防灾科技学院信息化管理中心

信息中心〔2021〕16 号

关于印发《防灾科技学院信息系统建设安全管理办法》的通知

学校各部门、各单位：

为加强学校信息系统建设过程中安全控制，保障信息系统本身以及开发、测试和上线运行过程中的安全性，规范信息系统获取、开发与维护过程中的职责定义与流程管理，特制定《防灾科技学院信息系统建设安全管理办法》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 10 月 7 日

防灾科技学院信息系统建设安全管理办法

第一章　总则

第一条　为加强防灾科技学院（以下简称“学院”）信息系统建设过程中安全控制，保障信息系统本身以及开发、测试和上线运行过程中的安全性，规范信息系统获取、开发与维护过程中的职责定义与流程管理，特制定本办法。

第二条　本办法适用于本学院各部门范围内的信息系统,涉及信息系统的获取和开发、实施及上线及下线全过程。

第二章　职责制度

第三条　项目需求部门责任：为提出该项目需求的部门，除功能需求外还负责在相关部门的协助下提出系统安全需求。

第四条　项目建设部门责任：为承担具体信息系统设计、开发和实施的部门或外部合同方,负责进行信息系统的安全需求分析，并保证系统在设计、开发、测试、验收和上线的各个阶段均能满足项目安全需求和现有的系统安全标准和规范。此外，在相关部门的组织下进行系统安全需求、设计和上线评审。

第五条　总体要求：信息系统建设项目各阶段（尤其是需求设计、测试及上线等重要阶段）的评审活动，评审内容必须包括相应的信息安全要求，根据项目的具体应用特性和安全需求进行完善。在信息系统的安全评审过程中，应提交相应安全设计、实现

或验证材料，对于评审中发现的问题，相关责任部门应及时整改。

第六条 信息系统的设计和建设过程中，应实现信息系统及重要信息数据的完整性保护，以防止未经授权的修改。同时，对信息系统中重要数据的修改和更新应遵循相关业务部门的管理规定，只有经过授权流程审批通过后才能修改相应信息。

第三章 需求及设计阶段的安全评审

第七条 安全需求分析：在项目的计划阶段，项目需求部门应与项目建设部门共同讨论信息系统的安全需求，明确重要的安全需求点，安全需求分析必须作为项目需求书的组成部分。

第八条 项目需求部门与项目建设部门应对系统进行风险分析，考虑业务处理流程中的技术控制要求、业务系统及其相关在线系统运行过程中的安全控制要求，在满足相关法律、法规、技术规范和标准等的约束下，确定系统的安全需求。

第九条 对系统安全应遵循适度保护的原则，需在满足以下基本要求的前提下，实施与业务安全等级相符合的安全机制。

第十条 通过必要的技术手段建立适当的安全管控机制，保证数据信息在处理、存储和传输过程中的完整性和安全性，防止数据信息被非法使用、篡改和复制。

第十一条 实施必要的数据备份和恢复控制。

第十二条 实施有效的用户和密码管理，能对不同级别的用户进行有限授权，防止非法用户的侵入和破坏。

第十三条 系统的安全需求及其分析需要经过项目组内部充

分讨论，项目需求方和项目建设方应对安全需求及其分析的理解达成一致。

第十四条 技术方案设计的安全性。项目建设部门应根据确定的安全需求设计系统安全技术方案，必须确保满足以下要求：

系统安全技术方案要满足所有安全需求，并且符合公安部等政府部门、上级主管部门的法规和标准要求；

系统安全技术方案应至少包括网络安全设计、操作系统和数据库安全、应用软件安全设计等部分；

系统安全技术方案涉及采用的安全产品，应符合国家有关法律法规和本学院现有安全制度的规定。

第四章 开发阶段的安全管理

第十五条 人员的安全管理：本学院员工在参与重要信息系统项目开发之前，应签订相关的保密协议。

第十六条 明确开发人员在信息系统开发过程中的安全职责和对信息系统的访问权限。

第十七条 严格加强对系统开发环境和开发场地的出入管理，进入开发现场必须经过必要的安全控制措施。

第十八条 开发设备使用的安全管理：应做好对信息系统开发环境的安全管理，信息系统的开发环境要相对独立，开发环境必须与运行环境进行分离；开发环境中的设备必须明确安全责任人，遵循“谁使用谁负责”的原则，公共用途的设备也应指定安全责任人进行保管和维护；信息系统的开发环境和实施场地应当

与生产环境和实施场地隔离；严格管理开发环境中的各种移动设备、个人信息处理设备，禁止未经允许的设备接入开发环境。

第十九条 开发文档的管理：信息系统开发过程中的资料、文档要按照有关规定进行管理；在文档的编写、整理过程中，要明确文档标准化格式规范。对文档的修改进行记录，并确保文档的一致性；文档中与安全相关的内容要准确、完整，并明确文档的密级以及分发范围；开发过程中的各种文档，只能在授权分发范围内流转，任何人不得以各种形式进行其非授权分发或外泄。

第二十条 开发过程中软件和源代码的安全管理：除因工作需要外，禁止任何人持有、复制本学院所拥有的软件源代码，禁止任何人外借或对外复制本学院所拥有的软件源代码；信息系统开发所使用的操作系统、数据库、开发工具软件等必须是本学院授权使用的软件，严禁使用非授权软件；应对编程语言和编程工具的使用进行培训，了解和掌握编程语言和编程工具已知的安全隐患，加强对源代码的检查，防止源代码中存在可疑程序和已知的安全隐患；信息系统所采用的关键技术措施和核心安全功能设计应严格控制发放范围。对于重要的秘密资源（如源程序、目标码等）应严格设置访问权限控制；对应用系统的编译过程进行严格监督，确保经正确编译的软件版本最终生成运行代码，并保证运行代码的完整性、安全性；严格控制对软件版本的管理，确保信息系统开发过程中源代码和执行代码的一致性和正确性。

第二十一条 开发过程中数据输入安全管理：在编制软件的过

程中，任何程序的编码都应对输入数据进行如下验证：使用强输入验证；检验输入数据长度；限制数值输入的范围；限制输入字符的类型。

第二十二条 在编制软件的过程中,应对应用数据进行如下安全控制：

原则上不允许使用真实数据进行测试，特殊情况需要使用真实测试数据时，对系统测试数据要进行安全保护，并经过信息技术与数据管理处主管领导的审批；

在测试过程中，如模拟真实数据，应确保测试数据和真实生产数据分离；测试完成之后，应立即将测试数据从测试系统中删除；

开发的系统要确保系统应用的数据完整性安全，防止信息在处理过程中被篡改；

开发的系统要确保系统应用的输出数据准确,检查输出数据，保证正确处理储存信息；

模糊性检查测试输出数据是否合理；

测验核实输出的相关提示。

第五章 测试阶段的安全管理

第二十三条 信息系统安全功能测试：在信息系统测试阶段，应确保所有设计的安全功能均能得到落实和实现。在测试报告或相关文档中应明确说明检查列表中各项安全功能的落实和实现情况。

第二十四条 测试过程的安全管理。在信息系统开发测试过程中，对于来自业务系统的数据要根据相关规定进行变形处理，禁止在开发或测试环境中直接使用业务系统的密钥和用户密码等重要数据。测试环境要依据相关规定进行合适的管理和安全防护，并通过相应的手段确保与生产系统、开发系统隔离。

第六章 系统安装、上线阶段的安全管理

第二十五条 新系统（新设施）安装上线前，应有相应管理者的授权，以授权设施的用途和使用；此外还应获得负责维护本地系统安全环境的管理者授权，以确保所有相关安全策略和要求得到满足。若需要，硬件和软件应进行检验，以确保他们与其它系统部件或 IT 基础设施组件的兼容性。

第二十六条 在信息系统安装部署时，应采取相应措施确保系统安全功能的实现，对操作系统、数据库、应用系统等软件的安装部署和配置应该符合。

第二十七条 信息系统上线前应进行安全评估或审查，通过审查系统设计文档中的安全功能设计、系统测试文档中的安全功能测试，确保系统本身安全功能的实现。通过审核系统安装与配置过程或文档，确保系统安全配置的落实与实现。

第七章 信息系统运行阶段的安全管理

第二十八条 信息系统上线运行期间至下线之前，随着技术的发展和应用环境的变化，系统主管部门应每年组织进行技术符合性检查，以检查信息系统与安全实施标准的符合程度。

第二十九条 信息系统下线前,所有介质上的业务数据应妥善清除或消磁处理。

第八章 外购、外包软件的安全管理

第三十条 对于需要外购的套装软件，软件的设计、实施方案的安全性也应遵循本文件中的要求，由相应的负责部门在安全需求、方案设计及上线阶段进行相应地安全管控。

第三十一条 对于与其他公司合作开发和外包的项目,要明确双方的信息安全责任，并对交付成果提出信息安全要求，对安全责任的落实和交付成果依照安全要求的实现情况进行监督检查。

第三十二条 由外部合作单位开发的软件在进行交付时,相应的负责部门应根据要求对交付软件进行安全测试和评估，并责成外部合作单位修改已发现的安全漏洞和问题，确保交付软件的安全性符合要求。

第九章 附则

第三十三条 本办法由信息化管理中心负责解释。

第三十四条 本办法自颁布之日起施行。

附表1

系统安全功能设计检查列表

系统建设部门		系统名称			
系统用途		系统预计上线日期			
安全检查点		**基线系统要求**	**重要系统要求**	**是否符合**	**备注**
应用程序访问控制					
具有基于用户或角色的权限管理		必须	必须		
管理员可以根据用户或角色赋予不同的权限		必须	必须		
具有用户密码复杂性检查		推荐	必须		
具有用户密码强制修改周期设置		推荐	推荐		
用户第一次登录强制修改密码		推荐	必须		
用户输入时屏幕不显示密码		必须	必须		
用户连接超时重新登录		推荐	必须		
用户连接时间区间控制		推荐	推荐		
建立统一的用户命名规范		可选	推荐		
系统、数据库账户使用					
建立应用程序专用帐户，不能使用系统根帐户作为应用程序帐户，比如FTP帐户，启/停数据库等不能使用Root用户		必须	必须		
不能使用Root帐户作为应用的安装帐户		必须	必须		
应用程序不能使用sa、dba等数据库管理员账户连接数据库，应为不同的程序应用建立不同的数据库账户连接		必须	必须		
应用程序帐户密码可修改，也就是账户密码不能固化在程序中		必须	必须		
重要数据安全					
用户密码信息和其它数据分开保存		推荐	必须		
用户密码信息加密保存		推荐	必须		
用户授权信息与其它数据分开、加密保存		可选	推荐		
对重要数据采用数据完整性保护技术措施		可选	推荐		
对重要数据进行加密存储		可选	推荐		
重要数据备份及加密备份功能		可选	推荐		
信息交换安全					
外部系统连接必须要有身份验证检查		可选	推荐		
外部系统连接身份验证信息加密传输		可选	推荐		
用户密码加密传输		推荐	必须		
其它重要数据加密传输		可选	推荐		
关键活动日志					
系统管理员登录成功		推荐	必须		
系统管理员登录失败		推荐	必须		
用户登录成功		推荐	必须		
用户登录失败		推荐	必须		
用户尝试访问非授权资源		可选	推荐		
系统错误		推荐	必须		
用户操作日志		可选	按需		
数据修改、更新日志		可选	按需		
输入输出验证					
用户数据输入范围验证		必须	必须		
用户数据输入非法字符验证		必须	必须		
外部程序传入数据验证		可选	推荐		
程序输出数据校验		可选	推荐		
法律法规特定要求					
等保相关系统的特定要求		按需	按需		

说明：	
必须	必须启用该功能
推荐	推荐启用该功能，没有特殊情况都应该启用该功能。
可选	可以启用该功能，如果启用可以增强系统安全性，如果不启用也不会给系统带来严重风险。
按需	根据具体系统、项目的需求而定，主要指法律法规方面的要求。
重要系统要求	对于业务系统等重要系统的更高层次的要求。
基线系统要求	对于所有应用系统都必须达到的要求。

附表2

序号	交付文档
1	可行性分析(研究)报告
2	合同会签表
3	项目合同
4	项目价格清单
5	合同技术协议
6	项目计划
7	项目启动会PPT
8	项目组管理规定
9	软件开发计划 （1.软件配置管理计划 2.软件质量保证计划 3.用户培训计划 4.软件安装(部署)计划）
10	项目详细实施方案
11	软件需求规格说明书（包括接口设计说明、数据流图和数据字典）
12	数据需求说明书
13	概要设计说明书
14	详细设计说明书（包括接口设计说明书和数据库设计说明书）
15	软件测试计划
16	软件测试说明（包括测试用例和测试过程）
17	软件测试报告（分为综合测试报告和验收测试报告,如需要 可提交软件测试日志。）
18	用户手册（包括操作,使用,安装,应急处理,维护。）
19	开发进度月报
20	试运行方案
21	软件维护报告
22	软件部署说明书
23	售后服务保证文件
24	知识产权说明、交付使用授权书
25	源程序
26	软件验收测试大纲
27	系统试运行报告,用户使用报告
28	应急预案
29	项目开发总结报告

防灾科技学院信息化管理中心　　2021年10月7日印发