信息系统项目信息安全管理历年真题及参考范文集

1、2012 年下半年考题

在组织的信息化工作中，建立信息系统安全策略是其中必不可少的环节，信息系统安全策略就是指：为避免因使用计算机或应用信息系统可能导致的单位资产损失而采取的各种措施、手段以及建立的各种管理制度、法规等。

请以“论构建信息系统安全策略问题，分别从以下三个方面进行论述”：

1、概要叙述你参与管理过的信息系统项目（项目的背景、项目规模、发起单位、目的、项目内容、组织结构、项目周期、交付的产品、项目安全需求等）

2、围绕以下两方面，结合项目实际论述构建信息系统安全策略的基本内容

（1）构建信息安全策略的核心内容

（2）构建信息安全策略的设计原则

3、请结合论文中所提到的信息系统项目，简要论述项目中涉及的几种具体的安全策略。并指出其中可以进一步改进之处。

【江山老师点评】对于本题的写作，江山老师认为此题有一定的难度。

如果非要写，请把安全管理相关内容学习下，针对问题 2 和 3 作答。此题不需要掌握。

2、2017 年下半年考题

2017 年 6 月 1 日《中华人民共和国网络安全法》正式实施，全社会对信息安全的关注提到前所未有的新高度，目前，很多单位都建立了信息安全管理体系，制定了信息安全相关的制度，规范或要求等。在项目实施过程中如何遵循这些制度、规范和要求，成为项目经理需要重点关注的问题。

请以“信息系统项目的安全管理”为题，分别从以下三个方面进行论述：

1、概要叙述你参与过的或者你所在组织开展过的信息系统相关项目的基本情况（项目背景、规模、目的、项目内容、组织结构、项目周期、支付成果等），并说明你在其中承担的工作。

2、结合项目实际，论述你对项目安全管理的认识，可以包括但不限于以下几个方面。

⑴信息安全管理的主要工作内容。

⑵信息安全管理中可以使用的工具、技术和方法等。

⑶信息安全管理工作内容、使用的工具、技术和方法如何在项目管理的各方面（如人力资源管理、文档管理、沟通管理、采购管理）得到体现。

3、请结合论文中所提到的信息系统项目，介绍你是如何进行安全管理的，包括具体做法和经验教训。

【江山老师点评】写这个题目的考生应该很少的，当然，这也是我们平时不需要掌握的内容

3、2019 年上半年考题

试题二 论信息系统项目的人力资源管理和成本管理

项目中的所有活动都是由人来完成的，因此在项目管理中，“人”的因素至关重要。如何充分发挥人的作用，使团队成员达到更好的绩效，对于项目管理者来说不容忽视.项目的人力资源管理就是有效地发挥每一个参与项目人员作用的过程。

请以“信息系统项目的人力资源管理和成本管理”为题，分别从以下三个方面进行论述：

1、概要叙述你参与管理过的信息系统项目（项目的背景、项目规模、发起单位、目的、项目内容、组织结构、项目周期、交付的成果等），以及该项目在人力资源方面的情况。

2、结合项目管理实际情况并围绕以下要点论述你对信息系统项目人力资源管理和成本管理的认识。

（1）项目人力资源管理的基本过程和常用方法。

（2）项目人力资源管理中涉及到的成本管理问题和成本管理中涉及的人力资源管理问题。

（3）信息系统发生成本超支后，如何通过人力资源管理来进行改善。

3、结合项目实际情况说明在该项目中你是如何进行人力资源管理和成本管理的（可叙述具体做法），并总结你的心得体会。

安全管理范文 1

摘要：

2017 年 6 月,受公司委托，我担任某省高速公路收费系统联网升级改造项目的项目经理，负责该项目的管理工作。该项目总投资 960 万元人民币，建设工期为 1 年，该项目于 2017 年 6 月 18 日开工，2018 年 6 月 17 日完工。项目主要目的为对原有收费系统进行升级改造，以解决通行量与日俱增后的收费效率提升问题，项目主要实施内容为部分服务器、工作站的更新，及全线软件系统的重新定义、开发、安装调试等，项目于 2018 年 5 月完工并通过验收，赢得了业主方好评。该项目的成功很大程度上归功于在项目过程中对安全的良好的管理和控制，本文结合作者的经验，主要从高速公路收费网络的安全现状、收费网络中存在的安全隐患进行了分析，并且提出了一些加强高速公路收费网络安全防护的措施进行详实论述，并就项目过程中采取的措施、方法作了介绍，最后总结了本次项目管理中的不足和取得的经验教训，提出了今后的改进思路。

正文：

2017 年 6 月，我参与了某省高速公路收费系统联网改造项目的建设工作，受公司委托，有我担任本项目的项目经理。该项目总投入 960 万元人民币，建设工期为 1 年，工期自 2017 年 6 月 18H 开工，2018 年 6 月 17 日完工，并于 2018 年 6 月正式通过业主方验收。该项目升级范围包含更新高速公路收费站服务器、工作站，更新车道收费系统设备、全面提高收费效率，收费数据上传至区域中心，再由区域中心上传至上一级管理中心，实现多级查询调用模式。项目实施的主要目的是解决高速公路通行量与日俱增与原收费系统工作效率不匹配的问题，通过改造升级后，可成倍提高通行效率，降低车辆拥堵的概率。系统采用 JAVA 语言开发，中间件采用 IBM 的 Websphere 并做集群，系统采用 B/S 架构，数据库使用 oraclellg 做数据管理，实现该系统的功能需求。

由于该信息化建设系统投资规模较大，技术复杂，参与的项目成员多，业主方对质量和安全的要求高。作为项目经理，我将主要精力放在项目安全管理上，在制定安全管理策略时，本人科学地运用信息安全管理的理论知识，结合高速公路收费系统信息安全管理体系的具体要求和系统的具体情况，从信息安全的制度、流程、岗位、职责、人员为出发点，制定了科学合理的信息安全制度体系。按照系统实际情况从主机、网络结构存、物理传输链路、操作系、数据安全等方面进行信息安全的有效管理，保障了系统的安全、高效、可靠，有效的保证高速公路联网收费系统能够安全稳定的运行，通过有效的项目安全管理，带领项目团队全体成员经过奋战获得了良好的绩效，取得了项目的成功。

1、建立科学合理的信息安全管理制度，完善岗位和人员的设置

在制定系统的信息安全管理制度时，本人参照本公司信息安全管理体系的要求，并结合系统实际情况，在充分征求了客户和公司领导的前提下，召集团队成员一起制定出了本系统的安全管理制度，并就制定出来的制度与相关的干系人进行讨论与评审，评审通过后请客户的领导签字确认，再正式实施。

1.制订信息安全方针文件，明确信息安全的目标是建立和完善信息安全的策略体系、组织体系、技术体系和运作体系，争取达到领先的信息安全保障水平，保障和促进高速公路收费管理系统业务目标的实现。

2.为了促使信息安全管理体系有效及明确地界定体系内的组织结构及成员的职责和义务，确保信息安全管理体系能有效运行，制订信息安全管理组织文件。在各方领导的积极配合下，在文件中，确定了信息安全领导小组、信息安全工作小组，设置了相关的系统安全管理人员，如机房管理员、网络管理员、系统工程师、安全审计人员等职位，并制订了详细的职责。例如像网络管理员的职责在于对网络设备进行安全配置，进行网络的集中实时监控、网络的连通性检测和检查，保证用户对网络设备的用户、口令的安全性进行管理,参照相应规定对网络设备登录用户进行监测和分析，根据对网络设备安装、配置、升级和管理的需要为用户设置相应的级别，并对各个级别用户能够使用的命令进行限制。

3.人员安全管理。为了防止信息滥用、丢失和泄密，同时规范人员录用和离职管理过程，制订了人员安全管理规范，规范共包括对人员招聘、入职培训、人员表用、人员转岗和离职、持续改进五个环节，在组织和流程上保证了信息安全的科学、合理、可靠。

2、主机的安全策略

主机操作系统作为软件的载体，其安全性至关重要。在硬件的选购上，经过充分考察后，我选用了 IBM 小型机、IBM 刀片服务器，从硬件上保证了服务器的安全性。在操作系统的选择上，我与党校领导也进行了交流

讨论，最后确定采用。racelllg 操作系统，其安全性得到有效保障。制定了服务器的安全使用规定，根据业务需求建立不同用户，且各个用户仅具有满足当前业务需求的最小权限，有限避免用户的越权访问;开启安全审计策略，审计用户的操作;关闭不必要的端口及服务;定期对操作系统进行更新;通过这些措施保证服务器的安全。

3、网络安全策略

网络的安全是整个系统安全的基础，因此保证网络的安全是非常重要的。在网络方面，利用 VLAN 对网络进行划分，有限隔离广播冲突:安装防火墙，并配置严格的访问控制策略，过滤粒度为端口级，开启日志访问，有效阻断并记录非法访问，加入 IDS、IPS,防范病毒木马攻击;在重要服务器上将网关 MAC 地址进行静态绑定，防止 ARP 欺骗攻击;同时；部署统一安管平台，实时监测网络设备的利用率与吞吐量，出现网络堵塞等问题时能迅速通过短信、邮件等方式进行报警，及时:加以整改，保证了网络的安全可靠。

4、应用安全策略

在前期程序员的开发阶段，我就召集程序员，要求他们要有安全意识，时刻将安全放在首位，遵循“用户端的输入是不可信”的原则，对用户端输入进行判断过滤，并只开放满足需求的最小权限，防范越权操作。系统开发完毕，光由功能性能测试小组进行测试，修正 Bug 后，再交由安全测试小组对系统进行安全渗透测试，抱据是否存在如 SQL 注入、跨站、越权操作等应用安全漏洞，再一一进行修补。

5、数据安全策略

在此次项目中，数据作为核心资源，其安全性尤为重要，卷本系统中采用了下面的数据保护策略。首先对数据库进行分域，不同的数据放到不同的域中，各个域互相独立，防止混用。设置当前数据库和历史数据库，当前数据库只存放两天的数据，其余的数据通过 DataStation 转移到历史数据库，保证了数据的安全可靠。在数据库的备份方面采用全量备份和增量备份相结合的方法，定期备份数据文件和日志文件，并且使用了某厂商的安全备份恢复管理软件，提高了备份的安全与效率。此外，关键数据采用加密算法加密后存放，保证数据安全可靠。

经过我们团队不懈努力，本项目最终通过了业主方组织的验收。该改造项目成功实施，收费系统联网智能控制如期上线，为用户解决了收费效率低下、车道拥堵等问题，得到了业主的好评。该项目是成功得益于完善的信息系统安全策略，有效避免了数据泄密的风险，保障了系统安全稳定运行。当然，任何系统的安全都不是一成不变的，因此仍必须不断加强系统安全完善措施，不断发现和改进漏洞，积极进行防护，才是保障教学教务管理系统安全的根本。通过这个项目，我积累了不少经验，在今后的工作中我也将继续努力，和同行交流，不断总结经验教训，提升自己业务管理水平，力争为信息化建设更好的服务。

安全管理范文 2

摘要

2017 年 1 月，我作为项目经理参与了 XX 市 XX 集团的资金管控系统建设的项目。该项目合同金额为 550 万元，建设工期为 1 年，建设内容包括资金管控系统的软硬件建设及运行环境解决方案。通过该项目的建设，实现了该集团提高资金使用效率、降低资金运作成本、加强资金使用监控、提高管理效率的建设目的。该项目于 2018 年 1 月顺利地通过了业主方的验收，赢得了用户好评。

本文结合作者的实际经验，以本项目为例，讨论了信息系统项目建设过程中的安全管理，主要从以下几个方面进行了阐述：信息安全管理制度体系建设、信息系统基础设施安全管理、网络环境安全策略、应用安全策略、数据安全方面策略等。

正文

2017 年 1 月，我作为项目经理参与了 XX 市 XX 集团的资金管控系统建设的项目。该项目合同金额为 220 万元，建设工期为 1 年，通过该项目的建设，实现了该集团提高资金使用效率、降低资金运作成本、加强资金使用监控、提高管理效率的建设目的。提高了整个集团的竞争实力，节约管理成本。创造了效益。

我作为项目经理，考虑到本项目的重要性。重要的设备全部采用了部件冗余设计，系统采用双机、负载均衡，当一台服务器出现问题时，另一台会立刻接管他的任务，保证业务不中断。设计中同时考虑了备份系统，针对操作系统和数据库文件制定了不同的备份策略，以备不时之需。该项目是一个开放、灵活、可扩展、性能

稳定的资金管控处理系统，采用了主流的 B/S 架构，系统采用了 MVC 设计模式，基于 J2EE 技术进行构建，分为数据层、业务逻辑层、WEB 展现层等。

信息系统安全策略是指针对本单位的计算机业务应用信息系统的安全风险（安全威胁）进行有效的识别、评估后，所采取的各种措施、手段，以及建立的各种管理制度、规章等。安全策略的核心内容就是“七定”，即定方案、定岗、定位、定员、定目标、定制度、定工作流程。

针对该项目时间紧、任务重、数据交换复杂度高、项目业务系统接口多、分阶段部署难度大等特点，我在项目管理过程中尤其重视系统建设过程中的安全管理。我采用了信息系统项目安全管理的理论知识及其指导方法，从安全管理的以下几个方面进行安全策略的制定。

1、建立科学合理的信息安全管理制度，完善岗位和人员的设置

在制定系统的安全信息安全管理制度是，本人参照我公司信息安全管理体系的要求，并结合实际情况，在充分征求了客户和公司领导的前提下，制定出本系统的安全管理制度，并就制定出来的制度与相关的干系人进行讨论与评审，评审通过后请客户的领导签字确认再正式实施。

1.制定信息安全方针文件，明确信息安全的目标是建立和完善信息安全的策略体系、组织体系、技术体系和运作体系，争取达到领先的信息安全保障水平，保障和促进资金管理系统的业务发展和业务目标的实现。

2.为了促使信息安全管理体系有效，我制定了信息安全管理组织文件，明确地界定了体系内的组织结构及成员的职责与义务，确保了信息安全管理体系能有效运行。在甲方领导的积极配合下，在文件中，确定了信息安全领导小组、信息安全工作小组，并设定了其相应的职责范围，设置了相关的系统安全管理人员，如机房管理员、网络管理员、系统安全管理员、安全审计人员等，并制定了详细的职责。例如网络管理员的职责在于对网络设备进行安全配置，进行网络的集中实时监控、网络连通性监测和检查，确保系统访问的网络通畅等。机房管理员负责信息系统所处环境的物理安全，如进出人员登记、温湿度环境监测设备的定期检查等。

3,人员安全管理。为了防止信息滥用、丢失和泄密，同时规范人员录用和离职的管理过程，制定了人员安全管理贵方，规范共包括对人员招聘、入职培训、人员录用、人员转岗和离职等环节，在组织和流程上保证了信息安全的科学、合理、可靠。

2、信息系统基础设施安全管理

考虑到资金管控系统的重要性，以及对业务连续性的严格要求，在基础设施建设方面，在征得甲方项目负责人的同意之后，部署了 UPS 系统，能在意外断电后自动为主要设备服务器持续提供电力 30min,保证资金管控系统不因意外断电而中断服务或造成服务器硬件损坏。为保证硬件设备运行环境良好，向甲方建议部署了两台艾默生精密空调，保障服务器等硬件设备的温湿度适宜，避免因温湿度环境影响硬件使用寿命。

3、网络安全策略

网络的安全是整个系统安全的基础，因此保证网络的安全是非常重要的。在网络方面，交易内网与互联网接入，采用一台入侵防御设备，抵御外来不安全流量和非法入侵等，充分保证网络的安全性。在网络接入边缘采用两台天融信 UTM 安全防火墙系统,采用双机方式部署,确保避免单点故障的存在,同时启用了对外的 SSLVPN 功能，实现外部办公用户安全的远程接入功能；

通过安全防火墙将交易网划分为三个区域，交易网办公区域、银行接入区和服务器区域；服务器区域根据此次设计需求实现核心交易系统、病毒服务器、备份服务器以及其他应用的部署；银行接入区实现外部银行的专线安全接入，通过防火墙对此区域提供高细度的安全策略保证业务系统的高可控和安全访问的需求。通过网络安全的考虑所有服务器和办公网络用户 PC 均部署趋势防病毒产品，保证终端接入的安全性，提供全网的安全统一管理，对用户和服务器执行分段分类的安全扫描任务。

4、应用安全策略

在此次项目中，在前期系统开发阶段，我就着急项目组成员，要求他们要有安全意识，时刻将安全放在首位，遵循"用户端的输入是不可信”的原则，对用户端输入进行判断过滤，并只开放满足需求的最小权限，防范越权操作，系统开发完毕后，先有功能性能测试小组进行测试，修正 bug 后，再交由安全测试小组进行安全渗透测试，进行安全测评，挖掘是否存在如 SQL 注入、跨站、越权操作等应用安全漏洞，并逐一修补。

5、数据安全策略

此次项目中，数据作为核心资源。其安全性尤为重要，要保证数据的防丢失、防泄漏、防篡改。首先对数

据库进行分域，不同的数据放到不同的域中，各个域相互独立防止混用。设置当前数据库和历史数据库，当前数据库只存放未完结业务档案，其余数据存放到历史数据库中保存，保证了数据的安全可靠。在数据库备份方面采用了全量备份及增量备份相结合的放大，定期备份数据文件和日志文件，并且是用来某厂商的安全备份恢复管理软件，提高了备份的安全与效率。此外，关键数据采用了加密算法加密后存放。

经过大家的努力，项目于 2018 年 1 月顺利完成并通过验收，目前运行稳定，使用情况良好。虽然整体来说，项目的安全策略管理做得比较全面，但是还存在一些不足。比如随着系统的稳定运行，业务量的增加，需要备份的数据量激增，就导致当时选用的 2M 专用备份专线的带宽不能满足备份要求，不能在一个业务日内完成当天数据的备份，经与甲方沟通，向运营商申请将带宽升级到 10M,解决了该问题。

此次问题的出现，使作为项目经理的我充分认识到项目安全管理在项目管理过程中的重要性。由于项目本身的不同、项目所处环境的不同，项目管理的方式、方法也不尽相同，只有针对信息系统定制完善的安全策略才能保障系统上线后稳定运行，达到系统建设目的。

安全管理范文 3

【摘要】

2017 年 6 月，我参加某集团 ERP 项目建设工作，作为项目经理负责项目的整体规划、分析设计、组织实施与管理控制等全面管理工作。该项目总投资 1200 万元，以 ERP 知名软件 SAP/R3 为核心，结合企业的行业特点打造 ERP 运营管理系统，功能包括人力资源、财务与成本、物资管理、销售管理共 4 个管理模块。经过 1 年的项目建设，最终通过业主方的验收上线，取得了用户的一致好评。在项目建设中，我深刻认识到实施完善的信息安全管理策略是本次项目成功实施的关键。主要从信息安全的制度、流程、岗位、职责、人员为出发点，制定了科学合理的信息安全制度体系。按照系统实际情况从主机、网络、应用服务、数据安全等方面进行信息安全的有效管理，保障了系统的安全、高效、可靠。

【正文】

某集团为了支撑集团整体业务架构，通过打造以 ERP 为核心的集团管控平台建设，达到提升业务管控力度与效率的目标，于 2017 年 6 月 6 日正式启动此项目。我公司中标该项目，金额为 1200 万元，建设工期为 1 年，我以项目经理的角色负责项目的全面管理工作，历时一年于 2018 年 6 月通过客户方的验收。

该项目以 ERP 业内知名软件 SAP/R3 为核心，根据该企业的行业特点为其打造 ERP 运营管理系统，功能覆盖人力资源（HR）、财务与成本（FICO）、物资（MM）、销售（SD）4 个管理模块。通过该项目的建设，统一基础数据的管理，规范业务流程，实现了跨部门、跨模块间业务流程的流转、集成和管理信息的共享，达到了企业纵向管理一体化、横向信息集成化的目标。该项目采用三层 C/S 体系结构客户端、Weblogic 应用服务器和 Oracle 数据库，开发平台支持 J2EE 和 ABAP 编程语言，支持各类平台的接口。SAPGUI 作为用户界面可移植运行于多种操作系统平台，实施时采用三系统模型，即开发系统、测试系统、生产系统。并通过 VSS 管理项目各阶段文档资料，作为后续查询、修改、跟踪、学习的依据。

该项目是一个综合性的系统工程项目，涉及集团总部、4 个大区公司及其下属 23 家子公司，在管理模式上存在较大差异，各地区工作流程也不一致，集成专业多。由此可见该项目组织构成复杂、质量要求高、干系人面广人多、不可控因素多，协调难度大。我将项目分为 HR、FICO、MM、SD、硬件集成部署、SAP 软件开发共 6 个项目小组，分别委派组长进行管理，明确其职责与权力。为了保证项目圆满完成，我组建了强矩阵的项目组织结构。由于系统中保存有用户的个人数据信息和公司业务经营数据，其安全性要求相当高，集团公司领导非常重视，一再要求确保安全性。通过有效的项目管理，特别是出色的安全管理，带领项目团队全体成员经过奋战获得了良好的绩效，取得了项目的成功，保障了系统的安全、高效、可靠。下面分别从建立信息安全管理制度体系、主机安全策略、网络安全策略、应用服务安全策略、数据安全策略等方面重点阐述项目安全管理。

1、建立科学合理的信息安全管理制度体系

在制定系统的信息安全管理制度时，本人科学地运用信息安全管理的理论知识，结合公司信息安全管理体系的具体要求和系统的具体情况，在充分征求客户和公司领导的前提下，从信息安全的制度、流程、岗位、职责、人员未出发点，制定了科学合理的信息安全制度体系。并对制定出来的制度与相关的干系人进行讨论与评

审，评审通过后，请客户方领导签字确认，正式实施。

制定信息安全方针文件，明确信息安全的目标是建立和完善信息安全的策略体系、组织体系、技术体系和运作体系，争取达到领先的信息安全保障水平，保障和促进 SAP 系统业务发展和业务目标的实现。

为了促使信息安全管理体系明确有效地界定体系内的组织结构及成员的职责和义务，确保信息安全管理系统能有效运行，制定信息安全管理组织文件。在客户领导的积极配合下，在文件中，确定了信息安全领导小组、信息安全工作小组，设置了相关的系统安全管理人员，如机房管理员、网络管理员、系统管理员、安全审计人员等职位，并制定了详细的职责。例如网络管理员的职责是对公司网络设备进行安全配置、集中实时监控、网络连通性监测和检查，保证用户对 SAP 系统的访问通畅，对网络设备的用户、口令的安全性进行管理，参照相应规定对网络设备登录用户进行监测和分析，负责所管理网络设备的用户账号管理，一用户一唯一账号，同时根据对网络设备安装、配置、升级和管理的需要为用户设置相应的级别，并对各级别用户访问权限进行设置。人员安全管理。为了防止信息滥用、丢失和泄密，同时规范人员录用和离职管理过程，制定了人员安全管理规范，包裹对人员招聘、入职培训、人员录用、人员转岗和离职、持续改进等 5 个环节，在组织和流程上保证了信息安全的科学、合理、可靠。

2、主机安全策略

主机操作系统作为软件的载体，其安全性至关重要。在硬件的选购行，经过充分考察后，我选用主流品牌服务器，从硬件上保证了服务器的安全性。在操作系统的选择上，经过与客户领导进行交流讨论，最后确定 SuseLinux 操作系统，虽然在图形化外观上有些不足，但其安全性是有目共睹的。制定了服务器的安全使用规定，根据业务需求建立不同用户，且每个用户竟有满足当前业务需求的最小权限，有限避免用户的越权访问；开启安全审计策略，审计用户的操作；关闭不必要的端口及服务；定期对操作系统进行更新；通过这些措施保证服务器的安全。

3、网络安全策略

网络安全是整个系统安全的基础，因此保证网络的安全是非常重要的。在网络方面，利用 VLAN 对网络进行划分，有限隔离广播冲突；安装防火墙，并配置严格的访问控制策略，过滤粒度为端口级，开启日志访问，有效阻断并记录非法访问；加入 IDS、IPS,防范病毒木马共计，在重要服务器上将网关 MAC 地址进行静态绑定，防止 ARP 欺骗攻击；同时，部署统一网络安全管理平台，实时监测网络设备的利用率与吞吐量，出现网络堵塞等问题时能迅速通过短信、邮件等方式进行报警，及时加以整改，保证网络的安全可靠。

4、应用安全策略

在前期程序开发极端，我就要求程序开发人员要有安全意思，时刻将安全放在首位，遵循“用户端的输入是不可信”的原则，对用户端输入进行判断过滤，并只开放满足需求的最小权限，防范越权操作。系统开发完毕，先由功能性测试小组进行测试，修正 BUG 后，再交由安全测试小组对系统进行安全渗透测试，挖掘是否存在 SQL 注入、跨站、越权操作等应用安全漏洞，在进行修补。

5、数据安全策略

在此次项目中，数据作为核心资源，其安全性尤为重要，在本系统中采用了下面的数据保护策略。首先对数据库进行分域，不同的数据放到不同的域中，各个域互相独立，防止混用。设置当前数据库和历史数据库，当前数据库只存放两天的数据，其余的数据通过 DataStation 转移到历史数据库，并把历史数据库中 6 个月前的数据转移到磁带库进行存放，保证了数据的安全可靠。在数据库的备份方面，采用全量备份和增量备份相结合的方式，定期备份数据文件和日志文件，并且使用了某厂商的安全备份恢复管理软件，提高了备份的安全与效率。此外，关键数据采用非对称加密算法加密后存放，保证数据安全可靠。

经过 1 年的紧张建设，项目与 2018 年 6 月 1 日成功全面上线运行，并顺利通过用户的验收，至今运行良好，得到了用户的高度评价。回顾起来，项目的成功很大程度上归功于制定了完善的信息系统安全策略，有效避免了数据泄密的风险，保障了系统安全稳定运行。诚然，任何系统的安全都不是一成不变的，因此，仍必须不断加强系统安全完善措施，预防为主，防治结合，不断发现漏洞，积极防护，才是保障系统安全的根本。

摘要

2018 年 12 月，我公司中标了某彩票中心“可信消息传递平台”建设项目，我担任项目经理一职，项目建设费用为 325 万，工期为 4 个月。彩票中心希望通过本项目为彩民提供多元化彩票真伪综合查询平台，为彩票销售系统交易信息第三方独立安全查询、信息存储及稽核审计等功能。本文以本项目为例，结合我的工作实践，探讨在项目安全管理中遇到的问题和解决方法，了解和掌握项目安全问题的来源、性质和发生规律，完成有效的安全应对措施，进一步树立客户对项目成功的信心，项目组提出以编制安全管理计划、安全脆弱性识别、安全管理策略制定、安全风险应对和安全监控等方面指导项目的安全管理，在安全管理过程中遇到的问题及时提出了解决方法，2019 年 4 月正式上线运行，系统至今运行稳定，取得客户的好评，很大程度上得益于项目成功的安全管理。

正文

2007 年 1 月，某彩票中心为了加快建设“透明彩票”发展新理论，提高彩票公信力，突显彩票的人民属性、国家属性和公益属性,从而推进深圳福彩的品牌推广和彩票业务的跨界融合，彩票中心将“可信消息传递平台”项目列为 2018 年重点工作，项目主要包括两大部分：一是系统应用软件开发，其主要功能为：消息安全传递系统、消息稽核审计系统、消息可信验证系统及消息历史追溯系统等；其二为网络系统集成其包括：防火墙、IPS、网闸、核心交换、接入层交换机等硬件设备集成。在本项目中我以项目管理为核心，采用 MSProject 项目管理工具，实现对项目整个生命周期各个环节进行有效监控，实时动态反应项目各阶段执行情况，进行控制和分析，同时对工作流程进行可配置化管理，实现任务督办，消息提醒，协同办公等功能，计划投资 450 万，工期 1 年，项目面向 SOA 的体系结构，采用 B/S 架构，后台数据库采用 DB2,中间件技术采用 Jboss,主要用 JAVA 语言开发。由于前期项目招标过程中我也是主要参与者之一，对项目情况比较了解，通过公司领导发布《项目章程》，我有幸获得了公司领导与甲方客户的信任，成为该项目经理，全面主持项目的管理工作。

为了保证该项目的顺利完成，我采用了项目型的管理方式和间接管理模式，将项目分解为软件开发和网络集成二个子项目，并任命李某、张某为子项目管理，PDCA 循环管理方法，控制和协调好项目的进度、成本和质量之间关系。由于系统是面对互联网的应用以及系统中存在个人数据信息，因此，其项目建设安全性要求相关高，特别是近年来《网络安全法》和《个人信息安全规范》颁布和实施，确保项系统和数据安全性是重中之重，我也深刻的认识到信息安全是项目成功实施的重要保证，本人科学地运用信息安全管理理论知识，结合彩票中心信息定管理体系的具体要求，项目组通过编制安全管理计划、安全脆弱性识别、安全管理策略制定、安全风险应对和安全监控等对项目过程中的安全进行监控和管理，良好的项目管理是本项目成功与否的关键要素，下面根据本项目的实际情况，论述一下在项目安全管理过程中遇到的问题及解决方法。

1、制定安全管理计划，完成项目脆弱性识别

在制定安全管理计划，识别项目信息资产脆弱性识别，谨慎、清晰的计划能够提高安全管理过程的成功概率，因此，我们采用会议的方法制定安全管理计划，所有的项目干系人代表都被邀请参加了安全管理会议，全面地考虑信息安全对项目的影响，确定如何为该项目处理和执行安全管理活动，在计划中，具体描述了基本安全管理活动，每 2 周进行一次安全评估会议，根据项目管理理论和我司项目经验，定义了项目中的安全管理过程，估计了安全管理的时间表和费用，并把安全管理活动纳入了项目计划，把安全管理费用纳入成本费用计划。根据项目的实际情况，将项目安全划分为系统安全、主机安全、网络安全、数据安全和人员安全五大类，根据福彩中心等级保护三级要求以及信息安全管理规范为依据，通过调查问卷和访谈的方式完成了本项目脆弱性识别，特别是把参与人员安全识别不足、系统开发安全、网络安全、物理安全等作为项目计划阶段的主要安全事件，确定安全事件的基本特性，引起这些安全事件的主要因素，以及可能会影响项目的范围，形成详细的项目安全列表记录，通过干系人评审，最终形成正式的《信息资产脆弱性列表》。

2、建立安全管理制度，完善岗位和人员设置

在制定系统安全管理制度时，本人参照本公司信息安全管理体系的要求，并结合系统实际情况，在充分征求客户和公司领导的前提下，制定出了本系统的安全管理制度，并就制定出来的制度与相关干系人进行讨论和评审，评审通过后请客户的领导签字确认，再正式实施。

制定信息安全方针文件，明确信息安全的目标是建设和完善信息安全的策略体系、组织体系、技术体系和动作体系，争取达到领先的信息安全保障水平，保障和促进彩票业务发展和业务目标的实现。

明确信息安全管理体系的组织结构和成员的职责和义务，确保信息安全管理体系能够有效运行，制定信息安全管理组织文件，在福彩中心领导的积极配合下，在文件中，确定了信息安全领导小组、信息安全工作小组，设置了相关系统安全管理人员，如机房管理员、网络管理员、系统工程师、安全审计人员等职位，并制定了详细的职责。

人员管理安全，为了防止信息滥用、丢失和泄密，同时规范人员录用和离职管理过程，制订了人员安全管理规范，规范共包括人员招聘、入职培训、人员录用、人员转岗和离职、持续改进五个环节，在组织和流程上保证了信息安全的科学家、合理和可靠。]

3、完成安全管理策略制定，建立安全应用对计划

根据福彩中心《信息等级保护三级》和《信息安全管理规范》要求，结合《信息资产脆弱性列表》建立安全管理策略和安全应用计划，采用聘请第三方安全领域专家，与项目干系人采用会议的方式制定了本项目安全管理策略，其主要内容包括：系统安全策略、主机安全策略、网络安全策略、数据安全策略和人员安全策略，通过评审，完成了《项目安全策略说明书》，指导项目建设过程中安全配置和管理工作。例如：一是系统安全策略，主要采用针对登陆用户端输入进行判断过滤，并只开放满足需求的最小权限，防范越权操作，系统完成功能测试后，由外聘的安全测试小组对系统进行安全渗透测试，挖掘是否存在如 SQL 注入、跨站、越权操作等安全漏洞。二是网络安全策略，采用防火墙和 IPS 并配置严格的访问控制策略，仅开放应用端口，关闭其它无用端口，开启日志访问，有效阻断并记录非法访问，核心交换机利用 WLAN 对网络进行划分进行业务逻辑隔离。三是数据安全策略，采用主数据库和查询数据库读定分离，在数据库的备份方面采用了全量备份和增量备份相结合的方法，定期备份文件和日志文件，敏感个人数据信息进入加密存储。

制定安全风险应对计划编制，加强安全监控，根据已识别安全风险列表，制定了安全应对计划，对不同安全风险，采用了不同的应用措施和缓解计划，对每个计划都制定了责任人，项目组定期对已识别出的风险状态进行跟踪，监控安全发生概率和影响度的变化，深入分析已识别出风险，继续识别项目中新出现的安全，审计安全应对策略的执行情况和效果，根据当前安全监控结果修改安全应对策略，根据新识别安全进行分析并制定新的安全应对措施。

4、做好安全监控，降低安全事件发生概率

加强荐安全监控和追踪，在各个阶段保持良好的安全意识，把系统软件安全、网络安全、数据信息安全、人员安全识别的培养等作为项目主要安全重点关注的对象，按级别排序以电子邮件方式告知项目干系人，这样效果明显，客户领导充分了解项目安全状态和安全情况，通过有效的安全控制，加之领导的重视，项目组积极性和自信心得到了显示增强，使项目得以顺利实施。

经过努力项目于 2019 年 4 月 1 日正式上线运行，并顺利通过了验收，回顾该项目的安全管理过程，主要存在以下不足：1、外部安全事件应对不足，在项目建设期间，网监通报 443 端口出现高危漏洞，容易被黑客利用，但是在项目安全评估会议上漏掉了高危安全漏洞，在参透测试过程中才被重视，我及时召集项目团队和相关干系人重新进行评估，评审通过后，关闭了此端口。2、信息安全体策略不完善，虽然从主机、网络和系统上进行针对性的安全策略制定，但在物理安全上，却忽略机房环境的安全性，本项目友商在没有取得客户同意的情况下随我们出入机房，被客户发现后，我召集项目团队要按照机房管理制度执行，避免出现类似情况。

综上所术，项目成功很大程度上归功于制定了完善的信息系统安全策略，有效避免了数据泄密的风险，保障了系统安全稳定运行，信息系统安全是无止境的，因此不断加强系统安全完善措施，不断发展和改进漏洞，积极进行防护，才是彩票业务健康发展和稳定运行的根本，在以后的项目管理中，我要以此为经验，加强项目的风险管理，更好的完成项目管理工作。

安全管理范文 5

摘要：

2018 年 3 月，我担任项目经理，主持实施采购平台信息系统开发项目，项目工期为 8 个月。该项目基于 JEE 技术，使用 Spring 框架，实现 MVC 三层结构的 Web 系统。通过该系统，实现 XX 公司采购信息在线发布，供应商在线报价，网上开标，在线公示，在线跟踪和供应商评价等功能，实现了阳光采购。该项目于 2018 年亶月底

顺利上线，获得了领导和用户的一致好评。

本文结合作者实践经验，以该项目为例，讨论了信息系统安全管理的重要性。从系统安全管理和安全技术应用两个方面；以安全目标、策略、人员岗位、制度流程 4 个管理角度，基础设施安全、网络安全、系统安全、应用安全、数据安全 5 个技术层次，实施全面的安全管理，保证了项目安全运行。

正文：

2018 年 3 月，我司为加强供应链管理，规范采购比价流程，扩大寻源范围，实施采购平台信息系统开发项目，为供应链采购提供支持。公司任命我为项目经理，主持项目建设工作，项目工期为 8 个月。该系统实现了信息发布，供应商注册、资质审核、报价，开标，结果在线公示，备货信息跟踪，入库信息采集，付款跟进，供应商评价等采购核心功能。系统通过 SOA 接口 ERP 系统对接，实现订单导入，库存接收数量核对，发票勾兑等关联业务自动化，减少了业务人员的重复劳动和出错概率，以互联网思维改造了传统采购模式，提高了效率，规范业务操作流程，打造了该企业的阳光采购平台。该系统使用 JAVA 语言开发，基于 Spring 框架，使用了 SpringMVC,MyBatis,阿里 druid、shiro 权限管理等众多的开源技术,以实现系统的快速构建。系统接口使用了 webservice 技术，通过 soap 协议与公司的 SOA 系统集成。系统为 B/S 结构，实现了移动端应用，通过 RESTFulAPI 与移动客户端进行交互。系统采用了 tomcat 容器，使用 Mysql 数据库，服务器操作系统使用了 CentOS7,降低了系统部署的成本。应用和数据库均部署在 VMWare 虚拟机集群上，底层硬件使用了多台 IBM 服务器。

采购系统涉及公司采购、库存、制造、财务、质量等多项业务，包含物料 BOM 数据、价格数据、供应商清单、库存信息、财务数据等多项敏感数据，系统安全不容小觑。我深感责任重大，为此从系统安全管理和安全技术应用两个方面；以安全目标、策略、人员岗位、制度流程 4 个管理角度，基础设施安全、网络安全、系统安全、应用安全、数据安全 5 个技术层次；以系统的整个生命周期，实施全面的安全管理。下面以本项目为例，结合我的实践经验，论述我对安全管理的体会：

1、确定安全目标，制定安全管理计划

凭借多年的经验，我深知系统绝对的安全是不存在的。设立系统安全目标，要以信息的私密性、完整性、可用性这些安全属性为源点;从设备安全、数据安全、内容安全、行为安全等层次出发;按照注重效费原则综合考虑和平衡安全风险可能会造成的损失和实现安全目标所付出的代价，合理的设定目标。为此我根据实际情况，在以安全机制、网络参考模型、安全服务形成的三维空间中，评估项目可以使用的技术、机制，分析实现难度和成本，找到合适的位置，然后和发起人及高层领导沟通确认，合理降低他们的期望。最终，按照信息系统安全保护等级，结合本系统服务于公司供应链采购业务，涉及采购、价格、财务等商业信息的实际情况，我们评估安全问题会严重损害公司利益，故适用于系统审计保护级别。

2、根据企业安全管理标准，制定系统安全策略、定员定岗，建立安全管理的流程制度

经过多年的信息化建设，我司制定了一套完善的安全管理标准。在项目建设初期，结合项目实际情况，落实定岗、定员、定目标、定制度、定流程等内容要求，编制系统的安全策略和制度。组织人员方面，依照主要领导负责原则，确定项目发起人、信息化分管领导和企信部领导为信息安全领导小组;成立项目的信息安全工作小组，要求系统上线后的运维人员参与其中；依照审计独立原则信息安全审计科和外部的第三方安全服务提供商对系统进行安全审计。同时,项目组明确了安全相关岗位的职责和具体人员名单，并要求参与项目的人员和公司签订了保密协议。在流程制度方面，我们在项目建设初期就建立了系统的安全管理流程。如，制定了账号权限变更流程、变更发布流程、系统日常巡检流程、系统安全检查流程等流程，明确了操作步骤、审批级别和执行单位。项目组还根据系统的角色清单，绘制了角色不相容矩阵，有审计人员定期对上述流程的过程文档和系统账号角色的不相容进行审计。

3、基础设施安全

我司的机房符合电子计算机机房涉及规范，机房设有门禁，采用市政双路供电，设有 UPS 电池间，机柜配备相应的安保措施，包括防水、防尘、防电磁干扰及报警设备。应用和数据库均部署在 VMWare 虚拟机集群上，底层硬件使用了多台 IBM 服务器，并使用了超融合技术，能够服务器硬件或网络发生故障时自动完成系统故障转移，具备一定的容错和冗余，提高设备的可用性。机房设立远程的灾备中心，系统数据定期备份到灾备中心的带库中。

4、网络安全策略

采购平台系统部分功能需要发布公网服务，其网络安全极为重要。为此，按照公司网络管理要求，该系统被部署在了防火墙后，对外网的非法访问进行限制。我门将不同的系统功能进行拆分部署对外网用户服务的功能放在了 DMZ 区。公司购买了深信服的入侵检测防护系统，可以实施监控记录网络流量，并能够对部分入侵和攻击行为进行阻断。公司每半年邀请外部顾问对网路安全进行检查，评估可能的威胁和防护的有效性。

5、系统安全

在系统安全方面，我们对操作系统和数据库建立不同的账户，依照最小权限原则每个账户均具有满足当前业务选哟的最小权限，有限避免用户的越权访问；开启安全审计策略，审计用户的操作。明确密码复杂度要求。关闭不必要的端口及服务。定期对系统进行更新和杀毒。

6、应用安全

PKI 技术是公钥基础设施，以不对称加密技术为基础，用于身份验证，确认你是谁；而 PMI 是权限管理基础设施，用于确认用户能作什么。项目中，我们从 WoSign 购买了数字证书服务，使用证书对系统网站进行认证。网站全部使用 https 协议，使用 SSL3.1 协议对网络传输进行加密。服务器受到请求后，将数字证书和公钥发送个用户，用户通过 CA 验证网站证书，然后生成一个对称加密的会话密钥，并通过服务器的公钥对其进行加密，发送给服务器。服务器收到后，用私钥解密，获得会话密钥，双方通过对称加密技术传递信息，建立一条安全通道。权限管理方面，我们使用基于角色的访问控制方式，功能中实现了系统的角色管理，建立角色和系统功能菜单和操作的对应关系；另外在数据权限控制方面，我们对数据设置了归属组织标识，对角色赋予数据范围标识，如跟人数据，组织及下属组织数据，公司数据，建立了角色的数据权限。在接口方面，使用了基于自定义 SoapHeader 验证的方式建立了和外围系统的双向验证。

7、数据安全

数据方面，我们在 druid 中配置了 sql 注入防火墙。Mysql 启用了主从分布式部署。要求数据库管理员每周进行数据库全备，每天进行增量备份，并每天检查数据库备份的完成情况。数据库备份在本地和灾备中心同时保存，保存期限一个月，定期进行备份数据的恢复测试。

通过项目组的努力，项目于 2018 年 11 月顺利上线，并运行至今未发生安全事故。信息安全工作小到关系个人隐私，达到关系国家安危，民族利益，不容小觑。所有的信息化工作者都必须树立安全以实，做好信息系统的安全管理和建设工作。对于一个系统来说安全是一个长期的、动态的管理过程，我们只有不断通过 PDCA 循环的方式促进信息安全的不断改进。我将继续学习信息化系统的安全管理知识，树立安全管理意识，将项目管理的相关支持应用到日常的工作中，不断努力，为我国的信息化事业做出自己的贡献。

安全管理范文 6

摘要

2018 年 6 月，我参加了**市人民检察院信息化平台升级改造项目，在本项目中担任项目经理。该项目总合同额 800 万元，总工期历时 8 个月。通过此次建设实现了综合布线子系统，时间轴子系统，机房建设子系统，网络子系统，固定资产子系统，检务公开查询子系统，微信公众号子系统，监控子系统，门禁道闸子系统，远程提讯子系统，智慧办公会议室子系统的建设。项目最终于 2019 年 1 月完成整个信息化平台的建设工作，获得客户的一致好评。本文将结合该项目实际情况，结合检察院的信息安全体系的具体要求和系统的具体情况，从信息安全的制度、流程、岗位、职责、人员为出发点，和以下就几个方面阐述项目中的信息安全管理：安全管理制度及体系建设、组织结构及人员管理、物理环境安全、网络通信安全、设备和计算安全、应用和数据安全。

正文

2018 年 6 月，我参加了**市人民检察院信息化平台升级改造项目，在本项目中担任项目经理。该项目总合同额 800 万元，总工期历时 8 个月。通过此次建设实现了综合布线子系统，时间轴子系统，机房建设子系统，网络子系统，固定资产子系统，检务公开查询子系统，微信公众号子系统，监控子系统，门禁道闸子系统，远程提讯子系统，智慧办公会议室子系统的建设。实现了检察院工作网络化，信息化。强化了检察队伍的专业性，提高了办案效率。让检察事务和工作更加透明化，保证法律的严肃性和公正性。通过机房系统、监控子系统和门禁道闸系统的建设，为检察院提供了安全可靠的物理环境安全基础，机关人员通过加入生物识别，如指纹和

人脸认证进出机关的公共区域和自己的办公室。通过网络系统的建设，将办理的案件通过工作网传输，通过网络安全手段，得到了不错的数据安全管理和流量控制。整个平台我们采用的 B/S 架构，JAVA 语言，oracle 数据库，并以租用阿里云服务的形式建设的一整套平台。通过租用服务器的形式，转移了对服务器的安全风险，为数据安全提供了可靠的支撑。在数据安全层面，我们还对用户的权限做了最小定义处理，让用户只处理满足自己业务的数据，以避免因操作失误导致数据不可逆的情况。以此保证平台的安全、可靠、高效、稳定运行。

1、安全管理制度

在制定安全管理制度及体系的时候，我们综合公司的安全管理体系和检察院的安全管理体系的共同要求，并结合项目的实际情况，充分征求公司领导和客户领导的意见后，制定了适用于本项目的安全管理制度，并就制定的安全管理制度通过会议的方式与项目主要干系人进行讨论，客户领导在会议中提出，系统中设计到很多用户数据和案件数据，有些属于敏感数据，一定要确保数据的安全和备份防灾工作。最终评审通过确认后，再正式实施。管理制度主要为组织机构及项目成员的安全管理，物理环境安全，网络通信安全，设备和计算安全以及应用数据安全的管理提供了基础依据。

2、组织结构及人员管理

为了促使信息安全管理体系有效及明确地界定体系内的组织结构及成员职责和责任，确保信息安全管理体系能有效运行，制定信息安全管理组织文件。在检察院领导的积极配合下，在文件中确定了，信息安全领导小组、信息安全工作小组、并针对各个子系统设立了响应的子系统安全员，如机房管理员、网络通信管理员、系统工程师、安全审计人员等职位，并制定相应的职责。例如机房管理人员负责监控机房的物理环境，如温湿度，是否有烟感报警，红外报警等信息，并在有上述情况下第一时间做按照安全应急方案进行处理。网络通信管理员主要检测网络的通断情况，流量是否有拥塞情况，访问速度是否异常，以此保证检察院的网络通信通畅。通过对网络设备用户口令的安全性管理，可以观测到用户登录网络设备的日志记录，可统计访问相应设备的访问量和请求量，做好网络负载均衡和优化的工作。系统工程师主要对现的运行各子系统的访问用户和运行强壮性进行定期检查，保证系统可以稳定的服务检察院业务的流转。并定期组织对业务人员相关系统安全培训，提高检察队伍对信息安全的防护专业性。同时系统工程师负责对机关用户的电脑系统和病毒库进行升级，提升用户电脑的强壮性。

3、物理环境安全

在对机房建设的过程中，我们选择的是二级防火材料，并且通过刷环氧地坪漆的方式和墙面挂沥青的方式做到机房的防尘防水处理，针对该市检察院有白蚁的情况，我们在机房基层建设过程中，通过喷洒白蚁防治药物和水泥中混有白蚁药的方式，来防治白蚁。通过在机房静电地板下铺放田字型紫铜已达到防雷的效果，并最终经过当地气象局的测量达到机房防雷标准。同时机房中配有温度传感器和湿度传感器，对机房的异常温湿度做到实时监控。并利用红外传感器和烟感传感器监控来保证机房的安全。当有异常情况发生时，利用短信平台发送报警短信至机房管理员，从而第一时间处理机房问题。除机房以外，我们对检察机关内的工作人员电脑进行了电脑的日常除尘和防护培训，为日常办公提供了一定的保障。

4、网络通信安全

该项目在网络上的通信主要通过防火墙、入侵检测、入侵防护和安全审计、路由协议及 mac 地址绑定的方式、acl 控制的方式来实现。我们通过设置防火墙的黑白名单设置，拒绝黑名单中的访问请求，但这远远不够的，应为防火墙无法抵御来自检察院内部的攻击，于是我们采用入侵检测的方式，对机关内部的情况进行定期检测，以避免对检察工作带来麻烦。同时定期更新特征库，以达到安全防护工作的前沿。同时我们为整个系统设立了“黑匣子”和“监护神”。即时系统因为攻击奔溃、瘫痪，通过安全审计也可查到其原因，留痕记录。安全审计同时也对发现的攻击进行处理，及时铲除威胁。在路由层面，我们通过设置可访问地址段和禁止访问地址段的控制，已达到路由层面的控制。以及 vlan 的划分，可以有效防止广播风暴的威胁和发生问题时波及的范围。通过 mac 地址与 ip 绑定，可以有效防止 arp 欺骗的攻击。以及利用 acl 控制协议，创建哪些用户可以访问，进一步可以控制某些用户可以访问哪些资源，这样就做到了权限的控制，不会让用户越权造成不可逆，无法追溯的事件发生。

5、设备和计算安全

在机房中的设备，我们采用登记，贴标签的方式记录每个设备的详细情况。并利用动环监控系统，实施检

测设备的内存使用率，硬盘使用率，cpu 使用率等信息，可以在出现问题时第一时间获知。每台设备都落实到具体人员负责，并对机房中的设备进行定期巡检，并针对巡检得到的问题进行分析，处理和解决。对检察机关用户使用的涉密电脑，我们采用禁用外设的形式，以保证终端安全。

6、应用和数据安全

在信息化平台应用中，我们通过设置角色，为角色赋权限的形式，将权限最小化，是的权限可控。为了保证数据安全，本项目采用租用阿里云的方式，租用服务器，同时本地也建立一个灾难备份冗余服务器，对数据进行热备份。以避免数据的丢失和意外发生。

项目最终于 2019 年 1 月完成整个信息化平台的建设工作，获得客户的一致好评。在整个项目建设过程中，严格遵守制定的信息安全制度，保证了检察院工作效率的同时，还提供了安全，可靠，稳定的办公环境。参照本次项目经验，我将从中汲取知识，为今后的项目建设贡献自己的一份力。

安全管理范文 7

摘要

2018 年 1 月，我作为项目经理，参与了 xx 省某三级医院的电子病历系统进了建设工作。该项目总投资 800 万元，建设工期为 1 年，在全院 30 多个科室建立起了电子病历和无线查房系统。其功能包含病历模块化书写与存储，移动医护查房工作站系统。移动医护查房工作站的使用，把医院的信息化建设连接到病人的床边，解决了信息化止步于办公室的最后 20 米问题。本项目于 2019 年 1 月顺利通过了验收，赢得了用户的好评。本文以该项目为例，讨论安全策略管理问题。特别是在管理实践中建立群防群治体系，以及建立人防、物防、技术等多重的安全管理策略，较好的实施了从硬件的防火防盗、数据的安全备份、网络的病毒防护以及各级操作权限的审批等一系列的安全策略，保证了项目的安全运行。

正文

该三级医院作为全省排名考前的三级综合医院，开房床位一千余张，年出院 3 万人次，年门诊量 60 万人次，一直以来，院领导十分注重医院的信息化建设，为了贯彻党中央国务院《关于深化医疗卫生体制改革的意见》精神，提高医护质量，全面建设数字化医院，院领导决定投资建设电子病历系统，最终我公司中标，并任命我为项目经理负责该项目的建设工作。该项目投资 800 万元，于 2018 年 1 月只 2019 年 1 月结束，分软件、硬件两部分。本系统采用 B/S 架构，数据库采用 SQLSERVER2012 企业版，将实时数据库与历史数据库作分库处理，将一些配置数据以及一些当天未处理信息存入实时数据库中，将历史处理信息存入历史数据库中。同时，为了提高数据查询性能，历史数据库中采用分区和索引的技术。采用两台 IBMX3650M 双四核机架服务器做双机备份。在各个病区，采用无限 AP 架设了服务 IEEE802.11g 规范的 2.4GHZ54MN/S 的无限局域网。软件部分包含医护电子病历的书写与存储系统和医护移动查房系统两个模块，按照卫生部《医院电子病历规范》和本院各科专家知识设置；各种病历模板，极大的减少了医护人员的时间，把他们从繁重的文字书写工作中释放出来，将更多的时间留给与病人的交流和护理。

由于本项目规模大、建设工期比较紧张，涉及到的干系人众多，为了保证项目的圆满成功，我通过有效的安全管理策略，带领团队成员经过分站取得了良好的绩效，获得了本项目的成功。本文结合我的实际经验围绕信息系统的安全管理，主要从以下几个方面进行讨论。

1、设备安全

设备安全就是要保证设备的可靠、可用和稳定。为此，在机房建设中，我将服务器置于防静电机房中，其建筑材料采取耐火等级为二级的材料，并且其面积约为 15m2,并设立一个安全出口，此安全出口设置为对外开启，且能自动关闭。同时，我要求院方在机房中不放置任何与服务器无关的杂物。空调保持常开启状态，将室温稳定在 20 摄氏度左右。在机房以及楼道重点区域安装烟雾传感器、温度传感器以及湿度传感器，并将数据进行汇总显示，当发生异常情况或者依据相关预警模型检测到即将发生火灾、水灾等情况时，能在各终端快速显示，同时触发各楼层保卫办公室紧急报警。为确保服务器的稳定性和可用，采用双机热备的方式，两个服务器分别位于主楼和保卫楼，两个服务器通过热备软件实时备份其数据库，两个服务器对外采用同一虚拟 IP,当一台服务器由于不可抗力原因不可用时，另一台服务器自动接管业务。同时，服务器采用独立备用电源，在供电电

源断开后，仍能通过备用电源工作 4 小时，为医护工作者在应急情况下，及时了解到当前未处理的紧急事务以及及时存储、查看相关业务。在机房外走廊中，设立灭火器，每天均安排专门的人去检查灭火器是否可用。

2、数据安全

数据安全主要就是保证数据的不被篡改和截取。针对病毒，我们购买了防火墙、VPN 和卡巴斯基杀毒软件，并给每个客户端进行了安装，定期为其升级病毒库。同时，对内网做了物理隔离，上外网的计算机绝不允许上内网。对于数据库中数据不被截取和篡改，在访问中，采用 https 加密技术，保证数据在传输过程中不被截取。同时，对于数据库中的重要信息，如病人就诊结果、就诊用药等关乎病人生命健康的信息和类似于值班记录、设备安全记录等关乎职责的数据，采用冗余加密存储，即同一份数据分别按照明文和密文的方式存放于两个数据表中，并且实时检查此两表的数据内容，当发现两表中数据有偏差时，拒绝此次修改并将此操作加以记录。同时，数据库的操作密码以及权限仅为数据库管理人拥有。将数据库作备份，通过热备软件实时备份至备机数据库。当主机数据库因故不可访问时，应用程序根据 UDP 连接返回值，主要切换数据库连接，而这对使用者而言，基本上察觉不到任何变化。

3、内容安全

由于本系统会对病人以往的病史进行记录，会涉及到病人的隐私，所以原则上，非本科室的医护人员不得查看到其他科室的相关病史。当然，对于一些特殊疾病会涉及到用药就诊的情况，如有心脏病史的病人在用药方面需特别谨慎的，则会明确标出其心脏病史，而对于一些比较隐私类的疾病，如 HIV 携带、乙肝携带等，则为了病人的隐私不会显示出来。最重要的就是对于相关备注类信息、页面的整体规范符合国家相关标准，绝不出现任何种族歧视、地域歧视、性别歧视、性少数歧视等相关字眼。

4、行为安全

行为安全就是要保证行为的可控性、秘密性和完整性。我们在机房或有关重点区域安装防爆摄像头，实时检测各地区安全。通过热成像技术智能分析摄像头内容，将存在安全隐患或人员进出重点区域记录存储并实时通知有关干系人。对于每份病历的录入以及对系统的相关配置信息的插入、修改、删除，查询机密信息等行为，都会记录于日志文件中，以便在发生纠纷或责任推诿时，据此来分析责任归属。对于输入系统的任何数据或即将存入系统的任何数据，都会对齐进行格式校验以及非法校验，绝不让任何不合理数据由于操作问题影响整个系统的正常运行。

通过我的不懈努力，历时 1 年，本项目终于于 2019 年 1 月通过了业主的验收，赢的了用户的一致好评，为医护工作者解决了病历填写复杂繁琐，查房不便等问题，本项目的成功得以于我出色的项目管理，最重要的是安全策略管理这方面。当然，本项目也存在些不足之处，如购买的防爆摄像头在断电上电后，会有三分钟缓冲时间，从而导致此三分钟内看不到任何数据或出现画质及其模糊的现象，我们已经联系厂家积极配合修改了此问题。在后续的学习中，我将不断学习安全知识，完善系统安全措施，为我国信息化建设多做贡献。

本人女，2016 年毕业，从事软件开发 3 年

安全管理范文 8

摘要：

2017 年 7 月，我作为项目参与了国内某港口散杂货理货信息化系统项目的建设，该项目总投资 800 万元，建设工期为 1 年。该项目主要由码头散杂货管理系统的改造、无线理货和其他部分组成。通过该项目的建设，实现了码头散杂货管理系统信息化的扩展，提高了码头装卸效率，减小了工作中人为因素的影响，使各部门协调一致，简化工作程序，大大提高港口散杂货理货服务水平和服务质量，加强码头竞争力。

2018 年 7 月，该项目顺利通过用户的验收，赢得甲方的一致好评。信息安全是信息系统正常运作的重要保障，下面根据我的实际工作经验，以本项目为例，讨论信息化管理项目中的安全管理，主要从规划安全管理计划、执行实施项目安全管理工作和控制安全管理这几个方面进行论述。

正文：

2017 年 7 月，我公司顺利中标国内某港口散杂货理货信息化管理系统项目，我有幸作为项目经理，全程参与了该项目的建设，该项目总投资 800 万元，建设工期为 1 年。通过该项目的建设，实现了码头散杂货管理系

统信息化的扩展，提高了码头装卸效率，减小工作中人为因素的影响，使各部门步伐协调一致，简化了工作程序。在充分了解国内外港口码头散杂货理货系统信息化的最新工作模式的基础上，结合码头实际情况和我们团队信息化项目建设的以往经验,把项目分为三部分：码头散杂货理货系统的改造部分、无线理货部分和其他部分。码头散杂货理货管理系统的改造部分主要包括商务管理、理货管理、调度管理、库场港存管理、统计系统等，主要负责装卸现场的的作业计划、调度、管理、统计分析等工作。无线理货部分是我们这次项目的主要核心模块，它的实现模式是：电子理货系统从中间层服务获取工作任务和配工调度信息后，并以内存数据库形式存储。现场使用手持终端，完成现场业务操作之后，通过多线程运行，利用 4G 网络自动上传到电子理货中间层。同时将电子理货中的行驶指令传递给倒运车辆 GPS 终端设备，指引倒运司机行驶到指定的地点，并且同步其他理货指令到相应系统，例如计量、外理等系统，并完成指令完整性校验。其他模块主要是计量系统和其他系统的接口等，根据理货指令，独立执行计量后信息自动上传到电子理货中间层。

随着港口行业的迅速发展，越来越多的港口管理部门开始重视理货系统信息化建设，提高码头装卸效率。由于本项目信息平台建设趋向于资源集中和共享化，各政府部门和企业主体共同从平台录入或获取所需要的信息，全信息化作业，既节约时间和费用成本，又便于集中管理，因此信息系统的安全管理显得尤为重要，为了保证项目圆满完成，我选择了项目型组织结构。下面我将围绕该项目的安全管理的规划安全管理，执行实施安全管理和控制安全管理等方面对信息系统项目安全管理进行重点讨论。

1、建立合理的信息安全管理制度

随着信息技术与应用的不断发展，伴随而来的信息系统安全问题越来越引起人们的关注。作为项目经理的我深知，信息系统一旦遭受破坏，将给使用单位带来不可估量的损失，因此加强信息系统安全工作，是信息化建设工作的重要工作内容之一，而制度的建设是安全前提。在项目启动后，我召集相关干系人和邀请熟悉码头理货系统业务的专家就本项目存在的安全问题进行评估，对各类安全隐患分门别类，尽可能识别出潜在的风险并记录下来。我们参照码头信息安全管理体系的要求，并结合系统实际情况，在充分征求客户和领导的前提下，逐步建立和完善了码头理货信息系统管理、安全保护、运行维护、人员培训等一系列制度，并就制定出来的制度与相关干系人进行讨论与评审，评审通过后请甲方签字确认，并请甲方签字确认，为后面安全管理工作起到重要的指导作用。

2、执行实施安全管理

有着多年项目管理经验的我深知，信息系统安全是一个动态的过程，今天看似安全的系统，明天可能发现新的漏洞，或者黑客研究出新的攻击技术等，因此安全风险识别是一个反复的过程。在对已识别的安全隐患制定了应对计划后，把潜在风险应对所需要的资源和费用加进项目的预算和项目项目管理计划中，并明确和分配实施风险应对措施的风险应对责任人，并且建立集团、职能科室、应用部门三级信息管理体系，分职责、分层次、分重点进行管理，我们根据信息安全制度和码头实际情况，对不同的安全隐患，我们采取不用的措施，针对码头散杂货理货平台不 EDI 中心熟悉的问题，采取了聘请 2 名专家做技术顾问，加强对有关人员进行架构培训措施；在安全管理过程中，我反复强调切忌把安全管理工作当作一种口号，把“整体安全规划”流于形式，缺少思考和探索，人为主观因素较多、随意性较大，从而导致在信息网络运行过程中出现这样那样的问题，使信息化建设发挥不了应有的作用。我们应从港口码头的现状和发展出发，求真务实，让总体规划、安全管理落到实处，确保信息安全无死角。

3、监控项目安全管理

安全管理的监控非常重要，可以说是信息系统安全的最后一道防线。在控制安全管理方面，我们主要从设备安全、数据安全、内容安全、行为安全，技术安全等方面进行监控。

1、设备安全

信息系统的设备安全是信息系统安全的首要问题，是信息系统安全的物质基础。除了硬件设备外，软件系统也是一种设备，也要确保软件设备的安全。为了更好地保障设备安全，我们采用虚拟网络技术将网络划分多个虚拟局域网，有效提高交换机的数据交换效率，增强了网络的安全性。另外我们采用基于高可用性的本地接管预案和基于双活数据中心的本异地互备预案等各种技术和管理手段将灾难的影响化解。昊

2、数据安全

数据是企业的核心资源，因此保证数据的安全尤为重要。根据项目实际情况，我们把数据安全主要分为数

据丢失和数据管理，而数据丢失包括存储系统硬件导致的数据丢失和应用程序、病毒、人为误操作导致的数据丢失。我们针对这两种情况，一是搭建存储虚拟化平台，对不同存储系统平台提供的物理卷进行镜像，完全可以确保在出现物理错误是数据不丢失、应用不中断；针对可能由于硬盘驱动器损坏、人为错误、黑客攻击、病毒破坏等原因造成的系统数据丢失、损害、篡改或无法访问等问题，我们采用全量备份和增量备份相结合的方法，定期备份数据文件和日志文件，并且使用了安全备份恢复管理软件，提高了备份的安全和效率。

3、应用安全

应用安全是继网络、主机系统的安全防护之后，信息系统整体防御的最后一道防线。而且应用系统安全的实现机制更具灵活性和复杂应用系统是直接面向最终的用户，为用户提供所需的数据和处理相关信息、因此应用系统可以提供更多与信息保护相关的安全功能。确保用户身份和信息的真实性以及网上数据信息存储和传输的安全性，从而实现理货信息的安全共享。对于应用系统的自身安全，我们对每一个系统的引进和开发都要进行反复的论证、调研，深入了解需求，结合码头实际进行系统的二次改造优化，使港口码头信息体系安全对接、有机融合、充分共享。并且对用户进行权限设置，严格账户管理，定期整理用户。强化操作应用和使用安全，使信息化技能成为工作人员必需技能，努力发挥系统的最大效益。

4、网络安全

网络作为信息的主要收集、存储、分配、传输、应用的载体，其安全对整个信息系统的安全起着至关重要甚至是决定性的作用。因此在本项目中，我非常重视网络安全的建设工作，为了抵御各种网络威胁并能及时发现网络攻击线索，修补有关漏洞，记录、审计网络访问日记，以尽可能地保护网络环境安全，我们采取了三种网络安全防御技术。一是应用入侵检测和网络监控技术检测网络信息系统的行为、安全日志以及审计数据等内容，对网络信息系统的入侵行为及企图进行分析和判断，发挥实时监控的作用，避免各网络系统遭受非法攻击；二是在港口码头理货系统、调度系统、商务综合服务等系统的实际应用中，用文件加密和数字签名技术避免外部不法人员窃取、更改或者损坏机密数据，从而保障信息数据的安全性和保密性。三是应用身份认证技术，包括 VPN、防火墙、入侵检测等技术，对网络信息系统用户数字身份权限进行有效管理，提升了网络信息系统权限管理的安全性。

通过上面的安全制度、措施和方法的应用，整个系统将是安全可靠以及高效的。在整个信息系统安全管理方面，还要加大对员工进行安全意识的教育与宣传,提高全员的安全防范意识，任何系统的安全都不是一成不变的，因此我们必须不断加强系统安全完善措施，不断发现和改进漏洞，积极进行防护，才是保障信息系统安全的根本。

在全体团队成员的共同努力下，历时一年，本项目终于于 2018 年 7 月顺利通过了甲方的验收，实现了港口现场管理信息化的扩展、提高了港口装卸效率、简化工作程序等功能。目前该散货码头信息化系统运行稳定，受到建设方领导和管理层员工的肯定与好评，该项目的成功很大程度上得益于成功的项目安全管理，采用科学的安全管理方法和工具技术，为项目的安全管理带来了事半功倍的效果。当然，在本项目中，也有一些不足之处，例如：供应商在提供网络产品拖沓，因此我已向工厂高层建议，在以后的其他项目中加强对供应商的进度管理，要把供货具体时间写进合同，明确违约责任。在后续的学习和工作中，我还需不断充电学习，多跟同行交流，提升自己的业务和管理水平，形成组织过程资产，力争为我国信息化建设付出努力。

安全管理范文 9

摘要

2018 年 1 月，我作为项目经理参加了国网 XX 市电力公司智慧用电云检测系统项目的开发。该项目总投资 780 万元，建设工期 12 个月。该系统主要功能包括用电“可视化”、报警信息“直观化”、历史数据存储查询、远程升级维护和 APP 短信推送。在项目建设过程中，我深刻认识到实施完善的信息安全管理策略是本次项目成功的关键，因此，在制定安全策略时，科学运用信息安全管理的理论知识，结合用电云检测系统信息安全体系的具体要求和具体情况，识别、评估该系统的安全威胁，并从制定方案、岗位、职责、人员、目标、制度和工作流程出发，对系统的设备、网络、操作系统、数据库和应用系统的安全进行全面管理，保证了项目的成功。

正文

XX 市智慧用电云检测系统项目是在政府提升用电单位安全管理和电气设备本质安全水平的背景下，于 2018 年 1 月由国网 XX 市电力公司启动的，我公司中标该项目，中标金额 780 万元，公司组建了项目型组织结构，任命我为项目经理，负责项目的全面管理，项目历时一年于 2019 年 1 月通过客户方的验收。该系统主要功能包括用电“可视化”、报警信息“直观化”、历史数据存储查询、远程升级维护和 APP 短信推送。该系统采用 J2EE 体系结构，可实现 B/S、手机客户端等多客户端接入，数据库采用 OradeIlg,服务器为 IBM3850X5,操作系统为 WindowsServer2008R2o 在项目开发过程中，我深刻认识到实施完善的信息安全管理策略是本次项目成功的关键，在制定安全策略时，科学运用信息安全管理的理论知识，结合用电云检测系统信息安全体系的具体要求和具体情况，识别、评估该系统的安全威胁后，从制定实施方案、岗位、职责、人员、目标、制度和工作流程出发，对计算机的设备、网络、操作系统、数据库和应用系统的安全进行全面管理，保障了系统的安全、高效、可靠，最终项目按预期顺利完成，项目组得到了公司和客户方的一致好评。

由于该项目涉及电力公司所有员工和广大用户，人员范围广，安全环境复杂，在病毒层出不穷，漏洞无处不在的压力下，我深感责任重大。安全无小事，因此，在本项目中，我坚持系统开发与系统安全同步规划、同步建设、同步运行，切实保障项目的信息安全。

1、制定科学的安全管理策略，完善岗位和人员设置

凡是预则立、不预则废，安全管理同样适应。在制定系统的安全管理策略时，本人参考了公司的信息安全管理体系的要求，结合本系统的实际，在充分征求了客户和公司领导的前提下，制定了出了项目的安全管理策略，并就制定出来的策略，与相关干系人进行了讨论与评审，评审通过后请客户方的领导签字确认，再正式实施。在制定策略过程我们主要开展了以下工作：

1、明确安全策略设计的原则。我们主要采用了对系统的访问最小特权原则，任何用户、管理员、进程，仅享有该主体需要完成其被指定任务所必须的特权，不应享有任何多余特权。还有用先进成熟的技术原则、普遍参与原则、标准化原则、注重效费比原则以及全面防范、突出重点等原则。

2、从人防入手，加强对安全工作领导。在文件中确定了信息安全管理领导小组，设置了相关的系统安全管理人员，如机房管理员、网络管理员、系统工程师、安全审计人员等职位，并制定了详细的职责。如网络管理员的职责在于对网络设备登录进行安全设置，进行网络的集中实时监控、网络的连通性检测和检查，保证用户对检测系统访问的通畅，对网络设备的用户、口令的安全性进行管理，参照相应规定对网络设备登录用户进行监测和分析等。

3、加强对成员的安全管理。制定相关安全规章制度和奖惩措施，组织项目组成员定期召开会议，培训相关信息安全知识，通过培训使团队成员的观念由“要我安全”变为“我要安全”。同时为了防止信息滥用、丢失和泄密，进一步规范人员录用和离职管理规范，包括对人员招募、入职培训、人员转岗离职、持续改进等环节，在组织和流程上保证了信息安全的科学、合理和可靠。

2、突出重点，切实加强信息安全技术的综合运用

1、加强计算机设备安全。旨在保护计算机服务器、存储介质、系统终端、网络交换等硬件设备免受自然灾害、人为破坏，确保其安全可用。我们采用了低泄射产品、电磁干扰器、电磁屏蔽室、滤波等技术来加强保护。同时我们还采用容错技术和故障诊断技术，来提高系统的可靠性。容错主要是采用了硬件冗余、软件冗余、时间冗余和信息冗余的设计，通过增强资源来换取设备的可靠性。当然还利用数据加密来保证数据的机密性，用数字签名来提供抗否认性，用审计来监控和捕捉各种安全事件，这些技术在项目中被广泛应用。

2、加强网络安全。网络安全是整个系统的安全基础，因此保证网络安全是非常重要的。在网络方面我们主要采取了防火墙技术，用于逻辑隔离外部网络与受保护的内部网络，并配置严格的访问控制策略，过滤粒度为端口级。对网络安全我们还设计了一种网络蜜罐技术，该系统是一个包含漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机和服务，给攻击者提供一个容易攻击的目标，攻击者往往在蜜罐上浪费时间，延缓对真正目标的攻击，该技术可以对入侵取证提供重要的信息和有用线索，便于研究入侵者的攻击行为。

3、加强操作系统安全。我们充分利用 PMI 和 PKI 技术，来实现对操作系统的身份认证和访问控制，PMI 主要是进行授权管理的，证明这个用户有什么权限，能干什么，即“你能做什么”。PKI 主要进行身份鉴别的，证明用户身份，即“你是谁”。在权限控制上我采用了严格的 RBAC 角色控制策略，我们把用户按组织身份和业务身份划分出不同角色，不同的角色对系统中的基础数据资源、单据资源、工作流程、工作看板、业务审核等资

源都有严格的设置，避免了用户越权使用而导致系统数据错乱。

4、数据库系统安全。我们采用了双机热备的运行方式，在服务端运行一主一备两台数据库服务器，数据库之间互为主从热备，保证数据的一致性，主备服务器间采用“心跳”机制来检测对方的状态，当一台机器出现故障时，自动切换到另一台服务器，从而保证业务系统的可用性。

5、应用系统安全策略。针对网络攻击者将关注点从传统网络服务器逐步转移到对 WEB 业务的实际问题，我们主要采取事前评估、事中防护、事后恢复的全天候 24 小时职守，及时发现攻击并溯源。通过 WEBRAY 的一体化漏洞扫描系统，管理员可以定期对网站系统进行安全检查，实时了解网站系统存在的安全隐患，并及时进行修补。通过内核级网页防篡改技术，杜绝网页篡改情况发送，并提供备份和恢复功能，从而确保了服务器可以正常提供服务。

经过大家的努力，项目在 2019 年 1 月顺利完成并通过验收，现在程序运行稳定，使用情况良好。回顾起来，项目的成功很大程度上归功于我们制定并实施了完善的信息系统安全策略，有效避免了数据泄密的风险，保障了系统的安全运行。诚然，任何系统的安全都不是一成不变的，因此仍必须不断完善系统安全措施，如随着云计算和移动互联网的广泛应用，加强无线网的安全防护越来越重要，要充分利用 802.111.WPA2 等无线网络安全技术的运用，不断改进安全措施，进行积极的防护，才是保证智慧用电云检测系统安全的根本。

安全管理范文 10

摘要

2017 年 8 月，我作为项目经理，参加了 xx 三甲医院的数字化医院信息系统建设项目，项目工期 9 个月，总投资 1200 万。医院全面推进数字化，打造智慧型医院。系统包括 HIS、LIS、EMR、PACS/RIS.手麻重症系统、信息发布系统、医院资源系统等 7 大系统及相应的服务器、网络等硬件系统。实现医院“人流、物流、资金流、业务流、信息流”的高效同步，打造办公电子化、网络化、无纸化系统平台。该系统于 2018 年 5 月，成功上线，顺利通过院方验收，赢得了用户的好评。本文结合作者的实际经验，以该项目为例，论述项目建设中的信息安全管理。从信息系统安全的人员、岗位、流程、制度入手，着重落实计算机、网络、服务器、数据库、应用全方面安全管理，建立全方位的信息安全防护体系。

正文

2017 年 8 月，我作为项目经理，参加了 xx 三甲医院的数字化医院信息系统建设项目，项目工期 9 个月，总投资 2400 万。医院全面推进数字化，打造智慧型医院。系统采用 B/S 架构，Java 语言,Oracle 数据库，weblogic 中间件，两台 IBM750 小机做数据库服务器，运行 AIX 系统，8 台 IBMX3850 做应用服务器，运行 Windows2012 系统。软件系统包括医院信息系统（HIS）、电子病历系统（EMR）、实验室系统（US）、医学影像系统（PACS/RIS）、手麻重症、信息发布系统、医院资源系统（HERP）等 7 大系统近百个模块，实现了“人流、物流、资金流、信息流、业务流”的高效同步，带来了方便、安全，高效的就医环境，打造网络化、电子化、无纸化的系统平台。患者可以通过电话、官网、自助机、微信、支付宝等多种方式，实现建卡、挂号、预约、充值缴费、查询打印报告、智能候诊、随访等各种便捷服务。患者病历信息、检查检验报告、影像图片登患者就诊信息实现无缝连接，实时同步发送至移动医护工作站，患者手机。医护可以随时登入移动工作站查看患者病情，进行查房、会诊、随访等。

随着信息化的不断发展进步，信息化已经深入到医院业务、管理的方方面面，带来高效快捷的同时，也不可避免的带来的各种各样的安全风险。医院作为医疗卫生机构的主体，承担着为社会提供公共卫生服务和医疗卫生服务的责任，一旦发生信息安全事件将对社会造成极大的损害。所以信息安全不容有失，项目建设过程中的安全管理至关重要，是项目成功的保障。本文将结合作者实际经历，以该项目为例，论述信息系统安全管理。主要从人员、岗位、流程、制度入手，着重落实计算机安全、网络安全、服务器、数据库安全、应用安全，建立全方位的医院信息系统的安全防护体系。

1、建立完善合理的信息安全规章制度，安全管理人员到岗到位

安全管理制度先行，只有制定科学合理的安全管理制度，才能有条不紊的安全落实到位。我们根据卫生部下发的等保工作指导意见明确要求全国所有三甲医院核心业务信息系统的安全保护等级原则上不低于第三级要

求，参照《信息系统安全等级保护基本要求》逐条细化，根据我院的实际情况编写信息系统安全管理办法。编写完成后组织召开评审会，邀请医院领导、信息中心同事、乙方各系统负责人共同讨论研究，经反复修订评审通过，用于指导我院的信息系统安全管理。有了完善的安全管理制度，还必须要有相应的安全管理人员抓落实，否则再好的制度也只能停留在纸面上。我们成立以院领导为组长，信息科、医务部、护理部等科室主任组成的信息安全领导小组，以信息中心为主体，医药护技等科室骨干组成的信息安全工作小组。设置信息中西机房、网络、数据库、服务器安全岗位以及科室安全联络员，制定详细的岗位职责，相应人员全部到岗到位责任到人。

2、网络安全

网络是数据传输的骨干，保障信息系统正常运转的基础。与供应商 Juniper 和锐捷共同制定网络拓扑结构，安全防护措施。网络采用三层架构，两台核心交换机做虚拟化，核心到汇聚、汇聚到介入层两对光纤做链路冗余，增强网络物理安全保障。我们将门诊、医技、临床、职能科室划分不同的 VLAN,有效隔离冲突域。安装防火墙，设置 DMZ 区域，放置官网、微信应用、健康管理等服务器，满足的患者访问医院信息的需求，同时有效的保护的内部网络。安装 IDS/IPS 有效监测和防止木马和病毒攻击。无线 AP 设置不同的 SSID 分别供患者和医护人员使用，医生查房 PAD 和护士执行医嘱的 PDA 由信息中心负责绑定 MAC 链接隐藏的 SSID,患者通过短信验证链接。部署开源的 zabbix 同意监控平台，实时监测网络流量，一旦发送网络拥塞等异常情况，立即邮件和微信报警。

3、服务器安全

医院业务不允许间断，必须 7X24 小时连续不间断的运行，稳定可靠的服务器关键保障。为此我们经过充分的调查研究，选择性能稳定可靠的 IBM 服务器。数据库选择两台 P750 运行 AIX 系统，两台服务器做 HA,提供高可用性、业务连续性和灾难恢复能力。8 台 IBMX3850 运行 Windows2012 接入负载均衡，扩展网络设备和服务器的带宽、加强网络数据处理能力。安装亚信服务器专用杀毒软件，有效防范病毒侵入。根据业务需要建立不通的用户，根据完成业务需求最小化需求，进行最小化授权，有效避免越权使用。根据业务需求开放必要的端口，其余端口一律关闭。持续关注 Windows 的补丁发布，先在测试库安装测试确认没有影响后，再在生产服务器安装补丁。通过这些措施，有效的保障了服务器的安全。

4、数据安全

数据库存放患者的个人信息和就诊信息，一旦发生丢失或泄露将造成难以估算的损失和影响。为此我们设置了专职的数据库管理员，负责数据的日常管理。对应数据库系统级别的参数调整，系统调优。必须由项目经理批准，数据库管理员评估确认后执行。根据业务需求为开发人员创建不通的用户，权限仅在完成工作范围之内。数据库中关键数据进行识别定义，开发相应加密处理功能，保障数据安全可靠。制定数据备份和备份恢复策略，每天凌晨进行数据库增量备份，每周日凌晨进行全备份。每月在测试系统进行全备份恢复测试，验证数据备份的有效性。

5、应用安全

应用的安全主要以服务器、网络、数据库等安全为基础，在做好以上安全的同时，我们制定系统的访问控制。系统登录采用密码和 ukey 双认证，确保了用户身份的真实可靠。根据医生、护士、挂号收费、出院结算等不同的岗位，结合临床、医技、职能、药房药库等不同的科室，制定不同的安全组，分别赋予不同的访问和操作权限。确保各岗位人员能够顺利的完成本职工作，同时也绝不运行未经授权的访问和操作，从而有效的保障岗位工作、避免误操作。此外，我们还要请第三方评测机构，对官网和微信进行安全测试，根据整改意见及时进行修补。

6、以人为本加强全员信息系统安全意识

安全问题大多是是人为原因造成的，所以信息系统的安全关键是增强人员的安全意识。安全管理不只是技术问题，也不只是项目团队的事情。需要院领导、各系统承包商、医院各科室共同参与，形成人人都关注信息安全的氛围，才能更加有效地落实安全措施，建立全方位的安全防护体系。定期进行安全技术培训，邀请安全专家和团队成员进行授课，在培训和受训中不断提高技术能力。对应非技术人员定期进行安全科普，进行安全考试，评选安全标兵，调动全员信息安全的热情。

经过项目团队不懈的努力，历时 9 个月，系统于 2018 年 5 月正式通过院方组织的验收，并成功上线，赢得了院方的好评。本项目的成功得益于我对信息系统的安全管理，从技术、设备、人员意识全方全方位制定安全

策略，在项目过程中严抓落实，构件起信息系统安全防护体系。但是，项目实施过程中还存在一些小问题，如由于工期紧任务繁重，对于团队建设做的有所欠缺，一定程度影响项目工作。在以后得工作学习中，加强这些方面的总结和学习，争取百尺竿头更进一步，为我国的信息化建设贡献自己更多的力量。

安全管理范文 11

摘要

2017 年 3 月，本人参与了某省党校的“教学教务管理系统”项目建设，担任承建方项目经理一职。该系统采用 B/S 模式开发，其面向的使用对象包括省委党校及下属各分校的教务工作人员、教师及学员，为其提供各类综合性服务。工作人员通过本系统完成所有日常教务工作，从招生到学员毕业离校，其在校内的所有和教务相关的数据都通过教务系统进行管理。学员通过该系统进行网上报名、选课及查询自己的个人相关信息（教学计划、课程表、成绩等）。教师可以查询自己的课程安排，上传自己的课件，录入学员成绩，查询教师业绩考核情况等。在项目建设中，我深刻认识到实施完善的信息安全管理策略是本次项目成功实施的关键。在制定安全管理策略时，本人科学的运用信息安全管理的理论知识，结合党校信息安全管理体系的具体要求和系统的具体情况，从信息安全的制度、流程、岗位、职责、人员为出发点，制定了科学合理的信息安全制度体系。按照系统实际情况从主机、网络、应用服务、数据安全等方面进行信息安全的有效管理，保障了系统的安全、高效、可靠。最终，项目按预期顺利完成，项目组得到了公司与客户方的一致好评。

正文：

随着信息化的发展，高校教学规模扩大，与传统方式相比，教学模式也发生很大转变。巨大的变革让学校教学教务管理任务越来越重，不仅增大了工作量，更是增加了工作难度。这些根本性变化的同时也对学校的教务管理提出了更高的要求，为了适应这些新变化，提高教学教务管理的工作效率，建立一套完整统一、技术先进、高效稳定、安全可靠的基于 IntemetAntranet 的教学管理信息系统成为一项当务之急的工作。鉴于以上原因，某省党校决定部署实施一套“教学教务管理系统”，利用此系统实时了解教务管理情况和学员反馈情况，有利于提高教务管理水平。通过党校面现向社会公开招标，我公司顺利中标。合同额 210 万元，历时 8 个月，于 2018 年 11 月全面通过系统验收。该系统采用 B/S 模式开发，其面向的使用对象包括省委党校及下属各分校的教务工作人员、教师及学员，为其提供各类综合性服务。工作人员通过本系统完成所有日常教务工作，从招生到学员毕业离校，其在校内的所有和教务相关的数据都通过教务系统进行管理。学员通过该系统进行网上报名、选课及查询自己的个人相关信息（教学计划、课程表、成绩等）。教师可以查询自己的课程安排，上传自己的课件，录入学员成绩，查询教师业绩考核情况等。项目启动后，本人被公司任命为该项目的项目经理，全面负责项目的建设工作。

由于系统中保存有用户的个人数据信息，其安全性要求相当高，党校领导相当重视，一再要求确保安全性。在项目建设中，我也深刻认识到信息安全是项目成功实施的重要保证，在制定安全管理策略时，本人科学地运用信息安全管理的理论知识，结合党校信息安全管理体系的具体要求和系统的具体情况，从信息安全的制度、流程、岗位、职责、人员为出发点,制定了科学合理的信息安全制度体系。按照系统实际情况从主机、网络、应用服务、数据安全等方面进行信息安全的有效管理，保障了系统的安全、高效、可靠。

一、建立科学合理的信息安全管理制度，完善岗位和人员的设置

在制定系统的信息安全管理制度时，本人参照本公司信息安全管理体系的要求，并结合系统实际情况，在充分征求了客户和公司领导的前提下，制定出了本系统的安全管理制度，并就制定出来的制度与相关的干系人进行讨论与评审，评审通过后请客户的领导签字确认，再正式实施。

1.制订信息安全方针文件，明确信息安全的目标是建立和完善信息安全的策略体系、组织体系、技术体系和运作体系，争取达到领先的信息安全保障水平，保障和促进党校教学教务管理系统业务发展和业务目标的实现。

2.为了促使信息安全管理体系有效及明确地界定体系内的组织结构及成员的职责和义务，确保信息安全管理体系能有效运行，制订信息安全管理组织文件。在党校领导的积极配合下，在文件中，确定了信息安全领导小组、信息安全工作小组，设置了相关的系统安全管理人员，如机房管理员、网络管理员、系统工程师、安全

审计人员等职位，并制订了详细的职责。例如像网络管理员的职责在于对网络设备进行安全配置，进行网络的集中实时监控、网络的连通性检测和检查，保证用户对党校教学教务管理系统的访问通畅，对网络设备的用户、口令的安全性进行管理，参照相应规定对网络设备登录用户进行监测和分析，负责所管理网络设备的用户账号管理，为不同的用户建立相应的账号，根据对网络设备安装、配置、升级和管理的需要为用户设置相应的级别，并对各个级别用户能够使用的命令进行限制。

3.人员安全管理。为了防止信息滥用、丢失和泄密，同时规范人员录用和离职管理过程，制订了人员安全管理规范，规范共包括对人员招聘、入职培训、人员录用、人员转岗和离职、持续改进五个环节，在组织和流程上保证了信息安全的科学、合理、可靠。

二、主机的安全策略

主机操作系统作为软件的载体，其安全性至关重要。在硬件的选购上，经过充分考察后，我选用了 IBM 小型机、华为刀片服务器，从硬件上保证了服务器的安全性。在操作系统的选择上，我与党校领导也进行了交流讨论，最后确定采用 AIX、SuseLinux 操作系统，虽然在图形化外观上面有些不足，但其安全性是有目共睹的。

制定了服务器的安全使用规定，根据业务需求建立不同用户，且各个用户仅具有满足当前业务需求的最小权限，有限避免用户的越权访问；开启安全审计策略，审计用户的操作；关闭不必要的端口及服务；定期对操作系统进行更新；通过这些措施保证服务器的安全。

三、网络安全策略

网络的安全是整个系统安全的基础，因此保证网络的安全是非常重要的。在网络方面，利用 VLAN 对网络进行划分，有限隔离广播冲突；安装防火墙，并配置严格的访问控制策略，过滤粒度为端口级，开启日志访问，有效阻断并记录非法访问；加入 IDS、IPS,防范病毒木马攻击；在重要服务器上将网关 MAC 地址进行静态绑定，防止 ARP 欺骗攻击；同时，部署统一安管平台，实时监测网络设备的利用率与吞吐量，出现网络堵塞等问题时能迅速通过短信、邮件等方式进行报警，及时加以整改，保证了网络的安全可靠。

四、应用安全策略

在前期程序员的开发阶段，我就召集程序员，要求他们要有安全意识，时刻将安全放在首位，遵循“用户端的输入是不可信”的原则，对用户端输入进行判断过滤，并只开放满足需求的最小权限，防范越权操作。系统开发完毕，先由功能性能测试小组进行测试，修正 Bug 后，再交由安全测试小组对系统进行安全渗透测试，挖掘是否存在如 SQL 注入、跨站、越权操作等应用安全漏洞，再一一进行修补。

五、数据安全策略

在此次项目中，数据作为核心资源，其安全性尤为重要，在本系统中采用了下面的数据保护策略。首先对数据库进行分域，不同的数据放到不同的域中，各个域互相独立，防止混用。设置当前数据库和历史数据库，当前数据库只存放两天的数据，其余的数据通过 DataStation 转移到历史数据库，并把历史数据库中 6 个月前的数据转移到磁带库进行存放，保证了数据的安全可靠。在数据库的备份方面采用全量备份和增量备份相结合的方法，定期备份数据文件和日志文件，并且使用了某厂商的安全备份恢复管理软件，提高了备份的安全与效率。此外，关键数据采用加密算法加密后存放，保证数据安全可靠。

2018 年 11 月 1 日，项目按既定的日期和预算完成，项目组赢得了公司与客户方的一致好评。回顾起来，项目的成功很大程度上归功于制订了完善的信息系统安全策略，有效避免了数据泄密的风险，保障了系统安全稳定运行。诚然，任何系统的安全都不是一成不变的，因此仍必须不断加强系统安全完善措施，不断发现和改进漏洞，积极进行防护，才是保障教学教务管理系统安全的根本。

安全管理范文 12

摘要

2011 年 1 月，我作为项目负责人，对所在单位某三级医院的电子病历系统进行了建设。该项目总投资 800 余万元，工期 10 个月，在全院 30 多个科室建起了电子病历和无线查房系统。建立以电子病历为中心的医院信息系统，是当前深化卫生体制改革的八项支撑之一。其功能包含病历的模块化书写与存储，移动医护查房工作站系统。移动医护查房工作站的使用，把医院的信息化建设连接到病人的床边，解决了信息化止步于办公室的

最后 20 米问题，本项目于 2011 年 11 月顺利通过验收，现运行稳定，使用良好。本文以该项目为例，讨论安全策略管理问题。特别是在管理实践中有针对性地充分发动群众，建立科室级项目安全管理责任制的方式，提高执行力，建立群防群治体系；建立人防、物防、技术等多重的安全管理策略，较好地实施了从硬件的防火、防盗、数据的安全备份、网络的病毒防护以及各级操作权限的审批等一系列的安全策略，保证了项目的安全运行。

正文

我院作为全省排名靠前的三级中医医院，开放床位一千一百张，年出院 3 万人次，年门诊量 60 万人次，一直以来，院领导十分重视医院的信息化建设，先后投资近千万元建立了 HIS、LIS、PACS、OA 等系统，为了贯彻党中央国务院《关于深化医疗卫生体制改革的意见》精神，提高医护质量，全面建设数字化医院。院领导决定和 × × 公司合作开发电子病历系统。由于 × × 公司是我院原有系统的开发商，与我院有数年合作基础，双方决定由我，医院信息科主任作为项目总负责人，全面负责该项目的管理工作。

该项目总投资 800 余万元，工期自 2011 年 1 月至 2011 年 10 月底结束，分软件、硬件两部分。本系统采用 B/S 架构，Sql Server 数据库，采用两台 HP580G6 双四核 4u 机架服务器的双机模式。在各个病区，用锐捷公司的无线 AP 架设了符合 IEEE801.11g 规范的 1.4 GHz 54 Mb/s 的无线局域网。

软件部分包含医护电子病历的书写与存储系统和医护移动查房系统两大模块。按照卫生部《医院电子病历规范》和本院各科专家知识设置各种病历的模板，原本一份要花费医护人员近 2 小时的书写时间才能完成的病历，现在用电子病历 20 分钟左右就可以完成，极大地节约了医护人员的时间，把他们从繁重的文字书写工作中解放出来，有时间与病人交流和护理，实现了把医生还给病人的理念。

无线网络的建设与移动医护工作站的使用，解决了医院信息化建设止步于办公室的最后 20 米问题。把信息化建设延伸到了病人的床头。查房时，医生用平板电脑连入医院网络，就可以查阅病人的所有住院信息、用药情况、各种检查报告单、各种影像图片等。护理人员利用带红外扫描功能的 PDA，可以实现床旁的体温、血压即时输入，输液药品条码与病人腕带条码的验证。把原来护理常规的“三查七对”用先进的技术手段做了保证，实现了护理工作的可查、可信、可追溯性。

比如说输液换药流程：病人入院即拥有一条本人信息的条码腕带作为身份识别标志，该病人的药品、检材都贴有带着病人信息的条码标志。护士给病人换药的时候，首先口头询问病人的基本信息并扫描病人的腕带，核对病人与腕带是否正确，然后扫描输液袋上的条码，核对是否与腕带信息一致。是否是该病人的药，是该病人的第几瓶药，并显示药品明细，如果扫描核对正确，系统会发出愉快的乐声，同时自动记录换药时间与换药人信息，如果有问题，则用报警声提醒护士注意。

该项目涉及全院所有的医生和护理人员，涉及范围广，安全环境复杂，在病毒层出不穷，漏洞无处不在的压力下，作为项目总负责人，我深感身上的责任重大：安全无小事，怎样才能保证项目的安全？

我首先制定了整体的安全管理计划，决定筹建科室级安全责任制体系，从人防、物防、技术防等多方面建立综合的防御体系，来保证设备、数据的安全。

首先是从人防来说，人的能动性永远是第一位的。在项目一开始，我就汇报医院领导批准，成立了以分管院长为组长，信息科、保卫科、医务科、护理部主任为骨干的信息化安全领导小组，并由各科室推举一名科主任具体负责本科室信息安全建设管理工作，同时选一名年轻大夫作为安全检查员，建立了全院的信息化安全管理体系，定期召开会议，培训相关知识，制定了相关的规章制度和奖惩措施，通过培训、学习计算机安全管理条例等办法，逐渐使各科人员意识到，医院的信息化已经逐步深入到科室的每一项业务，一旦出现问题，科室将无法正常运行，把原来大多数人“信息安全是信息科的事”的观点，变成“信息安全是我自己的事，管不好科室要受影响”的理念上来。同时让保卫科加强对重点区域的巡逻力度，保证了项目的各种设备的防盗工作做到位。建立了人员、权限的分级管理和审计制度，制定了密码口令的保密以及定期更换制度，制定了维护人员的定期巡检制度，通过一系列的措施，建立了全院的安全防护体系，保证了项目的顺利进行。

接下来是物防，俗话说“兵马未动粮草先行”，对机房等重点部位，在常规的配备 ABC 灭火器以及烟雾报警器等的基础上，安装了视频、音频网络监控系统，保护硬件设施的安全；对服务器的供电电源采用双 UPS 联机冗余设计，保证服务器的供电不间断；双服务器中一台挂 HPMAS2000 盘柜做主机，另一台配多块硬盘做 RAD5 当辅机，构成了双机，双硬盘的模式，保证业务的不间断；对主交换机等重要节点进行了双机冗余，就连各楼层交换机，也多购买了几台同样型号的机器，以备随时更换，来保证网络的畅通。

再者就是技术防，科技永远是第一生产力。针对病毒，我们购买了防火墙、VPN 和网络版的卡巴斯基杀毒软件，对每一个客户端都进行了安装，并定期升级病毒库。对内外网做了物理隔离，上外网的机器绝不允许上内网。为了规范操作人员的上网行为，我们购买了上海宝信公司的网络巡警内网管理软件，利用其强大的功能，制定了封闭光驱、封闭 USB、结束非法进程等策略，规范上网行为。针对无线 AP 容易造成网络的非法接入问题，首先设置 AP 不对外广播 SSID，并且需要用户名、密码接入，同时对合法接入的计算机的网卡和 MAC 地址进行了绑定，杜绝了非法接入的问题。

为了数据安全，只有数据库管理人员才拥有对数据库的操作密码和权限，并严格做好操作记录，同时用 NEC 的双机管理软件做数据备份，采用了双数据库，双应用的模式：双机建立心跳连接，一台服务器出现异常，另一台服务器立即接管所有数据和业务，保证应用业务的连续性。双机热备的采用，提高了系统的可用性和数据的安全性。

经过大家的努力，项目在 2011 年 11 月底顺利完成并通过验收，现在程序运行稳定，使用情况良好。

虽然整体来说，项目的安全策略管理做得还比较全面，但现在回想起来，也存在一些不足。比如说，双服务器双硬盘的双机热备模式，虽然相对于单机和双机单盘柜的模式在数据安全上更有所提高，但是在运行过程中如果出现主服务器出现数据读写错误，因为是双机镜像模式，写入伺服服务器的数据也会产生错误的情况，需要在条件允许的情况下，建立容灾备份服务器，最好实现数据的异地容灾备份，保证数据的安全性和可用性。再比如，宝信网络巡警软件的封闭 USB 口功能，对操作系统启动前插入的 U 盘，会有 3 分钟左右的时间可以进行读写，需要和厂商联系改进，堵塞这个漏洞。安全问题，是一件需要我们永远关注的大事。

安全管理范文 13

摘要

在信息系统工程建设管理中，信息安全在国家级信息系统工程建设中是极其重要的。本文结合作者的项目实践，以《2010 年国家通信网应急指挥平台》建设为例，讨论如何做好国家级信息系统工程的信息安全，包括在项目建设过程中应建立怎样的信息系统架构体系、如何进行信息系统安全风险评估以及制定符合实际需求的安全策略。该项目是以构建工业和信息化部应急指挥平台为中心，上行与国务院应急平台相联，下行与省（自治区、直辖市）通信管理局相联的上下贯通、信息共享、安全可靠的现代化国家通信网应急指挥平台。系统建设着重强调系统的安全可靠，要求系统必须符合 S2-MIS 的体系架构及系统安全级别至少达到国家标准 GB17859-99（计算机安全保护等级划分准则）中第四级结构化保护级或其以上，因此，如何做好信息安全，是项目经理在承担国家级信息系统工程中的一大难题。

正文

信息安全一般是指保护信息系统和信息，防止其因为偶然或恶意侵犯而导致信息的破坏、更改和泄漏，从而保障信息系统能够连续、可靠、正常地运行。通常把它理解为一个动态的管理过程，通过建立安全机制、安全服务，使用安全技术来保证用户对信息系统的安全需求得到持续满足，并通过认证、设置各级权限、采用多种数据加密技术等方式来保障信息系统的保密性、完整性、可用性、防抵赖性、可追溯性和真实性。因此，一个有信息安全保障的信息系统是一个在网络上，集成各种硬件、软件、密码设备，以保障其业务应用信息系统能正常运行，以及与之相关的岗位、人员、策略、制度和规程的总和。

2010 年 2 月，笔者参加了《2010 年国家通信网应急指挥平台》的项目建设，担任承建方项目经理。该项目被划分成 3 个子系统：应急指挥基础设施系统、基础支撑系统、综合应用系统，其中综合应用子系统包括 8 个组成部分：宽带 VSAT 应急网监测预警系统、通信物理网监测预警系统、通信业务网监测预警系统、应急预案管理系统、通信保障应急物资管理系统、多媒体档案管理系统、通信保障应急事务处理系统、通信保障应急工作决策支持系统。该项目除具有大项目中建设规模大、涉及的项目干系人多、沟通协调管理复杂、工程进度控制难等特征以外，更重要的它是国家级公共建设项目，系统的安全稳定将是本项目能否通过业主及监理单位验收的关键。作为项目经理，为保证系统的信息安全符合 S2-MIS 系统架构体系以及计算机安全保护等级达到第四级结构化保护级的要求，笔者在本项目的实施过程中采取了如下措施。

（1）从系统的开发及硬件产品的购买上，保证系统架构达到 S2-MIS 标准。

众所周之，信息安全保障系统有三种不同的系统架构：MIS+S、S-MIS 和 S2-MIS。MIS+S 是一个初步的、低

级的信息安全保障系统，不能从根本上解决业务应用系统的安全问题，因此不符合本项目的建设要求；S-MIS 虽将信息系统直接建立在 PKI/CA 的安全基础设施上，且软硬件都需要通过 PKI/CA 认证，但软硬件可通用，一旦软件或硬件中某一个部件出现 BUG 问题，都可能导致整个系统的瘫痪，因此也不符合本项目建设要求。只有 S2-MIS 标准，系统硬件和系统软件都是专用的，能从多方面对系统进行安全保护和隔离。因此，在本项目的建设中，为避免因操作系统的漏洞而遭受外网过多的黑客攻击，笔者所在的项目团队选择了 Linux 操作系统，同时为了实现跨平台兼容，采用了符合 J2EE 工业标准的表现层、服务层和持久层的框架，利用 Eclipse 开发工具，使用 Java 语言组织项目团队成员开发了基于 Oracle 数据库的综合应用子系统，并为实现与另两个子系统互联提供了中间件。而在采购硬件设备时，笔者所在项目团队主要从通过国际信息安全标准 ISO/IEC27001：2005 和具有国内一级保密资质的设备厂家中，通过公开招标方式，最终确定服务器设备厂家为 IBM、路由器、交换机设备厂家为华为、防火墙设备厂家为东软，从而实现了系统软件与硬件的独立专用，符合 S2-MIS 架构体系要求。

同时，在实施综合应用子系统过程中，为了保障 PKI/CA 安全基础设施的安全稳定，笔者采用了 X.509 V3 证书标准，将 PKI 中的数字证书、认证中心（CA）、数字证书注册审批等权限与管理完全集中在工业和信息化部的中心机房，并对证书数据库实现双向存储备份，对各省（自治区、直辖市）通信管理局在本平台上的权限设置按照业主的组织结构来实现权限的分级管理。

（2）采用风险评估方法对系统安全薄弱环节进行鉴定，判断系统是否达到国标 GB17859-99 中的第四级结构化保护级。

信息系统的安全风险主要来源包括自然事件风险、人为事件风险、软件系统风险、项目管理风险、用户使用风险等。而对于本项目的信息安全是否达到结构化保护级的要求，笔者主要采取数学模型计量风险（风险=威胁*弱点*影响）的方法，对于公式中威胁、弱点、影响的量化值是通过项目干系人之间进行头脑风暴、设备及系统进行超负荷测试、专家咨询等方式获得的，本系统的安全薄弱环节主要有：设备是否防震、是否能在断电下使用，以及软件是否有自我容错功能和出错报警等，通过这种方法，我们判断出设备断电是项目最大的风险，它将会导致整个系统无法实现正常互联，为了避免这样的风险，我们对设备采取两种供电方式：一是通过大楼的市电接入，另一种是通过 UPS 供电；其他薄弱环节也采取了相应的保护措施。其次，采用了类比法，通过与现已建成的、达到结构化保护级安全标准的系统进行各种信息安全性能参数对比，判断是否达到国标的结构化保护级。本系统的信息安全主要是与我国财务部的“金税二期工程”的系统进行了对比，对比结果显示，本系统的各项指标都明显优于财务部的系统。再则，笔者邀请了工信部专门从事信息安全保护等级评审的专家团对本系统进行了评审、验证。评审中，发现了 IBM 服务器与华为路由器设备在互通时有时存在较大延时，后经咨询 IBM、华为的技术人员，通过排查法，发现是 IBM 服务器与华为路由器 NE80E 中主板兼容问题，于是更换能与之实现兼容的华为主板后，问题解决。

（3）根据我国通信管理局各级行政组织结构，制定本系统的安全管理策略。

信息系统的安全管理策略，一般是指人们为保护因为使用计算机业务应用系统可能招来的对单位资产造成损失而进行保护的各种措施、手段，以及建立各种管理制度及法规等。对于本系统，笔者除了在技术上采用加密、PKI/CA 等方式外，还帮助业主建立了以行政组织结构为系统权限基石的安全管理策略。通过对不同省（自治区、直辖市）的各级管理者进行定岗、定位、定员、定目标、定制度、定工作流程来确定其“责、权、利”。如在本系统中，笔者帮助业主建立了机房设备安全管理制度、主机和操作系统管理指南、网络和数据库管理手册、应急事故预警方案、信息安全审计及人员培训上岗管理办法等。

最后，本系统在 2011 年 2 月完工，并通过了业主验收委员会的验收，我公司于 2011 年 3 月 11 日，在合同规定工期内，将系统及有关交付物移交给了业主。

信息系统的信息安全，大到关系国家安危、民族利益，小到关系一个公司商业机密，个人隐私，因此，无论是信息系统的建设者，还是参与者，都不可忽视其重要性。同时，在看待任何一个系统的信息安全，不是没有发现信息安全问题，就意味着系统本身就不存在安全问题，而是它本身就强调一个持续的动态管理，就像产品的质量管理一样，需要持续改进。因此，本系统虽然完成了建设，但系统的所有者或使用者需要对系统的信息安全采用类似 PDCA 循环方法来对系统的信息安全进行持续改进，只有这样，才能保障系统长期的安全稳定。