南开大学文件

南发字〔2017〕12 号

关于印发《南开大学网站建设与管理规定》的通知

各学院、各单位、机关各部门：

《南开大学网站建设与管理规定》业经 2016 年 12 月 19 日第十五次校长办公会议审议通过，现印发你们，请遵照执行。

南开大学

2017 年 3 月 13 日

（此件主动公开）

南开大学网站建设与管理规定

第一章 总则

第一条 为充分发挥网络优势，加强我校网站的规范化建设与管理，根据《中华人民共和国网络安全法》、《信息系统安全等级保护基本要求》等法律法规和国家标准的规定，依照《教育部关于进一步加强直属高校直属单位信息技术安全工作的通知》、《关于进一步强化天津市高校校园网站信息安全管理及备案工作的通知》等上级文件精神，结合我校实际，制定本规定。

第二条 本规定中的网站是指在南开大学校园网上使用HTML等工具制作的用于展示特定内容相关网页的集合；对于采用B/S架构，通过网页实现其部分或全部功能的信息系统，同样适用于本规定。

第二章 机构及职能

第三条 南开大学网络安全和信息化领导小组是我校网站建设与管理的领导机构，负责审议和审批网站建设申请，并对网站建设与运维管理过程中发生的重大事件进行研究与决策。

第四条 信息化建设与管理办公室（以下简称“信息办”）是学校网站建设与管理的归口部门，具体工作内容包括：

（一）负责南开大学主页的日常管理与维护；

（二）审核所有接入校园网的网站建设申请；

（三）负责网站的信息安全等级保护工作，包括网站定级、备案、安全建设和整改、信息安全等级测评、信息安全检查等事项；

（四）定期对校园网进行安全评估，制定应急预案，根据风险等级采取相应的处置措施；

（五）定期开展网站年审工作，对学校网站信息进行备案，及时关停不再使用的网站。

第五条 学校各单位自行负责建设和管理本单位网站，并对本单位网站所发布的信息负责。

第六条 学校办公室和党委宣传部负责网站内容的监管工作。

第三章 网站建设

第七条 所有接入校园网的网站必须在向信息办提出书面申请（见附件 1），经学校网络安全和信息化领导小组批准后方可建立。

第八条 任何未经批准建立的网站，一经发现将立即予以关停，并追究相关人员责任。

第九条 南开大学主页由信息办负责向上级主管部门申请建立和备案，并负责日常管理和维护工作。主页各栏目内容由各单位负责提供。

第十条 各单位在网站建设完成后，须通知信息办进行网络安全评估，安全评估不合格的网站不得开放互联网访问。

第十一条 各单位应确定一名主管领导对网站建设和管理工作负责，并至少指定一名网络信息联络员负责具体工作，每个网站应指定至少一名管理员。主管领导、联络员和网站管理员名单须报学校办公室和信息办备案，并签订《网站建设与管理安全目标责任书》（见附件 2）。

第十二条 各单位应将网站建设作为一项重要工作纳入议事日程，为网站建设提供必要的支持，并将网站建设列入涉及人员的岗位职责，作为履岗考核的重要内容。

第十三条 网站服务器可由各单位自行购置，或采用向信息办申请虚拟主机的方式获得。自行购置服务器的单位可自行管理，也可采取主机托管的方式委托信息办进行管理，托管应按信息办规定办理相应手续。

第四章 信息发布

第十四条 网站信息发布实行统一管理、分级负责制。学校办公室和党委宣传部负责南开大学主页信息的审核与发布，信息办负责提供技术支持；各单位网站发布的信息由各单位自行审核。

第十五条 网站信息发布实行谁发布、谁负责的原则。各单位须建立规范的网站信息采集、审核和发布机制，明确人员

责任。

第十六条 网站发布的信息内容应真实准确，语义表述清晰、文字规范。

第十七条 南开大学主页各栏目的信息提供单位须准确、及时的向学校办公室提供信息，以确保主页信息内容的准确性和时效性。

第十八条 各单位网站应从对外宣传的实际出发，设计相应的栏目和内容，做到全面、真实、准确，并能实时反映本单位的情况和发展动态。动态内容如新闻、公告等栏目应及时更新。

第十九条 对网站中的互动性栏目，应加强内容监管，确保信息的健康与安全。实行发言预审制度，建立互动应用的接收、处理、反馈等工作机制。

第二十条 任何网站不得制作、复制、提供和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权、推翻社会主义制度的；

（三）煽动分裂国家、破坏国家统一的；

（四）涉及国家安全、国家秘密的；

（五）煽动民族仇恨、民族歧视，破坏民族团结的；

（六）捏造或歪曲事实，散布谣言，扰乱社会秩序的；

（七）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、

恐怖，教唆犯罪的；

（八）公然侮辱他人或者捏造事实诽谤他人的；

（九）损害学校形象和学校利益的；

（十）侵犯他人知识产权的；

（十一）其他违反宪法和法律法规的。

（十二）对于违反上述规定的网站，学校将予以关闭，并追究相关人员的责任。对于涉嫌触犯法律法规的，将移交司法机关处理。

第五章 运行维护

第二十一条 学校虚拟主机和网站群平台系统由信息办负责运行和维护，各单位自行购置的服务器（包括办理托管的）及自建的网站系统（包括运行在虚拟主机上的）由各单位自行管理和维护。

第二十二条 各单位应采取积极措施，保障网站系统 24 小时稳定运行并正常提供服务。

第二十三条 各单位网站须规范地址链接，如有变动，应及时报信息办备案。网站要进行改版、升级或变更运行模式等工作时，应报信息办审核，审核通过后方可实施。

第二十四条 各单位应针对网站安全建立相应的安全机制，安全机制应至少包括以下部分：

（一）定期备份机制：对网站重要数据、文件及应用系统

进行定期备份，特别重要的数据和文件还应进行异地备份；

（二）口令更新机制：网站后台管理及内容上传的登录口令应定期更新，口令的位数应不少于8位，口令的内容应混合使用字母数字等；

（三）应急响应机制：要充分考虑网站发生各种突发事件的可能性，制定应急响应预案，以最大限度的减少损失、控制影响；

（四）机房管理机制：网站机房应建立严格的门禁制度和日常管理制度，由专人负责管理，有值班和设备运行情况等记录；

（五）网站设备巡检机制：定期对网站服务器及相关网络设备进行检查，发现硬件故障要及时解决；

（六）系统安全检查机制：定期对系统进行安全性测评，发现安全隐患时应视风险等级判定是否关闭互联网访问，并立即开展相应的修复工作；及时对服务器系统进行补丁升级和版本更新，应安装防病毒和防火墙等安全软件，防止黑客入侵；

（七）安全事件报告及处理机制：网站发生安全突发事件后，除在第一时间组织人员进行处理外，还应立即向网络安全和信息化领导小组报告，以便获得及时的指导和必要的技术支持。

第六章 网站安全

第二十五条 实行网站安全、保密领导负责制，各单位党政一把手作为本单位网站安全、保密的责任主体，向学校网络安全和信息化领导小组负责,各网站管理员向单位一把手负责。

第二十六条 按照国家规定实行信息安全等级保护机制，对网站进行定级、备案、安全建设和整改、信息安全等级测评、信息安全检查等工作。

第二十七条 新建网站实行安全准入制，在接入互联网之前须由信息办对其进行安全评估，若评估结果为不合格，由网站建设单位负责进行漏洞修复并重新提交评估，直到评估合格后方可接入互联网。

第二十八条 由信息办定期对全校所有网站进行安全评估，并将评估结果通报各单位。信息办根据评估结果，对有轻度或中度安全问题的网站责令限期修复，超过修复期限未修复的停止其互联网访问；对有严重安全问题的网站在责令限期修复的同时直接停止其互联网访问，超过修复期限未修复的予以关闭。

第二十九条 实行网站年度审查制度，由信息办每年组织一次网站年度审查工作，更新所登记网站信息和人员信息，注销不再使用的网站，回收不再使用的虚拟机等资源，各单位应积极予以配合。

第三十条 一旦发生网站安全突发事件，信息办应立即根据《南开大学网络与信息安全类突发公共事件应急处置预案》

（见附件三）启动应急响应机制。

第三十一条 信息办定期举办网站管理和安全技术培训，对网站管理人员进行培训和考核。

第七章 监督管理

第三十二条 学校网络安全和信息化领导小组定期检查各单位信息采集报送、网站运行管理及更新维护情况，检查结果在校内予以通报。

第三十三条 信息办会同网络安全和信息化领导小组其他成员单位，不定期开展网站测评工作，对优秀网站进行表彰奖励，对存在问题的网站，责令限期整改。对未能按期整改，或拒不执行整改意见的单位，取消单位和涉及人员各种年度评优资格。

第九章 附则

第三十四条 本规定由南开大学信息化建设与管理办公室负责解释。

第三十五条 本规定自发布之日起施行。

附件：1.《南开大学新建网站申请表》

2.《南开大学网站建设与管理安全目标责任书》

3.《南开大学网络与信息安全类突发公共事件应急

处置预案》

附件 1

南开大学新建网站申请表

单位名称（盖章）：　　申请日期：

所属部门			
网站名称			
网站域名		使用反向代理	□是 □否
IP 地址			
可访问范围	□校园网访问 □互联网访问		
服务器存放地			
网站用途			
	主管领导	网站管理员	
姓名			
门户账号			
办公电话			
移动电话			
电子邮箱			
备注信息			

负责人（签字）：　　填表人：

附件 2

南开大学网站建设与管理安全目标责任书

为进一步加强网络信息技术安全防范和监督，实现校内网站的规范、统一、有序管理，根据《南开大学网站建设与管理规定》，订立本责任书。

一、责任对象

凡经学校网络安全和信息化领导小组批准，在南开大学校园网上建立网站的各单位为责任单位，单位主管领导是本单位网站建设与安全管理的第一责任人，对本单位建立的网站信息安全管理负全面责任，网站管理员是网站建设与安全管理的直接责任人。

二、责任内容

1.严格遵守国家有关计算机信息系统和网络安全管理的有关法律、法规，认真贯彻执行《南开大学网站建设与管理规定》。

2.加强本单位网络建设和管理安全工作的组织领导，做好网络信息资源管理，完成网站日常技术维护和内容更新。单位发生人事变动时应及时调整人员职责，避免出现责任真空，确保工作不受影响。

3.做好网站域名管理，对于使用南开大学二级域名的，严禁私自指向校园网之外的服务器，有极特殊需要的，须由单位

主管领导签署安全承诺书，经信息办提交学校网络安全和信息化领导小组批准后方可实施。

4.定期对本单位网站系统及服务器进行漏洞修补、程序升级、查杀病毒等维护工作，防止病毒程序存在或传播，确保校园网络信息安全。

5.网站发布的信息内容必须健康向上，符合国家法律、法规和学校规定，网站引用的数据、表述须与学校网站保持一致。严禁发布商业广告。

6.在网站建设和管理过程中出现下列情况的，将根据《南开大学网站建设与管理规定》追究相关人员责任。涉嫌触犯国家法律、法规的，移交司法部门处理。

（1）因疏于维护或维护不当，损害校园网络信息安全的；

（2）因监管不严，出现有害信息后未及时删除，导致有害信息蔓延，造成学校形象受损或影响学校安全稳定的；

（3）因审核不严，发布涉及国家秘密或敏感信息的；

（4)各单位网站出现上述问题后,相关责任人隐瞒不报的。

7.认真完成学校部署的有关网络信息安全管理的其他工作。

责任单位：（盖章）

第一责任人（签字）：

附件 3

南开大学网络与信息安全类突发公共事件应急处置预案

为加强南开大学信息技术安全工作，及时掌握和处置信息技术安全事件，协调相关力量做好应急响应处理，降低安全事件带来的损失与影响，维护正常工作秩序和营造健康的网络环境，根据国家有关法律法规，以及标准文件，结合我校实际情况，制定本预案。

第一条 信息技术安全事件定义。根据《信息安全事件分类分级指南》（GB/T 20986-2007，以下简称《指南》），本流程中所称的信息技术安全事件（以下简称安全事件）是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件。

第二条 适用范围。本预案适用于在南开大学发生的网络与信息安全类事件的报告与处置工作。涉及信息内容安全事件的报告与处置工作需按信息内容安全相关规定执行。

第三条 安全事件等级划分。根据《指南》并结合我校实际情况，将安全事件划分为四个等级。

（一）特别重大事件（I 级）

信息系统发生大规模瘫痪，信息泄漏或损坏，事态发展超

出管理单位的控制范围，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的突发公共事件，超过24小时不能恢复。

（二）重大事件（Ⅱ级）

业务系统发生较大规模瘫痪，信息泄漏或损坏，对国家安全、社会秩序、经济建设和公共利益造成严重损害，超过12小时未能恢复，需要跨部门协同处置的突发公共事件。

（三）较大事件（Ⅲ级）

业务系统发生瘫痪，信息泄漏或损坏，对国家安全、社会秩序、经济建设和公共利益造成一定损害，但在8小时内可以恢复，不需要跨部门协同处置的突发公共事件。

（四）一般事件（Ⅳ级）

业务系统部分瘫痪，信息泄漏或损坏，对系统用户的权益有一定影响，但在4小时内可以恢复，不危害国家安全、社会秩序、经济建设和公共利益的突发公共事件。

第四条 安全事件自主判定。一旦发生安全事件，应根据第三条所述，视信息系统重要程度、损失情况以及对工作和社会造成的影响自主判定安全事件等级。

第五条 Ⅰ至Ⅲ级安全事件的报告与处置。报告与处置分为三个步骤：事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置。

（一）事发紧急报告与处置

1. 网络与信息系统运维操作人员一旦发现上述安全事件，应根据实际情况第一时间采取有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位主管领导和网络信息联络员。

2. 上述人员接到报告后，应立即组织技术人员赶赴现场进行紧急处置，并将相关情况通报至信息化建设与管理办公室（以下简称“信息办”）。涉及人为主观破坏事件应同时报告学校保卫处。

3. 信息办接到报告后，负责组织技术人员协同报告单位人员进行应急处置。同时，应进一步判定安全事件等级，对确认属Ⅰ至Ⅲ级安全事件的，应报告学校网络安全和信息化领导小组（办公室设在党委宣传部），由其负责向上级报告。

4. 紧急报告内容包括：（1）时间地点；（2）简要经过；（3）事件类型与分级；（4）影响范围；（5）危害程度；（6）初步原因分析；（7）已采取的应急措施。

5. 信息办应及时跟进事件发展情况，出现新的重大情况应及时补报。

（二）事中情况报告与处置

1. 事中情况报告应在安全事件发现后 6 小时内以书面报告的形式进行报送，报送内容和格式见附表 1。

2. 事中情况报告由事件发生单位组织相关人员和运维单位共同填写，由单位主管领导审核后，签字并加盖公章报送信息

办和党委宣传部。

3. 安全事件的事中处置包括：及时掌握损失情况、查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为主观破坏的安全事件应积极配合保卫处和公安部门开展调查。

（三）事后整改报告与处置

1.事后整改报告应在安全事件处置完毕后5个工作日内以书面报告的形式进行报送，报送内容和格式见附表2。

2.事后情况报告由事件发生单位组织相关人员和运维单位共同填写，由单位主管领导审核后，签字并加盖公章报送信息办和党委宣传部。

3. 安全事件事后处置包括：进一步总结事件教训，研判安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力。如涉及人为主观破坏的安全事件应继续配合保卫处和公安部门开展调查。

第六条 一般安全事件报告与处置。各单位发生一般安全事件，应及时、自主组织应急处置工作，在事件处置完毕后 7 天内将整改报告保送信息办和党委宣传部，报告内容和格式见附表2。

第七条 安全事件参考处置方案。当发生网络与信息安全事件时，首先应区分事件性质，然后再根据不同情况分别进行处置。

（一）根据事件性质，网络与信息安全事件可划分为三类

1. 自然灾害。指地震、雷电、火灾、洪水等灾害引起的计算机网络与信息系统的损坏。

2. 事故损毁。指电力中断、网络损坏或是软件、硬件设备故障等引起的计算机网络与信息系统的损坏。

3. 人为破坏。指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的计算机网络与信息系统的损坏。

（二）针对上述事件的处置办法

1. 属自然灾害类事件时，应根据实际情况，在保障人身安全的前提下，首先保障数据安全，然后再保障设备安全（包括硬盘拔出与保存、设备断电与拆卸、搬迁设备等）。

2. 属事故损毁类事件时，应迅速分析故障特征，查明原因，若事件发生单位不能独立处理，必须立刻通知相关单位（供电局、网络运营商、软硬件产品维护单位等），马上组织人员进行系统修复。

（1）外电中断处置。外电中断后，立即切换到备用电源；迅速查明断电原因，如因内部线路故障，马上组织恢复；如因供电部门原因，立即与供电单位联系，尽快恢复供电；如被告知将长时间停电，应做好以下工作：（a）预计停电 1 小时以内的，由 UPS 供电；（b）预计停电 1-4 小时的，关掉非关键设备，确保各主机、路由器、交换机供电；（c）预计停电超过 4 小时的，做好数据备份工作，及时关闭有关设备。

（2）机房火灾处置。一旦机房发生火灾：首先切断所有电源，按响火警警报；其次，检查自动喷淋系统是否启动，并使用灭火器进行灭火；最后，如果需要，应通过 119 电话向公安消防部门请求支援。

（3）网络线路中断处置。网络线路中断后：首先，应迅速判断故障节点，查明原因、尽快修复。如属网络运营商负责维护运营的线路，立即与运行商维护部门联系，及时进行修复。如属局域网内部线路故障，应立即判断故障节点，查明故障原因，迅速组织修复；如属路由器、交换机等网络设备故障，立即与设备供应商联系修复；如属路由器、交换机配置文件破坏，迅速按照要求重新配置；其次，如遇本地技术无法解决的技术问题，应立即向厂商请求支援。

（4）设备故障处置。发现服务器等关键设备损坏，应立即查明设备故障原因；能自行恢复的，立即用备件替换受损部件；难以自行恢复的，立即与设备供应商联系，请求派维修人员前来维修；若设备一时不能修复，应及时采取必要措施，并发布通知告知有关单位暂缓上传、上报数据。

3. 属人为破坏类事件时，应首先判断破坏来源与性质，然后断开影响安全的网络设备，断开与破坏来源的网络连接，跟踪并锁定破坏来源 IP 地址或其它用户信息，修复被破坏的信息，恢复信息系统。

（1）有害信息处置。首先，尽快采取屏蔽、删除等有效措

施对有害信息进行清理，并做好相关记录；其次，指派专人对存在问题的网站、网页及邮件信息等进行全时监控；再次，采取技术手段追查有害信息来源；最后，如发现涉及国家安全、稳定的重大有害信息，还要及时向保卫处或公安局网警支队报告。

（2）黑客攻击处置。当发现网页内容被篡改或通过入侵检测系统发现黑客攻击时：首先,将被攻击服务器等设备从网络中隔离；其次，组织相关人员对事件进行安全评估，评估破坏程度，并视其严重程度对事件进行定级并上报相关部门；再次，采取技术手段追查非法攻击来源；最后，恢复或重建被破坏的系统。

（3）病毒侵入处置。当发现计算机系统感染病毒后：首先，立即将该计算机从网络上物理隔离，同时备份硬盘数据；其次，启用防病毒软件进行杀毒处理，并使用病毒检测软件对其他机器进行病毒扫描和清除；再次，一时无法查杀的新病毒，要迅速与相关病毒软件供应商联系解决；最后，如感染病毒的是服务器或主机系统，要立即告知使用部门并做好相应清查工作。

（4）数据库安全防范处置。一旦发生数据库崩溃：首先，应关停服务，立即通知有关单位暂缓上传、上报数据；其次，组织技术人员对主机系统进行维修；再次，如遇本地技术人员无法解决的问题，应立即请求软硬件供应商协助解决；最后，系统修复启动后，将最新的备份数据恢复到数据库中。

第八条 相关配套机制。各单位应根据实际建立本单位值守制度，做到安全事件早发现、早报告、早控制、早解决。各单位应建立健全本单位安全事件应急处置机制，制定安全事件应急预案，定期组织应急演练。

第九条 问责制度。各单位应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，将对责任人员进行约谈，对单位予以通报，必要时给予进一步处罚。

附表：1.信息技术安全事件情况报告

2.信息技术安全事件整改报告

附表 1

南开大学信息技术安全事件情况报告

单位名称：（需加盖公章）　事发时间：_____年___月__日__分

<table>
<tr><td rowspan="2">联系人姓名</td><td rowspan="2"></td><td>手机</td><td></td></tr>
<tr><td>电子邮箱</td><td></td></tr>
<tr><td>事件分类</td><td colspan="3">□ 有害程序事件　□ 网络攻击事件
□ 信息破坏事件　□ 设备设施故障
□ 灾害事件　　□其他_____</td></tr>
<tr><td>事件分级</td><td colspan="3">□Ⅰ级　□Ⅱ级　□Ⅲ级　□Ⅳ级</td></tr>
<tr><td>事件概况</td><td colspan="3"></td></tr>
<tr><td>信息系统的基本情况（如涉及请填写）</td><td colspan="3">1. 系统名称：_____
2. 系统网址和 IP 地址：_____
3. 系统主管单位/部门：_____
4. 系统运维单位/部门：_____
5. 系统使用单位/部门：_____
6. 系统主要用途：_____
_____
7. 是否定级 □是　□否，所定级别：_____
8. 是否备案 □是　□否，备案号：_____
9. 是否测评 □是　□否
10. 是否整改 □是　□否</td></tr>
</table>

事件发现与处置的简要经过	
事件初步估计的危害和影响	
事件原因的初步分析	
已采取的应急措施	
是否需要应急支援及需支援事项	
信息联络员意见 （签字）	
主管领导意见 （签字）	

附表 2

南开大学信息技术安全事件整改报告

单位名称：（需加盖公章）　　报告时间：_____年___月__日

联系人姓名		手机	
		电子邮件	
事件分类	□ 有害程序事件　□ 网络攻击事件 □ 信息破坏事件　□ 设备设施故障 □ 灾害事件　　□其他_____		
事件分级	□Ⅰ级　□Ⅱ级　□Ⅲ级　□Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.系统网址和 IP 地址：_____ 3.系统主管单位/部门：_____ 4.系统运维单位/部门：_____ 5.系统使用单位/部门：_____ 6.系统主要用途：_____ _____ 7.是否定级 □是　□否，所定级别：_____ 8.是否备案 □是　□否，备案号：_____ 9.是否测评 □是　□否 10.是否整改 □是　□否		

事件发生的最终判定原因（可加页附文字、图片以及其他文件）	
事件的影响与恢复情况	
事件的安全整改措施	
存在问题及建议	
信息联络员意见（签字）	
主管领导意见（签字）	

南开大学办公室　　2017 年 3 月 14 日印发