大连海事大学文件

连海大校发〔2019〕404号

大连海事大学关于印发《大连海事大学网络安全事件应急预案》的通知

各单位（部门）：

《大连海事大学网络安全事件应急预案》已经2019年第26次党委常委会会议审议通过，现予以印发，请遵照执行。

特此通知。

大连海事大学

2019年9月23日

大连海事大学网络安全事件应急预案

第一章 总则

第一条 为提高预防、处理网络安全事件的能力和水平，形成快速高效、科学有序的应急工作机制，有效预防网络安全事件的发生，最大限度地消除网络安全事件的危害和影响，依据相关法律法规要求，结合学校实际，特制定本预案。

第二条 按照“谁主管谁负责，谁运行谁负责”的原则，建立和完善网络安全事件应急工作机制，分工负责、快速反应，联动处置。

第二章 组织机构及职责

第三条 学校网络安全事件应急处置工作由学校网络安全与信息化委员会（以下简称网信委）统一决策和指导。网信委统筹协调组织网络安全事件应对，建立健全跨部门联动处置机制，指挥重大网络安全事件应急处置。

第四条 学校网络安全和信息化委员会办公室（以下简称网信办）是网络安全事件应急处置的执行机构，负责网络安全事件的定级判定，具体组织协调网络安全事件应急处置。

第五条 网络信息与综合服务中心（以下简称网服中心）负责网络安全事件的应急处置的技术支持，网络安全态势监测和预警，配合上级部门完成应急处置要求。宣传部负责网络安全事件中媒体应对、舆情处置，消除不良影响。保卫处负责网络安全事件中涉及违法犯罪情况的处置，配合公安部门开展调查。

第三章 事件分类分级

第六条 网络安全事件是指学校范围内由于自然或者人力以及软硬件本身缺陷或故障的原因，影响到所属网络和信息系统的正常运行，出现业务中断、系统瘫痪、数据破坏、信息失窃或泄密等，从而对社会造成不良影响以及造成一定程度间接或直接经济损失的事件。

第七条 根据网络安全事件的起因、表现、结果等，网络安全事件主要分为七类。

(一) 有害程序事件：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网络安全事件。主要包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等。

(二) 网络攻击事件：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网络

安全事件。主要包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等。

(三) 信息破坏事件: 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、窃取等而导致的网络安全事件。主要包括信息篡改事件、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。

(四) 信息内容安全事件: 利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的网络安全事件. 主要包括违反宪法和法律、行政法规的网络安全事件; 针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的网络安全事件; 组织串连、煽动集会游行的网络安全事件; 其他信息内容安全事件等。

(五) 设备设施故障: 由于信息系统自身故障或外围设施故障而导致的网络安全事件,以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的网络安全事件。主要包括软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障等。

(六) 灾害性事件: 由于不可抗力对信息系统造成物理破坏而导致的网络安全事件。主要包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的网络安全事件。

(七) 其他网络安全事件: 不能归为以上六类的网络安全事件。

第八条 网络安全事件的分级，根据对国家、社会、学校和师

生利益造成的影响情况，分为两级。

(一) 重大网络安全事件: 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成重大威胁的网络安全事件;个人信息和重要数据大量丢失,对国家安全、社会秩序、学校发展和师生利益构成重大影响的网络安全事件。

(二) 一般网络安全事件: 对学校发展和师生利益构成一定影响的网络安全事件。

第四章 判定与处置流程

第九条 发生网络安全事件后，各单位（部门）按照应急处置方式处理，并报告网信办。网信办判定安全事件的等级和类别，启动相应处置流程。

第十条 重大网络安全事件的处置流程分为事件的应急处置、事中处置、事后处置。

（一）应急处置: 各单位（部门）发生、发现网络安全事件后，第一时间采取应急措施，并报告网信办。经判定属于重大网络安全事件，网信办 2 小时内电话报告上级主管部门。

（二）事中处置: 迅速查找和分析原因，掌握损失情况，采取措施，降低影响。网信办 24 小时内书面报告上级主管部门。

（三）事后处置: 完成整改后，网信办组织调查原因、处置过程和损失状况，总结经验教训，进行责任认定，形成书面材料。网

服中心组织力量，评估安全风险，提升安全防护能力。网信办5个工作日内将整改情况报告上级主管部门。

第十一条 重大网络安全事件报告上级主管部门包括:交通运输部、辽宁省教育厅、大连市公安局、大连市网信办。

第十二条 一般网络安全事件发生后，相关部门报告网信办，并组织处置。在事件处置完毕后 3 个工作日内向网信办报送整改报告。

第十三条 根据事件分类采取不同应急处置方式。

（一）网络攻击和有害程序事件：根据攻击的来源与性质，关闭影响安全的网络设备(或端口)，断开网站与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址，记录相关信息。

（二）信息破坏和信息内容安全事件：发现校内网站出现不良信息后，应立即屏蔽该网站的网络端口或断开网络连接，阻止有害信息传播。具体处置流程，按照网络意识形态应急处置有关规定执行。

（三）设备故障事件：判断故障发生点和故障原因，迅速联系技术支撑单位尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（四）灾害性事件：根据实际情况，依次保证人员安全、关键数据安全、关键设备安全和一般设备安全。

（五）其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理。

第五章 附则

第十四条 未经网信办批准，任何单位（部门）和个人不得擅自发布网络安全事件相关信息。

第十五条 涉密网络安全事件应急处置工作按照保密管理有关规定执行。

第十六条 本预案由网信办负责解释。

第十七条 本办法自 2019 年 9 月 25 日起施行。

大连海事大学网络信息与综合服务中心　　2019年9月23日印发