大连医科大学
信息安全审计管理办法(草案)

第一章 总则

第一条 为规范信息系统安全审计工作，完善我校信息系统安全审计机制，衡量信息系统现有安全措施的整体状况，验证是否应该继续执行现有安全措施，确保现有的安全措施符合相关的安全标准、策略和要求，特制定本管理办法。

第二条 本办法适用于我校信息系统规划设计、开发运行和管理维护的审计管理，主要涉及信息系统的开发管理、信息系统内部控制功能、运行管理、基础设施及综合管理等方面。

第二章 职责

第三条 大连医科大学网络安全和信息化领导小组办公室负责建立和维护健全有效的内部审计体系，由学校委托专业技术人员作为信息安全审计员，并由信息安全审计员负责内部信息系统的安全审计工作。

第四条 大连医科大学网络安全和信息化领导小组对内部审计的适当性和有效性承担最终责任，大连医科大学网络安全和信息化领导小组办公室组织指导内部审计工作，定期检查和研究信息系统安全审计工作。

第五条 安全审计员的审计职责权限如下：

（一）对于自身的判断要有明确的依据；

（二）有权要求被审计部门提交审计所需的相关资料；

（三）安全审计员要向被审计部门负责人报告审计实施状况及有关改进事项。

第六条 安全审计员的审计任务应以第三方的立场，对信息系统的可靠性、安全性、紧急对策、灾害恢复计划、隐私机密数据的保护、系统开发与维护的有效性及系统的运行效率等有关各项目进行检查、评价并报告结果。

第三章 审计权限

第七条 安全审计员有权及时、全面了解信息系统管理信息，并就有关问题向审计对象和相关人员进行调查、质询、取证。

第八条 对拒绝接受或不配合内部安全审计、拒绝提供或提供虚假资料、打击报复或陷害安全审计员的，有权向上级报告，要求及时予以制止并做出处理。

第四章 信息系统开发审计

第九条 信息系统审计内容主要包括信息系统开发、信息系统内部控制功能、信息系统运行管理、基础设施管理、综合管理等方面。

第十条 信息系统开发审计，包括检查软件开发项目的组织管理和开发过程控制存在的问题。主要审计项目如下：

（一）信息战略审计：主要检查是否符合业务经营战略要求等；

（二）整体计划审计：主要检查是否得到最高领导的认可，依照立案规则决定，是否明确信息系统的整体概貌等；

（三）开发计划审计：主要检查是否在对信息技术调查的基础上决定，是否明确目的、对象业务、费用效果等内容；

（四）系统分析、需求定义审计：主要检查是否得到开发方及用户方的认可，明确对象、范围及方法，对随着信息系统引入而产生的风险进行分析等；

（五）系统设计审计：主要检查是否得到开发方与用户方负责人的认可，系统性能是否满足用户需求等；

（六）程序设计审计：主要检查程序设计是否规范，是否按照系统设计报告进行程序设计等；

（七）编码审计：主要检查编码过程是否安全，是否按程序说明书进行编码，重要的程序是否由程序作者以外的人员进行测试等；

（八）系统测试审计：主要检查系统测试结果是否得到开发及用户的负责人的认可等；

（九）试运行审计：主要检查是否制定合理的试运行计划，明确试运行结束的验收方法等。

第五章 信息系统内部控制功能审计

第十一条 信息系统内部控制功能审计，包括系统和数据的安全控制和对它们的操作控制、审计管理功能设置等情况。主要审计项目如下：

（一）查阅审计日志，应检查以下内容：

1、用户 ID；

2、日期、时间和关键事态的细节，例如登录和退出；

3、若有可能，终端身份或位置；

4、成功的和被拒绝的对系统尝试访问的记录；

5、成功的和被拒绝的对数据以及其他资源尝试访问的记录；

6、系统配置的变化；

7、特殊权限的使用；

8、系统实用工具和应用程序的使用；

9、访问的文件和访问类型；

10、网络地址和协议；

11、访问控制系统引发的警报；

12、防护系统的激活和停用，例如防病毒系统和入侵检测系统。

（二）使用监视系统，应检测以下内容：

1、授权访问；

2、所有特殊权限操作；

3、未授权的访问尝试；

4、系统警报或故障；

5、改变或企图改变系统的安全设置和控制措施。

第六章 信息系统运行管理审计

第十二条 信息系统运行管理审计，包括有关制度建设、系统运行环境、系统软件和硬件管理、网络和通讯管理、数据输入和输出管理、病毒防范、防灾和应急管理、系统维护、系统升级和废止管理。主要审计项目如下：

（一）运行管理审计；主要检查输入管理、数据管理、输出管理、软件管理、硬件管理、网络管理、用户操作行为、入侵行为、用户访问控制、系统操作等方面内容。

（二）系统维护审计：主要检查维护计划、维护实施、维护顺序、维护确认、试运行管理、旧信息系统废除等方面内容。

（三）有关制度审计：主要检查制度的完整性、合理性及有效性，制度文档管理等方面内容。

第七章 基础设施管理审计

第十三条 基础设施管理审计，包括计算机机房管理、网络管理和个人办公计算机管理情况。主要审计项目如下：

（一）设备管理审计；

（二）机房管理制度审计；

（三）机房的门禁系统管理审计；

（四）供电系统、空调系统管理审计；

（五）防灾措施和防灾监控系统管理审计；

（六）个人办公计算机管理审计。

第八章 综合管理审计

第十四条 综合管理情况审计，包括信息系统在计划、开发、运行维护等各阶段相同的文档管理、进度管理、人员管理、外部委托及灾害对策等。主要审计项目如下：

（一）文档管理审计：包括文档制作、文档管理审计等方面内容；

（二）进度管理审计：包括进度实施、进度评价审计等方面内容；

（三）人员管理审计：包括人员职责权限、业务分配、教育培训审计等方面内容；

（四）外包管理审计：包括委托计划、委托单位选定、委托合同审计、委托业务审计等方面内容；

（五）灾难对策审计：包括风险分析、灾难应急计划、备份恢复审计等方面内容。

第九章 信息系统的审计实施

第十五条 在进行信息系统审计前，必须制定审计计划，计划应包括以下内容：

（一）作为信息系统审计对象的系统及领域；

（二）具体的信息系统审计项目、审计目的及风险；

（三）信息系统审计方法及顺序；

（四）信息系统审计日程安排；

（五）信息系统审计负责人、承担者及作业的分配；

（六）信息系统审计报告日期。

第十六条 信息系统审计计划必须以文档化形式提交给被审计系统的部门负责人，并得到其认可。

第十七条 在进行信息系统审计前，必须准备信息系统审计工具。包括编制信息系统审计实施表，选择适用的审计软件包和其他审计工具,主要工具如下：

（一）信息系统审计实施表包括信息系统审计顺序、内部审计评价表、安全检查实施表等；

（二）信息系统审计用的工具软件包括通用信息系统审计程序、审计模块、业务管理的程序等；

（三）信息系统监控工具包括网络监控、主机监控、数据库监控、应用系统监控以及专用安全工具等。

第十八条 在审计实施阶段，安全审计员应完成以下主要工作：

（一）收集资料；

（二）决定审计或测试的方式，包括符合性测试、实质性测试；

（三）列出需要访谈的人员名单及主要内容；

（四）查阅有关部门的政策、标准及准则，以供审计使用；

（五）利用审计方法，对所有控制进行测试和评价。

第十九条 在审计过程中，针对各个阶段进度方面出现的问题，必须提交以下报告：

（一）针对项目中某一问题的专题分析报告，提出紧急改进方案或一般改进方案；

（二）阶段性报告，在每一个阶段结束后，提交阶段性审计报告；

（三）综合审计报告。

第十章 信息系统的审计方法

第二十条 在信息系统审计中，应通过现场核查获取相关信息，进行安全性、可靠性、有效性评估分析。

第二十一条 安全审计员核查评估应保证分析依据具有代表性，分析方法的正确性。

第二十二条 在信息系统审计中，必要时应按照以下方法进行符合性测试、实质性测试等审计测试。

第二十三条 安全审计员进行审计测试应保证测试条件符合实际运行情况，以及测试方法的正确性和准确性。

第二十四条 在信息系统审计中，应对行为记录、审计日志记录、网络活动记录、重点监控记录等有关审计记录进行查阅。

第二十五条 安全审计员进行记录查阅应保证提取信息的完整性和准确性，以及分析方法的正确性。

第十一章 信息系统的报告跟踪

第二十六条 信息系统审计报告的内容要点包括：

（一）安全审计员制作信息系统审计报告的时间；

（二）对信息系统的可靠性、安全性及有效性进行评价的结果；

（三）系统存在的问题；

（四）根据存在的问题提出的改进劝告；

（五）根据改进的劝告提出的改进方案；

（六）还可记载其他的必要事项。

第二十七条 安全审计员在完成信息系统审计后，对审计结果迅速记录与归纳，应尽快向领导报告。

第二十八条 信息系统审计结果最终应以报告形式归纳，向领导提交。信息系统审计报告由承担该审计的安全审计员完成，并在得到信息系统审计负责人的认可后方可提交。

第二十九条 信息系统审计报告要向被审计部门即信息技术部门和有关业务部门负责人及信息系统审计部门提交。

第三十条 信息系统审计不应以提交报告书为结束，必须对审计报告中提出的问题，特别是重大问题，要跟踪整改的状况，确立信息系统审计跟踪制度。

第三十一条 信息系统审计跟踪必须做到以下几点：

（一）被审计部门要在规定期限内提交整改计划，安全审计员随时与被审计部门接触，了解跟踪整改的状况；

（二）如整改进展缓慢，要帮助找出原因，促使整改的完成；

（三）信息系统审计要达到最终目的，审计结果的跟踪是不可缺少的，并要使其成为一种制度。

第十二章 信息系统的其他要求

第三十二条 对信息系统审计的周期要求如下：

（一）对信息系统的全面审计应每 2 年进行一次；

（二）对信息系统开发审计，应与开发项目同步进行；

（三）对信息系统内部控制功能审计、基础设施管理审计、综合管理审计，应每年进行一次；

（四）对信息系统运行管理审计，应每半年进行一次。

第三十三条 对信息系统审计过程中产生的文档按照以下要求进行管理：

（一）对信息系统审计中产生的各种文档，应进行归档，并由机要室专人保管；

（二）对信息系统审计中产生的各种文档的查阅，应按照管理权限要求进行审批；

（三）对信息系统审计中产生的各种文档的保存期限，分别为：

信息系统审计产生中间文档，保存 2 年；

信息系统审计产生最终文档，保存 5 年。

第三十四条 信息系统审计过程中，相关部门应做好以下配合工作：

（一）安全审计员应做好与有关业务部门的协调工作，取得有关业务部门对信息系统审计工作的支持；

（二）对系统整体进行信息系统审计时，安全审计员事先明确各方的职责，并与有关各方研究和落实；

（三）信息技术部门和有关业务部门负责人应支持安全审计员的工作，必须提供便利的工作条件和足够的资源；

（四）信息技术部门人员应配合安全审计员的工作，对安全审计员使用计算机来辅助实施审计，提供必要的技术支持；

（五）根据信息系统审计需要，信息技术部门和有关业务部门人员应认真接受安全审计员就相关问题的调查、质询、取证；

（六）对信息系统审计，信息技术部门和有关业务部门人员不得提供虚假资料。

第三十五条 根据我校重要信息系统的安全性需要和信息系统安全审计技术的发展，定期检查和评估信息系统安全审计管理的强度及有效性，对信息系统安全审计管理进行适时调整。

第十三章 附则

第三十六条 本办法由大连医科大学现代教育技术中心负责解释。

第三十七条 本办法自发布之日起实行。

2018 年 9 月

附件：

1、 信息系统安全管理员责任书

2、 信息系统安全审计员责任书

3、 系统管理员信息安全责任书

附件 1

信息系统安全管理员责任书

一、遵守国家法律法规、大连医科大学校园网及信息系统安全管理的相关规定，按照“谁主管谁负责，谁运营谁负责，谁使用谁负责”的原则，做好本信息系统的运维和管理工作。

二、用户自行建设的信息系统，需要负责系统软件、应用软件和系统内容的建设、维护和管理，并承担全部的安全和管理责任。现代教育技术中心提供网络接入和域名解析服务。

三、用户应建立信息安全责任制度，落实信息系统管理员、日常运维人员，做好信息安全事故应急处置预案，严格审核网站发布内容，合理分配信息发布权限，保证信息发布内容的合法和安全。

四、用户应确定专人做好信息系统的日常维护和管理工作，记录和保存访问日志，及时跟踪运行状况，及时对信息系统进行安全升级和技术维护，出现异常情况应按应急处置预案处置，并向现代教育技术中心报告。

信息系统管理人员有义务按照现代教育技术中心的要求报告系统的使用情况、运行情况和维护情况等，并接受相关安全技术检查。

五、定期对信息系统进行安全扫描和检测，对发现安全隐患的，应关闭外网访问并限时整改，信息系统安全管理人员有责任在规定时间内按规范做好信息系统的安全整改工作。

六、本责任书自签署之日起生效。责任书各条款不因信息系统安全管理员变化而变更或解除，接任安全管理员应履行相应职责。

信息系统基本信息

信息系统名称	
信息系统用途	
信息系统域名/IP	
所提供服务端口	

责任单位(盖章):

信息系统安全管理员(签字/盖章):

签订日期:

附件 2

信息系统安全审计员责任书

为了进一步落实网络安全和信息安全管理工作,确保信息系统的安全可靠运行,特明确安全审计员职责如下:

一、监督信息部门对各项信息安全规章制度的执行,并对关键信息文件进行备份,及时查处安全隐患。

二、负责对整个信息系统进行安全审计,对安全管理员做的安全评估报告进行审计。

三、协助安全管理员制定网络设备安全配置规则,并监督落实执行。

四、负责做好有关审计资料的原始调查的收集、整理、建档工作,按规定保守秘密和保护当事人合法权益。

五、在安全审计过程中,详细记载发生异常时的现象、时间和处理方式,并及时上报。

六、负责对所有涉及的审计事项,编写内部审计报告,及时报主管领导审核,并提出处理意见和建议。

七、负责参与网络安全事故调查,对于由于安全审计员工作疏忽或失误而产生的安全事故,应追究其相应责任。

八、本责任书自签署之日起生效。

责任单位(盖章):

安全审计员(签字/盖章):

签订日期:

附件 3

系统管理员信息安全责任书

为了保证信息系统以及网络、硬件设备的正常运行,切实加强系统管理的严密性与保密性,促进系统设备管理的有效性,特制定本责任书:

第一条 签订对象:

第二条 责任期限:系统管理员任职期间。

第三条 在责任期内,杜绝因管理不善而发生安全责任事故。具体必须做好以下工作:

一、遵守《全国人民代表大会常务委员会关于维护互联网安全的决定》、《中华人民共和国电信条例》、《互联网信息服务管理办法》、《互联网安全保护技术措施》、《大连医科大学网络安全工作责任制实施细则》、《大连医科大学信息化建设项目管理办法》等相关法律法规的有关规定,管理机房内系统设施。

二、应有维护计算机信息系统安全运行的足够能力,设置安全可靠的防火墙,安装防病毒软件,定期进行安全风险分析与系统漏洞测试适时对软硬件进行升级,具有防止病毒入侵以及电脑黑客攻击的能力确保系统安全、可靠、稳定地运行。

三、定期查看设备的外观状态、Power 状态、CPU 利用率、硬盘空间、进程状态日志检查、网络接口状态、安全状态、确保设备系统的正常运行。

四、根据设备的服务功能,负责整机的系统管理、主要服务进程的健康性检查以及日常的物理维护;

五、所有设备的超级用户口令需提交给安全管理员掌握,每次修改均需重新提交。

六、为每台设备建立“运行登记簿”,记录所有与该机器有关的信息。

七、有权在所管辖的机器上增减用户账号(除超级用户账号),但要在确保不影响系统安全的前提下进行。

八、设备配置或账号要写明用途或身份。

九、负责设备软件包的管理和维护:应对本机所安装的软件有

详细的清单,包括系统软件的名称、版本,所装应用软件的名称、版本、功能及安装时间

十、系统管理员在服务器上增减软件,需要做好记录。

十一、Email/DNS 服务器/其他应用服务器,每天做一次增量备份,每周做一次全备份。备份数据保存 6 个月以上。

十二、用户密码的制定和维护规则;

(一)任何账号生成后,禁止使用缺省密码作为密码使用;

(二)长度应大 6 位,且应是字母(大小写)、符号、数字混合使用;

(三)避免使用自己(或亲属、朋友)的姓名、生日等易被人猜到的信息作为密码;避免使用与自己的用户名相关的信息作为密码;

(四)用户要妥善管理自己的账号/密码,用户的密码严禁被他人使用,(若有需求,可以在“设备管理员”的同意下开临时账号)。

(五)由于设备用户自己的账号/密码管理不善,造成系统安全性问题(如,口令过于简单,被黑客猜到,进入系统),由该密码的所有者负相应的责任。

(六)当用户登录设备(输入密码)的时候,应让他人回避,以避免密码泄露。

(七)设备用户最少每月修改一次自己的密码;超级用户口令最少每月检查一次,最少 2 个月修改一次;

第四条 本责任书自签订之日生效。

责任单位(盖章):

系统管理员(签字/盖章):

签订日期: