大连海事大学文件

连海大校发〔2022〕293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2022年第42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

2022年12月1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 为提高预防和处理网络安全事件的能力,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，降低网络安全事件的危害和影响,依据相关法律法规及标准文件，结合学校实际，制定本预案。

第二条 各单位按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”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。

第三条 本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。本预案适用于校园网络安全事件的应对工作，其中有关信息内容安全事件的应对，参照学校相关预案。

第四条 网络安全事件分为七类四级，具体标准按照《国家网络安全事件应急预案》执行。

第二章 组织机构及职责

第五条 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。

第六条 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等级判定，组织应急处置。

第七条 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。党委宣传部负责网络安全事件中媒体应对、舆情处置。保卫处负责网络安全事件中涉及违法犯罪情况的处置。

第八条 各单位信息化负责人和信息安全员负责组织本单位的应急处置工作，制定针对本部门的应急预案，落实到具体责任人和操作步骤，定期组织应急演练。重大活动保障期间建立值守制度，保持联络人员手机电话通畅。

各单位应该按照流程及时、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，将对相关单位进行约谈或通报。

第三章 事件判定与处置流程

第九条 发生网络安全事件后,网信办组织判定安全事件的等级和类别，启动相应处置流程。

第十条 较大及以上等级网络安全事件的处置流程。

（一） 事发紧急报告与应急处置：

1.各单位发现网络安全事件后，第一时间报告网信办。网服中心实施“一分钟”断网等有效措施进行处置，保留现场并报告学校领导。网信办2小时内电话报告上级主管部门，如涉及人为主观破坏情形应同时报告当地公安机关。

2.网服中心组织技术人员进行处置。保留6个月以上的运行日志，截图或拍照主机受侵害状况，查明并记录原因。如涉及人为主观破坏事件，应保护现场，静待公安机关等部门到场处理。

3.紧急报告内容包括：事件地点、简述经过、事件类型与分级、影响范围、危害程度、初步原因、已采取的应急措施。

（二） 处置整改及情况报告

1.处置整改包括:及时掌握损失情况、查找和分析事件原因，修复系统漏洞，加固安全措施，恢复系统服务，尽可能减少安全事件对正常工作的影响。进一步总结事件教训，分析研判安全现状、排查安全隐患，完善管理制度，提升安全防护能力。如果涉及人为主观破坏的安全事件应积极配合公安部门开展调查。

2.网信办组织网服中心、校内主管单位、运维单位共同编写情况报告，报网信办负责人和主管校领导审核后，24小时内报送上级主管部门。

上级主管部门包括但不限于:交通运输部、辽宁省教育厅、大连市网信办、大连市公安局。

第十一条 一般网络安全事件报告和处置。

发生一般安全事件后，应及时、自主组织应急处置工作，在事件处置完毕后7天内提交报告到网信办。

第十二条 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。

（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。

第四章 附 则

第十三条 未经网信办批准,任何单位和个人不得擅自发布网络安全事件相关信息。

第十四条 本预案由网信办负责解释。

第十五条 本办法自2021年12月1日起施行，原《大连海事大学网络安全事件应急预案（连海大校发〔2019〕404号）》同时废止。

附件

典型安全事件应急处置流程

一、网页被篡改事件应急处置流程

1.管理员执行断网、关闭网站等措施。

2.电话上报网信办，组织技术人员进行排查和分析，妥善保存日志等相关信息，追查攻击路径来源，提取相关数据样本，清理网站非法信息，彻查系统漏洞、病毒、木马后门等威胁，确保隐患排除后恢复系统。

3.2小时内，网信办完成对事件进行定性，确定类别和等级，向主管校领导、属地网警支队和交通运输部科技司电话汇报。

4.网信办梳理基本情况、定性、核查、处置、措施等内容形成报告，24小时内上报上级相关部门。

二、钓鱼邮件事件应急处置流程

1.邮件系统管理员暂停涉事邮箱，保存相关信息后删除异常邮件;

2.网信办在“海大信息安全员”群发布预警信息:“【预警】各位信息安全员，*月*日*时，我校发现学校邮箱收到大量疑似钓鱼邮件(详见截图)，已启动应急处置预案，请大家提醒本单位教

工切勿打开，直接删除，避免造成经济损失或泄密。如已发生损失，请立即与我联系。网信办”；

3.2 小时内，完成对事件进行定性，确定类别和等级，向主管校领导、属地网警支队和交通运输部科技司电话汇报。

4.联系涉事当事人，了解事件经过等详细信息，掌握影响面和处置经过，完成溯源和复盘。

5.网信办梳理基本情况、定性、核查、处置、措施等内容，形成报告，24 小时内上报上级相关部门。

三、LED 显示屏被篡改事件应急处置流程

1.管理员第一时间关闭学校 LED 屏的电源，断开控制系统的网络连接；

2.保留现场并上报网信办，组织排查问题原因，拍照记录相关信息；

3.2 小时内，完成对事件进行定性，确定类别和等级，向主管校领导、属地网警支队和交通运输部科技司电话汇报。

4.对事件进行彻底调查，重点排查安全措施漏洞和管理，确保处置无问题后恢复 LED 显示屏；

5.网信办梳理基本情况、定性、核查、处置、措施等内容，形成报告，24 小时内上报上级相关部门。

四、木马病毒事件应急处置流程

1.第一时间立即切断涉事主机的校园网连接，并报告网信办；

2. 对重要数据进行数据备份，备份主机日志，利用病毒专杀软件对该计算机进行病毒查杀，理清感染途径;

3. 彻底清理木马病毒后，将主机重新接入网络;

4. 评估造成的损失，对主机进行安全加固，针对特征在安全设备进行策略调整;

5. 梳理基本情况、定性、核查、处置、措施等内容形成报告，24 小时内上报网信办。

五、数据泄漏事件处置流程

1. 第一时间立即切断涉事主机系统的校园网连接，并报告网信办;

2. 对系统进行全面安全检查，包括日志、账户、进程、木马病毒文件的查杀等，同时排查系统及应用漏洞，查找数据泄露原因;

3. 评估造成的损失，评估系统安全风险，在安全设备进行策略调整，恢复系统服务上线运行。

4. 梳理基本情况、定性、核查、处置、措施等内容形成报告，24 小时内上报网信办。

六、物理环境事件应急处置流程

1. 若发生以下电源故障事件，首先进行紧急处理，然后进行事发紧急报告。

● 短路、断路: 采取切断电源、更换短路器件方法恢复供电;

- 防雷防静电设备故障:采取切断电源跳过防雷防静电设备直接供电的方法，及时维修损坏设备并更换;
- UPS 故障：采取跳过 UPS 逆变输出的方法临时恢复供电，及时维修或更换损坏设备;
- 火灾：切断电源，同时向保卫处报告火警，请求支援，如有人遇险，应先救人后救物;
- 水渗：切断电源，更换浸水设备，采取防水措施，恢复供电。

2.评估事件产生的损失情况,核查事件原因,采取防范措施，总结处置经验，形成事件报告。

大连海事大学网络信息与综合服务中心　　2022 年 12 月 1 日印发