中 南 大 学 文 件

中大信字〔2016〕5 号

关于印发《中南大学网站与信息系统安全事件报告及处置办法》的通知

各二级单位:

《中南大学网站与信息系统安全事件报告及处置办法》已经 2016 年 7 月 14 日第十六次校务会议讨论通过，现印发给你们，请认真遵照执行。

中南大学

2016 年 8 月 24 日

中南大学网站与信息系统安全事件报告及处置办法

（2016 年 7 月 14 日第十六次校务会议讨论通过）

为加强中南大学网络与信息安全工作，根据教育部《进一步加强直属高校直属单位信息技术安全工作的通知》（教技〔2015〕1 号）、《信息技术安全事件报告与处置流程》（教技厅函〔2014〕75 号）以及《中南大学网络与信息安全管理办法》（中大信字〔2014〕2 号）精神，结合学校实际，制定本办法。

第一章　总　则

第一条　本办法中所指的网站与信息系统安全事件（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、系统攻击事件、信息破坏事件和其他信息安全事件。

第二条　本办法适用于我校各单位、各部门发生的安全事件的报告及处置工作，学校附属医院及其他具有法人资格的机构，参照本办法执行。

第三条　中南大学网络与信息安全领导小组是安全事件报告及处置的领导机构。学校信息与网络中心负责安全事件报告及处置的日常工作。涉及信息内容安全事件的报告及处置归口学校宣传部；涉嫌违法犯罪的安全事件的报告及处置归口学校保卫处，保卫处应协助公安机关做好相关取证和处置工作。

第二章　安全事件的责任主体、等级划分与判定

第四条　按照“谁主管谁负责，谁审核谁负责，谁使用谁

负责，谁发布谁负责”的原则，学校各单位、各部门为安全事件的责任主体，各单位、各部门主要负责人为安全事件的责任人。

第五条　安全事件划分为四个等级:特别重大事件(Ⅰ级)、重大事件（Ⅱ级)、较大事件（Ⅲ级）和一般事件（Ⅳ级)。详见附件 1。

第六条　根据网站与信息系统的重要程度、损失情况、对工作和社会造成的影响,按照附件 1 对安全事件进行分类标准。安全事件责任单位负责安全事件等级的初步判定，信息与网络中心负责进行确认，必要时报告学校网络与信息安全领导小组做出最终判定。

第三章　安全事件的处置与整改

第七条　各单位、各部门安全事件责任人负责组织本单位安全事件的报告和处置。安全事件责任单位的网络与信息系统运维操作人员一旦发现安全事件时，应根据实际情况第一时间赶赴现场，采取断网等有效技术措施进行紧急处置，将损害和影响降到最小范围；同时保留现场，以口头通讯的方式报告本单位安全事件责任人和学校信息与网络中心。信息与网络中心在技术上协助责任单位进行安全事件的处置。涉及信息内容的安全事件应同时报告学校宣传部，涉嫌违法犯罪的安全事件应同时报告学校保卫处。

第八条　责任单位应在安全事件发生后 4 个工作日内向信息与网络中心报送整改报告（报送内容和格式见附件 2）。

报告需经本单位主要负责人审核签字，并加盖单位公章。发生安全事件后，责任单位应当认真做好整改落实工作，坚持

做到安全事件原因不查清不放过、整改措施未落实不放过、责任人员未受到教育或处理不放过，努力杜绝类似安全事件的再次发生。

第九条　出现以下情形，信息与网络中心应当采取必要的技术措施，中止网站或信息系统的网络接入服务:

1.未在信息与网络中心登记、备案，未参加年度审核、及时更新联系信息的网站和信息系统;

2.未通过信息与网络中心漏洞扫描和安全检查，擅自发布上网的网站或对外提供服务的信息系统;

3.未按照本处置流程的要求进行安全事件报告和处置的网站和信息系统;

安全事件处置完毕后，信息与网络中心视安全事件责任单位整改情况，决定是否恢复网络接入服务。

第十条　各单位、各部门应当严格按照要求完成上级单位以及学校安排的预防、预警类网络与信息安全工作。

第四章　配套机制与问责

第十一条　安全事件处置的相关经费纳入学校信息化建设总体预算。

第十二条　各单位、各部门应完善相关配套制度，进一步畅通信息报送渠道，相关分管领导、联络员等发生变更的，应及时向信息与网络中心备案；进一步建立本单位的网络与信息安全值守制度，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，做到安全事件早预警、早发现、早报告、早控制、早解决。

第十三条　各单位、各部门应按照本办法及时、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，学校将根据《中南大学网络与信息安全管理办法》等进行问责处理。

第五章　附　则

第十四条　本办法由中南大学网络与信息安全领导小组负责解释，自发布之日起施行。

附件：1.网站与信息系统安全事件分类与等级划分

2.中南大学网站和信息系统安全事件整改报告

附件 1

网站与信息系统安全事件分类与等级划分

根据《信息安全事件分类分级指南》(GB/Z 20986-2007),结合网站与信息系统安全事件的特点，将网站与信息系统安全事件分为有害程序事件、系统攻击事件、信息破坏事件和其他信息安全事件 4 个基本分类，每个基本分类分别包括若干个子类；根据网站与信息系统的重要程度、系统损失和社会影响，将网站与信息系统安全事件划分为 4 个等级。

一、网站与信息系统安全事件分类

1.有害程序事件

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、网页内嵌恶意代码事件和其它有害程序事件等。

2.系统攻击事件

系统攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。信息系统攻击事件包括后门攻击事件、漏洞攻击事件、干扰事件和其他系统攻击事件等。

3.信息破坏事件

信息破坏事件是指通过网络或其他技术手段，造成信息

系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件等。

4.其他事件

其他事件是指不能归为以上基本分类的网站和信息系统安全事件。

二、网站与信息系统安全事件等级划分

1.特别重大事件（Ⅰ级）

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况:

（1）会使特别重要信息系统遭受特别严重的系统损失;

（2）产生特别重大的社会影响。

2.重大事件（Ⅱ级）

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况:

（1）会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失;

（2）产生重大的社会影响。

3.较大事件（Ⅲ级）

较大事件是指能够导致较严重影响或破坏的信息安全事件，包括以下情况:

（1）会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失;

（2）产生较大的社会影响。

4.一般事件（IV级）

一般事件是指不满足以上条件的信息安全事件，包括以下情况:

（1）会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失;

（2）产生一般的社会影响。

附件 2

中南大学网站与信息系统安全事件整改报告

单位名称:　　（公章）　事发时间:　　年　月　日　分

联系人 姓　名		移动电话	
		电子邮箱	
事件分类	☐ 有害程序事件　☐ 系统攻击事件 ☐ 信息破坏事件　☐ 其他		
事件分级	☐ I 级　☐ II 级　☐III级　☐IV级		
事件概况	（包括：1. 网站或信息系统所在的地点、名称及主要用途；2. 网址和 IP 地址、MAC 地址；3. 安全事件发生的原因、处理经过及整改措施。可加页附文字、图片以及其他补充说明）		

造成的危害和影响	
信息化工作分管领导意见	签名：　　年　　月　　日
单位主要负责人意　见	签名：　　年　　月　　日

抄送：各二级党组织、党群部门。

中南大学办公室　　主动公开　　2016 年 8 月 24 日印发