

广东财经大学文件

粤财大〔2017〕120号

关于印发《广东财经大学加强信息系统 (网站)安全管理实施方案》的通知

各党政管理、群团、教学、科研、教辅、附属单位：

《广东财经大学加强信息系统（网站）安全管理实施方案》业经2017年11月1日校长办公会议审议，11月2日党委常委会审定，现予以印发，请严格遵照执行。

特此通知。



广东财经大学加强信息系统（网站） 安全管理实施方案

为建立学校信息安全的长效机制，切实加强信息系统（网站）安全管理，根据上级有关文件精神和学校实际，制定本方案。

一、实施目标

通过全面普查、整改和进一步的建设，加强我校校园网络信息安全的保护，维护好我校网络空间的安全，规范网络信息发布的内容，加大网上信息的监管力度，制止和防范网上有害信息的传播，推进网络文明建设，创造良好的校园网络环境，盘活信息资产、无形资产，变无序为有序，初步形成我校全方位多层次的信息安全保障体系。

二、实施原则

（一）问题导向原则。针对我校信息系统（网站）实践中长期存在的小、散、乱等突出问题，提出切实可行的解决方案。

（二）安全与发展并重原则。坚持网络安全与信息化同步规划、同步建设、同步发展，以安全保发展，以发展促安全，用发展的理念解决网络安全问题，科学、主动、有效应对安全挑战，防止和避免以限制信息技术应用、拒绝资源共享等消极方式保安全。

（三）集中分类分区、内外有别原则。全校的网站原则上在网站群系统上进行建设、集中管理。在访问方式上，根据访问主体的不同，做到内外有别。

（四）方便用户原则。在注重安全的同时，也要结合实际，注重用户体验与感受，为广大师生提供便捷服务。

三、主要任务

（一）开展信息系统（网站）、IP 地址的全面摸排清理

1. 开展信息系统（网站）普查

摸清我校信息系统（网站）的基本信息，摸清全校信息系统（网站）的使用情况。

2. 清理“僵尸”信息系统（网站）

根据教育厅对“僵尸”网站的界定，符合下列条件之一，则可视为“僵尸”信息系统（网站）：网站年访问量在 1000 人次以下，网站长期 180 天以上未更新的；系统每年录入的信息在 100 条以下（结合我校实际，暂定为 30 条）；专题网站已完成工作使命的。对于这些网站，应以清理。

3. 清理“双非”信息系统（网站）

“双非”信息系统（网站），主要是指各单位在校外开展有合作办学、培训等教学活动并以我们学校名义建设的信息系统（网站），具有以下特征：非学校 IP 地址，即采用学校域名但服务器不在校内；非学校域名，即采用学校地址，但域名不在校内；非学校域名和服务器。

4. 清理无防护措施的 IP 地址

无防护措施的公网 IP，不再由相关二级部门使用，由网络信息中心集中管理。

(二) 信息系统(网站)的建设

1. 网站的建设

学校网站分四种类型：各单位的部门网站、专题网站、教学网站、“双非”网站。以下若无特别说明，均指各单位的部门网站和专题网站。

(1) 网站群系统平台的建设

网络信息中心、资产与实验室管理处负责网站群系统平台的选型、采购和部署等建设工作。

(2) 网站内容的迁移与建设

网站内容的迁移。学校首页及各二级单位已备案的网站,网络信息中心负责迁移至网站群。

网站内容的建设。学校首页及各二级单位的网站按照“内外有别”原则进行更新、维护与建设。不对外提供服务、不宜对外公开的网站或栏目，原则上限制在校园网内访问，校园网外教职工若需使用，可通过 VPN 特殊通道进行访问。学校中文版网页、英文版网页分别由校办、国际交流与合作处牵头进行建设。各二级单位的网站，直接在网站群上进行更新与维护；网站群平台的操作使用培训，安排在 10 月 26 日上午进行。

2. 信息系统的建设

按照《广东财经大学信息化建设项目管理办法》执行。

(三) 建设过程中注意的问题

1. 对于长期没有维护、存在安全隐患的网站，一定要负责建设与更新，不能带“病”运行。

2. 网站上论坛原则上不能开通。若需开通，必须申报，经校级领导同意，并有人严格监管。

3. 不能随意链接来路不明的网站，尤其是国外网站。

4. 不对外服务的网站，是否需要限制访问，由相关单位决定，网络信息中心做技术上的处理。

5. 信息发布一定要有明确的流程，有起草、审核、发布等环节，秉持“谁审核、谁发布、谁负责”的原则，确保发布内容不涉及国家机密。

四、信息系统(网站)的安全管理

(一) 建立备案与退出机制

凡在校园网内开设信息系统(网站)的单位需向网络信息中心备案，其中网站的开设还需向党委宣传部(新闻中心)进行备案，明确安全责任主体，按照“谁主管谁负责、谁使用谁负责”的原则，落实“分工负责、责任到人”的管理办法进行。

对于由于单位变更或不再使用的信息系统(网站)，请各单位联系人及时通知网络信息中心进行清理。如果存在以下情形的，网络信息中心有权立即停止、关闭其服务：信息系统(网站)到期或长期无人管理、网站已经停止提供对外服务或运营、

僵尸网站、没有定期到网络信息中心进行备案的。

(二) 集中分类分区管理

学校所有的网站原则上集中在网站群系统上进行集中管理。不对外提供服务的信息系统（网站），原则上限制在校园网内访问，校园网外确有需要，通过 VPN 特殊通道进行访问。

重要的信息系统（网站），网络信息中心划分重点区域进行重点安全防患，日常运维管理仍由原单位负责。

(三) 分级保护管理

对于学校网站、重要的信息系统，如办公、财务、人事等系统，网络信息中心按照国家有关管理规范、技术标准协助建设部门确定信息系统（网站）的安全保护等级。对新建、改建、扩建的信息系统，建设单位必须在规划、设计阶段确定信息系统的安全保护等级，做好相关建设预算，并同步建设符合该系统安全保护等级要求的信息安全设施。

(四) 建立数据安全的管理

1. 数据安全防护

信息系统使用部门，要积极采取切实有效的方法和手段，保证信息系统数据的安全，不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

2. 数据备份与异地容灾备份

信息系统建设部门应建立备份机制，对应用系统应用系统

定期进行数据备份。条件成熟时，构建全校性数据异地容灾备份。

在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施；数据要由专人管理和保存。

（五）专项漏洞扫描常态化

信息系统（网站）建设完成后，网络信息中心对全校已经备案的信息系统（网站）进行定期的漏洞、木马扫描，并将结果反馈给相关部门。对存在问题的信息系统（网站），要求整改，并限制其使用，待符合要求后方可上线。网络信息中心落实云防护措施，解决防攻击、防篡改、防木马等。

（六）建立网络安全值守与应急处理制度

1. 特殊时期，实行 7*24 小时值守制度

当班值守人员要向网络安全专员汇报值班情况，网络安全专员按时向上级主管部门汇报学校情况。

2. 应急处理制度

网络信息中心负责建立紧急情况下的应急处理机制，包括但不限于技术手段，甚至包括断网等。

（七）网络安全行为预防与分析管理

1. 建立网络安全运维检测体系

能及时对网络故障、网络流量异常等情况提前处理；对重要的服务器、虚拟机、重要的应用系统进行监控，及时发现问题，确保核心业务安全运行。

2. 建立敏感词汇检测系统，完善行为审计系统，挖掘与预判敏感词汇与安全问题。

3. 开展网络安全教育与培训

针对信息系统（网站）安全负责人、技术管理员，在一定范围内开展网络安全教育与培训。

4. 制定《广东财经大学网络信息安全管理办法》等相关制度。

五、组织保障与人员经费保障

（一）成立网络信息安全应急响应小组

组长由网络安全与信息化领导小组组长担任，组员由网络安全与信息化领导小组成员和信息系统（网站）安全负责人、技术管理员担任。

（二）建立健全网络安全责任制

各单位要守土有责、守土尽责，统一思想认识，切实增强网络安全的责任感与使命感。

（三）网络安全保障工作小组：网络信息中心有关人员。

（四）人员与经费保障

学校保障一定的定期安全检测费用，必要的软硬件投入费用以及一定的安全保障人员。

附件：信息系统（网站）安全管理的实施方案任务分解

附件

信息系统（网站）安全管理的实施方案任务分解

主要任务	内 容	负责单位	完成时间
一、开展信息系统（网站）、IP地址的全面清理	校园网内的网站	网络信息中心、校办牵头，其他各单位。	2017年10月15日
	校园网外的网站	各单位，若有发送到邮箱：XXB@gdufe.edu.cn	2017年10月27日
二、网站建设	（一）网站建设		
	1. 网站群系统平台的建设	网络信息中心	2017年10月15日
	2.1 网站内容的迁移（第一批）	网络信息中心	2017年10月20日
	2.1 网站内容的迁移（第二批）	网络信息中心	2018年6月1日
	2.2 网站内容的建设（注意内外有别）	各单位	2017年12月15日
	2.3 网站群平台的操作使用培训	各单位网站维护人	2017年10月26日
三、信息系统（网站）安全管理	（一）建立网站备案与退出		各单位 2017年10月15日
	（二）实行集中分类分区管理		
	1. 网站内外有别访问	网络信息中心、各单位	2018年1月20日
	2. 信息系统的VPN配置	网络信息中心、信息系统的建设单位	2018年5月1日
	（三）开展分级保护建设		网络信息中心、相关的7个建设单位 2018年1月20日
	（四）强化数据安全管理工作		
	1. 数据安全防护	信息系统使用部门	2017年12月15日
	2. 数据备份	信息系统使用部门	2017年12月15日
3. 数据异地容灾备份	资产与设备管理处、财务处、网络信息中心	2018年12月1日	

	(五) 实施常态化漏洞扫描	网络信息中心	2018年9月1日
	(六) 建立网络安全值守与应急处理制度	网络信息中心	2017年10月15日
	(七) 加强网络安全行为预防与分析管理		
	1. 建立网络安全运维检测体系	网络信息中心	2018年12月1日
	2. 敏感词汇检测系统	网络信息中心	2019年12月1日
	3. 行为审计系统	网络信息中心	
	4. 制定《广东财经大学信息安全管理办法》	网络信息中心	2017年11月1日

广东财经大学校长办公室 主动公开 2017年11月20日印发