JD院校智慧教室安全保密方案

1. **安全保密方案**

项目的安全设计整体遵循《军队计算机信息系统安全保密防护要求及检测评估方法》（GJB 5612A）的安全防护体系来进行设计，主要包括计算环境安全、网络安全、应用安全、数据安全、安全管理、保密安全设计等内容。

本方案首先从多个角度对安全保密方案进行了合理的全方位的设计，同时也从技术角度和安全管理角度对安全保密方案的细节进行了合理的设计。我方在安全保密方案中依据各项安全保密措施的可操作性分别给出了详细的描述。

为了满足军队信息系统的安全防护需求，智慧教室整体建设项目的安全保密方案遵守军事综合信息网安全保密建设要求的GJB5612-2021《军队计算机信息系统安全保密防护要求及检测测评方法》。

* 1. **计算环境安全**

计算环境安全设计主要包括系统安全加固、主机管控审计、主机身份认证、主机病毒查杀、主机漏洞修复等部分。

* + 1. **系统安全防护**

在该建设项目中，计算环境的安全加固是确保系统稳定运行的基础。系统加固措施包括以下几个方面：

复杂口令策略：对于BIOS和操作系统，应设置至少10位的复杂口令，包含大小写字母、数字和特殊字符，以防止暴力破解和字典攻击。

屏幕保护与自动锁定：启用屏幕保护程序，并设置较短的等待时间，如5分钟，以减少未授权访问的风险。

禁用不必要的引导方式：关闭所有非必要的引导方式，如光驱、软驱、USB和网络引导，以防止恶意软件通过这些途径启动。

网络唤醒与远程开机：禁用网络唤醒和远程开机功能，以防止远程攻击者利用这些功能进行攻击。

内存保护：启用内存保护功能，以防止恶意软件攻击系统的低层内存。

终端系统防护：办公计算机需基于可信根对设备的系统固件、系统引导程序、系统内核程序和重要配置参数等进行可信验证，可信性受到破坏后报警

操作系统和软件更新：定期更新操作系统和软件，以修补已知的安全漏洞，防止攻击者利用这些漏洞进行攻击。

* + 1. **主机审计管理**

主机管控与审计是确保计算环境安全的关键环节。通过实施以下措施，可以实现对终端和服务器的有效管理和监控：

部署主机安全管理软件：在所有终端和服务器上安装主机安全管理软件客户端，以便收集和监控设备信息和状态。

统一管控策略：通过主机安全管理软件控制中心，统一定制和下发管控策略，对网络访问、进程运行、外设使用、文件流转、打印输出等行为进行管控和审计。

非法联接行为阻断：对于非法联接行为，系统应能够自动阻断并发出告警，以防止未授权的设备接入网络。

用户登录审核：对用户登录行为进行严格审核，确保只有授权用户才能访问系统资源。

软件可信性审核：对安装在主机上的软件进行可信性审核，确保只有经过认证的软件才能运行。

违规告警：对于违规行为，如未授权的外设使用、非法网络访问等，系统应能够发出告警，并采取相应的措施。

可信密码软件：依托可信密码软件，实现主机环境的安全可信，防止恶意软件的攻击。

保密综合管理系统：通过保密综合管理系统，提供文件集中管控、集中文印控制、标签水印等安全保密服务，以保护敏感数据不被泄露。

外设使用策略：通过控制中心下发外设使用策略，禁用不安全的外设功能，如光驱刻录、USB存储和本地打印，以防止数据泄露。

服务和端口管理：关闭不必要的服务和端口，禁止自动播放，禁用远程登录服务，限定服务器的远程管理IP地址，以减少潜在的攻击面。

* + 1. **统一身份认证**

项目的统一身份认证基于用户目前现有的身份认证平台，并对现有平台进行设置调整。主要包括以下几个方面：

统一身份鉴别方式：利用现有的终端认证设备，设置统一的身份鉴别方式，如多因素认证，包括密码、智能卡、生物识别等。

强化密码策略：设置强密码策略，要求密码复杂度高，定期更换，防止密码猜测和暴力破解。

账户管理：对账户进行严格管理，包括账户的创建、修改、禁用和删除，确保只有授权用户才能创建和修改账户。

账户权限控制：对账户权限进行严格控制，确保用户只能访问其授权的资源，防止权限滥用。

账户审计：对账户登录行为进行审计，记录登录时间、登录地点、登录设备等信息，以便在发生安全事件时进行追踪和分析。

账户锁定策略：设置账户锁定策略，如连续多次输入错误密码后锁定账户，以防止暴力破解。

身份认证日志：记录身份认证日志，包括成功和失败的登录尝试，以便进行安全分析和监控。

身份认证系统维护：定期维护身份认证系统，更新认证设备，修补已知的安全漏洞，确保系统的安全性。

* + 1. **主机病毒防护**

病毒查杀与防护是计算环境安全的重要组成部分。项目的主机病毒查杀设计主要根据用户现有网络的病毒查杀能力，实现主机病毒的防护，主要包括以下内容：

启用防火墙功能：在所有终端和服务器上启用防火墙功能，以防止未经授权的网络访问。

网络防病毒系统：依托网络中的防病毒系统，实现网络防病毒功能，提供病毒库升级、可疑代码上报处理、病毒检测与查杀等功能服务。

病毒库更新：确保病毒库至少每15天更新一次，以应对新出现的病毒和恶意软件。

可疑代码上报处理：对可疑代码进行上报处理，以便进行深入分析和研究，及时更新病毒库。

病毒检测与查杀：定期进行病毒检测和查杀，确保系统中没有病毒和恶意软件的存在。

用户教育：对用户进行安全教育，提高他们的安全意识，教育他们不要打开来历不明的邮件附件和链接，以防止病毒的传播。

系统和软件更新：定期更新操作系统和软件，修补已知的安全漏洞，防止病毒和恶意软件利用这些漏洞进行攻击。

安全策略：制定严格的安全策略，禁止用户安装未经认证的软件，以防止恶意软件的安装。

病毒防护日志：记录病毒防护日志，包括病毒检测、查杀和上报处理的详细信息，以便进行安全分析和监控。

病毒防护系统维护：定期维护病毒防护系统，更新病毒库，修补已知的安全漏洞，确保系统的安全性。

* + 1. **主机漏洞修复**

项目的主机漏洞修复主要依托用户现有网络主机漏洞修复功能，检测系统中已安全的补丁和需要安装的补丁，同时实现补丁库30天内的升级更新。主要包括以下内容：

补丁管理：依托防病毒与补丁管理系统的补丁管理功能，定期检测系统中已知的补丁和需要安装的补丁。

补丁库更新：确保补丁库至少每30天更新一次，以应对新出现的安全漏洞。

补丁安装：及时安装必要的补丁，修补系统中的安全漏洞，防止攻击者利用这些漏洞进行攻击。

补丁测试：在安装补丁之前，进行充分的测试，确保补丁不会影响系统的稳定性和性能。

补丁审计：对补丁安装行为进行审计，记录补丁安装的时间、地点、设备等信息，以便在发生安全事件时进行追踪和分析。

补丁策略：制定严格的补丁策略，确保所有终端和服务器都及时安装必要的补丁。

用户教育：对用户进行安全教育，提高他们的安全意识，教育他们及时更新操作系统和软件，修补已知的安全漏洞。

系统和软件更新：定期更新操作系统和软件，修补已知的安全漏洞，防止攻击者利用这些漏洞进行攻击。

安全策略：制定严格的安全策略，禁止用户安装未经认证的软件，以防止恶意软件的安装。

漏洞修复日志：记录漏洞修复日志，包括补丁检测、安装和测试的详细信息，以便进行安全分析和监控。

* + 1. **主机管理终端**

项目终端管理主要根据以下内容进行设计：

数据导入导出审批：建立数据导入导出审批机制，对数据流动进行管控和审计，确保只有授权的数据才能被导入导出。

数据加密：对导入导出的数据进行加密，以防止数据在传输过程中被截获和篡改。

数据备份：定期对数据进行备份，以防止数据丢失和损坏。

访问控制：对管理终端的访问进行严格控制，确保只有授权用户才能访问管理终端。

审计日志：记录管理终端的访问日志，包括访问时间、访问地点、访问设备等信息，以便在发生安全事件时进行追踪和分析。

系统和软件更新：定期更新管理终端的操作系统和软件，修补已知的安全漏洞，防止攻击者利用这些漏洞进行攻击。

安全策略：制定严格的安全策略，禁止用户在管理终端上进行未经授权的操作。

* 1. **网络安全**

网络安全设计主要包括网络分区分域、网络链路加密、网络访问控制、网络入侵检测与审计、网络漏洞扫描、网络接入安全等部分。

* + 1. **网络分域分区**

项目主要根据数据中心建设需求和客户目前的实际情况，在网络架构中实施分区分域策略，旨在通过物理或逻辑手段将网络划分为多个隔离的区域，以降低安全风险并简化管理。这种策略允许网络管理员对不同区域实施不同的安全策略，从而更有效地控制和监控网络流量。

细致的区域划分：基于业务需求和安全要求，网络被划分为多个逻辑区域，每个区域都有明确的功能和访问权限。例如，可以为研发、生产、测试和外部访问创建不同的网络区域。

访问控制策略：在网络核心和汇聚层交换机上配置精细的访问控制列表（ACL），以限制不同区域之间的流量。这些ACL基于最小权限原则，仅允许必要的通信，从而减少潜在的攻击路径。

隔离与互联：通过路由器、防火墙或虚拟局域网（VLAN）技术，实现不同安全域之间的隔离。同时，确保关键业务系统和数据存储设备位于受保护的安全区域，与公共区域隔离。

动态访问控制：随着业务需求的变化，动态调整ACL和其他访问控制措施，以适应新的安全挑战。

通过这些措施，网络分区分域策略能够为网络提供灵活性和安全性，同时为未来的扩展和变更提供便利。

* + 1. **网络漏洞扫描**

项目的网络漏洞扫描能力主要根据用户现有的网络漏洞扫描设备进行展开，主要包括以下内容：

定期全面扫描：使用自动化的漏洞扫描工具，定期对网络中的所有设备和系统进行全面扫描。这包括服务器、工作站、网络设备和应用程序。

漏洞评估与修复：对扫描发现的漏洞进行评估，确定它们的严重性和潜在影响。然后，开发和实施修复措施，以消除这些漏洞。

漏洞数据库更新：定期更新漏洞扫描工具的漏洞数据库，以包括新发现的漏洞。这确保了扫描工具能够识别最新的安全威胁。

合规性检查：将漏洞扫描结果与行业标准和最佳实践进行比较，以确保网络系统的配置符合安全要求。

* + 1. **网络访问控制**

项目的网络访问控制主要根据用户网内现有的防火墙，实现网络访问控制与网络攻防范的能力，主要包括：

防火墙策略：部署防火墙作为网络的第一道防线，实施基于角色的访问控制策略。这些策略定义了哪些用户和设备可以访问特定的网络资源。

白名单机制：采用白名单机制，只允许已知和信任的设备和用户访问网络。这种机制可以有效地阻止未知和潜在的恶意访问。

实时监控与响应：通过网络入侵防御系统（NIDS）和网络入侵防护系统（NIPS），实时监控网络流量，并对可疑行为进行自动响应。这包括阻断恶意流量、隔离受感染的设备和通知管理员。

定期审计与更新：定期审计访问控制策略和防火墙规则，确保它们仍然符合当前的安全需求。同时，及时更新防火墙和入侵检测系统，以应对新的威胁。

* + 1. **网络入侵检测**

项目的网络入侵检测主要根据用户现有的入侵检测设备进行网络入侵防护能力的建设，主要包括以下内容：

全面的流量监控：部署入侵检测系统（IDS）和入侵防护系统（IPS），以监控所有进入和离开网络的流量。这些系统能够检测已知的攻击模式和异常行为。

实时分析与响应：对监控到的流量进行实时分析，以识别潜在的攻击。一旦检测到攻击，系统可以自动采取响应措施，如阻断恶意流量、隔离受感染的设备或通知管理员。

攻击模式更新：定期更新入侵检测系统的攻击模式数据库，以识别新的威胁。这确保了系统能够检测到最新的攻击手段。

日志记录与审计：记录所有安全事件的详细日志，包括攻击的时间、来源、目标和采取的响应措施。这些日志对于事后分析和取证至关重要。

* + 1. **网络接入安全**

网络接入安全是确保只有授权设备能够连接到网络的过程。通过实施严格的接入控制措施，可以防止未授权设备接入网络，减少安全风险。

端口安全策略：在网络交换机上实施端口安全策略，如端口隔离、端口安全和动态VLAN分配。这些策略限制了哪些设备可以接入网络。

MAC地址过滤：在网络接入点实施MAC地址过滤，只允许已知和信任的设备的MAC地址接入网络。这可以防止未授权设备接入网络。

无线网络安全：对于无线网络，实施WPA2或WPA3等强加密标准，并定期更改无线网络的密码。这可以防止未授权用户接入无线网络。

* + 1. **网络链路加密**

网络链路加密是保护数据在传输过程中不被窃听或篡改的关键技术。项目根据用户网内现有的千兆IP网络密码机对重要及涉密数据的远程传输提供加密保护通过加密链路，可以确保数据的机密性和完整性，即使数据在传输过程中被截获，也无法被解读。

加密技术选择：选择强大的加密算法和协议，如IPSec或SSL/TLS，来保护网络链路。这些协议提供了强大的加密和认证机制，确保数据传输的安全性。

端到端加密：在网络的端点，如服务器和客户端，部署加密设备或软件，以实现端到端的加密。这确保了数据在传输过程中的每一步都受到保护。

密钥管理：实施严格的密钥管理策略，定期更换密钥，并确保密钥的安全存储和分发。这有助于防止密钥泄露导致的安全风险。

性能与安全平衡：在选择加密解决方案时，平衡安全性和网络性能。虽然加密可能会增加网络延迟，但通过优化加密算法和硬件加速，可以最小化这种影响。

通过这些措施，网络链路加密为网络数据传输提供了一个安全的通道，保护了数据不被未授权访问。

* 1. **应用安全**

应用安全设计主要包括应用身份鉴别、应用系统防护、系统运维管理部分。

* + 1. **应用身份鉴别**

项目的应用身份鉴别是确保只有授权用户能够访问应用系统的重要环节。通过实施统一的身份鉴别机制，可以有效地控制对应用系统的访问。

统一身份认证平台：利用用户已建的统一身份认证平台，整合现有的身份认证系统和终端认证设备，实现用户身份的集中管理。

多因素认证：采用多因素认证机制，结合密码、证书、生物识别等认证因素，提高身份验证的安全性。

单点登录（SSO）：实现单点登录机制，允许用户使用一套凭证访问多个应用系统，减少密码疲劳并提高用户体验。

集中用户管理：集中管理用户账户，包括账户的创建、修改、禁用和删除，确保账户信息的一致性和准确性。

访问控制：根据用户的角色和职责，实施细粒度的访问控制策略，确保用户只能访问其授权的资源。

证书管理：提供证书的签发、撤销和备份功能，确保证书的生命周期管理。

自动锁定机制：当应用系统检测到未认证的用户尝试访问时，自动退出或锁定用户会话，防止未授权访问。

* + 1. **应用系统防护**

项目的应用系统防护是保护应用系统免受恶意攻击和数据泄露的重要手段。通过实施一系列的防护措施，可以提高应用系统的安全性。

数据加密：在应用系统中启用SSL/TLS等加密协议，确保数据在传输过程中的机密性和完整性。

Web应用防火墙（WAF）：在Web服务器前部署Web应用防火墙，防御SQL注入、跨站脚本攻击、网页内容篡改等常见的Web攻击。

输入验证：对用户输入进行严格的验证，防止恶意输入导致的安全问题，如注入攻击。

输出编码：对输出数据进行编码，防止跨站脚本攻击。

定期安全扫描：定期对应用系统进行安全扫描，发现并修复安全漏洞。

安全配置：确保应用系统的配置符合安全最佳实践，如关闭不必要的服务和端口。

* + 1. **系统运维管理**

项目的系统运维管理是确保应用系统稳定运行和数据安全的重要环节。通过实施严格的运维管理措施，可以提高应用系统的可靠性和安全性。

职责分离：实施管理员、安全员、审计员三权分立的职责划分，确保不同角色之间的职责相互制衡，防止权限滥用。

最小权限原则：遵循最小权限原则，确保运维人员只拥有完成其任务所必需的最小权限。

操作审计：记录所有运维操作的详细日志，包括操作的时间、地点、操作人员等信息，以便在发生安全事件时进行追踪和分析。

定期安全培训：对运维人员进行定期的安全培训，提高他们的安全意识和操作技能。

变更管理：实施严格的变更管理流程，确保所有变更都经过审批和测试，防止未经授权的变更。

备份和恢复：定期对应用系统和数据进行备份，并确保备份数据的安全性。同时，制定数据恢复计划，以便在数据丢失或损坏时能够迅速恢复。

应急响应：制定应急响应计划，以便在应用系统遭受攻击或发生故障时能够迅速响应。

* 1. **数据安全**

数据安全设计主要包括数据集中存储、数据备份安全和数据存储加密、数据访问鉴权四部分。

* + 1. **数据安全备份**

项目的数据安全备份主要利用现有的存储设备，提供数据本地备份的能力，实现数据热备、冷备、数据快照等功能，自动备份存储设备中的重要数据和敏感数据。

本地备份：提供数据的本地备份能力，确保在发生数据丢失或损坏时能够从备份中恢复。

自动备份：实施自动备份策略，定期备份集中存储设备中的重要数据和敏感数据。

快照功能：利用快照功能，定期创建数据的即时副本，以便于快速恢复。

备份验证：定期验证备份数据的完整性和可用性，确保在需要时能够成功恢复数据。

备份数据安全：确保备份数据的安全性，防止备份数据被未授权访问或破坏。

* + 1. **数据访问鉴权**

项目的数据访问权限主要根据数据平台来实现，通过对数据库、数据表、数据字段的访问限制，来完成不同密级数据的不同访问策略。

服务限制：关键数据库和大数据平台仅向授权的应用系统提供服务，屏蔽终端用户的直接数据服务请求。

数据库审计：部署数据库审计系统，实时记录数据库访问活动，对数据库操作进行细粒度的审计。

合规性管理：通过对数据库操作的审计，实施合规性管理，确保所有数据访问行为符合政策和法规要求。

认证鉴权：对所有数据访问、调阅和下载等操作实施认证鉴权，确保只有授权用户能够进行这些操作。

风险行为告警：对数据库遭受的风险行为进行实时告警，以便及时响应和处理。

行为分析：对用户访问数据库的行为进行记录、分析和汇报，帮助事后生成合规报告和事故追根溯源。

* + 1. **数据存储加密**

项目的数据存储加密主要利用用户现有的存储加密机，将数据信息以密文的形式存储在存储设备中，对重要涉密数据进行存储加密保护，提升数据存储的安全性。

加密机制：利用网络存储密码机或其他加密设备，对存储在设备中的数据进行加密。

密文存储：确保数据以密文形式存储，即使数据被未授权访问，也无法被解读。

加密策略：制定严格的加密策略，包括加密算法的选择、密钥的管理等。

* + 1. **数据集中存储**

项目的数据存储是利用用户现有的存储设备，将采集上报的在数据中心统一存储。

集中存储设备部署：利用现有的存储设备，建立一个集中的数据存储平台，用于存储关键数据和敏感信息。

数据整合：将分散在不同系统和位置的数据整合到集中存储设备中，以便于管理和监控。

数据可用性：通过实施数据集中存储，提高数据的可用性，确保在需要时能够快速访问数据。

存储优化：对存储设备进行优化，包括存储空间的分配、数据的索引和检索，以提高数据访问效率。

访问控制：实施严格的访问控制措施，确保只有授权用户和系统能够访问集中存储的数据。

* 1. **安全管理**

安全管理设计主要包括组织机构、规章制度、管理实施、安全资产管理等四个部分。

* + 1. **组织机构**

为了确保系统的安全性，需要建立一个多层次的安全管理组织结构。

安全管理领导机构：成立一个专门的安全管理领导机构，负责制定安全政策、监督安全措施的实施，并在必要时提供决策支持。

技术管理人员：配备专业的系统安全保密技术管理人员，他们负责执行具体的安全保密技术措施，确保系统的安全运行。

应急响应体系：建立一个完善的应急响应体系，以便在突发事件发生时能够迅速有效地应对，减少潜在的损失。

通过这些组织机构的建立，可以确保安全管理工作的有序进行，提高系统的整体安全性。

* + 1. **规章制度**

制定一系列规章制度，以规范安全管理行为，确保系统的安全性。

备份制度：建立日常系统备份制度，确保关键数据的定期备份，以及备份数据的安全性和可恢复性。

存储载体使用管理制度：制定存储载体使用管理制度，规范存储设备的使用，防止数据泄露或丢失。

脆弱性分析规程：建立脆弱性分析规程，定期对系统进行脆弱性评估，及时发现并修复安全漏洞。

通过这些规章制度的制定和执行，可以提高安全管理的规范性，减少安全风险。

* + 1. **管理实施**

具体的管理实施是确保安全措施得到有效执行的关键。

安全保密策略文档：制定与实际情况相符且完整的安全保密策略文档，详细记录安全保密技术和产品的配置。

安全审计：安全保密技术管理人员应对每日网络和系统运行情况进行安全审计，确保系统的安全运行。

安全性检测：每季度组织本级网络的安全性检测，编写安全审计与评估报告，并形成记录。

系统配置变更管理：在系统配置发生变化的情况下，应及时组织安全检测评估，确保变更不会引入新的安全风险。

* + 1. **安全资产管理**

项目通过采购的泰合信息安全运营中心系统，可以实现对网络安全设备的集中管理和监控，包括天清Web应用安全网关和天玥数据库审计系统等。系统提供了以下功能：

集中资产管理：实现对网内安全设备的统一策略下发和管控，包括设备升级、日志备份等配置操作功能。支持对安全设备的状态、型号、版本、端口状态、功能模式等信息的查看。

运行监控：监控总览界面包括事件数量和安全设备连接状态，支持事件实时监控和关联分析功能，具备分析事件的起源设备、目标设备、及其所经过的保护设备，匹配的规则、关联的其他事件等综合分析能力。

告警信息管理：支持监控未知设备接入的实时告警，迅速发现系统中存在的非法接入，支持对违法使用USB存储设备的报警。

安全设备集中管理：通过对相应设备和系统管理模块进行授权，开启不同安全设备和系统的管理功能。在配置维护操作过程中只需要一键进入相应的管理模块，即可对相应安全设备和系统进行系统配置、拓扑管理、设备状态监控等。

* 1. **系统软件安全**
     1. **系统级安全**

系统级安全措施包括：访问IP段的限制，登录时间段的限制，连接数的限制，特定时间段内登录次数的限制等；对于重要敏感数据采用HTTPS协议可进行128位加密传输，实现基于SSL的安全访问；系统级安全保障措施是平台的第一道防护大门。

SSL(加密套接字协议层)位于HTTP层和TCP层之间，建立用户与服务器之间的加密通信，确保所传递信息的安全性。SSL是工作在公共密钥和私人密钥基础上的，任何用户都可以获得公共密钥来加密数据，但解密数据必须要通过相应的私人密钥。使用SSL安全机制时，首先客户端与服务器建立连接，服务器把它的数字证书与公共密钥一并发送给客户端，客户端随机生成会话密钥，用从服务器得到的公共密钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器，而会话密钥只有在服务器端用私人密钥才能解密，这样，客户端和服务器端就建立了一个唯一的安全通道。

* + 1. **程序资源访问控制安全**

程序资源访问控制分为客户端和服务端两个层面，类似于表单数据校验分为服务端和客户端校验两个层面。

对程序资源的访问进行安全控制，在客户端上，为用户提供和其权限相关的用户界面，仅出现和其权限相符的菜单，操作按钮；在服务端则对URL程序资源和业务服务类方法的调用进行访问控制。

在系统中，需要指定各个应用层次中的每一个用户所能够访问的业务资源和系统资源，亦即访问控制和权限分配策略。

这里的权限不但包括用户能否访问的业务范围、业务数据、数据的访问方式、操作类型等，还包括系统相关的系统资源。通常情况下，系统中的权限按照角色进行分配，亦即对所有权限进行分组，一个角色将对应于一个权限的组合。这样在对用户进行权限分配的时候，只需要直接赋予用户不同的角色即可。

访问控制技术是在保护资源安全的前提下实现资源共享，以访问控制表的形式来规定主体(如用户)对客体(如文件、数据库、设备)的访问权限(如可读、可写)。在文件系统、数据库系统、设备管理、WWW等之中，都采用访问控制技术来控制用户访问权限。还可以通过IP地址控制和端口的控制来加强访问控制。

* + 1. **身份认证安全**

用户身份认证一般发生于用户登录系统时或者与其它应用支撑系统之间传递数据时的情况。在用户登录系统时，需要对登录用户持有的数字证书进行认证，以保证只有合法持有有效数字证书的用户才能够登录系统，同时还需要进行安全审计和记录系统安全日志。对于发生在教务管理工作中的业务流程跳转、请求发生变化等情况产生的身份认证问题，可以视同不同用户的登录或同一用户对平台不同部分的访问以及相应的用户数字证书认证过程。在平台与其它应用支撑系统之间传递数据的时候，数字校园数据交换与信息发布服务器之间也需要进行身份认证以保证发送和接收数据主体的合法性。

* + 1. **安全加密技术**

系统采用了包括数据加密与解密、数据摘要及验证、数字签名及验证、时间戳加盖及验证等在内的安全技术保证系统的安全性、完整性和不可否认性。

数据加密的方法划分为对称加密和非对称加密两种，典型的加密方法包括自定义加密算法、MD5加密算法、RSA加密算法等。数据加密主要用于保证数据存储或者传输的安全性，防止窃取。数据摘要方法主要包括MD、SHA等，通常具有两个特点，其一是对于源数据的任何一个Bit的改变，数据摘要将有很大改变，其二是源数据不同，对应的数据摘要则不同。因此通过对源数据产生8字节的摘要信息并连同源数据一起传输，然后通过对数据摘要的验证能够有效检测和防止数据非法篡改，保证数据的完整性。数字签名方法主要包括DSA方法等，数据的发送方利用自己的私有签名密钥对源数据对应的数据摘要进行签名，保证数据发送方的合法性，同时防止抵赖，数字签名的使用依赖于公正的认证中心CA所发放的合法的、有效的数字证书。时间戳加盖是对传递的数据包加入时间戳标志，数据的接收方能够根据时间戳标志进行数据操作顺序的判断并进行数据包的重新组织，这种方法一定程度上可以防止旁路重发所带来的风险。

对于十分重要的数据，系统采用了DES或FWZ1及散列算法(MD5)等加密算法，DES和FWZ1可同时配置，用户依据效率、安全性和传输速度选择最佳方式。每一个加密通信将产生一对高度保密的公共和专有密钥，利用SRA技术，实现通信的确认授权。为了防止黑客(非法用户)通过网络监听或者截取用户登录系统的数据包，系统采用了散列算法(MD5)加密方式，在服务器端预置散列函数，用户在客户端登录时，散列函数自动将数据加密，产生128位的数据包，即使非法用户截获数据包，也不可能通过黑客工具解密，建立较高的系统数据安全机制。

* + 1. **数据域安全**

数据域安全包括两个层次，其一是行级数据域安全，即用户可以访问哪些业务记录，一般以用户所在单位为条件进行过滤；其二是字段级数据域安全，即用户可以访问业务记录的哪些字段。

对于系统的权限，可以细致到一个程序文件（超链接），对每类角色用户甚至每个用户可将权限配置到按钮级，部分功能可设置到数据级，以此对前端用户进行有效的数据安全授权管理。

* + 1. **安全日志和审计**

系统利用安全日志记录和审计，以保证在发生安全相关问题的时候能够做到追踪问责，通过对安全日志记录的查询和分析以及相关的审计操作找到安全问题的根源所在。安全日志和审计的范围根据系统的实际需要进行设置，但是对于安全密切相关的用户登录事件、访问控制事件以及身份认证、访问控制、数据加密、数字签名等行为安全事件等应该进行安全审计操作，并记录系统安全日志。

安全审计是一个安全的网络必须支持的功能特性，审计(日志管理)是记录用户使用平台进行所有活动的过程，它是提高安全性的重要工具。本系统提供了详细的安全审计功能，它不仅能够识别谁访问了系统，还能指出系统正被怎样地使用。对于确定是否有网络攻击的情况，审计信息，确定问题和攻击源很重要。同时，系统事件的记录能够更迅速和系统地识别问题，并且它是后面阶段事故处理的重要依据，为网络犯罪行为及泄密行为提供取证基础。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据、防范措施。

* + 1. **其它安全策略**

1、在可以进行数据导入、附件上传的功能模块中，对所有上传文件的扩展名在客户端和服务端都进行严格的判断，自动筛查可执行文件，防止木马、病毒程序的上传。

2、所有上传文件不允许直接在浏览器中直接打开，文件上传后，系统自动以数据流的方式加密文件名，客户端进行下载时自动解密，防止通过文件上传木马。

3、所有客户端文本输入时过滤< ></>，eval等相关脚本代码，防止SQL注入。

4、对于选课处理，成绩处理，分配权限时，强制要求启用usb-key加密狗功能，脚本异常时无法操作，保障系统关键模块的安全。

5、系统在任何时候都不暴露错误信息给客户，提供友好信息给客户，防止非法用户通过错误信息发现系统漏洞。

6、数据库连接地址采用DES加密，防止数据库地址的泄露；传递参数时如果是通过脚本传递，则采用脚本异或加密与HASH校验，防止传输过程中脚本被篡改。

7、后续将提供操作系统级的系统安全监控服务，包括：可视化的监控系统端口的开放情况、监控教务软件防篡改、发现异常时自动记录并通过短信或邮件通知等。

* 1. **保密性与安全设计**

网络安全保密系统是业务信息系统的基石，它不仅为整个信息系统提供全面的安全防护，而且其自身也具备高度的安全特性，能够有效地抵御各种网络攻击。在设计上，保密性主要从两个方面进行考虑：一是面向业务信息系统的安全防护，二是系统自身安全防护的能力。

* + 1. **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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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，严格注意防止其他组织或他人以“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。

* + - 1. 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。

* + - 1. 保密管理制度
         1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + 1. **安全架构设计**
       1. 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。

* + - 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - 1. 安全技术方案设计
         1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + 1. **系统信息安全设计**

本安全方案的目标是支撑和保障数据中心和业务系统的安全稳定运行，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。

* + - 1. 信息安全体系结构
         1. 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。

* + - * 1. 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。

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。

* + - * 1. 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。

* + - 1. 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，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。

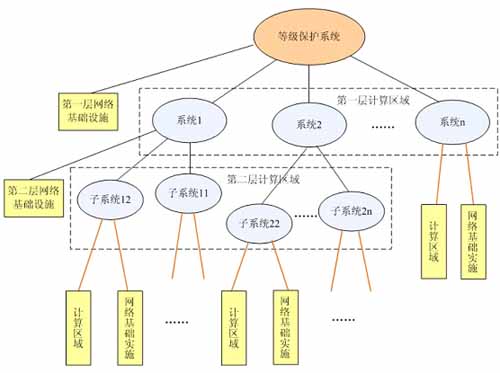


图 系统安全保护对象框架

* + - 1. 系统安全设计思路
         1. 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。

* + - * 1. 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。

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。

* + - * 1. 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）。

* + - * 1. 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。

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。

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。

* + - * 1. 安全措施选择

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。

* + - * 1. 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 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。

* + - * 1. 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。

* + - 1. 安全培训

安全意识教育和培训做到以下方面的内容：

应知应会要求：应让本项目相关员工知晓信息的敏感性和信息安全的重要性，认识其自身的责任和安全违例会受到纪律惩罚，以及应掌握的信息安全基本知识和技能等；

有计划培训：制定并实施安全教育和培训计划，根据不同培训对象的需要，每季度或每半年进行安全培训，培养本项目各类人员安全意识，并提供对安全政策和操作规程的认知教育和训练等；

针对不同岗位培训：针对不同岗位，制定不同的专业培训计划，包括安全知识、安全技术、安全标准、安全要求、法律责任和业务控制措施等；

按人员资质要求培训：对所有工作人员的安全资质进行定期检查和评估，使相应的安全教育成为组织机构工作计划的一部分；

培养安全意识自觉性：对所有工作人员进行相应的安全资质管理，并使安全意识成为所有工作人员的自觉存在。

* + 1. **容灾和备份方案**
       1. 备份方式设计

应支持7\*24业务不中断的原则，因此，备份方式采用在线备份方式。在线备份系统设计将在设备级FC-SAN存储的基础上，通过设置不同的资源池，通过数据镜像技术，以逻辑卷的方式，将高端存储资源池的数据镜像至备份存储资源池，从而保证存储数据的高可用。 存储系统的数据镜像复制包括同步，异步两种方式。本次项目将两者结合使用。根据业务数据重要程度和影响范围定义，重要业务采用同步方式镜像。

同步方式可以保证完全实时的数据复制，但受到距离的限制，而且可能带来较高的实施成本。异步方式相比同步方式，可以在更广的距离范围内实现数据复制，实施成本较低，且能保证数据一致性，但在灾难发生时需要承担一定的数据损失。

与同步复制方式相比，异步复制方式对带宽和距离的要求低很多，而且基本不影响本地生产系统性能。

* + - 1. 备份策略设计

备份策略参照国家安全等级保护相应要求，采用每天增量，每周全备份，数据保留3个月的备份策略。备份对象与备份策略如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 备份对象 | 备份单位 | 备份策略 | 备份路径 | 备份时间 |
| FC-SAN | LUN | 差异备份 | 以实际为主 | 每天凌晨  2：00 |
| 分布式存储 | OSD | 差异备份 | 以实际为主 | 每天凌晨  2：00 |
| 数据库 | backup文件 | 差异备份 | 以实际为主 | 每天凌晨  2：00 |
| 虚拟机镜像 | ISO等云格式文件 | 全备份 | 以实际为主 | 周六2：00 |
| 虚拟机数据 | VM数据 | 差异备份 | 以实际为主 | 每天凌晨  2：00 |
| 云平台系统配置 | 配置文件 | 全备份 | 以实际为主 | 周六2：00 |

1.全备模式优点是：当发生数据丢失时，只要用一盘磁带（即灾难发生前一天的备份磁带）就可以恢复丢失的数据。它也有不足之处：首先，由于每天都对整个系统进行完全备份，难免造成备份数据大量重复。这些重复的数据占用了大量的磁带空间。其次，如果备份的数据量很大，那么备份所需的时间也就较长。对于一些业务繁忙、备份时间有限的单位来说，选择这种备份策略是不明智的。

2.增量备份是以上次备份为基准，只对变动的数据进行备份。这种备份策略的优点是：只备份当天更新或者增加的数据，因而数据量小，节省了磁带空间，缩短了备份时间。当然，它也是有缺点的。备份的可靠性也很差。在这种备份方式下，各个备份间的关系就像一个链子，环环相扣，其中任何一个备份出了问题都会导致整条链子脱节。

3.差异备份是以完全备份为基准，对变动的数据进行备份。差异备份方式避免了上面两种备份策略的缺陷，同时，又具有以上两种备份方式的所有优点。

* + - 1. 数据备份过程

在整个系统之中，提供自动策略备份方式，自动将数据备份到备份服务器上，采用指定的加密或压缩方式保存到先前指定的介质中。

对于定时备份而言，在备份结束后，系统会报告备份的状况，然后，系统管理员就可在Web监控管理界面上清楚地看到已经备份的数据的描述，也可按需要生成作业报表。定时备份对数据的备份采用的是在线备份，通过客户端备份代理，可以在不停止数据库、不关闭正在使用的文件的情况下，对数据库、应用文件数据进行备份，而对虚拟系统的备份，采用无代理备份方式，直接抽取有效收据进行备份。

* + - 1. 数据恢复过程

当发生数据损坏时，需要从存储介质中恢复数据。通过Web监控管理界面，恢复数据库、应用文件数据和虚拟操作系统、物理操作系统。

定时备份的数据，可以选择任意的时间点进行恢复操作，无论是完全备份、增量备份或者日志备份，都能一步到位恢复数据（无需先恢复完全备份时间点，再恢复增量或差异备份时间点）。

* + 1. **应急管理方案**
       1. 应急预案与流程

a. 预案制定

识别潜在风险：对运营过程中可能出现的风险进行全面识别，这包括但不限于自然灾害、技术故障、供应链中断、人为错误等。

风险评估：对识别出的风险进行评估，确定其可能性和影响程度，以便为后续的预案制定提供依据。

预案编写：针对每种风险，编写详细的应急预案。预案应包括应急响应的触发条件、响应流程、责任人、资源需求、通信联络和信息报告等方面的内容。

b. 流程设计

明确响应流程：设计清晰、简洁的应急响应流程，确保在紧急情况下能够迅速启动应急响应。

建立指挥体系：明确应急响应的指挥体系和各级指挥人员的职责，确保指挥畅通、决策迅速。

资源调配：设计资源调配流程，包括人力、物力、财力等资源的调配和使用。

* + - 1. 应急组织与人员

a. 组织建设

成立应急响应小组：成立专门的应急响应小组，负责应急预案的制定、更新和实施。

明确组织架构：明确应急响应小组的组织架构和各部门、各岗位的职责分工。

b. 人员培训与演练

培训：定期对应急响应人员进行培训，提高其应急意识和技能水平。培训内容包括但不限于应急预案、应急设备使用、紧急情况下的自救互救等。

演练：定期组织应急演练，模拟真实场景下的紧急情况，检验应急预案的可行性和有效性。演练后应及时进行总结和评估，针对发现的问题进行改进。

* + - 1. 数据备份与恢复

数据备份策略：制定详细的数据备份策略，包括备份频率、备份方式、备份存储位置等。

数据恢复计划：制定详细的数据恢复计划，明确恢复步骤、所需时间和资源等。同时，应定期进行数据恢复演练，以验证备份数据的可用性和恢复计划的可行性。

* + - 1. 通信与信息保障

建立通信联络机制：建立多种通信联络机制，包括固定电话、移动电话、电子邮件、即时通讯工具等，确保在紧急情况下能够迅速联系到相关人员。

信息发布与更新：建立信息发布和更新机制，通过内部网站、公告板、短信等方式及时向员工发布紧急信息和更新情况。

* + - 1. 风险评估与持续改进

定期风险评估：定期对运营环境和业务流程进行风险评估，识别新的潜在风险和脆弱性。

持续改进：根据风险评估结果和应急演练的反馈，对应急预案进行持续改进和优化。同时，应关注新技术和新方法的发展，及时将其应用于应急技术方案中。

* + - 1. 合规与监管

确保合规性：确保应急技术方案符合相关法律法规和标准要求。这包括但不限于安全生产法、消防法、环境保护法等。

加强与监管机构的沟通：定期与监管机构进行沟通，了解其对应急管理的最新要求和指导意见，及时将相关信息传达给用户内部相关部门。

监管与评估：定期对自身的应急管理工作进行监管和评估，确保其有效性并符合法律法规的要求。这可以通过内部审查、外部审计或第三方评估等方式实现。

* 1. **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。

* + 1. 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。

* + 1. 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。

* + 1. 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。

* + 1. 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。

* + 1. 保密管理制度
       1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* 1. **保密组织架构与人员配置**
     1. ‌三级保密管理体系**‌**

‌保密委员会‌：由分管副职领导牵头，整合教育、技术、保卫等部门负责人，负责审批涉密信息分级、年度保密工作计划及重大事项决策13。

‌专职保密办公室‌：配置2名以上具备军队保密资质的专职人员，负责日常监督检查、技术风险评估及应急预案演练。

‌科室保密岗‌：指定1名技术军官担任保密联络员，负责设备使用登记、存储介质管控及异常行为上报。

‌人员准入机制‌

涉密人员上岗前需通过政治审查、保密知识考试（合格线90分）及心理健康评估，并签署《保密承诺书》。

建立涉密岗位动态调整机制，对借调人员、外包技术人员实行“临时涉密资格认证”。

* + 1. ‌保密管理制度规范

**‌物理空间管控**‌

执行“三铁一器”标准：安装防爆铁门、金属格栅窗、密码文件柜及红外报警系统，电磁屏蔽等级达到GJB5792-2006要求。

涉密教学设备（如战术推演系统）单独设置屏蔽机房，与非涉密区域物理隔离，门禁系统记录精确到0.1秒。

**‌数据全流程管理**‌

存储：使用国产加密固态硬盘（GM/T 0028标准），禁止外接存储设备，涉密文件柜实行双人双锁管理。

传输：教学数据通过军营专网双向加密传输（国密SM4算法），禁止使用无线投屏、云同步功能。

销毁：过期数据由保密办公室双人操作，采用NSA认证的消磁设备处理，留存销毁视频记录备查。

**‌行为监管制度**‌

实行“四严禁”：严禁私携智能设备入室、严禁截屏录屏、严禁未授权数据导出、严禁非涉密终端接入。

部署DLP系统监控屏幕信息，对涉密课件内容自动模糊处理。

* + 1. ‌保密培训机制

采用“理论+实操”双轨制考评，涉密人员年审不合格者暂停权限，累计2次不通过调离岗位。

建立培训档案数字化管理系统，与晋升评优挂钩。

* 1. **安全架构设计**
     1. 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。

* + 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + 1. 安全技术方案设计
       1. 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。

* + - 1. 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。

* + - 1. 网络安全
         1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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

* + - * 1. 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。

* + - * 1. 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。

* + - 1. 数据安全
         1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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

* + - * 1. 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。

* + 1. 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。

* + - 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* + - 1. 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。

* 1. 系统信息安全设计

本安全方案的目标是支撑和保障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。

* + 1. 信息安全体系结构
       1. 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。

* + - 1. 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。

文本

低可信度描述已自动生成

信息安全体系结构

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - 1. 安全体系设计依据
         1. 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

* + - * 1. 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。

* + 1. 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。

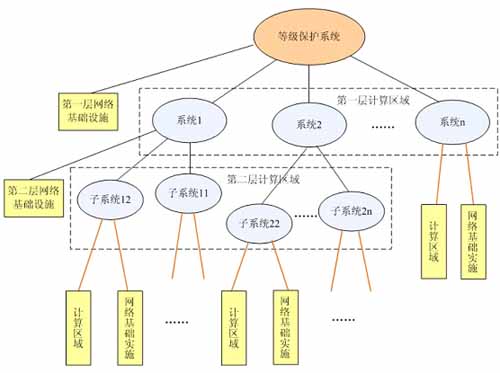


图 1 系统安全保护对象框架

* + 1. 系统安全设计思路
       1. 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。

* + - 1. 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。

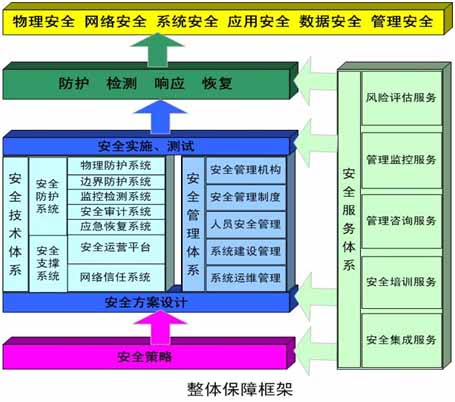


图 2 信息安全整体保障框架

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。

* + - 1. 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）。

* + - 1. 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。

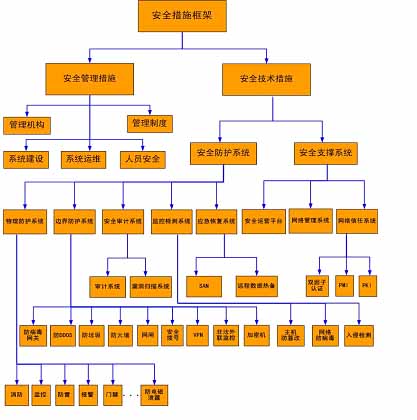


图 3 安全措施框架

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。

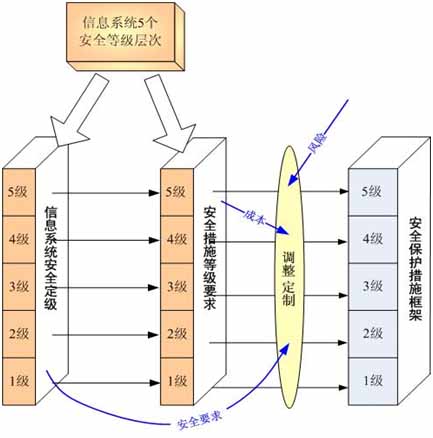


图 4 信息系统安全措施选择

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。

* + - 1. 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。

* + - 1. 安全技术体系设计
         1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - 1. 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：

* + - * 1. 安全管理制度

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

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

信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，定期或不定期对安全管理制度进行评审和修订，修订不足及进行改进。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* + - * 1. 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。

* 1. 容灾和备份方案
     1. 备份方式设计

应支持7\*24业务不中断的原则，因此，备份方式采用在线备份方式。在线备份系统设计将在设备级FC-SAN存储的基础上，通过设置不同的资源池，通过数据镜像技术，以逻辑卷的方式，将高端存储资源池的数据镜像至备份存储资源池，从而保证存储数据的高可用。 存储系统的数据镜像复制包括同步，异步两种方式。本次项目将两者结合使用。根据业务数据重要程度和影响范围定义，重要业务采用同步方式镜像。

同步方式可以保证完全实时的数据复制，但受到距离的限制，而且可能带来较高的实施成本。异步方式相比同步方式，可以在更广的距离范围内实现数据复制，实施成本较低，且能保证数据一致性，但在灾难发生时需要承担一定的数据损失。

与同步复制方式相比，异步复制方式对带宽和距离的要求低很多，而且基本不影响本地生产系统性能。

* + 1. 备份策略设计

备份策略参照国家安全等级保护相应要求，采用每天增量，每周全备份，数据保留3个月的备份策略。备份对象与备份策略如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 备份对象 | 备份单位 | 备份策略 | 备份路径 | 备份时间 |
| FC-SAN | LUN | 差异备份 | 以实际为主 | 每天凌晨  2：00 |
| 分布式存储 | OSD | 差异备份 | 以实际为主 | 每天凌晨  2：00 |
| 数据库 | backup文件 | 差异备份 | 以实际为主 | 每天凌晨  2：00 |
| 虚拟机镜像 | ISO等云格式文件 | 全备份 | 以实际为主 | 周六2：00 |
| 虚拟机数据 | VM数据 | 差异备份 | 以实际为主 | 每天凌晨  2：00 |
| 云平台系统配置 | 配置文件 | 全备份 | 以实际为主 | 周六2：00 |

1.全备模式优点是：当发生数据丢失时，只要用一盘磁带（即灾难发生前一天的备份磁带）就可以恢复丢失的数据。它也有不足之处：首先，由于每天都对整个系统进行完全备份，难免造成备份数据大量重复。这些重复的数据占用了大量的磁带空间。其次，如果备份的数据量很大，那么备份所需的时间也就较长。对于一些业务繁忙、备份时间有限的企业来说，选择这种备份策略是不明智的。

2.增量备份是以上次备份为基准，只对变动的数据进行备份。这种备份策略的优点是：只备份当天更新或者增加的数据，因而数据量小，节省了磁带空间，缩短了备份时间。当然，它也是有缺点的。备份的可靠性也很差。在这种备份方式下，各个备份间的关系就像一个链子，环环相扣，其中任何一个备份出了问题都会导致整条链子脱节。

3.差异备份是以完全备份为基准，对变动的数据进行备份。差异备份方式避免了上面两种备份策略的缺陷，同时，又具有以上两种备份方式的所有优点。

* + 1. 数据备份过程

在整个系统之中，提供自动策略备份方式，自动将数据备份到备份服务器上，采用指定的加密或压缩方式保存到先前指定的介质中。

对于定时备份而言，在备份结束后，系统会报告备份的状况，然后，系统管理员就可在Web监控管理界面上清楚地看到已经备份的数据的描述，也可按需要生成作业报表。定时备份对数据的备份采用的是在线备份，通过客户端备份代理，可以在不停止数据库、不关闭正在使用的文件的情况下，对数据库、应用文件数据进行备份，而对虚拟系统的备份，采用无代理备份方式，直接抽取有效收据进行备份。

* + 1. 数据恢复过程

当发生数据损坏时，需要从存储介质中恢复数据。通过Web监控管理界面，恢复数据库、应用文件数据和虚拟操作系统、物理操作系统。

定时备份的数据，可以选择任意的时间点进行恢复操作，无论是完全备份、增量备份或者日志备份，都能一步到位恢复数据（无需先恢复完全备份时间点，再恢复增量或差异备份时间点）。

* 1. 应急管理方案
     1. 应急预案与流程

a. 预案制定

识别潜在风险：对运营过程中可能出现的风险进行全面识别，这包括但不限于自然灾害、技术故障、供应链中断、人为错误等。

风险评估：对识别出的风险进行评估，确定其可能性和影响程度，以便为后续的预案制定提供依据。

预案编写：针对每种风险，编写详细的应急预案。预案应包括应急响应的触发条件、响应流程、责任人、资源需求、通信联络和信息报告等方面的内容。

b. 流程设计

明确响应流程：设计清晰、简洁的应急响应流程，确保在紧急情况下能够迅速启动应急响应。

建立指挥体系：明确应急响应的指挥体系和各级指挥人员的职责，确保指挥畅通、决策迅速。

资源调配：设计资源调配流程，包括人力、物力、财力等资源的调配和使用。

* + 1. 应急组织与人员

a. 组织建设

成立应急响应小组：成立专门的应急响应小组，负责应急预案的制定、更新和实施。

明确组织架构：明确应急响应小组的组织架构和各部门、各岗位的职责分工。

b. 人员培训与演练

培训：定期对应急响应人员进行培训，提高其应急意识和技能水平。培训内容包括但不限于应急预案、应急设备使用、紧急情况下的自救互救等。

演练：定期组织应急演练，模拟真实场景下的紧急情况，检验应急预案的可行性和有效性。演练后应及时进行总结和评估，针对发现的问题进行改进。

* + 1. 应急资源与设施

应急设备：储备必要的应急设备，如备用电源、应急照明、消防器材等。

应急物资：储备必要的应急物资，如食品、水、药品等，以满足紧急情况下的基本生活需求。

* + 1. 数据备份与恢复

数据备份策略：制定详细的数据备份策略，包括备份频率、备份方式、备份存储位置等。

数据恢复计划：制定详细的数据恢复计划，明确恢复步骤、所需时间和资源等。同时，应定期进行数据恢复演练，以验证备份数据的可用性和恢复计划的可行性。

* + 1. 通信与信息保障

建立通信联络机制：建立多种通信联络机制，包括固定电话、移动电话、电子邮件、即时通讯工具等，确保在紧急情况下能够迅速联系到相关人员。

信息发布与更新：建立信息发布和更新机制，通过企业内部网站、公告板、短信等方式及时向员工发布紧急信息和更新情况。

* + 1. 风险评估与持续改进

定期风险评估：定期对企业的运营环境和业务流程进行风险评估，识别新的潜在风险和脆弱性。

持续改进：根据风险评估结果和应急演练的反馈，对应急预案进行持续改进和优化。同时，应关注新技术和新方法的发展，及时将其应用于应急技术方案中。

* + 1. 合规与监管

确保合规性：确保应急技术方案符合相关法律法规和标准要求。这包括但不限于安全生产法、消防法、环境保护法等。

加强与监管机构的沟通：定期与监管机构进行沟通，了解其对应急管理的最新要求和指导意见，及时将相关信息传达给企业内部相关部门。

监管与评估：定期对自身的应急管理工作进行监管和评估，确保其有效性并符合法律法规的要求。这可以通过内部审查、外部审计或第三方评估等方式实现。

* 1. **系统安全性设计**
     1. **传输层面安全**

平台只需简单设置即可支持SSL加密访问。SSL协议支持可以增强系统安全性，通过网络传递的数据均会使用RSA算法进行不对称加密，可以完全杜绝数据包被截获后泄密的可能性，加上第三方权威的CA（CertificateAuthority）认证支持，可以完全确保数据的传输安全。

* + - 1. DMZ区域+端口映射

解决安装[防火墙](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99" \t "_blank)后外部网络的访问用户不能访问内部[网络服务器](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)的问题，而设立的一个非[安全系统](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E7%B3%BB%E7%BB%9F" \t "_blank)与安全系统之间的缓冲区。该缓冲区位于内部网络和外部网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服务器[设施](https://baike.baidu.com/item/%E8%AE%BE%E6%96%BD" \t "_blank)，如Web服务器、[FTP服务器](https://baike.baidu.com/item/FTP%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部[网络](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C" \t "_blank)。通将移动应用服务器放置在DMZ区域，PC应用服务器放置在服务器区域，通过端口向外映射的方式进行对外通讯，仅开放一个端口，利用多重防火墙保护，系统策略设置方便；带宽占用相对较小，充分提高系统的外网与内网间访问的安全性。

* + - 1. SSL中间件生成

数据通过Https加密保证传输安全，SSL协议位于[TCP/IP协议](https://baike.baidu.com/item/TCP%2FIP%E5%8D%8F%E8%AE%AE" \t "_blank)与各种[应用层](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E5%B1%82" \t "_blank)协议之间，为[数据通讯](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E9%80%9A%E8%AE%AF" \t "_blank)提供安全支持。SSL协议可分为两层：SSL记录协议（SSLRecordProtocol）：它建立在可靠的[传输协议](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE" \t "_blank)（如TCP）之上，为高层协议提供[数据封装](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%B0%81%E8%A3%85" \t "_blank)、压缩、加密等基本功能的支持。SSL[握手协议](https://baike.baidu.com/item/%E6%8F%A1%E6%89%8B%E5%8D%8F%E8%AE%AE" \t "_blank)（SSLHandsh安可eProtocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行[身份认证](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E8%AE%A4%E8%AF%81" \t "_blank)、协商[加密算法](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95" \t "_blank)、交换加密[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5" \t "_blank)等。SSL(SecureSocketsLayer[安全套接层](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E5%A5%97%E6%8E%A5%E5%B1%82" \t "_blank)),及其继任者[传输层安全](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%B1%82%E5%AE%89%E5%85%A8" \t "_blank)（TransportLayerSecurity，TLS）是为[网络通信](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E9%80%9A%E4%BF%A1" \t "_blank)提供安全及[数据完整性](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%AE%8C%E6%95%B4%E6%80%A7" \t "_blank)的一种安全协议。TLS与SSL在[传输层](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%B1%82" \t "_blank)对网络连接进行加密，以确认文件、数据包、请求传输过程中的安全。

* + 1. **数据层面安全**
       1. 数据库加密

对数据库中的关键数据如账号密码、表单信息等关键信息进行加密，有效加密防止入侵者直接通过获取数据库文件，获得系统数据。

* + - 1. 数据文件加密

对于所有存储在磁盘中的文档资料从文件名称、文件内容都进行了加密，并且进行了分卷压缩，防止入侵者直接通过服务器磁盘获获取平台中的文档资料。

* + - 1. AES加密概述

AES加密过程是在一个4×4的字节矩阵上运作，这个矩阵又称为“体（state）”，其初值就是一个明文区块（矩阵中一个元素大小就是明文区块中的一个Byte）。加密时均包含4个步骤：

AddRoundKey—矩阵中的每一个字节都与该次回合金钥（roundkey）做XOR运算；每个子密钥由密钥生成方案产生。

SubBytes—通过个非线性的替换函数，用查找表的方式把每个字节替换成对应的字节。

ShiftRows—将矩阵中的每个横列进行循环式移位。

MixColumns—为了充分混合矩阵中各个直行的操作。这个步骤使用线性转换来混合每列的四个字节。

* + - 1. 程序代码加密

对于关键程序代码进行加密，让入侵者无法通过解读程序来了解数据读取存储方式和加密方式，防止入侵者通过解读程序来读取已经加密过的数据文件。

* + - 1. 数据防篡改

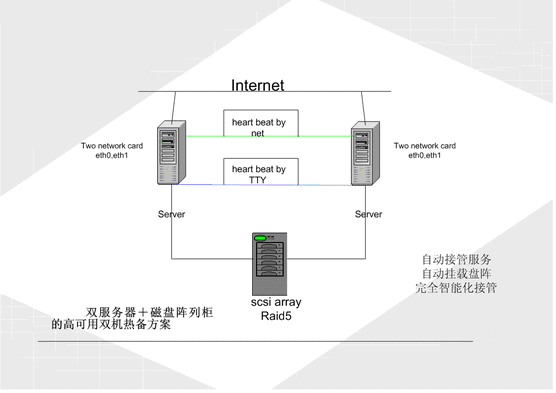
针对敏感数据（比如公文、流程、文档等），可以启用更高安全级别的保护，集成CA证书验证功能，防止数据被恶意篡改。

当存储数据时，会对数据利用CA证书生成数字签名，签名时会校验当前用户和签章是否匹配。如果是他人的签章，是无法执行签章和撤销签章的动作的。

当打开资源的时候会针对数据进行校验，检测数据有无被篡改，并给出相应的验证结果。

* + 1. **硬件层面安全**
       1. 双机热备

在应用平台时，为了避免由于服务器的原因宕机而造成系统的正式运行，可同时部署两套平台系统，相互之间可快速切换，即双机热备，由两台服务器+磁盘阵列柜构成双机热备系统，在两台服务器中安装所有的服务模块



由“两台服务器+共享磁盘阵列柜”构成高可用系统。通过系统的服务监测模块来互相监测对方的心跳及服务，服务监测模块通过网络和串口来定时监测对方心跳，该系统具有三种运行状态：

1.服务器A运行服务1，且在工作时使用磁盘阵列，服务器B运行服务2。

a)当服务器A出现故障时：

服务器B监测到服务器A出现故障，接管服务器A的IP地址，然后再mount上磁盘阵列,最后启动服务1。

b)当服务器B出现故障时：

服务器A监测到服务器B出现故障，监管服务器B的IP地址，然后启动服务2。

故障服务器恢复后，两台服务器又开始工作，回到状态1。

双机热备方案一般可直接由硬件提供商完成。

* + - 1. 不间断电源UPS

通过部署不间断电源UPS，保证必要的网络设备和服务器，在断电的情况下仍然可以持续工作。

* + - 1. 服务器安全

平台采用JAVA技术并采用OPENJDK标准研制，使得平台能在不同的平台上运行，这样，用户可以选择安全系数相对较高的国产化操作系统，此外对于操作系统还需要通过补丁和安全防护软件来增强安全性：

建议使用国产化硬软件安装平台系统

及时更新操作系统补丁，防止漏洞攻击

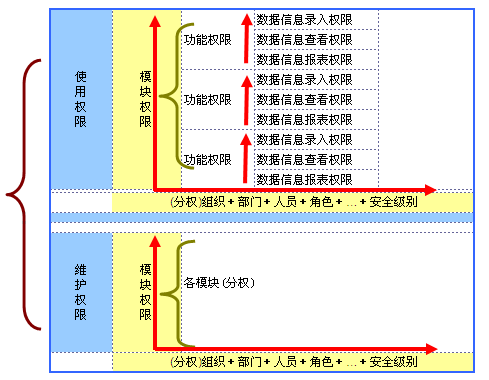
为服务器安装病毒防护软件，目前主流的病毒防护软件如下：

* + 1. **实施运维层面安全**

平台系统权限体系实现了单位内部用户的权限划分，能从多维度控制用户对系统功能的使用和维护权限以及对系统内部资源的访问权限。

* + - 1. 系统权限架构

整个平台系统充分把后台维护、模块使用、数据权限体现出来，并组合组织人员的权限使用，全方位的部署权限管理体系。



通过六维管控模型将平台系统权限从组织范围、角色范围、动作范围、模块范围、被控对象、数据范围六个维度细分，六个权限对象横向纵向交错构成了平台权限矩阵。

* + 1. **系统维护权限**

常规维护权限：可通过角色把各个模块及其模块下的各个功能的维护权限分配下去，如专人一维护人力资源管理模块、专人二维护知识文档管理模块、专人三维护工作流程管理模块；

分权维护权限：可把组织、人员、流程(字段、表单)维护权限分配给各分部管理员，各分部管理员只能维护本机构或下级机构的组织人员、流程等。

* + 1. **支持三员分立**

系统管理员(oaadmin)

负责用户管理和系统日常运作相关的维护工作。

安全管理员(securityadmin)

负责安全策略的配置和系统资源安全属性的设定，主要负责用户权限分配及权限调整，以及系统的安全策略设定。

审计管理员(auditadmin)

对系统审计信息进行管理，主要负责审计相关日志，确保系统所有操作都是合规的。其具备的权限如下章：操作日志审计。

* + 1. **支持资源密级设定，资源访问受资源密级控制**

针对资源（比如文档、公文等）可以设定资源的密级，人员信息也有密级概念，和其他资源的密级对等。如此一来，对应密级的人员只能访问其同等密级或者更低密级的资源。

* 1. **安全保密技术**
     1. **物理层安全技术**

1、环境安全

对系统所在环境的安全保护，如区域保护和灾难保护；（参见国家标准GB50173－93《电子计算机机房设计规范》、GB2887－89《计算站场地技术条件》、GB9361－88《计算站场地安全要求》。

2、设备安全

设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等；设备冗余备份；通过严格管理及提高校园的整体安全意识来实现。

3、媒体安全

包括媒体数据的安全及媒体本身的安全。显然，为保证信息网络系统的物理安全，除在网络规划和场地、环境等要求之外，还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多，在理论和技术支持下的验证工作也证实这种截取距离在几百甚至可达千米的复原显示技术给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间上的扩散，通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。

* + 1. **网络层安全技术**

1、防火墙安全技术建议

在网络的边界都应安装防火墙，并需要实施相应的安全策略控制。另外，根据对外提供信息查询等服务的要求，为了控制对关键服务器的授权访问控制，建议把对外公开服务器集合起来划分为一个专门的服务器子网，设置防火墙策略来保护对它们的访问。

2、数据传输安全建议

为保证数据传输的机密性和完整性，同时对拨号用户接入采用强身份认证，建议在网络中采用安全VP系统，对于移动用户安装VPN客户端软件。

VPN应具有以下功能：

1）信息透明加解密功能：支持网络IP数据包的机密性保护。网络密码机串联在以太网中，凡是流经的IP报文无一例外地都要受到它的分析和检查，根据需要进行加解密和认证处理。信息加解密功能支持商务系统专有的业务服务，及WWW、FTP、SMTP、Telnet等基于TCP/IP的服务。

2）信息认证功能：支持IP数据包的完整性保护。流过的IP报文在被加解密的同时，还要进行认证处理，由加密方在每个报文之后都自动附有认证码，其他人无法伪造，在接收方对该认证码进行验证，保证了信息的完整性和不可篡改性。

3）防火墙功能：支持网络访问控制机制，防止外部非法用户攻击。在操作系统底层直接实现报文包过滤技术、IP地址伪装技术（NAT），并与信息加密、认证机制无缝结合。可以保证局域网的边界安全，防止了通常的类似于IP地址欺骗的攻击。

4）远程分布式集中统一管理功能

5）安全审计及告警功能：支持对网络非法访问操作的审计和自动告警。VPN网关对流过的报文进行动态过滤分析，根据网络安全审计策略，自动调度审计进程，进行审计记录，产生审计报告，并以多种方式，如语音、电子邮件等方式对非法事件进行实时告警，以便安全管理员在第一时间了解情况，做出正确的应对措施，以尽可能的将非法事件造成的损失降低至最小。

* + 1. **系统层安全技术**

1、操作系统安全技术

操作系统是所有计算机终端、工作站和服务器等正常运行的基础，操作系统的安全十分重要。目前的商用操作系统主要有IBMAIX、Linux、AS/400、OS/390、SUNSolaris、HPUnix、Windows98/XP、Windows2000/2003等。针对操作系统应用环境对安全要求的不同，电子商务系统对操作系统的不同适用范围作如下要求：关键的服务器和工作站（如数据库服务器、WWW服务器、代理服务器、电子邮件服务器、病毒服务器、DHCP主域服务器、备份服务器和网管工作站）应该采用服务器版本的操作系统。典型的有：SUNSolaris、HPUnix、Linux、Windows2000Server。

2、操作系统安全管理

操作系统因为设计和版本的问题，存在许多的安全漏洞；同时因为在使用中安全设置不当，也会增加安全漏洞，带来安全隐患。在没有其它更高安全级别的商用操作系统可供选择的情况下，安全关键在于操作系统的安全管理。

为了加强操作系统的安全管理，要从物理安全、登录安全、用户安全、文件系统和打印机安全、注册表安全、RAS安全、数据安全、各应用系统安全等方面制定强化安全的措施。

3、数据库安全技术

目前的商用数据库管理系统主要有MSSQLSever、Oracle、Sybase、DB2等。数据库管理系统应具有如下能力：

1）自主访问控制（DAC）：DAC用来决定用户是否有权访问数据库对象；

2）验证：保证只有授权的合法用户才能注册和访问；

3）授权：对不同的用户访问数据库授予不同的权限；

4）审计：监视各用户对数据库施加的动作。

* + 1. **应用层安全技术**

根据网络的业务和服务，我们采用加密技术、防病毒技术、以及对各种应用服务的安全性增强配置服务来保障网络系统在应用层的安全。

1、防病毒技术

目前主要采用病毒防范系统解决病毒查找、清杀问题。根据网络结构和计算机分布情况，病毒防范系统的安装实施要求为：能够配置成分布式运行和集中管理，由防病毒代理和防病毒服务器端组成。防病毒客户端安装在系统的关键主机中，如关键服务器、工作站和网管终端。在防病毒服务器端能够交互式地操作防病毒客户端进行病毒扫描和清杀，设定病毒防范策略。能够从多层次进行病毒防范，第一层工作站、第二层服务器、第三层网关都能有相应的防毒软件提供完整的、全面的防病毒保护。以下是全方位防毒系统所需提供的应对策略：

1）来自系统外部（互联网或外网）的病毒入侵

这是目前病毒进入最多的途径。因此在与外部连接的网关处进行病毒拦截是效率最高，耗费资源最少的措施。可以使进入内部系统的病毒数量大为减少。但很明显，它只能阻挡来自外部病毒的入侵。

2）病毒集散地之一，网络邮件/群件系统

如果网络内采用了自己的邮件/群件系统实施办公和信息自动化，那么一旦有某个用户感染了病毒，通过邮件方式该病毒将以几何级数在网络内迅速传播，并且很快会导致邮件系统负荷过大而瘫痪。因此在邮件系统上部署防病毒也显得尤为重要。

3）病毒集散地之二，文件服务器

文件资源共享是网络提供的基本功能。文件服务器大大提高了资源的重复利用率，并且能对信息进行长期有效的存储和保护。但是一旦服务器本身感染了病毒，就会对所有的访问者构成威胁。因此文件服务器也需要设置防病毒保护。

4）最终用户

病毒最后的入侵途径就是最终的桌面用户。由于网络共享的便利性，某个感染病毒的桌面机可能随时会感染其它的机器，或是被种上了黑客程序而向外传送机密文件。因此在网络内对所有的客户机进行防毒控制也很有必要。

5）内容保护

随着病毒所采用的技术日趋复杂，单纯依靠病毒码和被动的文件分析技术往往造成防病毒的响应时间过长。为了能够在第一时间主动的阻止新型病毒的入侵，在防病毒系统中附加内容过滤和保护功能就显得十分重要。例如，由于目前邮件系统的使用异常方便，造成了用户很容易在不经意间将重要的、机密的或是不当的信息通过邮件发送出去；另一方面，来自互联网上的垃圾邮件也到处都是，导致用户需花大量的精力和时间去处理，降低了工作效率。因此对往来的邮件内容进行过滤也很重要。

6）集中管理

一个缺少管理的系统就是一个无效的系统。对于一个大型网络来说，部署的防毒系统将十分复杂和庞大。尤其在各网点在地域上分离的情况下，通过一个监控中心对整个系统内的防毒服务和情况进行管理和维护显得十分重要。这样可以大大降低维护人员的数量和维护成本，并且缩短了升级、维护系统的响应时间。

防毒系统的最大特点是需要不断的升级和更新防毒软件，以应对新产生的各类病毒。因此确保各点的防毒软件集中进行部署、升级和监控也是有效防毒的重要一环。

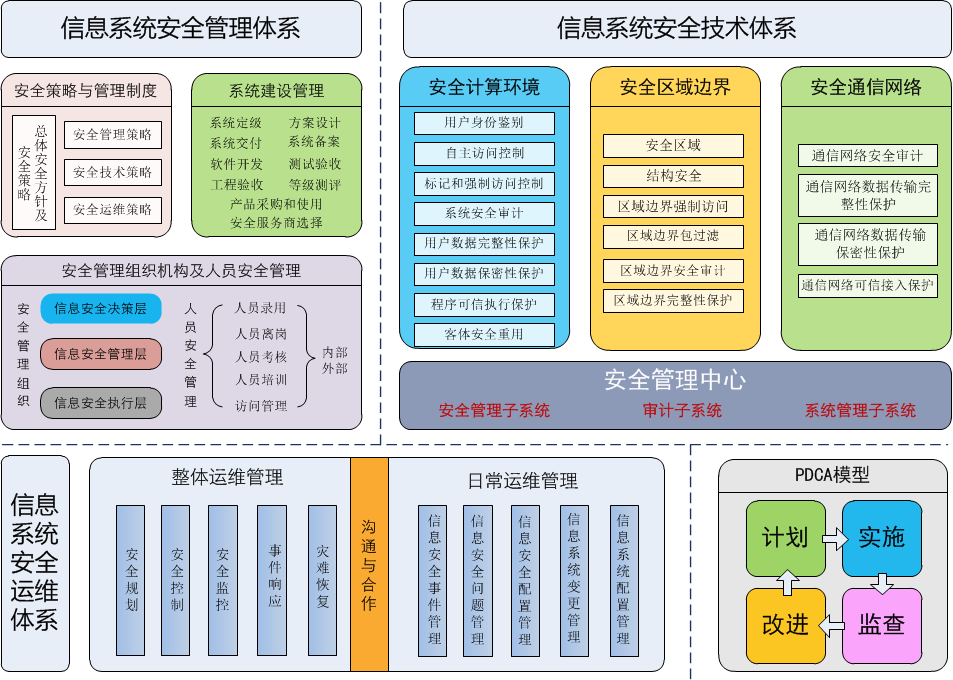
2、服务器安全性增强

服务器安全性增强的内容包括：Web服务器自身安全、Web服务器参数配置、Web服务器权限配置、Web服务器配置安全、网络信息加密配置、Web应用代码审计。

* 1. **安全保障设计**
     1. **系统等级保护的要求**

本项目所涉及系统建设总体安全须达到《信息安全技术安全可靠应用信息系统等级保护基本要求（试行）》二级/三级要求，整个系统管理须达到《信息安全技术安全可靠应用信息系统等级保护测评要求（试行）》的相关管理要求。

* + 1. **安全部署架构图**



在本项目进行信息安全等级保护安全建设工作中，将严格遵循国家等级保护有关规定和标准规范要求，坚持管理和技术并重的原则，将技术措施和管理措施有机结合，建立信息系统综合防护体系，提高信息系统整体安全保护能力。

在本项目进行信息安全等级保护安全建设工作中，将严格遵循国家等级保护有关规定和标准规范要求，坚持管理和技术并重的原则，将技术措施和管理措施有机结合，建立信息系统综合防护体系，提高信息系统整体安全保护能力。

* + 1. **安全技术体系设计**
       - 1. 设计原则

等级保护是国家信息安全建设的重要政策，其核心是对信息系统分等级、按标准进行建设、管理和监督。对于信息安全建设，应当以适度风险为核心，以重点保护为原则，从业务的角度出发，重点保护重要信息系统，在方案设计中应当遵循以下的原则：

适度安全原则

任何信息系统都不能做到绝对的安全，在进行信息安全等级保护规划中，要在安全需求、安全风险和安全成本之间进行平衡和折中，过多的安全要求必将造成安全成本的迅速增加和运行的复杂性；

适度安全也是等级保护建设的初衷，因此在进行等级保护设计的过程中，一方面要严格遵循基本要求，从网络、主机、应用、数据等层面加强防护措施，保障信息系统的机密性、完整性和可用性，另外也要综合成本的角度，针对信息系统的实际风险，提出对应的保护强度，并按照保护强度进行安全防护系统的设计和建设，从而有效控制成本；

重点保护原则

根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统；本方案在设计中将重点保护涉及生产、研发、销售等关键业务的信息系统，对其他信息系统则降低保护等级进行一般性设计和防护；

技术管理并重原则

信息安全问题从来就不是单纯的技术问题，把防范黑客入侵和病毒感染理解为信息安全问题的全部是片面的，仅仅通过部署安全产品很难完全覆盖所有的信息安全问题，因此必须要把技术措施和管理措施结合起来，更有效的保障信息系统的整体安全性，形成技术和管理两个部分的建设方案；

分区分域建设原则

对信息系统进行安全保护的有效方法就是分区分域，由于信息系统中各个信息资产的重要性是不同的，并且访问特点也不尽相同，因此需要把具有相似特点的信息资产集合起来，进行总体防护，从而可更好地保障安全策略的有效性和一致性，比如把业务服务器集中起来单独隔离，然后根据各业务部门的访问需求进行隔离和访问控制；另外分区分域还有助于对网络系统进行集中管理，一旦其中某些安全区域内发生安全事件，可通过严格的边界安全防护限制事件在整网蔓延；

动态调整原则

信息安全问题不是静态的，它总是随着管理相关的组织策略、组织架构、信息系统和操作流程的改变而改变，因此必须要跟踪信息系统的变化情况，调整安全保护措施；

标准性原则

信息安全建设是非常复杂的过程，在设计信息安全系统，进行安全体系规划中单纯依赖经验，是无法对抗未知的威胁和攻击，因此需要遵循相应的安全标准，从更全面的角度进行差异性分析，是本方案重点强调的设计原则；

成熟性原则

本方案设计采取的安全措施和产品，在技术上是成熟的，是被检验确实能够解决安全问题并在很多项目中有成功应用的；

科学性原则

本方案的设计是建立在进行安全评估基础上的，在威胁分析、弱点分析和风险分析方面，是建立在客观评价的基础上而展开分析的结果，因此方案设计的措施和策略一方面能够符合国家等级保护的相关要求，另一方面也能够很好地解决信息网络中存在的安全问题，满足特性需求。

* + - * 1. 设计依据

安全技术体系的设计，遵循以下依据：

《中华人民共和国网络安全法》

《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）

* + - * 1. 安全物理环境

机房使用门禁系统、人员出入严格遵守管理制度，满足等级保护二级/三级要求中物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等具体要求。

* + - * 1. 安全通信网络

网络架构安全

为了对应用系统实现良好的安全保障，参照等级保护的要求对系统安全区域进行划分设计，实现内部办公、数据共享交换与外部接入区域之间的安全隔离，并对核心区域进行冗余建设，用以保障关键业务系统的可用性与连续性。

根据整体安全需求并结合《网络安全等级保护基本技术要求》和《网络安全等级保护安全设计技术要求》中的相关要求，区域划分如下：

（1）终端用户域

访问应用系统的终端用户。

（2）核心业务域

应用系统部署区域，包括应用服务器、数据库服务器、共享文件服务器、存储阵列、备份一体机等。

（3）安全管理域

包含堡垒机、运维管理平台、网络审计、入侵检测系统等，与所有的区域都有通信，连接核心网络区。

（4）核心交换域

系统核心交换机所在区域。

每个区域之间通过防火墙进行隔离和访问控制，实现网络架构的安全。

通信传输安全

通过服务器密码机和数字证书认证系统，实现本地链路的传输层加密，确保信息通过互联网传输时的机密性和完整性。为实现高可用性。

可信验证

通过部署国产化通信设备的可信验证技术的实现，可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

产品部署主要是通过部署自主可控技术的国产化通信设备来实现。

* + - * 1. 安全区域边界

边界防护与访问控制

针对新的边界安全威胁，边界防护与访问控制已经成为基本安全措施，必不可少，但为了更加有效的应对当前的网络威胁，利用部署的防火墙设备，通过相关功能实现及策略配置，实现边界防护与访问控制。

产品部署主要是通过部署自主可控技术的防火墙设备来实现。

入侵防范

在网络区域的边界处，需要通过部署入侵检测设备对网络攻击行为进行检测与阻断，并及时产生报警和详尽的报告。

产品部署主要是通过部署自主可控技术的入侵检测设备来实现。

恶意代码防范

为实现对恶意代码的实时阻断，在终端部署病毒防治系统，实现从网络层检测和阻断恶意代码。

产品部署主要是通过部署自主知识产权、支持安可平台的病毒防治系统来实现。

安全审计

网络安全审计系统通过镜像获取通过核心交换机上流量数据可对整个网络的流量进行审计分析，可对用户的行为进行审计。

网络安全审计系统通过旁路部署在核心交换机，通过分析网络流量进行用户行为的分析审计。

产品部署主要是通过部署自主可控技术的网络安全审计设备来实现。

可信验证

通过部署国产化边界设备的可信验证技术的实现，可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

产品部署主要是通过部署自主可控技术的国产化边界设备来实现。

安全计算环境

身份鉴别与访问控制

应用系统环境涵盖了服务器、终端和网络设备操作系统、系统软件、应用系统、数据库等。这些设备和系统用户在登录时，应进行身份鉴别，并对系统进行最小化授权。

应用系统环境系统所有涉及的系统用户（包括技术支持人员，如操作人员、网络管理员、系统程序员以及数据库管理员等）应当具备仅供其个人或单独使用的独一无二的标识符（即用户ID），以便跟踪后续行为，从而责任到人。

通过在建设信任体系平台PKI/CA认证体系，实现身份鉴别、信息完整性校验、抗抵赖等功能。配合基于PKI/CA基础上实现基于USBKEY+数字证书的强制访问控制、安全审计等功能，通过为每个用户、主机颁发数字证书，使操作系统、应用访问控制等设施实现高安全性的访问控制、安全策略，达到用户、系统、设备的统一身份认证。PKI/CA身份认证系统涉密信息系统用户身份进行统―的管理，确保用户身份在所涉密信息系统中的唯一性，身份认证系统为所涉密信息系统提供用户证书申请、颁发、更新、撤销等服务，同时为所有应用系统提供用户身份信息的管理。所有的证书管理操作都有审计记录。

通过服务器密码机、数字证书认证系统、签名验签服务器等系统来实现。

安全审计

应用系统环境所涉及终端和服务器等设备中的操作系统、网络设备、安全设备、应用系统、数据库管理系统等，需要开启安全审计策略。相应的审计满足：

应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

应用系统的审计需要与业务系统紧密结合，此审计功能应与业务系统统一开发。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。

入侵防范

对终端和服务器等设备中的操作系统、网络设备、安全设备等采取入侵防范措施，包括：

应遵循最小安装的原则，仅安装需要的组件和应用程序。

应关闭不需要的系统服务、默认共享和高危端口。

另外根据系统类型进行其它安全配置的加固处理。

部署漏洞扫描进行系统安全性检测。漏洞扫描系统针对传统的操作系统、网络设备、防火墙、远程服务等系统层漏洞进行渗透性测试。测试系统补丁更新情况，网络设备漏洞情况，远程服务端口开放等情况并进行综合评估，在黑客发现系统漏洞前提供给客户安全隐患评估报告，提前进行漏洞修复，提前预防黑客攻击事件的发生。

针对入侵防范，除进行相应的安全加固外，通过在安全管理区部署主机监控与审计系统来实现。

恶意代码防护

对终端和服务器等设备中的操作系统采取恶意代码防范措施，安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

产品部署主要是通过在终端和服务器上部署自主可控技术的防病毒系统来实现。

**可信验证**

通过部署国产化终端、服务器，实现了终端和服务器的设备的可信验证技术的实现，可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

国产化设备安全管理平台对所有接入终端进行统一管理，国产化设备在终端操作系统中的安全执行软件，可信软件库为信息系统提供可信软件，可信芯片提供可信根，为国产化设备终端、服务器的重要组成部分。

可信机制在国产操作系统中的安全执行机制，是实现系统运行过程中度量、存储、报告功能的实际执行部件，可利用可信芯片的特性，为应用和系统的运行建立可信的计算环境通过可信连接形成可信网络，并将可信计算功能的接口提供给应用和操作系统使用。完成对国产操作系统核心行为的度量，进一步掌握操作系统内核自身运行状态的可信性。在承载业务系统的操作系统之中，实现可信认证、可信度量、可信存储、可信连接和可信监控等功能。

产品部署主要是通过部署自主可控技术的国产化终端、服务器配合国产化操作系统实现。

**数据完整性**

应用系统对信息完整性校验提出了一定的需求。在后续的项目建设中，主要从两方面来实现：

对终端和服务器等设备中的操作系统、网络设备、安全设备、应用系统、数据库管理系统等采用校验技术保证重要数据在传输过程中的完整性。

通过信任体系平台PKI/CA认证体系，实现信息完整性校验等功能。

**数据备份与恢复**

数据的备份与恢复，当前主要采取两方面的措施：

数据备份与恢复。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。

关键网络设备、线路以及服务器等硬件设备的冗余。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。

产品部署主要是通过部署自主可控技术的备份一体机设备实现数据的备份与恢复。

**剩余信息保护**

对终端和服务器等设备中的操作系统、应用系统、数据库管理系统等应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。因此，针对应用系统而言，该功能应与系统统一开发，保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

在应用场景下，服务器端采集和使用用户个人信息及其他信息后，如后续工作不再需要相关信息，采用数据定期清理的方式对涉及个人隐私等数据进行保护性维护，同时备份信息确认不包括需要被删除个人隐私数据。

建立程序流程检查机制，对用户剩余信息进行安全检查，并定期进行安全验证，确保用户信息在使用完成后被成功删除，不存在未删除或部分删除等情况。

**个人信息保护**

对用户数据、业务应用系统和数据库系统等，要求：

应仅采集和保存业务必须的用户个人信息。

应禁止未授权访问和非法使用用户个人信息。

因此，针对应用系统而言，该功能应与系统统一开发。在服务设计过程及使用过程，针对用户信息采集首先进行范围控制，严格限定个人信息采集范围和数量，避免采集范围过大而造成的个人信息泄露。同时已使用数据应采取安全控制措施，避免非相关人员和系统对个人信息的访问和使用。采用后台审计机制对个人信息访问进行安全审计，便于进行事后追责。

安全管理中心

由于应用系统网络覆盖面广，用户众多，技术人员水平不一。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、审计管理两方面进行建设。

构建先进高效的安全运维管理中心，实现对系统、产品、设备、策略、信息安全事件、操作流程等的统一管理，在该中心搭建安全运行平台和运维管理平台，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服务器、网络设备、安全设备、应用系统进行统一的管理。

系统管理由安全运行平台完成。主要部署自主可控的堡垒机系统，将运维人员与被管理设备或系统隔离开来，所有的运维管理访问必须通过堡垒机进行。运维人员在操作过程中首先连接到堡垒机，由堡垒机进行身份认证和权限检查后，代替用户连接到目标设备完成远程管理操作，并将操作结果返回给运维人员，同时堡垒机对所有的运维操作及结果进行审计记录。堡垒机实现了运维管理的集中权限管理和行为审计，同时也解决了加密协议和图形协议等无法通过协议还原进行审计的问题。

堡垒机采用旁路部署，运维操作本身不会产生大规模的流量，堡垒机不会成为性能的瓶颈。

* + - * 1. 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。

系统管理由运维管理平台完成。通过部署自主可控的运维管理系统，实现审计的集中管理。

* + 1. **安全管理体系设计**
       - 1. 安全管理体系设计目标

安全管理体系的建设需要满足《信息系统安全等级保护管理要求》和《信息系统安全等级保护基本要求》中对于管理部分的要求，同时为等级保护技术部分提供安全补充。

通过安全管理体系的建设，建设起一整套适用于各个层面的安全流程、制定、运行维护作业计划和检查标准，使用户方信息安全工作规范化、流程化，长期稳定的保障各业务系统安全运行。

安全机制的实现应具有相对固定的模式，即“人在安全策略指导下借助于一定的安全技术手段进行持续的运作”。大量证据显示，技术手段通常是为了更加有效地实施某种管理思想或者理念而得到发展的，信息安全也是如此。如果安全管理手段不能被清晰地表达，那么安全技术手段就很难得到有效的利用。因此组织必须首先将其安全管理思想和手段以策略文件的形式进行阐明，然后根据策略选择恰当的安全技术方案。

我们将根据等级保护相关标准对安全管理措施的要求，结合用户方的安全组织架构体系及业务应用特点，进行安全管理方针、策略、制度、流程和规范等的制定和优化，为用户方安全管理和运维提供更好的指导和支持，确保信息安全管理正规有序。

* + - * 1. 制定安全管理策略和制度

信息安全管理制度体系应结合实际业务需要，建立符合本单位实际情况的安全制度体系，需包括信息安全方针、安全策略、安全管理制度、安全技术规范以及流程等。

当前单位已建立相应的安全管理制度，后续项目建设过程中，根据安可项目的特点，进一步完善相关的安全管理制度。

信息安全管理策略体系建设过程

信息安全管理策略体系是信息安全组织、运作、技术体系标准化、制度化后形成的一整套信息安全管理规定。信息安全管理策略体系建设的重点是帮助组织确定信息安全工作的总体方针，完善信息安全管理规章制度、办法和操作流程，制定安全操作的技术标准和规范等，加强安全管理制度的执行力度，约束和指导本项目各层管理和使用人员的操作行为，使信息安全工作规范化、流程化，有效保障本项目长期、稳定、安全地运行。

信息安全管理策略体系的建立和运行步骤如下：

制定信息安全方针；

明确信息安全管理体系的范围，根据组织的特性、地理位置、资产和技术来确定界限；

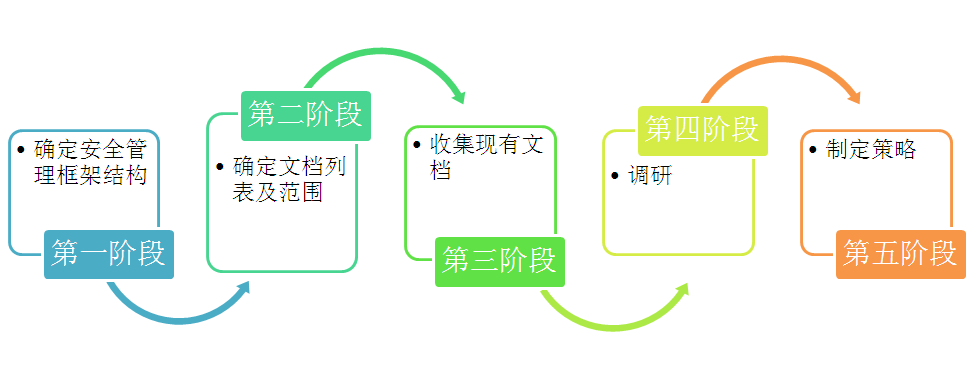
根据组织的信息安全方针和需要的保证程度来确定应实施管理的风险；

选择适宜的控制目标和控制方式；

有效地实施选定的控制目标和控制方式；

进行内部审核和管理评审，保证体系的有效实施和持续适宜。

信息安全管理策略体系实施的步骤一般如下：



首先，制定信息安全管理策略体系框架；然后，在此框架基础上，确定文档列表；并通过对现有制度的分析，及对相关人员的访谈，相关领域的调研，获得安全管理制度所需资料，并获取风险评估结果；最后，依据管理制度访谈结果，制定完整的安全管理策略体系文档。

信息安全管理策略体系框架

信息安全策略体系通常包括以下内容：

信息安全方针和策略：是纲领性的安全策略主文档，阐述了安全策略的目的、适用范围、信息安全目标、信息安全的管理意图等，是信息安全各个方面所应遵守的原则方法和指导性策略。是安全方面工作的最高指导文件。

管理制度和规定：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，是必须具有可操作性，而且必须得到有效推行和实施的。

技术标准和规范：包括各个网络设备、主机操作系统和主要应用程序的应遵守的安全配置和管理的技术标准和规范。技术标准和规范将作为各个网络设备、主机操作系统和应用程序的安装、配置、采购、项目评审、日常安全管理和维护时必须遵照的标准，不允许发生违背和冲突。

安全操作流程：详细规定主要业务应用和事件处理的流程和步骤，和相关注意事项。作为具体工作时的具体依照，此部分必须具有可操作性，而且必须得到有效推行和实施的。

记录表格：实施各项信息安全程序的成果记录，是信息安全策略体系得以持续、有效运行的有力证据。

本项目安全管理策略体系可以分为纵向和横向两个维度。从纵向划分，包括说明信息安全工作的总体目标、范围、原则和安全框架等的总体方针和安全策略、针对安全管理活动中重要的管理内容所建立的安全管理制度、以及针对安全管理人员或操作人员执行的重要管理操作所建立的操作规程；从横向划分，覆盖本项目的物理层、网络层、系统层、应用层四个层次以及人员管理和通用安全管理等方面。

信息安全管理策略体系框架如下图所示：



纵向是制度/规定的层次化结构，分为信息安全总体方针和安全策略、信息安全管理制度、信息安全操作规程三个层面，通过这三个层面将信息安全战略逐步细化、落实，指导本项目的信息安全工作：

信息安全总体方针和安全策略是纲领性的安全策略主文档，阐述了信息安全工作的目的、适用范围、信息安全目标、信息安全的管理意图等，是信息安全各个方面所应遵守的原则方法和指导性策略，是安全方面工作的最高指导原则。高层领导通过此文档传达信息安全的目标和方向。所有制度、规范和流程必须遵从此策略的要求。此策略的执行也需要由制度和规程作为支撑。安全方针和策略独立于具体的技术实施，是概念上的陈述，保持相对稳定，不随技术、组织架构的变化而频繁变化。

信息安全管理制度是在信息安全总体方针、策略的思想指导下，制定的信息安全管理活动执行标准，定义确保安全策略有效执行的具体要求，方法等信息。根据本项目的具体技术和管理环境制定不同的管理制度，如机房安全管理制度、人员安全管理标准、网络安全管理制度、系统安全管理制度等。安全管理制度必须具体、可操作，并严格遵守。

信息安全操作规程包括具体的操作流程、细则和操作手册等，是为了贯彻、落实信息安全管理制度而制定的，将信息安全标准与规范与具体实践相结合的详细规定。是具体执行单位，为确保安全策略、制度的执行，设定的跨部门或部门内的执行步骤。

横向是信息安全对象，涵盖本项目中的管理、应用、系统、网络、物理和人员等层面。根据针对对象的不同，在纵向的每个层次中应当分别制定相应的政策、制度和规程等。

层次分明的安全制度体系，既充分体现了“纵深防御”的安全思想，又便于进行安全设计、实施和监督。

信息安全总体方针

信息安全方针是从用户方整体管理层面对信息安全的最高指导原则，是为组织管理、保护、和信息资源分派制定的原则。信息安全方针是信息安全政策与标准体系中最高层级的声明，提供较广泛的领导方向以及说明管理阶层的目标和目的。

信息安全方针针对管理的特定需求对以下方面应该给出明确的规定，具体内容包括：

信息安全风险管理

对信息安全风险管理的方式、方法进行说明和规定，明确管理原则。按照评估、执行、监控和完善的风险管理循环阶段分别提出信息安全风险管理的要求和目标。信息安全风险管理相关政策将对用户方各信息安全标准与规范中的信息安全风险控制措施和方法进行指导。

信息安全意识建设

信息安全意识建设目的是提高用户方全体员工的信息安全意识，保证其了解自身的信息安全职责，并做到所有的人都能够具备必需的信息安全相关技能，从而使得用户方员工能够从日常行为做起，防范信息安全风险。因此信息安全意识建设须对信息安全意识工作的开展方式、方法进行规定，明确该项工作的对象、内容，期望达到的具体目标以及实现的管理原则。

信息安全组织

组织管理是信息安全保障体系架构中的重要组成部分。根据信息安全全员参与原则，用户方信息安全组织管理相关政策需要对各单位和部门在信息安全工作中扮演的角色，承担的责任，相互之间的分工以及协作、汇报的机制进行规定，以保证信息安全管理控制各个环节的风险都有适当的组织负责。

信息安全审计

信息安全审计目的是对信息安全保障体系和运作机制进行监督和评价。为了保证审计工作的质量和效果，需要在用户方内部审计过程中对信息安全的审计内容、目标及方法进行规范。

信息安全法律法规符合性

信息安全法律法规符合性是信息安全管理中的一个特殊领域。需要明确信息安全法律法规管理的目标以及为达到该目标必须遵从的规定、方法等，并将其以管理制度的形式固定下来。信息安全法律法规符合性政策还应当包括法律法规符合性声明。该声明具有时效性，需要定期更新.

* + - * 1. 信息安全策略

信息安全策略，是在一个组织内指导如何对包括敏感信息在内的资产进行管理、保护和分配的规则和指示。本项目安全策略不仅是系统建设的重要依据，而且也是系统安全维护的重要文档，是制定安全标准和管理制度的重要基础。

在总体安全方针的指导下，制订四个层面的信息安全策略：

(1)业务安全策略

业务管理制度参照了国家等保标准和其它相关要求，明确了机构业务的管理控制要求。业务安全总体策略就是在此基础之上制定更加科学合理的内部控制机制。在明确内部控制要求和建立内部控制机制后，需要制定业务的流程，保障业务的顺利进行，这需要涉及到业务管理安全、业务事务完整性等方面。该部分由各业务部门加以落实。

业务安全策略可以包括以下内容：

1)根据业务访问控制策略对用户严格授权；

2)严格限制业务人员越过应用程度对后台数据库或操作系统直接访问；

3)建立和维护应用系统的用户权限表。

(2)应用系统安全策略

首先是通过应用系统的实现将制定的内部控制制度进行落实，将业务流程加以实现，同时要保证该过程确实将这些要求落实。其次，保证实现后的业务系统能够对业务处理的信息和数据在整个生命周期中的保密性、完整性、抗抵赖性，保障重要信息的真实性和完整性。该部分由各业务部门和信息化部门共同加以落实。

主要包括：

应用系统开发策略

1)建立并遵循安全开发标准；

2)在系统分析阶段，进行风险分析和风险管理，确定系统安全控制机制；

3)操作人员只保留可执行代码；

4)程序源代码尽可能不要保留在运行系统上；

5)在开发过程中的关键点进行安全评审；

6)对系统源代码进行安全审核。

运作流程

1)必须明确并遵循本项目运作的变更流程；

2)必须明确并遵循安全问题处理流程；

3)本项目的生产环境和开发测试环境需要分离；

4)系统的超级管理权限应采取双人控制，互相制衡。

本项目管理

1)必须对本项目进行定期备份；

2)必须对系统操作人员的活动进行日志记录；

3)必须定期检查和处理系统日志；

用户访问管理

1)帐户开户

根据工作相关性原则并经过审批后为个人分配权限；

建立帐户开户和销户的闭环流程，控制用户对系统的访问权限；

含有保密信息的系统禁止建立公用帐户；

用户的岗位或职责发生变化时，应立即变更或取消相应的访问权限；

对分配的权限必须记录和进行维护。

2)口令管理

必须明确口令的管理责任人，并设置口令；

口令的设置要遵循单位有关规定，开户时应设置随机口令。

3)权限检查

对用户访问权限进行定期检查，每3个月一次；

对于特别的授权，每1个月进行一次；

一人不应具有多方面的权限，权限须多层分离互相制约。

4)用户责任

用户应采取适当的方式保证口令安全；

不得共享个人的口令；

定期更改口令。

(3)基础设施安全策略

业务和应用系统不是孤立存在的，是在IT环境中运行的，所以IT支撑环境的安全直接影响着整个业务的安全性。IT支撑环境安全策略就是保证数据库、操作系统、业务中间件、网络、物理环境和设备等支撑业务应用的IT基础设施安全。该部分由信息化部门加以落实。

主要包括：

网络安全策略

1)网络划分

根据用户方内部业务和保密要求的不同，将本项目划分成不同的逻辑网络域，每个网络域的安全控制措施必须是明确的。

2)网络连接和服务

所有与用户方网络进行的连接都需要经过信息安全实施组的批准；

所有与用户方外部网络相连的出入口处必须设立防火墙；

通过接入服务器接入用户方内部网络必须经过AAA认证（认证、授权、记帐）；

与本项目相连接的系统必须有专人负责管理；未经批准，不得建立网络服务。

3)网络设备

网络设备的安装、配置、变更、撤销等操作必须经过审批；

网络的拓扑结构、IP地址等信息未经授权，严禁泄露；

对网络设备的远程登录操作应限定在指定网段范围内。

操作系统安全策略

1)必须及时安装系统安全补丁；

2)关闭所有系统不需要的系统服务；

3)服务器的密码文件须加密存放；

4)定期修改用户口令；

5)删除所有系统上不使用的帐号；

6)严格控制操作系统管理员对系统文件和业务数据的操作权限；

7)根据工作相关性原则授予用户相应权限；

8)系统建立的日志必须满足审计要求；

9)系统日志必须安全存放，防止被非授权的访问。

物理安全策略

1)场地安全

对本项目的核心设备的部署地点必须根据业务内容的不同划分相应的控制区域；

用户方根据本项目工作性质划分相应的安全级别，并建立相应的访问控制措施；

在选定位置时应根据部门的安全级别选择相应控制区域；

所有受控区域必须指定信息安全管理责任人。

2)设备安全

根据设备及其运行系统的重要程度，将设备放置到相应级别控制区域；

根据设备及其运行系统的重要程度建立防盗、报警、监控等保护措施；

建立设备的应急备份系统。

3)存储介质

存储介质的使用必须有授权和记录；

存储介质的销毁必须按用户方批准通过的销毁方式销毁。

(4)运行维护安全策略

前面三个方面只是强调了如何实现整个业务系统，如何保证业务系统的安全性，但是如何保证业务系统确实按照内控和既定业务流程正常的运行，如何建立运行过程安全性的评价机制，这些需通过运行管理安全来实现。运行管理安全策略是：监控业务和系统的有效运行。该部分由信息化部门加以落实。

主要包括：

业务连续性、数据备份策略

根据业务重要程度、优先级制订灾难恢复计划；

建立安全事故处理流程；

对关键的业务系统要建立异地数据备份，对关键业务系统建立热备份；

定期备份并检查备份；

进行紧急事故响应演练。

病毒防护策略

禁止员工未经授权以任何名义制造、传播、复制、收集计算机病毒或发布病毒预警消息；

用户方的计算机系统都必须安装、运行统一部署的防病毒软件，并及时升级。未经批准，不能安装其它的防病毒软件；

用户方人员接收和发布信息时须进行病毒检测；

重要的和与外部网络相连接的服务器必须实时运行防病毒软件；

禁止内部主机通过外网直接到WEB网站上自动升级防病毒软件，必须在用户方内部指定服务器上升级。

安全审计策略

信息安全实施组应该定期组信息安全检查和审计，并对总体的信息安全状况进行评估，向信息安全部门提交审计和评估报告；

对于攻击类行为应该进行实时监控和报警，其它违规行为视情况实时、每周或每月定期处理；

对网络上关键的信息流进行检查与监控，对异常情况及时输出报告；

对内部网络上关键服务的操作系统、应用系统、网络设备的存取控制记录进行检查和监控；

对个人计算机、办公区域定期进行安全检查与通报；

本项目建立日志，日志记录的信息必须满足内外部的安全审计要求；

* + - * 1. 信息安全管理制度的有效发布和执行

安全管理制度系列文档制定后，必须有效发布和执行。发布和执行过程中除了要得到管理层的大力支持和推动外，还必须要有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。

这是一个长期、艰苦的工作，需要付出艰苦的努力，而且由于牵扯到单位许多部门和绝大多数人，可能需要改变工作方式和流程，所以推行起来的阻力会相当大；同时安全策略本身存在的缺陷，包括不切实可行，太过复杂和繁琐，部分规定有缺欠等，都会导致整体策略难以落实。

* + 1. **安全管理机构**

根据管理工作需要设立安全管理机构，建立信息安全领导小组和信息安全管理职能部门，后续项目建设过程中，将根据实际情况决定是否需要进行调整。

信息安全的管理职责可分为三个层次，每一级都有明确的责任：

决策层：建议成立信息安全委员会，作为信息安全工作最高领导决策机构，不隶属于任何部门，直接对用户方最高领导层负责，负责用户方信息安全工作的宏观管理。信息安全委员会建议由用户方分管信息安全的领导牵头，成员包括各部门负责人。

管理层：在信息安全委员会下设立信息安全管理办公室，作为一个常设的管理机构，在用户方信息安全委员会直接领导下进行工作，不受其它任何组织、部门的领导，负责处理用户方信息安全管理的日常工作。信息安全管理办公室建议由用户方信息中心主管信息安全的领导牵头，成员包括各部门信息安全专员。

执行层：为用户方的各类信息安全工作人员，包括安全专职管理员、系统管理员、网络管理员、数据库管理员、应用管理员、机房管理员等，负责落实规章制度和技术规范。也可以设立专门的网络安全员、系统安全员，与现有网络管理员、系统管理员形成主备岗。

此外，用户方组织内部安全技术骨干并邀请行业内或社会上信息安全技术专家、学者成立信息安全顾问专家组，定期或不定期为信息安全管理提供安全动态、面临的风险、先进技术、改进建议、采取措施、接受咨询。安全顾问专家组不必是常设机构，对用户方信息安全委员会负责。

信息安全组织结构图如下所示：



在整个信息安全工作期间：

信息安全委员会进行各项信息安全工作的部署、决策、受理、审批、监督等各项工作。

单位高层领导在信息安全委员会监督和建议下进行协调工作。

信息安全管理办公室将信息安全委员会部署的各项信息安全工作在整个单位中进行相应的执行。

单位领导的协调工作和信息安全管理办公室的执行工作都在信息安全监管机构的监督下完成。

* + 1. **安全人员管理措施**

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。

当前单位已建立相应的安全管理人员规定，后续项目建设过程中，根据项目的特点，进一步完善相关的安全管理规定。

* + - * 1. 人员考核

人员考核的做到以下方面的内容：

定期的人员考核：应定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考；

定期的人员审查：对关键岗位人员，应定期进行审查，如发现其违反安全规定，应控制使用；

管理有效性的审查：对关键岗位人员的工作，应通过例行考核进行审查，保证安全管理的有效性；并保留审查结果；

全面严格的审查：对所有安全岗位人员的工作，应通过全面考核进行审查，如发现其违反安全规定，应采取必要的应对措施。

* + - * 1. 安全培训

安全意识教育和培训做到以下方面的内容：

应知应会要求：应让本项目相关员工知晓信息的敏感性和信息安全的重要性，认识其自身的责任和安全违例会受到纪律惩罚，以及应掌握的信息安全基本知识和技能等；

有计划培训：制定并实施安全教育和培训计划，根据不同培训对象的需要，每季度或每半年进行安全培训，培养本项目各类人员安全意识，并提供对安全政策和操作规程的认知教育和训练等；

针对不同岗位培训：针对不同岗位，制定不同的专业培训计划，包括安全知识、安全技术、安全标准、安全要求、法律责任和业务控制措施等；

按人员资质要求培训：对所有工作人员的安全资质进行定期检查和评估，使相应的安全教育成为组织机构工作计划的一部分；

培养安全意识自觉性：对所有工作人员进行相应的安全资质管理，并使安全意识成为所有工作人员的自觉存在。

* + - * 1. 外部人员访问管理

外部人员访问管理做到以下方面：

应对硬件和软件维护人员，咨询人员，临时性的短期职位人员，以及辅助人员和外部服务人员等第三方人员签署包括不同安全责任的合同书或保密协议；规定各类人员的活动范围，进入计算机房需要得到批准，并有专人负责；第三方人员必须进行逻辑访问时，应划定范围并经过负责人批准，必要时应有人监督或陪同；

在重要区域，第三方人员必须进入或进行逻辑访问（包括近程访问和远程访问等）均应有书面申请、批准和过程记录，并有专人全程监督或陪同；进行逻辑访问应使用专门设置的临时用户，并进行审计；

关键区域管理要求：在关键区域，一般不允许第三方人员进入或进行逻辑访问；如确有必要，除有书面申请外，可采取由机构内部人员带为操作的方式，对结果进行必要的过滤后再提供第三方人员，并进行审计；必要时对上述过程进行风险评估和记录备案，并对相应风险采取必要的安全补救措施。

* + 1. **安全建设管理**

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。

* + 1. **安全运维管理**

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。

* + 1. **安全管理体系流程**

本项目安全管理体系建设工作内容如下：

(1)落实信息安全责任制

明确领导机构和责任部门，设立或明确信息安全领导机构，明确主管领导，落实责任部门。建立岗位和人员管理制度，根据职责分工，分别设置安全管理机构和岗位，明确每个岗位的职责与任务，落实安全管理责任制。建立安全教育和培训制度，对本项目运维人员、管理人员、使用人员等定期进行培训和考核，提高相关人员的安全意识和操作水平。

(2)确定安全管理策略，制定安全管理制度

根据安全管理需求，确定安全管理目标和安全策略，针对本项目的各类管理活动，制定人员安全管理制度、系统建设管理制度、系统运维管理制度、定期检查制度等，规范安全管理人员或操作人员的操作规程等，形成安全管理体系。

(3)落实安全管理措施，具体包括：

1)人员安全管理

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。规范人员录用、离岗、过程，关键岗位签署保密协议，对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，对关键岗位的人员进行全面、严格的安全审查和技能考核。对外部人员允许访问的区域、系统、设备、信息等进行控制。

2)系统运维管理

安全运行与维护是等级保护实施过程中确保本项目正常运行的必要环节，通过在安全运行管理阶段实施操作管理和控制、变更管理和控制、安全状态监控、安全事件处置和应急预案、安全评估和持续改进以及监督检查等活动，在安全管理基本要求的基础上，指导系统运行的动态管理。该涉及的工作内容较多，包括安全运行与维护机构和安全运行与维护机制的建立，环境、资产、设备、介质的管理，网络、系统的管理，密码、密钥的管理，运行、变更的管理，安全状态监控和安全事件处置，安全审计和安全检查等内容。对其中的主要工作内容简单描述如下：

运行管理和控制

运行管理职责确定——通过对运行管理活动或任务的角色划分，并授予相应的管理权限，来确定安全运行管理的具体人员和职责。

运行管理过程控制——通过制定运行管理操作规程，确定运行管理人员的操作目的、操作内容、操作时间和地点、操作方法和流程等，并进行操作过程记录，确保对操作过程进行控制。

变更管理和控制

变更需求和影响分析——通过对变更需求和变更影响的分析，来确定变更的类别，计划后续的活动内容。

变更过程控制——确保变更实施过程受到控制，各项变化内容进行记录，保证变更对业务的影响最小。

安全状态监控

监控对象确定——确定可能会对本项目安全造成影响的因素，即确定安全状态监控的对象。

监控对象状态信息收集——选择状态监控工具，收集安全状态监控的信息，识别和记录入侵行为，对本项目的安全状态进行监控。

监控状态分析和报告——通过对安全状态信息进行分析，及时发现安全事件或安全变更需求，并对其影响程度和范围进行分析，形成安全状态结果分析报告。

安全事件处置和应急

安全事件分级——结合本项目的实际情况，分析事件对本项目的破坏程度，所造成后果严重程度，将安全事件依次进行分级。

应急预案制定——通过对安全事件的等级分析，在统一的应急预案框架下制定不同安全事件的应急预案。

安全事件处置——对监控到的安全事件采取适当的方法进行处置，对安全事件的影响程度和等级进行分析，确定是否启动应急响应。

安全检查和持续改进

安全状态检查——通过对本项目的安全状态进行检查，为本项目的持续改进过程提供依据和建议，确保本项目的安全保护能力满足相应等级安全要求。

改进方案制定——依据安全检查的结果，调整本项目的安全状态，保证本项目安全防护的有效性。

安全改进实施——保证按照安全改进方案实现各项补充安全措施，并确保原有的技术措施和管理措施与各项补充的安全措施一致有效地工作。

等级保护巡检

通过国家管理部门对本项目定级、规划设计、建设实施和运行管理等过程进行监督检查，确保其符合本项目安全保护相应等级的要求。

在这个阶段，对于本项目的运营、使用单位来说，主要工作是对已经完成安全等级保护建设的本项目进行维护管理，发现问题及时整改；定期进行安全状况检测评估，及时消除安全隐患和漏洞；制定不同等级信息安全事件的响应、处置预案，加强本项目的安全管理。而相关的信息安全监管机构也要按照等级保护的管理规范和技术标准的要求，对本项目的安全等级保护状况进行监督检查；发现存在安全隐患或未达到等级保护的管理规范和技术标准要求的，限期整改，使本项目的安全保护措施更加完善。

在本项目实施完毕后，将由专业的安全服务人员根据等级保护中对安全运行与维护阶段的相关要求，为用户方提供全面的安全运维支撑服务，确保本项目能够得到全过程的运行保障。

3)系统建设管理

在系统定级、规划设计、实施过程中，协助用户对工程的质量、进度、文档和变更等方面的工作进行监督控制和科学管理。制定系统建设相关的管理制度，明确系统定级备案、方案设计、产品采购使用、软件开发、工程实施、验收交付、等级测评、安全服务等内容的管理责任部门、具体管理内容和控制方法，并按照管理制度落实各项管理措施。具体活动内容包括：

质量管理

质量管理首先要控制系统建设的质量，保证系统建设始终处于等级保护制度所要求的框架内进行。同时，还要保证用于创建系统的过程的质量。在系统建设的过程中，要建立一个不断测试和改进质量的过程。在整个系统的生命周期中，通过测量、分析和修正活动，保证所完成目标和过程的质量。

风险管理

为了识别、评估和减低风险，以保证系统工程活动和全部技术工作项目都成功实施。在整个系统建设过程中，风险管理要贯穿始终。

变更管理

在系统建设的过程中，由于各种条件的变化，会导致变更的出现，变更发生在工程的范围、进度、质量、费用、人力资源、沟通、合同等多方面。每一次的变更处理，必须遵循同样的程序，即相同的文字报告、相同的管理办法、相同的监控过程。必须确定每一次变更对系统成本、进度、风险和技术要求的影响。一旦批准变更，必须设定一个程序来执行变更。

进度管理

系统建设的实施必须要有一组明确的可交付成果，同时也要求有结束的日期。因此在建设系统的过程中，必须制订项目进度计划，绘制网络图，将系统分解为不同的子任务，并进行时间控制确保项目的如期完成。

文档管理

文档是记录项目整个过程的书面资料，在系统建设的过程中，针对每个环节都有大量的文档输出，文档管理涉及系统建设的各个环节，主要包括：系统定级、规划设计、方案设计、安全实施、系统验收、人员培训等方面。

(4)安全自查与调整

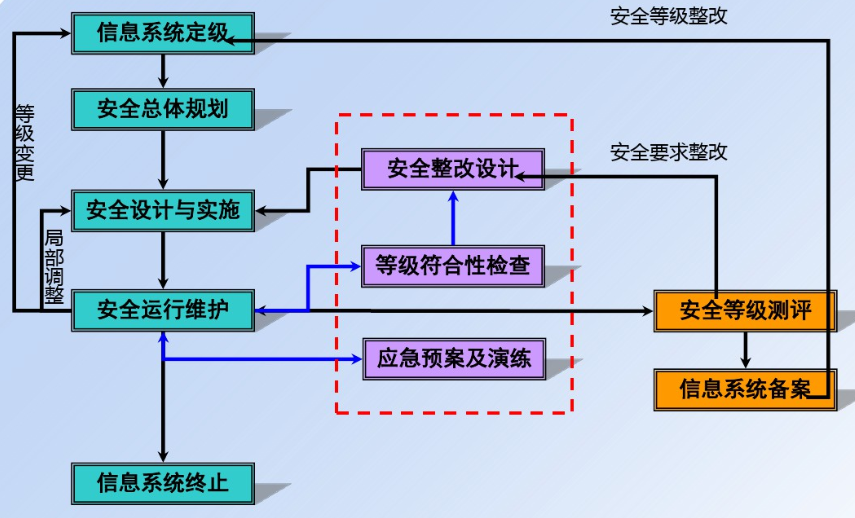
制定安全检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善。实现定期对本项目安全状况进行自查。

* + 1. **协助等保测评**

根据公安部出台的有关等级保护的政策，信息系统的等级保护已经是国家的一项基本国策和信息安全的基本保障，同时等级保护工作的开展也是各行各业信息化建设的内在需求。

其测评目的在于对信息系统当前安全防护能力做出客观评价。通过对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理、安全管理体系等方面的安全检查，以国家信息安全等级保护基本要求作为安全基线，进行客观符合性判定，进一步衡量当前系统的安全防护能力，以及系统所面临的威胁和风险所在，为将来的安全整改和安全建设提供有力依据。

信息系统的等级保护测评流程如下图所示：

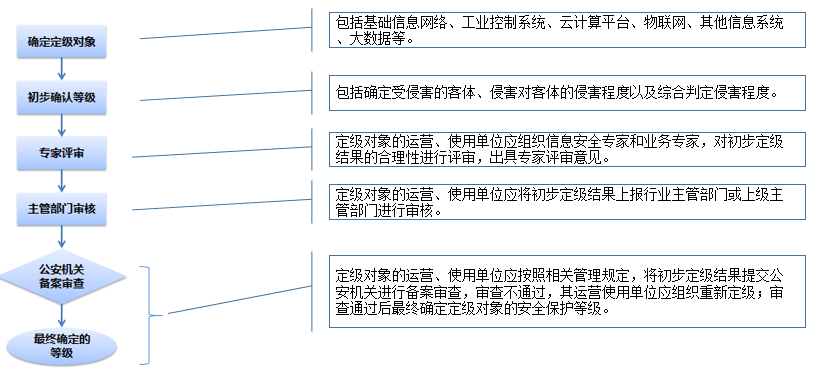


针对信息系统进行等级保护测评的过程中，我们将协助进行等保测评工作。具体工作内容包括：

1）协助定级

信息安全等级保护工作的第一个环节是系统定级。对信息系统进行定级是等级保护工作的基础，信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。定级工作流程是确定定级对象、确定信息系统安全等级保护等级、组织专家评审、主管部门审批、公安机关审核。信息系统定级以后，应到所在地区地市级上公安机关办理备案手续，备案工作的流程是信息系统备案、受理、审核和备案信息管理等。

对系统情况进行分析，通过分析系统所属类型、所属信息类别、服务范围，了解系统的可用性、完整性、保密性需求，清晰确定保护对象，确定受侵害的客体、确定客体受侵害的程度，最终确定系统的系统服务保护等级和业务信息保护等级，协助用户编制定级报告。



2）协助备案

协助用户填写《信息系统安全等级保护备案表》，协助用户到各地公安机关进行系统备案，获得系统备案证。

3)技术培训

根据丰富的为企业提供信息安全服务的经验，总结出对于信息安全教育不同方式的特点和效果，可以为公司开展信息安全教育提供参考建议。信息安全意识培训的目标是提高员工的信息安全意识，加深对信息安全的认识，加强识别信息安全风险的能力和信息安全风险防范技能。

4）协助系统测评

信息系统的等级保护测评项目的实施主要分为现场测评和复测评。

现场测评分为四个阶段：

（1）测评准备活动阶段；

（2）方案编制活动阶段；

（3）现场测评活动阶段；

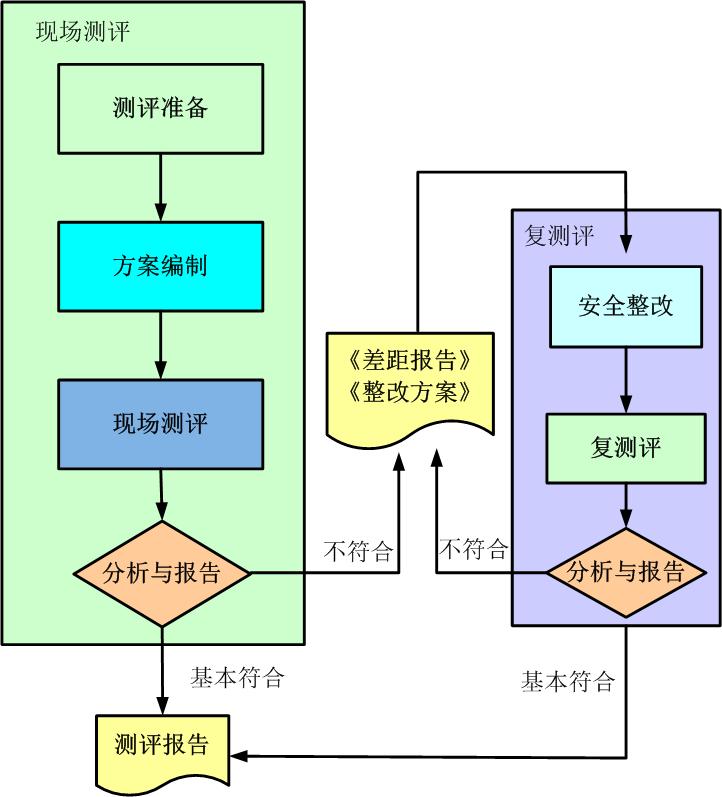
（4）分析和报告编制活动阶段；

复测评分为三个阶段：

（1）安全整改活动阶段，

（2）复测评活动阶段

（3）分析和报告编制活动阶段。



5）协助整改

安全建设整改工作是开展等级保护工作的核心和落脚点，无论是定级、测评还是监督检查工作最终都要服从和服务于安全建设整改工作。

安全建设整改是指在符合等级保护的要求的基础上，对新建或已经建的信息系统进行建设和整改。目的是使确定了等级的信息系统能够达到相应等级的基本的保护水平和满足自身需求的安全保护能力。

信息系统安全建设整改工作具体实施可以根据实际情况，将安全管理和安全技术整改内容一并或者分步实施，做到技术为基础，管理是关键，服务做支撑。

* + 1. **交付文档和资料**

交付的文档和资料主要包括：

《信息系统定级报告》

《信息系统等级保护设计方案》

《信息系统等级保护实施方案》

《信息系统等级保护实施报告》

《系统基础信息调研表》

《信息系统等级保护备案表》

《信息系统差距分析报告》

《信息系统实施报告》

《信息系统等级保护测评报告》

《信息系统登记保护整改方案》