中共中央民族大学委员会文件

民大党发〔2018〕21号

关于印发《中央民族大学网络安全工作责任制实施细则》（试行）的通知

各二级单位党委、党总支，学校各单位、各部门：

《中央民族大学网络安全工作责任制实施细则》（试行）已经学校党委常委会议审议通过，现印发给你们，请遵照执行。

特此通知。

中共中央民族大学委员会

2018年3月15日

中央民族大学网络安全工作责任制实施细则

（试行）

第一条 为了贯彻落实中共中央办公厅关于《党委（党组）网络安全工作责任制实施办法》（厅字〔2017〕32 号），进一步加强学校网络安全工作，明确和落实各级领导干部和各二级单位（含各单位、各部门、院、系、所和中心）（以下简称“各单位”）网络安全责任，保证学校信息化健康持续发展，根据《中华人民共和国网络安全法》、《中央民族大学安全稳定事故责任倒查暂行规定》、《中央民族大学网络与信息安全管理办法》等有关法律和规定，制定本细则。

第二条 网络安全工作关系到学校的安全稳定和广大师生的切身利益，关系到学校教学、科研和管理等各项工作的稳定运行，关系到学校信息化建设健康、持续发展，具有十分重要的战略意义。各单位应全面提高对网络安全重要性认识和安全防范意识，要按照国家对网络安全工作的总体要求和建设“双一流”大学对学校信息化工作的特殊需要，以及当前网络安全面临的严峻形势，切实把网络安全工作作为日常工作的一项重要内容。

第三条 责任划分

（一）学校党政一把手是学校网络安全工作的主要负责人，对学校网络安全工作负总的领导责任，同时负有组织、管理、监督、检查、奖惩的权力和责任。

（二）学校党政副职是学校网络安全工作的直接责任人，分管网络安全与信息化工作的学校党政副职对学校总体网络安全工作负有直接领导责任，学校其他党政副职对其管辖部门和分管工作的网络安全负有领导责任。

（三）信息化建设管理处是学校网络安全工作的主管部门，对学校网络安全工作负指导监管责任。

（四）学校各单位负责本单位各类自建网络信息系统的安全，各单位的主要负责人是本单位网络安全工作的主要责任人，负责本单位的网络安全工作，其分管网络安全的领导对本单位网络安全工作负有直接管理责任。

（五）学校校园网用户在校期间因不遵守相关规定，造成网络安全事故的，本人负有全部责任。

第四条 责任人处理方式

违反本规定的责任人，按照干部管理条例和学校其他有关规定，由学校根据事件责任事故情节轻重，给予当事人从通报批评直至撤职的行政处分；构成违法犯罪的由司法机关依法追究刑事责任。

第五条 责任追究范围

在校园内发生下列网络安全事件，学校将根据有关法律、法规和本规定对有失职、渎职情况或负有领导责任的相关责任人追究行政责任：

（一）学校门户网站、新闻网、其他重点网站及重要信息系

统被攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；

（二）学校门户网站、新闻网、其他重点网站及重要信息系统受到攻击后没有及时组织处置，且瘫痪6小时以上的；

（三）发生学校秘密泄露、大面积个人信息泄露或者大量教学、科研、行政等基础数据泄露的；

（四）关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响学校师生工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；

（五）封锁、瞒报网络安全事件情况，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的；

（六）阻碍公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的；

（七）发生其他严重危害网络安全行为的。

第六条 学校依照有关法律、法规，履行下列职责：

（一）建立网络安全责任制检查考核制度，完善健全考核机制，明确考核内容、方法、程序，并将考核结果作为对领导班子和有关领导干部综合考核评价的重要内容；

（二）组织各单位对容易发生网络安全事件的网站、信息系统、网络设备等进行定期巡查和检测；

（三）指导和要求各单位制定网络安全事件的应急处理预案，

应急处理预案经主要领导签署后，报信息化建设管理处备案；

（四）信息化建设管理处和有关部门对本规定第五条所列的各类网络安全事件的隐患进行查处，发现重大网络安全隐患的，责令立即整改，无法整改或在整改过程中无法保证安全的，可以责令暂时停止使用，并上报学校主要领导；发现一般网络安全隐患的，责令本单位限期整改，以排除安全隐患；

（五）网络安全事件发生后，信息化建设管理处值班人员立即进行应急处置，并报信息化建设管理处领导和相关单位责任人。相关单位负责人应当立即组织应急处理工作，并迅速上报学校，学校按规定报国家民委、教育部、北京市公安局内保局、北京市委教育工委等上级单位。学校要协助有关部门按照国家有关规定调查处理在我校发生的网络安全事件，必要时可以对网络安全事件的有关责任人员做出处理决定。

第七条 信息化建设管理处和有关部门在职责范围内，依照国家有关法律、法规和学校的规章制度，进行网络安全日常监控、业务指导、预防各类网络安全事件的发生，并履行下列职责：

（一）宣传、贯彻、落实国家和上级有关部门关于网络安全的各项工作要求和预防发生各类网络安全事件的有关规定，研究、部署维护学校网络安全工作措施和防范各类网络安全事件的预防措施；

（二）定期组织开展网络安全检查，及时发现网络安全隐患，协助相关责任单位及时采取措施进行排查和整改，若发现重大网

络安全隐患应责令有关单位暂时关闭存有隐患的网站、信息系统或网络设备，待隐患排除后方可继续开放使用；

（三）网络安全事件发生后，要参加学校组织的调查处理工作组，并及时上报公安等有关安全管理部门，取得其指导和帮助，及时处理已发生的安全事件。

第八条 任何部门和个人对已发生的网络安全事件不得隐瞒不报、谎报、拖延报告或阻碍、干涉事件调查。若发生此类情况，学校将对有关单位责任人，根据情节轻重，给予相应的行政处分。

第九条 本细则自公布之日起施行。

中央民族大学党委办公室　　2018年3月20日印发