防灾科技学院信息化管理中心

信息中心〔2021〕23 号

关于印发《防灾科技学院信息系统建设管理制度》的通知

学校各部门、各单位：

为加快学校信息系统安全建设步伐，规范信息系统工程项目建设的安全管理。特制定《防灾科技学院信息系统建设管理制度》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 12 月 3 日

防灾科技学院信息系统建设管理制度

第一章　总则

第一条　为加快学校信息系统安全建设步伐，规范信息系统工程项目建设的安全管理，特制定本制度。

第二条　本制度的目的是对学校信息系统建设过程中的各阶段进行规范和管理，保证学校信息系统建设安全、可控。

第二章　管理职责

第三条　信息化管理中心负责信息系统安全规划和建设等工作。

第四条　各部门配合信息化管理中心完成相关信息系统安全建设工作。

第三章　项目建设安全管理的总体要求

第五条　信息系统项目的生命周期包括：项目申报、项目审批和立项、项目实施、项目验收和投产；从项目建设的角度来看，这些生命周期的阶段则包括以下子阶段：需求分析、总体方案设计、概要设计、详细设计、系统实施、系统测试和试运行，如下表所示。

项目管理生命周期	
项目申报	需求分析
项目审批和立项	总体方案设计
项目实施	概要设计、详细设计、系统实施
项目验收和投产	系统测试、试运行和投产

第六条 信息系统项目建设安全管理应遵循如下原则：

（一）全生命周期安全管理：网络安全管理必须贯穿信息化项目建设的整个生命周期；

（二）成本-效益分析：进行网络安全建设和管理应考虑投入产出比；

（三）明确职责：参与项目建设和项目管理的人员都应该明确安全职责；

（四）管理公开：应保证项目参与人员都知晓和理解安全管理的模式和方法；

（五）最小特权：人员对项目资产的访问权限制到最低限度，即仅赋予其执行授权任务所必需的权限。

第七条 项目建设安全管理要求：项目安全管理工作应强化责任机制，规范管理程序。在项目的申报、审批、立项、实施、验收等关键环节中，必须依照规定的职能行使职权，并在规定的时限内完成各个环节的安全管理行为，否则应承担相应的行政责

任。

第四章　项目申报

第八条　项目申报阶段应对信息系统项目及其建设的各个环节进行统一的安全管理规划，确定项目的安全需求、安全目标、安全建设方案，以及生命周期各阶段的安全需求、安全目标、安全管理措施。

第九条　应由系统申请部门提出项目需求，信息化管理中心组织相关部门、专家对项目进行系统定级、需求分析、确定总体目标和建设方案。系统申请部门进行项目申报时应填写相应申请表。

第十条　系统定级

依据国标《信息安全技术-网络安全等级保护定级指南》（GB/T22240-2020）对项目中的系统进行定级，明确信息系统的物理边界和安全保护等级；

以书面的形式说明确定信息系统为某个安全保护等级的方法和理由，形成信息系统定级报告；

组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定，上报上级主管单位进行审定；

信息系统的定级结果向本地公安机关进行备案。

第十一条　安全需求分析

安全需求分析至少包括以下网络安全方面的内容：

安全威胁分析报告：分析待建系统在生命周期的各个阶段中可能遭受的自然威胁或者人为威胁（故意或无意），具体包括威胁列表、威胁可能性分析、威胁严重性分析等；

系统脆弱性分析报告：分析待建系统自身存在的脆弱性，包括对系统脆弱性的定性或定量的描述，这些脆弱性是指被攻击的可能性、被攻击成功的可能性；

影响分析报告：分析安全威胁利用系统的脆弱性给系统造成的不良影响。影响可能是有形的，例如资金的损失或收益的减少，或可能是无形的，例如声誉和信誉的损失；

风险分析报告：分析待建系统存在的安全风险，安全风险分析取决于威胁分析、脆弱性分析和影响分析，应提供风险清单以及风险优先级列表；

系统安全需求报告：针对安全风险，应提出安全需求，对于每个不可接受的安全风险，都至少有一个安全需求与其对应。

第十二条 安全可行性

在可行性报告中应增加相应的网络安全方面的内容：

增加信息化项目的总体安全目标，并针对安全需求提出相应的安全对策，安全对策的强度应根据相应资产的重要性来选择；

增加描述如何从技术、运作、组织以及制度四个方面来实现

所有的安全对策，并形成安全方案；

增加项目各承担单位的网络安全方面的资质和经验介绍，并增加介绍项目主要参与人员的网络安全背景；

增加项目建设中的安全管理模式、安全组织结构、人员的安全职责、建设实施中的安全操作程序和相应安全管理要求；

对安全方案进行成本-效益分析。

第十三条 对投入使用的应用软件需要升级改造的，虽不需另行立项，但仍需参照上述方法进行一定的安全性分析，并针对可能发生的安全问题提出和实现相应安全对策

第五章 安全方案设计

第十四条 项目设计方依据项目安全需求对安全方案进行设计，确定安全方案的可行性和安全性，必要时可以聘请外单位的专家参与论证工作。

第十五条 安全方案设计原则

根据该信息系统的安全保护等级选择基本安全措施，设计安全标准必须达到等级保护相关等级的基本要求，并依据风险分析的结果进行补充和调整必要的安全措施；

指定和授权专门的部门对该信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

应根据该信息系统的等级划分情况，统一考虑安全保障体系

的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；

根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

第六章　方案论证和审批

第十六条　本阶段主要是项目审批部门对项目申报内容进行审批，对项目进行安全性论证，必要时可以聘请外单位的专家参与论证工作。

第十七条　安全性论证应着重对项目的安全需求分析、安全对策以及总体安全方案进行成本-效益、合理性、可行性和有效性分析。对论证结论为“需作复议”的项目，通知申报部门对有关内容进行必要的补充或者修改后，再次提交复审。

第十八条　项目安全立项：项目审批后，信息化管理中心对项目进行立项，在《信息系统项目任务书》中应增加相应的系统安全方面的内容：

项目的管理模式、组织结构和责任：增加项目建设中的安全管理模式、安全组织结构以及人员的安全职责；

项目实施的基本程序和相应的管理要求：增加项目建设实施中的安全操作程序和相应安全管理要求；

项目实现功能和性能指标：增加描述系统拥有的具体安全功能以及安全功能的强度；

项目验收考核指标：增加安全性测试和考核指标。

第十九条 已经立项的项目如采用合作开发或者外包开发等形式，则需与项目开发承担单位签订安全保密协议。

第七章 项目实施方案和实施过程安全管理标准

第二十条 项目实施阶段包括3个子阶段：概要设计、详细设计和项目实施，本阶段的主要工作由项目开发承担单位来完成，信息化管理中心负责监督工作。

第二十一条 概要设计子阶段至少应达到以下安全要求：

应当按子系统（子模块）来描述系统的安全体系结构；

应当描述每一个子系统（子模块）所提供的安全功能；

应当标识所要求的任何基础性的硬件、固件或软件，和在这些硬件、固件或软件中实现的支持性保护机制提供的功能表示；

应当标识子系统（子模块）的所有接口，并说明哪些接口是外部可见的；

描述子系统（子模块）所有接口的用途与使用方法，并适当提供影响、例外情况和错误消息的细节；

确证子系统（子模块）的安全功能指标满足系统安全需求。

第二十二条 详细设计子阶段的安全要求至少要包括以下网络安全内容：

详细设计中应提出相应的具体安全方案，标明实现的安全功能，并应检查其技术原理；

对系统层面上的和模块层面上的安全设计进行审查；

完成安全测试和评估要求（通常包括完整的系统的、软件的、硬件的安全测试方案，至少是相关测试程序的一个草案）；

确认各模块的设计，以及模块间的接口设计能满足系统层面的安全要求。

第二十三条 项目实施子阶段的安全要求：本阶段的主要目的是将所有的模块（软硬件）集成为完整的系统，并且检查确认集成以后的系统符合要求。本阶段中，应完成以下具体网络安全工作：

找出并描述实现安全方案后系统和模块的安全要求和限制，以及相关的系统验证机制及检查方法；

完善系统的运行程序和全生命期支持的安全计划，如密钥的分发等；

对项目参与人员进行网络安全意识培训；

对参加项目建设的安全管理和技术人员的安全职责进行检查。

第二十四条 在系统实施阶段需要采购的网络安全设备（IDS、防火墙等）、操作系统、数据库等必须由单位进行统一采购。

第二十五条 采购和使用商用密码产品对不涉及国家秘密的信息和信息系统进行保护时，应当遵照《信息安全等级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

第二十六条 按照《商用密码产品目录》选用商用密码产品。使用的商用密码产品，应当是国家密码管理局批准使用或者准予销售的产品，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

第二十七条 软件开发外包应当考虑如下几点：

检查代码的所有权和知识产权情况；

在合同上有代码质量方面的要求，按照代码编写规范编写代码；

在安装之前进行测试以检测恶意代码；

提供源代码以及相关设计、实施文档；

重要的项目建设中要对源代码进行审核。

第二十八条 安全服务商选择应当考虑以下几点：

信息系统建设过程中，选择具有服务资质的信誉较好的厂商，要求其已获得国家主管部门的资质认证并取得许可证书、能有效实施安全工程过程、有成功的实施案例。

对重要的信息系统工程建设项目，需在主管部门指定或在特定范围内选择具有服务资质的、信誉较好，并经实践证明是安全可靠的厂商。

在确定好安全服务商后，与安全服务商签订安全责任合同书或保密协议，明确约定相关责任。

在确定好安全服务商后，与其签订服务合同，确保其提供技术培训和服务承诺。

第八章 项目验收与备案测评

第二十九条 系统建设完成后，项目开发承担单位要依据项目合同的交付部分向学校进行项目交付，交付的内容至少包括：

信息系统交付清单，对交付的设备、软件和文档进行清点；

对系统运维人员进行技能培训，使系统运维人员能够进行日常的维护；

提供系统建设的过程文档，包括实施方案、实施记录、需求分析说明书、软件设计说明书，软件操作手册或使用指南等；

提供系统运行维护的帮助或操作手册。

第三十条 系统交付需要项目开发承担单位和学校的相关项目负责人进行签字确认。

第三十一条 在项目实施完成后，由信息化管理中心、项目开发承担单位及相关部门共同组成项目测试组对项目进行测试。测试内容应至少包括以下安全性测试：

配置管理：系统开发单位应提供安全配置文档，并验证安全配置的有效性；

安全功能测试：对系统的安全功能进行测试，以保证其符合详细设计并对详细设计进行检查，保证其符合概要设计以及总体安全方案；

脆弱性分析：使用漏洞扫描、渗透测试的方法对系统进行脆弱性分析，以判断它们在实际应用中是否会被利用。

第三十二条 测试完成后，项目测试组应提交信息系统安全性测试报告，其中应包括安全性测试和评估的结果。不能通过安全性测试评估的，由测试组提出修改意见，项目开发承担单位作进一步修改。

第三十三条 测试通过后，交付项目使用部门进入试运行阶段，试运行具体工作如下：

监测系统的安全性能，包括事故报告；

监测新发现的对系统安全的攻击、系统所受威胁的变化以及其它与安全风险有关的因素；

组织与系统安全有关的培训；

监测系统物理和功能配置，包括运行过程、运行状态。

第三十四条 系统安全试运行半年后，信息化管理中心组织由项目开发承担单位、项目使用部门对项目进行验收。项目验收应至少包括以下安全内容：

项目是否已达到项目任务书中制定的总体安全目标和安全指标；

项目建设过程中的各种文档资料是否规范、齐全；

安全专家及安全验收评价意见是否通过。

第三十五条 系统备案

系统备案的相关材料由信息化管理中心负责组织编写和管理；

系统备案材料编写完成后，报领导审批；

系统备案材料审批通过后，到相应的公安机关备案。

第三十六条 等级测评

系统进入运行过程后，三级的系统每年聘请第三方测评机构对系统进行一次等级测评，二级的系统每年内部测评一次，发现不符合相应等级保护标准要求应及时整改；

信息系统发生重大变更导致信息系统等级发生变化时，应及时调整信息系统级别并进行安全改造，改造完成后进行信息系统等级测评工作；

测评机构要选择具有国家相关技术资质和安全资质的单位。

第三十七条 测试验收方案

测试验收方案基本内容应包括以下内容：

（一） 工程概况

（二） 建设依据

（三） 验收的组织

（四） 测试时间、范围、方法和主要过程

（五） 验收检查的质量指标与评定意见

严格按照测试验收方案规定的范围、项目、流程、方式、方法进行验收。

对测试验收的控制方法和人员行为准则进行明确规定。

测试服务部应组织相关人员对测试验收方案进行评审和论证，确定方案的可行性、规范性和安全性。

在测试验收过程中所做的一切操作，应先报告后实施。不得向任何无关的第三方人员泄露测试验收相关的信息资料。

第九章 采购申请

第三十八条 采购申请、评估与审批集中采购由本单位信息

化管理中心负责。

第三十九条 采购申请由需求部门提出，提交给信息化管理中心进行采购前评估。 采购前评估包括以下三个方面：

（一）信息化管理中心针对此次采购对当前基础架构的影响进行评估，其中包括技术层面、管理层面以及系统安全方面的评估；

（二）信息化管理中心根据需求部门的业务需求，对申请采购软硬件的功能和性能进行评估。

（三）信息化管理中心根据市场行情，对 IT 软硬件采购成本进行评估。 集中采购申请由信息化管理中心和财务部门负责人审核后，交主管领导审批。 经批准的采购需求由信息化管理中心签订合同进行采购，需要进行招投标工作的按照招投标流程开展。未被批准的采购申请，在采购需求表上写明原因，并将其返回给需求部门。

第十章 到货验收

第四十条 采购的 IT 软硬件到货后，必须经过验收，才能正式投入使用。设备到货后，验收工作按照合同要求执行，信息化管理中心根据合同规定当场验货，有条件的须检查设备是否有损坏，备品、配件、资料、软件等是否齐全。软件到货后，验收方须检查软件介质是否有损坏，相关资料是否齐全等。 到货验

收合格后，签收到货单，并复印存档；若不合格，则拒绝签收。采购的设备和软件到货签收后，根据本单位相关规定办理出入库手续。

第十一章　附则

第四十一条　本制度由网络安全办公室负责解释。

第四十二条　本制度正式发布之日起施行。

防灾科技学院信息化管理中心　　2021 年 12 月 3 日印发