数据库表级。

权限控制：对于制定的访问控制规则要能清楚的覆盖资源访问相关的主体、客体及它们之间的操作。对于不同的用户授权原则是进行能够完成工作的最小化授权，避免授权范围过大，并在它们之间形成相互制约的关系。

账号管理：严格限制默认账户的访问权限，重命名默认账户，修改默认口令；及时删除多余的、过期的账户，避免共享账户的存在。

访问控制的实现主要采取两种方式：采用安全操作系统，或对操作系统进行安全增强改造，且使用效果要达到以上要求。

3）系统安全审计

系统审计包含主机审计和应用审计两个层面：

主机审计

部署终端安全管理系统，启用主机审计功能，或部署主机审计系统，实现对主机监控、审计和系统管理等功能。

监控功能包括服务监控、进程监控、硬件操作监控、文件系统监控、打印机监控、非法外联监控、计算机用户账号监控等。

审计功能包括文件操作审计、外挂设备操作审计、非法外联审计、IP地址更改审计、服务与进程审计等。审计范围覆盖到服务器上的每个操作系统用户和数据库用户；内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等；保护审计记录，避免受到未预期的删除、修改或覆盖等。同时，根据记录的数据进行统计分析，生成详细的审计报表，

系统管理功能包括系统用户管理、主机监控代理状态监控、安全策略管理、主机监控代理升级管理、计算机注册管理、实时报警、历史信息查询、统计与报表等。

应用审计

应用层安全审计是对业务应用系统行为的审计，需要与应用系统紧密结合，此审计功能应与应用系统统一开发。

应用系统审计功能记录系统重要安全事件的日期、时间、发起者信息、类型、描述和结果等，并保护好审计结果，阻止非法删除、修改或覆盖审计记录。同时能够对记录数据进行统计、查询、分析及生成审计报表。

部署数据库审计系统对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握数据库系统的整体安全。

应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

4）入侵防范

针对入侵防范主要体现在主机及网络两个层面。

针对主机的入侵防范，可以从多个角度进行处理：

入侵检测系统可以起到防范针对主机的入侵行为；

部署漏洞扫描进行系统安全性检测；

部署终端安全管理系统，开启补丁分发功能模块及时进行系统补丁升级；

操作系统的安装遵循最小安装的原则，仅安装需要的组件和应用程序，关闭多余服务等；

另外根据系统类型进行其它安全配置的加固处理。

针对网络入侵防范，可通过部署网络入侵检测系统来实现。将网络入侵检测系统位于有敏感数据需要保护的网络上，通过实时侦听网络数据流，寻找网络违规模式和未授权的网络访问尝试。当发现网络违规行为和未授权的网络访问时，网络监控系统能够根据系统安全策略做出反应，包括实时报警、事件登录，或执行用户自定义的安全策略等。

入侵检测系统可以部署在本项目的核心处以及主要服务器区，这里我们建议在这些区域的交换机上部署入侵检测系统，监视并记录网络中的所有访问行为和操作，有效防止非法操作和恶意攻击。同时，入侵检测系统还可以形象地重现操作的过程，可帮助安全管理员发现网络安全的隐患。

需要说明的是，IDS是对防火墙的非常有必要的附加而不仅仅是简单的补充。入侵检测系统作为网络安全体系的第二道防线，对在防火墙系统阻断攻击失败时，可以最大限度地减少相应的损失。因此，IDS应具备更多的检测能力，能够和其他安全产品（边界防火墙、内网安全管理软件等）进行联动。

5）主机恶意代码防范

各类恶意代码尤其是病毒、木马等是对本项目的重大危害，病毒在爆发时将使路由器、3层交换机、防火墙等网关设备性能急速下降，并且占用整个网络带宽。

针对病毒的风险，我们建议重点是将病毒消灭或封堵在终端这个源头上。比如，在所有终端主机和服务器上部署网络防病毒系统，加强终端主机的病毒防护能力并及时升级恶意代码软件版本以及恶意代码库。

在安全管理安全域中，可以部署防病毒服务器，负责制定和终端主机防病毒策略，在内网建立全网统一的一级升级服务器，在下级节点建立二级升级服务器，由管理中心升级服务器通过互联网或手工方式获得最新的病毒特征库，分发到数据中心节点的各个终端，并下发到各二级服务器。在网络边界通过防火墙进行基于通信端口、带宽、连接数量的过滤控制，可以在一定程度上避免蠕虫病毒爆发时的大流量冲击。同时，防毒系统可以为安全管理平台提供关于病毒威胁和事件的监控、审计日志，为全网的病毒防护管理提供必要的信息。

6）软件容错

软件容错的主要目的是提供足够的冗余信息和算法程序,使系统在实际运行时能够及时发现程序设计错误,采取补救措施,以提高软件可靠性,保证整个计算机系统的正常运行。因此在应用系统软件设计时要充分考虑软件容错设计，包括：

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数据格式或长度符合系统设定要求；

具备自保护功能，在故障发生时，应用系统应能够自动保存当前所有状态，确保系统能够进行恢复。

7）数据完整性与保密性

SSL的英文全称是“Secure Sockets Layer”，中文名为“安全套接层协议层”，它是基于WEB应用的安全协议。SSL协议指定了一种在应用程序协议（如Http、Telenet、NMTP和FTP等）和TCP/IP协议之间提供数据安全性分层的机制，它为TCP/IP连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。

SSL与IPSec安全协议一样，也可提供加密和身份验证安全方法，因此安全性上二者无明显差别。

SSL VPN使用SSL/HTTPS技术作为安全传输机制。这种机制在所有的标准Web浏览器上都有，不用额外的软件实现。使用SSL VPN，在移动用户和内部资源之间的连接通过应用层的Web连接实现，而不是像IPSec VPN在网络层开放的“通道”。

产品部署方面，SSL VPN只需单臂旁路方式接入。单臂旁路接入不改变原有网络结构和网路配置，不增加故障点，部署简单灵活，同时提供完整的SSL VPN服务。远程用户只需应用标准IE浏览器即可登陆网关，通过身份鉴别，在基于角色的策略控制下实现对医院内部资源的存取访问。远程移动用户只需打开标准IE浏览器，登陆SSL VPN网关，经过用户认证后即可根据分配给该用户的相应策略进行相关业务系统的访问。

8）备份与恢复

备份与恢复主要包含两方面内容，首先是指数据备份与恢复，另外一方面是关键网络设备、线路以及服务器等硬件设备的冗余。

数据是最重要的系统资源。数据丢失将会使系统无法连续正常工作。数据错误则将意味着不准确的事务处理。可靠的系统要求能立即访问准确信息。将综合存储战略作为计算机信息系统基础设施的一部分实施不再是一种选择，而已成为必然的趋势。

数据备份系统应该遵循稳定性、全面性、自动化、高性能、操作简单、实时性等原则。备份系统先进的特性可提供增强的性能，易于管理，广泛的设备兼容性和较高的可靠性，以保证数据完整性。广泛的选件和代理能将数据保护扩展到整个系统,并提供增强的功能，其中包括联机备份应用系统和数据文件，先进的设备和介质管理，快速、顺利的灾难恢复以及对光纤通道存储区域网（SAN）的支持等。

本地完全数据备份至少每天一次，且备份介质需要场外存放。

提供能异地数据备份功能，利用通信网络将关键数据定时批量传送至异地备用场地。

对于核心交换设备、外部接入链路以及系统服务器进行双机、双线的冗余设计，保障从网络结构、硬件配置上满足不间断系统运行的需要。

9）资源控制

为保证本项目的应用系统正常的为用户提供服务，必须进行资源控制，否则会出现资源耗尽、服务质量下降甚至服务中断等后果。通过对应用系统进行开发或配置来达到控制的目标，包括：

会话自动结束：当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够及时检测并自动结束会话，释放资源；

会话限制：对应用系统的最大并发会话连接数进行限制，对一个时间段内可能的并发会话连接数进行限制，同时对单个帐户的多重并发会话进行限制，设定相关阈值，保证系统可用性。

登陆条件限制：通过设定终端接入方式、网络地址范围等条件限制终端登录。

超时锁定：根据安全策略设置登录终端的操作超时锁定。

用户可用资源阈值：限制单个用户对系统资源的最大或最小使用限度，保障正常合理的资源占用。

对重要服务器的资源进行监视，包括CPU、硬盘、内存等。

对系统的服务水平降低到预先规定的最小值进行检测和报警。

提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

10）客体安全重用

为实现客体的安全重用，及时清除剩余信息存储空间，应通过对操作系统及数据库系统进行安全加固配置，使得操作系统和数据库系统具备及时清除剩余信息的功能，从而保证用户的鉴别信息、文件、目录、数据库记录等敏感信息所在的存储空间（内存、硬盘）被及时释放或再分配给其他用户前得到完全清除。

11）抗抵赖

解决系统抗抵赖特性最有效的方法就是采用数字签名技术，通过数字签名及签名验证技术，可以判断数据的发送方是真实存在的用户。数字签名是不对称加密算法的典型应用。数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性同时，通过对签名的验证，可以判断数据在传输过程中是否被更改。从而，可以实现数据的发送方不能对发送的数据进行抵赖，发送的数据是完整的，实现系统的抗抵赖性和完整性需求。

PKI体系具备了完善的数字签名功能。因此部署PKI体系可解决抗抵赖的问题，同时提供身份鉴别和访问控制。

##### 区域边界安全设计

1）边界访问控制

通过对系统的边界风险与需求分析，在网络层进行访问控制需部署防火墙产品，可以对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。同时可以和内网安全管理系统、网络入侵检测系统等进行安全联动，为网络创造全面纵深的安全防御体系。

在各安全域边界部署防火墙产品，部署效果如下：

网络安全的基础屏障

防火墙能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。防火墙同时可以保护网络免受基于路由的攻击，如IP选项中的源路由攻击和ICMP重定向中的重定向路径。防火墙可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密口令系统和其它的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙一身上。

对网络存取和访问进行监控审计

如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而曝露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节如Finger，DNS等服务。

精确流量管理

通过部署防火墙设备，不仅可以实现精准访问控制与边界隔离防护，还能实现阻止由于病毒或者P2P软件引起的异常流量、进行精确的流量控制等。对各级节点安全域实现全面的边界防护，严格控制节点之间的网络数据流。

2）安全隔离网闸

根据外网的业务需求，数据中心提供对互联网的访问服务。对这些访问行为，需要对数据交换、传输协议、传输内容、安全决策等进行严格的检查，以防止有互联网引入风险。数据中心内部划分了专门的互联网服务器安全域，将对外提供服务的Web服务器等部署在防火墙的DMZ区，负责接收和处理来自互联网的业务访问请求。防火墙进行严格的访问控制的设定，确保访问身份的合法性。

但是，防火墙无法高度保证传输内容、协议、数据的安全性。同时，需要对互联网业务服务器对数据中心内网数据库的访问进行严格的管理控制，不允许互联网用户访问到互联网业务服务器的数据库。

可以通过在互联网服务器安全域与数据中心内网的安全边界上，在互联网服务器安全域中的业务服务器与单个部门服务器安全域中的业务数据库之间部署安全隔离网闸，对各部门的数据库实现按需数据同步。用户可以通过互联网访问到互联网服务器区中的指定业务前置服务器中，互联网服务器区的业务前置服务器负责接收用户的业务访问请求，并通过安全隔离网闸访问内网某个部门前置受理服务器，在内部安全域实现内网前置处理服务器对相应数据库完成业务处理，并将业务处理结果，按照用户部门的不同，存储在单个部门服务器安全域中、访问用户所在的部门的数据库中，完成用户通过互联网对自己部门业务服务器的访问。

通过这种方式，可以为访问提供更高的安全性保障。安全隔离网闸两侧网络之间所有的TCP/IP连接在其主机系统上都要进行完全的应用协议还原，还原后的应用层信息根据用户的策略进行强制检查后，以格式化数据块的方式通过隔离交换矩阵进行单向交换，在另外一端的主机系统上通过自身建立的安全会话进行最终的数据通信，即实现“协议落地、内容检测”。这样，既从物理上隔离、阻断了具有潜在攻击可能的一切连接，又进行了强制内容检测，从而实现最高级别的安全。

3）边界完整性检查

边界完整性检查核心是要对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查，维护网络边界完整性。通过部署终端安全管理系统可以实现这一目标。

终端安全管理系统其中一个重要功能模块就是非法外联控制，探测内部网中非法上互联网的计算机。非法外联监控主要解决发现和管理用户非法自行建立通路连接非授权网络的行为。通过非法外联监控的管理，可以防止用户访问非信任网络资源，并防止由于访问非信任网络资源而引入安全风险或者导致信息泄密。

终端非法外联行为监控可以发现终端试图访问非授信网络资源的行为，如试图与没有通过系统授权许可的终端进行通信，自行试图通过拨号连接互联网等行为。对于发现的非法外联行为，可以记录日志并产生报警信息。

终端非法外联行为管理可以禁止终端与没有通过系统授权许可的终端进行通信，禁止拨号上网行为。

4）边界入侵防御

在各区域边界，防火墙起到了协议过滤的主要作用，根据安全策略在偏重在网络层判断数据包的合法流动。但面对越来越广泛的基于应用层内容的攻击行为，防火墙并不擅长处理应用层数据。

在本项目网络边界和主要服务器区安全域均已经设计部署了防火墙，对每个安全域进行严格的访问控制。鉴于以上对防火墙核心作用的分析，需要其他具备检测新型的混合攻击和防护的能力的设备和防火墙配合，共同防御来自应用层到网络层的多种攻击类型，建立一整套的安全防护体系，进行多层次、多手段的检测和防护。入侵防护系统（IPS）就是安全防护体系中重要的一环，它能够及时识别网络中发生的入侵行为并实时报警并且进行有效拦截防护。

IPS是继“防火墙”、“信息加密”等传统安全保护方法之后的新一代安全保障技术。它监视计算机系统或网络中发生的事件，并对它们进行分析，以寻找危及信息的机密性、完整性、可用性或试图绕过安全机制的入侵行为并进行有效拦截。IPS就是自动执行这种监视和分析过程，并且执行阻断的硬件产品。

将IPS串接在防火墙后面，核心服务器区的前面，在防火墙进行访问控制，保证了访问的合法性之后，IPS动态的进行入侵行为的保护，对访问状态进行检测、对通信协议和应用协议进行检测、对内容进行深度的检测。阻断来自内部的数据攻击以及垃圾数据流的泛滥。

由于IPS对访问进行深度的检测，因此，IPS产品需要通过先进的硬件架构、软件架构和处理引擎对处理能力进行充分保证。

5）边界安全审计（上网行为管理）

各安全区域边界已经部署了相应的安全设备负责进行区域边界的安全。对于流经各主要边界（重要服务器区域、外部连接边界）需要设置必要的审计机制，进行数据监视并记录各类操作，通过审计分析能够发现跨区域的安全威胁，实时地综合分析出网络中发生的安全事件。一般可采取开启边界安全设备的审计功能模块，根据审计策略进行数据的日志记录与审计。同时审计信息要通过安全管理中心进行统一集中管理，为安全管理中心提供必要的边界安全审计数据，利于管理中心进行全局管控。边界安全审计和主机审计、应用审计、网络审计等一起构成完整的、多层次的审计系统。

6）网页防篡改

在外网数据中心的互联网服务器区对外提供Web服务，Web应用的普及使得外网信息系统中存在的Web服务器很容易成为黑客的攻击目标。需要专业的主页防篡改工具有效阻止主页篡改事件的发生，维护Web页面的安全。

在办公外网的互联网服务器区中的每个web服务器配置一套主页防篡改系统，全面监测WEB服务器的页面是否正常。对于突破网站防火墙的篡改行为，进行实时监控，确保网站信息安全。一旦发现网站信息被篡改之后，立刻通知监控中心并迅速恢复正常的网页文件。7×24不间断地保护网站，任何恶意篡改痕迹将被实时保留，并主动和及时通知管理人员，做到防范于未然。

外网互联网服务器区Web部署的主页防篡改系统可以保障主要的WEB页面信息的安全和准确性。全面的监测和保障外网Web服务的安全。防止黑客对网页进行恶意篡改。通过网络扫描网站的网页，监测网页是否被修改，当发现网页被修改后，系统能够自动报警和恢复。

7）边界恶意代码防范（防毒墙）

一个完善的安全体系应该包含了从桌面到服务器、从内部用户到网络边界的全面地解决方案，以抵御来自黑客和病毒的威胁。

在办公外网边界部署防病毒网关，采用透明接入方式，在最接近病毒发生源安全边界处进行集中防护，对夹杂在网络交换数据中的各类网络病毒进行过滤，可以对网络病毒、蠕虫、混合攻击、端口扫描、间谍软件、P2P软件带宽滥用等各种广义病毒进行全面的拦截。阻止病毒通过网络的快速扩散，将经网络传播的病毒阻挡在外，可以有效防止病毒从其他区域传播到内部其他安全域中。通过部署AV防病毒网关（防毒墙），截断了病毒通过网络传播的途径，净化了网络流量。

部署的防病毒网关应特别注意设备性能，产品必须具备良好的体系架构保证性能，能够灵活的进行网络部署。同时为使得达到最佳防毒效果，AV防病毒网关设备和桌面防病毒软件应为不同的厂家产品，两类病毒防护产品共同组成立体病毒防护体系。

为能达到最好的防护效果，病毒库的及时升级至最新版本至关重要。对于能够与互联网实现连接的网络，应对自动升级进行准确配置；对与不能与互联网进行连接的网络环境，需采取手动下载升级包的方式进行手动升级。

##### 通信网络安全设计

1）网络结构安全

网络结构的安全是网络安全的前提和基础，选用主要网络设备时需要考虑业务处理能力的高峰数据流量，要考虑冗余空间满足业务高峰期需要；网络各个部分的带宽要保证接入网络和核心网络满足业务高峰期需要；按照业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要主机；合理规划路由，业务终端与业务服务器之间建立安全路径；绘制与当前运行情况相符的网络拓扑结构图；根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

2）网络安全审计

网络安全审计系统主要用于监视并记录网络中的各类操作，侦察系统中存在的现有和潜在的威胁，实时地综合分析出网络中发生的安全事件，包括各种外部事件和内部事件。

交换机处并接部署网络行为监控与审计系统，形成对全网网络数据的流量监测并进行相应安全审计，同时和其它网络安全设备共同为集中安全管理提供监控数据用于分析及检测。

网络行为监控和审计系统将独立的网络传感器硬件组件连接到网络中的数据会聚点设备上，对网络中的数据包进行分析、匹配、统计，通过特定的协议算法，从而实现入侵检测、信息还原等网络审计功能，根据记录生成详细的审计报表。

网络行为监控和审计系统采用旁路技术，不用在目标主机中安装任何组件。同时网络审计系统可以与其它网络安全设备进行联动，将各自的监控记录送往安全管理安全域中的安全管理服务器，集中对网络异常、攻击和病毒进行分析和检测。

3）网络设备防护

为提高网络设备的自身安全性，保障各种网络应用的正常运行，对网络设备需要进行一系列的加固措施，包括：

对登录网络设备的用户进行身份鉴别，用户名必须唯一；

对网络设备的管理员登录地址进行限制；

身份鉴别信息具有不易被冒用的特点，口令设置需3种以上字符、长度不少于8位，并定期更换；

具有登录失败处理功能，失败后采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

启用SSH等管理方式，加密管理数据，防止被网络窃听。

对于鉴别手段，三级要求采用两种或两种以上组合的鉴别技术，因此需采用USBkey+密码进行身份鉴别，保证对网络设备进行管理维护的合法性。

4）通信完整性

信息的完整性设计包括信息传输的完整性校验以及信息存储的完整性校验。

对于信息传输和存储的完整性校验可以采用的技术包括校验码技术、消息鉴别码、密码校验函数、散列函数、数字签名等。

对于信息传输的完整性校验应由传输加密系统完成。部署SSL VPN系统保证远程数据传输的数据完整性。对于信息存储的完整性校验应由应用系统和数据库系统完成。

5）通信保密性

应用层的通信保密性主要由应用系统完成。在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；并对通信过程中的敏感信息字段进行加密。

对于信息传输的通信保密性应由传输加密系统完成。部署SSL VPN系统保证远程数据传输的数据机密性。

6）网络可信接入

为保证网络边界的完整性，不仅需要进行非法外联行为，同时对非法接入进行监控与阻断，形成网络可信接入，共同维护边界完整性。通过部署终端安全管理系统可以实现这一目标。

终端安全管理系统其中一个重要功能模块就是网络准入控制，启用网络阻断方式包括ARP干扰、802.1x协议联动等。

监测内部网中发生的外来主机非法接入、篡改 IP 地址、盗用 IP 地址等不法行为，由监测控制台进行告警。运用用户信息和主机信息匹配方式实时发现接入主机的合法性，及时阻止 IP 地址的篡改和盗用行为。共同保证边界完整性。具体如下：

在线主机监测

可以通过监听和主动探测等方式检测系统中所有在线的主机，并判别在线主机是否是经过系统授权认证的信任主机。

主机授权认证

可以通过在线主机是否安装客户端代理程序，并结合客户端代理报告的主机补丁安装情况，防病毒程序安装和工作情况等信息，进行网络的授权认证，只允许通过授权认证的主机使用网络资源。

非法主机网络阻断

对于探测到的非法主机，系统可以主动阻止其访问任何网络资源，从而保证非法主机不对网络产生影响，无法有意或无意的对网络攻击或者试图窃密。

网络白名单策略管理

可生成默认的合法主机列表，根据是否安装安全管理客户端或者是否执行安全策略，来过滤合法主机列表，快速实现合法主机列表的生成。同时允许管理员设置白名单例外列表，允许例外列表的主机不安装客户端但是仍然授予网络使用权限，并根据需要授予可以和其他授权认证过的主机通信的权限或者允许和任意主机通信的权限。

IP和MAC绑定管理

可以将终端的IP和MAC地址绑定，禁止用户修改自身的IP和MAC地址，并在用户试图更改IP和MAC地址时，产生相应的报警信息。

##### 安全管理中心设计

为了能准确了解系统的运行状态、设备的运行情况，统一部署安全策略，应进行安全管理中心的设计，根据要求，应在系统管理、审计管理和安全管理几个大方面进行建设。

在安全管理安全域中建立安全管理中心，是有效帮助管理人员实施好安全措施的重要保障，是实现业务稳定运行、长治久安的基础。通过安全管理中心的建设，真正实现安全技术层面和管理层面的结合，全面提升用户网络的信息安全保障能力。

1）系统管理

通过系统管理员对系统的资源和运行进行配置、控制和管理，包括：

用户身份管理：统一管理系统用户身份，按照业务上分工的不同，合理地把相关人员划分为不同的类别或者组，以及不同的角色对模块的访问权限。权限设置可按角色划分，角色分为普通用户、系统管理员、安全管理员、审计管理员等。

系统资源配置与监控：进行系统资源配置管理与监控，包括CPU负载、磁盘使用情况、服务器内存、数据库的空间、数据库日志空间、SWAP使用情况等，通过配置采样时间，定时检测。



图 5 信息安全管理体系

系统加载和启动：进行系统启动初始化管理，保障系统的正常加载和启动。

系统运行的异常监控：系统资源和设备受到攻击，或运行异常时，会以告警等信息方式，通知管理员。安全管理平台可提供多种自动处理机制，协助用户监控最新告警，全方位掌控网络异常和攻击。

数据备份与恢复：数据的定期备份与恢复管理，识别需要定期备份的重要业务信息、系统数据及软件系统，规定备份信息的备份方式、备份频度、存储介质、保存期等；根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，定期执行备份与恢复策略。

恶意代码防范管理：建立恶意代码管理中心，进行防恶意代码软件的统一管理，并根据情况建立二级管理中心。恶意代码管理中心实现：杀毒策略统一集中配置；自动并强制进行恶意代码库升级；定制统一客户端策略并强制执行；进行集中病毒报警等。

系统补丁管理：集中进行补丁管理，定期统一进行系统补丁安装。注意应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

系统管理员身份认证与审计：对系统管理员进行严格的身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

2）审计管理

通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括：根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等；对安全审计员进行严格的身份鉴别，并只允许其通过特定的命令或界面进行安全审计操作。

具体集中审计内容包括：

日志监视

实时监视接收到的事件的状况，如最近日志列表、系统风险状况等；监控事件状况的同时也可以监控设备运行参数，以配合确定设备及网络的状态；日志监视支持以图形化方式实时监控日志流量、系统风险等变化趋势。

日志管理

日志管理实现对多种日志格式的统一管理。通过SNMP、SYSLOG或者其它的日志接口采集管理对象的日志信息，转换为统一的日志格式，再统一管理、分析、报警；自动完成日志数据的格式解析和分类；提供日志数据的存储、备份、恢复、删除、导入和导出操作等功能。日志管理支持分布式日志级联管理，下级管理中心的日志数据可以发送到上级管理中心进行集中管理

审计分析

集中审计可综合各种安全设备的安全事件，以统一的审计结果向用户提供可定制的报表，全面反映网络安全总体状况，重点突出，简单易懂。

系统支持对包过滤日志、代理日志、入侵攻击事件、病毒入侵事件等十几种日志进行统计分析并生成分析报表；支持按照设备运行状况、设备管理操作对安全设备管理信息统计分析；支持基于多种条件的统计分析，包括：对访问流量、入侵攻击、邮件过滤日志、源地址、用户对网络访问控制日志等。对于入侵攻击日志，可按照入侵攻击事件、源地址、被攻击主机进行统计分析，生成各类趋势分析图表。

系统可以生成多种形式的审计报表，报表支持表格和多种图形表现形式；用户可以通过IE浏览器访问，导出审计结果。可设定定时生成日志统计报表，并自动保存以备审阅或自动通过邮件发送给指定收件人，实现对安全审计的流程化处理。

3）网络运维及应用监控管理系统

本项目对网络和系统的稳定性、可靠性、服务质量的要求很高。大量软硬件的投入和增加，也导致了本项目运维管理难度的增大和系统管理人员的工作压力越来越大。

此外，系统运维还需要对应用系统的整体运行状况进行有效监控，需要及时发现潜在的问题，这对网络管理工程师又是一个很大的挑战。网管工程师过去经常是在故障发生后，才能去进行处理，工作处于被动状态。有时即使发现了故障，也要花费很长时间去寻找和诊断故障，极大地影响了工作效率。由于没有直观的网络拓扑功能，应用系统的监测和管理显得非常繁琐。如何对各种应用系统进行有效的监测管理，不断提高各种应用的服务质量，是系统管理人员急需解决的问题。

 为了保障业务系统正常运转，提高服务和维护水平，特别是要管理分布式的网络、系统环境，有必要使用一套全面的网络运维管理系统，制定相应的管理策略和制度，实现集中统一管理，并实现：

监测管理自动化，故障处理变被动为主动，主动发现系统问题，在最短的时间内实现故障报警，管理人员可以快速采取解决措施。

完善的性能分析报告，更能帮助系统管理人员及时预测、发现性能瓶颈，提高系统的整体性能。

帮助管理者制定并执行良好的实施、管理和分析策略，使本项目系统运维管理水平上升到新的高度。

4）不同等级系统互联互通

在明确等级划分之后，不同等级的系统间面临着互联互通的问题，系统间需要进行数据交换。

不同安全等级的系统互联互通，应遵循以下原则：

不同等级安全域互联后各级系统须能够满足本级各项基本技术要求，高安全等级的系统要充分考虑引入低安全等级系统后带来的风险，不能因为互联而无法达到相应的基本要求，破坏本等级的安全边界。

互联手段中重点是互联边界应采取相应的边界保护、访问控制等安全措施，防止高等级系统的安全受低等级系统的影响。边界产品可有针对性的选择安全隔离网闸、防火墙、入侵防护等边界安全设备。

根据系统业务要求和安全保护要求，制定相应的互联互通安全策略，包括访问控制策略和数据交换策略等，严格控制数据在不同等级之间的流动。

#### 安全管理体系设计

安全体系管理层面设计主要是依据《信息系统安全等级保护基本要求》中的管理要求而设计。分别从以下方面进行设计：

##### 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。

## 安全保密管理

我公司确保对项目技术文件以及由采购人提供的所有内部资料、技术文档和信息予以保密。我公司确保遵守与采购人签订的保密协议，未经采购人书面许可，投标人不得以任何形式向第三方透露本项目标书以及本项目的任何内容。

为做好本项目的保密工作，我公司根据该项目的具体情况结合保密原则制定了相应的保密方案，在项目的实施过程中将严格按照保密方案做好保密工作。

### 目的

为维护项目双方的自身利益，保守国家秘密，工作秘密和商业秘密，依据《中华人民共和国保守国家秘密法》，制定本保密方案。

### 适用范围

本方案适用于国家秘密，工作秘密和商业秘密的管理。其中工作秘密和商业秘密在本方案中定义为内部秘密。

### 保密措施

* 对于项目中涉及国家秘密的事项的保密措施

 涉及国家秘密的传递，使用，存储，销毁等流程严格遵守《中华人民共和国保守国家秘密法》、甲方的相关保密规定。严禁非涉密人员和非项目涉密岗位人员接触知悉相关秘密事项，具体措施有以下几点：

涉及国家秘密的事项传递必须通过公司保密办指定的保密员进行传递，不允许通过邮政或快递等非机要渠道传递。

涉及国家秘密的信息处理必须在公司保密机要室内的涉密计算机上进行，由公司保密办进行涉密计算机的管理，严格限定知悉范围和使用范围，知悉人员由公司保密工作领导小组依据秘密事项范围要求确定。

对参与项目的技术研发人员，由公司保密办定期进行技术检查，杜绝泄密。

对相关涉密载体的管理，由公司保密办严格按照《中华人民共和国保守国家秘密法》、甲方的中对涉密载体的管理规定进行管理。项目部涉密人员严禁在保密机要室以外的范围使用涉密载体。

对项目部相关涉密和非涉密人员的保密教育由公司保密办分别以涉密人员每周一次和非涉密人员每周2次的频度进行保密教育。通过教育和谈话掌握相关人员的思想状态，防范可能产生的泄密情况，对思想状态不佳的项目部成员，由公司保密办报公司保密领导小组同意后调离相关岗位。

* 对于项目中产生的内部秘密的保密措施

凡属于项目部内部秘密，项目部按照相关保密措施，指定专人具体负责落实，严格注意防止外企业或他人以“洽谈业务、开发合作、学习参观”等名义从中获取内部秘密。

涉及内部秘密部门不允许无关人员接触或外界参观，如必须参观的，需经甲方和公司保密办主任审批，由公司保密办负责预先做好保密措施。

内部会议或处理公务提供、发放文件、资料、图纸时，由项目部项目经理审批，统一编写受控号，严格按照文件发放范围登记发放，并向发放对象提出保密要求，事后要指定专人负责收回。

凡向外提供的各类学术交流论文、资料等，涉及到项目内部秘密的，应事先经项目部项目经理和公司保密办审查批准，并做好保密技术处理。

凡属项目内部秘密，但不需存档的文件、资料、图纸、刊物等，均应集中由公司保密办统一监销。

项目部工作人员不得擅自将企业内部秘密事项进行对外报导，不得用公用电话或无线电话谈论内部秘密事项。

### 责任与奖惩

在保守、保护项目说涉及的国家秘密和内部秘密以及改进保密技术措施等方面成绩显著的项目部成员，公司保密领导小组将给予现金和通报奖励。

凡违反规定，泄露国家、内部秘密、不够刑事处罚的，可视情节严重程度给予通报批评、警告等处分。

对有意向外界泄露、出卖内部秘密的人员，将根据危害程度追究经济赔偿或依法起诉。

凡发生泄露涉及国家秘密案件的，将根据《中华人民共和国保守国家秘密法》和《刑法》中有关规定移送国家司法机关依法追究刑事责任。

### 保密管理制度

##### 保密总则

为确保项目的绝对安全，维护本项目参与方的合法利益，保障本项目顺利，促进项目的顺利进展，特制定本管理制度。

本项目关系到各方的权利和利益，依照特定的程序确定，在一定时间内只限一定范围人员知悉的事项。

本项目现场所有人员都有保守项目秘密之义务。

对保守、保护秘密及改进保密技术、措施等方面成绩显著的现场人员实施奖励。

本制度由涉密项目维护办公室负责维护。

##### 保密等级划分

分为“绝密”“机密”“秘密”三级。

项目维护中，直接影响采购人权益的重要文件资料为绝密：

项目的规划、图纸设计、技术参数、统计资料、重要会议纪要等视为机密级。

项目档案资料、合同、协议等为秘密级。

##### 保密守则

全体人员均自觉地遵守下列保密守则：

不该说的项目涉密资料，绝对不说；

不该问的项目涉密资料，绝对不问；

不该看的项目涉密资料，绝对不看；

不该记录的项目涉密资料，绝对不记录；

不在私人通信中涉及项目涉密资料；

不在公共场所和家属、子女、亲友面前谈论项目相关资料；

不在不利于保密的地方存放涉密文件、资料；

不携带涉密材料游览、参观、探亲、访友和出入公共场所；

不将内部文件、资料、刊物作废纸出售；

不得擅自翻印、复印、全抄、录音秘密以上文件、资料、刊物；

不得因工作便利调取、泄露项目相关监控点视频内容。

档案室管理制度：

档案室应当设在有利于安全保密的地方，安装各项保密设施。

项目涉密文件、资料，由档案室的管理人员负责收发。

对发出、收进的涉密文件、资料，应当逐件进行登记、编号、办好收发手续。

传递涉密文件、资料，应当按照资料规定的阅读范围阅，不得擅自扩大传阅范围。

对涉密文件、资料，应当定期清查、清退，定期进行清查、清退一次。

##### 保密制度

本项目工作人员经常性接触项目机密材料，必须以身作则，模范遵守各项保密法规和制度。

严格执行文件管理制度。坚持在办公室阅办秘密文、电资料，特殊情况需在家阅办时，应采取必要的安全保密措施，阅办后及时向档案室清退。

禁止携带秘密文件、资料出入公共场所。

严禁擅自决定复制秘密文件、资料，确需复制时，应履行审批手续。涉及工程机密及其它党和国家机密，经本项目相关管理人员同意，可以翻印；其它秘密文件、资料的复制，必须征求发文机关同意。

召开重要和有保密内容的会议，要采取安全防范措施，并对与会人员进行保密教育。

用户的办公室、机要室、档案室、文印室、收发室等属办公重点保密场所，未经许可，外来人员不准擅自入内。

禁止在无保密措施的有线、无线通信中传递本项目秘密；不准通过普通邮政传递秘密文件、资料。

严禁在公共场所和家属及其他无关人员面前谈论项目秘密、工程机密。

全体员工应当做到不该说的不说，不该问的不问，不该看的不看，不该听的不听，不该记的不记。相互监督，共同负责，逐步实现保密工作经常化、制度化、规范化。

发现项目秘密、公司秘密已经泄露或者可能泄露时，应当立即采取补救措施，并迅速报告有关部门及时处理。

文件的管理规定：

文件一律由指定保管人签收、拆封、登记、清点。

文件只能在办公室阅读，不准外带。确因工作需要必须把文件带出时，须经本会领导批准，办理借阅手续，用后及时退还。借阅人不准把文件转借他人。

文件要由保密员专人保管，存放文件要有专柜、专室。不准将文件放置在无专人管理、无严密加锁的箱柜内。下班时不准将文件放在办公桌上。发现下落不明(丢失)文件要及时报告，并认真查找、处理。

##### 现场保密措施

项目维护人员务必增强保密意识，不该问的不问，不该说的不说，不该看的不看。每天开工和收工时，对现场维护人员进行安全检查，防止摄像器材进入现场。

秘密文件、资料和其他物品的制作、收发、传递、使用、复制、摘抄保存和销毁，由现场项目经理或委托专人执行。

对于密级文件、资料或其他物品，采取如下保密措施：

不经现场项目经理签批，不得复制和摘抄。

收发、传递和外出携带由指定人担任，并采取必要的安全措施。

所有资料在设备完善的保险装置中保存。

在对外交往合作中，需要提供保密事项的要事先报请现场项目经理签批。

项目维护过程中属于保密内容的会议，要选择具备保密措施的场所，限定参会人员的范围，依据保密规定使用会议设备和管理会议文件，确定会议是否传达及传达范围。

现场实维护作人员发现秘密泄露或者可能泄露时，要采取补救措施并及时报现场项目经理，项目经理要及时做出处理。

计算机信息系统使用管理规定：

不得在与网络联网的计算机信息系统中存储、处理、传递项目秘密信息。任何人不得在公众网上发布、存储、处理、传递、转发、抄送涉及项目秘密信息。

对秘密数据、资料载体如：磁盘、磁带、光盘等视同“三密”文件，履行借阅、使用、复制、传递、携带、移交、保存、销毁等登记手续。

存储过项目秘密信息的计算机媒体(包括软盘和硬盘)不能降低密级使用，维修时应保证所存储的项目秘密信息不被泄露，不再使用的应及时销毁。

##### 涉密人员的培训管理

保密办公室负责保密法规知识的宣传教育工作。要充分利用报纸、杂志、板报宣传保密法规普及保密知识，提高全体员工的保密意识。

保密宣传教育工作，由公司保密办负责计划、安排，并组织实施。保密办小组每年至少安排一次对全体涉密人员的保密宣传教育，一年至少安排两次涉密人员培训，使涉密人员熟悉基本的保密法规，知悉其必须承担的保密责任和义务以及应当享有的权利。

新调入或新任用涉密岗位人员，必须先由人事行政部负责进行保密制度培训并考试合格后方可上岗工作。各部门负责人有责任教育调离涉密岗位的人员离岗后自觉遵守保密纪律，承担保密义务，不泄露本项目秘密。

保密办公室负责对因公、因私调离本项目岗位的涉密人员进行保密教育，使其了解保密范围，明确保密责任，掌握处理保密问题的方法。

保密培训工作由保密办公室拟定《年度培训计划》，纳入部门职工培训教育计划，由人事行政部负责组织，保密办公室参与实施，培训人员按规定在《培训签到表》签到。

##### 保密协议的签订

所有参与本项目的项目组成员树立保密意识，遵守保密规定，与采购人签订保密协议，因利用工作便利调取、泄露视频内容的，按国家相关法律处理，承担相应的法律责任。

我方保证对在讨论、签订、执行本协议过程中所获悉的属于对方的且无法自公开渠道获得的文件及资料（包括商业秘密、公司计划、运营活动、财务信息、技术信息、经营信息及其他商业秘密）予以保密。未经该资料和文件的原提供方同意，另一方不得向任何第三方泄露该商业秘密的全部或部分内容。但法律、法规另有规定或双方另有约定的除外。

具备以下主要条款：

* 保密的内容和范围；
* 保密合同双方的权利和义务；
* 保密协议的期限；
* 违约责任。

在保密合同有效期限内，员工应履行下列义务：

* 严格遵守本项目保密制度，防止泄漏项目秘密；
* 不得向他人泄漏项目秘密；
* 非经书面同意，不得利用该项目秘密进行生产与经营活动，不得利用项目秘密进行新的研究和开发。

##### 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。

##### 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。

##### 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。

##### 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。