课后报告三

系统开发安全管理是指对信息系统的获取的管理，主要包括系统选购安全与系统开发的安全管理。系统的获取过程直接影响到系统自身的质量和安全性，以及使用系统进行信息处理的安全性，因此，对系统的获取过程实施安全管理，是保证系统安全可靠的关键。

学生管理系统的系统开发安全管理要满足软件可靠性和硬件可靠性：软件满足用户功能需求的性能度和软件在规定环境下的故障率，硬件满足软件运行的计算机系统整体环境的支持度和性能度。并且遵循系统安全原则，系统安全原则主要包括保护最薄弱的环节、纵深防御、保护故障、最小特权以及分隔等：使用多重防御策略来管理风险；及时发现故障、分离故障，找出失效的原因，并在可能的情况下解决故障；最小特权策略是指只授予主体执行操作所必需的最小访问权限，并且对于该访问权限只准许使用所需的最少时间。分隔的基本思想是，如果将系统分成尽可能多的独立单元，那么就可以将对系统可能造成损害的量降到最低。

在进行系统安全设计时，要系统的整个开发过程可以划分为系统规划、系统分析、系统设计、系统实现和系统运行 5 个阶段。

系统选购通过版本控制、安全检测与验收等，保证所选购系统的安全性。系统开发安全管理通过可行性评估、项目管理、代码审查、程序测试、可靠性管理及版本管理等，保证系统开发的安全。

系统应采取一致的建设思路和可互通的接口，在统一的信息平台上进行建设，各应用系统必须充分考虑彼此之间的关联关系，组成一个完整的信息化应用环境，以便系统的整体运行和日后的功能扩充调整。

在设计架构时，应该从业务、标准、技术、管理等各个方面充分考虑系统架构的开放性。存在动态数据交互，所以一个开放的架构是保证不同系统之间交互的必要条件。
采用的技术本身首先应该是开放的，同时内容平台本身也应该是开放的，对外提供符合标准的接口，各子系统必须结构化、标准化、模块化和可配置化，软硬件配置要具备可伸缩及动态平滑扩展能力，通过系统框架和相应服务单元的配置，适应业务量的变化，以获得良好的性能价格比。

由于学校的业务和技术的不断发展变化，要求管理系统架构在一定范围内支持业务的快速变化，并能够适应新技术的应用。本系统必须适应项目需求的这种变化。系统必须架构在开放的安全应用支撑体系结构之上，并易于扩展。的业务特点，要求系统能够实现按需配置。

在选择本系统的实现技术时，需要选择既有先进性又有较成熟应用的方案，保证系统在一定时期内具有技术上的优势，同时要求保证在系统设计方案上的成熟性，即在相当长的一段时期内，保持技术上的稳定性和可扩展性。

系统应保证高可靠性及稳定性。充分考虑和利用系统的自诊断能力、高容错和容灾能力、抗攻击能力以及系统的恢复能力来保证系统运行的高可靠性和稳定性。同时，具有抵御外界环境和人为操作失误的能力。
系统的总体体系架构应该在一定时期内保持相对稳定。稳定性是评价体系架构的一个重要指标。保持系统稳定性的一个基本方法就是分离业务和框架，在设计本系统时，应充分利用这一方法，首先建立一个基础层，再在这个基础层上构造相关的业务系统。

业务系统中采用的编码标准和规范体系的建设，应符合国家标准的有关规定，注重对信息的合理分类和信息结构的描述。既要注重与现行信息技术有关的国家标准、行业标准和国际标准的相互衔接，又要充分考虑基金管理系统不断发展对标准提出的更新、扩展和延伸的要求。

在建设过程中，各应用系统要模块化，减少各系统直接的耦合，降低整个系统的复杂性，便于各系统分别实施和整合，同时，也有助于提高系统整体的可扩展性。

系统必须具备高度的安全性、可靠性、容错性和稳定性，整体系统应实现 7*24 小时不间断工作，对具体的业务子系统和应用模块，根据不同系统承载业务和数据的重要性，应采用相应的安全防护、冗余和容错设施，保障主要业务的连续运转以及各项业务应用的快速恢复运行。

系统在硬件、网络、数据库和数据、应用操作权限和身份认证方面，应实现全面的安全防护措施。系统应根据用户的不同身份以及各业务模块的不同重要性，划分多个具有不同安

全保护等级的安全域，实现不同强度的安全保护和安全审计；安全体系设计的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患；安全建设工作应尽可能小的影响系统和网络的正常运行，不能对网络的运行和业务的正常提供产生明显的负面影响（包括系统性能明显下降、网络拥塞、服务中断）；同时本系统相关的过程数据和结果数据，要求做到严格保密，未经授权不得泄露给任何单位和个人。

应用系统应突出实用，切合实际使用情况，易于实施、管理和维护。对各类使用者来说，操作简便、易用。系统的用户界面要友好、通俗、易懂、便于操作。系统能通过远程控制、集中化管理，通过提高系统自动化管理水平，降低系统的管理和维护费用。

作为优秀重要的信息服务窗口，面对所处理的用户请求和吞吐的信息量根据业务需求不断出现大幅度动态变化的状况，系统的易部署、可维护、处理能力的动态可伸缩和保障系统运行的稳定可靠性，是本系统建设应当遵循的重要原则。一旦任何一个环节崩溃，整个信息系统就会处于瘫痪状态，这可能会带来不可估计的损失。在本系统的管理和运行维护过程中应保证基金业务系统的稳定可靠和安全。

在系统的设计阶段，应考虑系统未来升级和维护面临的问题，应该选择易于部署和维护的技术架构。包括：系统在设计时应充分考虑到管理维护的可视化、层次化及控制的实时性，做到系统的所有资源状况一目了然；能充分保证将设备故障控制在有限范围，不影响故障设备之外的其余设备和系统，保证整个系统的正常运行；确保系统具有完善的日志和审计机制，做到无论是业务系统的操作，还是硬件设备的运行，都有完整的记录，易于进行分析和统计；在技术实现时，应采取可以“热部署”和“可动态伸缩部署”的方案，降低系统的升级过程对服务的影响。

学校学生安全管理系统系统的设计还应该遵循通用和专业的标准和规范，提高系统间资源共享的能力，使得服务具有良好的扩展性。具体体现在：系统选择的产品和技术应遵循相应的国家、国际标准；网络安全设计遵循国家相关的标准和规范；软件项目开发过程遵循软件工程项目管理的标准和规范；设计和开发文档规范、统一等。