长春师范大学文件

长师校字〔2020〕106号

关于印发《长春师范大学网络安全事件报告、处置流程及应急预案（试行）》的通知

各单位、各部门：

现将《长春师范大学网络安全事件报告、处置流程及应急预案（试行）》印发给你们，请认真贯彻执行。

长春师范大学

2020年10月6日

长春师范大学
网络安全事件报告、处置流程及应急预案（试行）》的通知

1 总 则

1.1 编制目的

根据《国家网络安全事件应急预案》和教育部《教育系统网络安全事件应急预案》要求，建立健全学校网络安全事件应急响应工作机制，规范网络安全事件工作流程，提高网络安全事件应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校的安全稳定。

1.2 编制依据

依据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规，《国家突发公共事件总体应急预案》《突发事件应急预案管理办法》《国家网络安全事件应急预案》《关于加强教育行业网络与信息安全工作的指导意见》《教育系统网络安全事件应急预案》《吉林省教育系统网络安全事件应急预案（试行）》《信息安全技术信息安全事件分类分级指南》(GB/Z 20986-2007)等文件。

1.3 适用范围

本预案适用于全校范围发生的网络安全事件的报告、处置和应急响应工作。按照《吉林省教育系统网络安全事件应急预案（试行）》规定，本预案所指的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、设备设施故障、灾害性事件和其他事件等。信息内容安全事件的应对，参照有关规定和办法。

1.4 网络安全事件分类、等级与判定

1.4.1 网络安全事件分类

根据《信息安全技术信息安全事件分类分级指南》，将安全事件划分为以下六类：有害程序事件、网络攻击事件、信息破坏事件、设备故障事件、灾害性事件和其他事件。

（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网络安全事件。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、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 7 个子类。

（2）网络攻击事件。网络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网络安全事件。网络攻击事件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 7 个子类。

（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、窃取等而导致的网络安全事件。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网

络破坏事件等6个子类。

（4）设备设施故障。设备设施故障是指由于信息系统自身故障或外围保障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。设备设施故障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4个子类。

（5）灾害性事件。灾害性事件是指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。灾害性事件包括水灾、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。

（6）其他事件。其他事件是指不能归为以上基本分类的网络安全事件。

1.4.2 网络安全事件等级划分

参照《吉林省教育系统网络安全事件应急预案（试行）》，结合学校实际情况和可能造成的危害，将安全事件划分为四个等级:特别重大网络安全事件（Ⅰ级）、重大网络安全事件（Ⅱ级）、较大网络安全事件（Ⅲ级）和一般网络安全事件（Ⅳ级）。

（1）符合下列情形之一的，为特别重大网络安全事件（Ⅰ级）：

①关键信息基础设施或统一运行的核心业务信息系统（网站）遭受特别严重损失，造成系统大面积瘫痪，丧失业务处理能力。

②网络病毒在全国教育系统或多省教育系统大面积爆发。

③关键信息基础设施或统一运行的核心业务信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改。

④其他对全省教育系统安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件（Ⅱ级）：

①关键信息基础设施或核心业务信息系统（网站）遭受严重系统损失，造成系统瘫痪，业务处理能力受到重大影响。

②网络病毒在全省教育系统范围内大面积爆发。

③核心业务信息系统（网站）的重要敏感信息或关键数据发生丢失或被窃取、篡改。

④其他对全省教育系统安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件（Ⅲ级）：

①校园网多个校区大量用户无法正常上网。

②学校关键信息基础设施或重要信息系统（网站）遭受严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力，对全校正常秩序构成严重威胁。

③学校关键信息基础设施或重要信息系统（网站）的关键数据或重要敏感信息发生丢失或被窃取、篡改、假冒，对全校安全稳定和正常秩序构成严重威胁。

④其他对学校安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

（4）符合下列情形之一且未达到较大网络安全事件的，为一般网络安全事件（Ⅳ级）：

①校园网某个校区大量用户无法正常上网。

②学校关键信息基础设施或重要信息系统（网站）遭受较大系统损失，造成系统中断，明显影响系统效率，业务处理能力受到严重影响，对全校正常秩序构成较严重威胁。

③学校重要信息系统（网站）的数据发生丢失或被窃取、篡改、假冒，对全校安全稳定和正常秩序构成较严重威胁。

④网络病毒在学校范围内广泛传播。

⑤其他对学校安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

1.4.3 网络安全事件判定

校内各单位（部门）一旦发生安全事件，应根据《吉林省教育系统网络安全事件应急预案(试行)》，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迅速自主判定安全事件等级。学校网络安全和信息化工作领导小组办公室(以下简称“网信办”）在接到报告后，根据事件情况，进一步做出判定。必要时，组织专家组进行判定或报告学校网络安全和信息化工作领导小组判定。

1.5 工作原则

（1）统一指挥、密切协同。学校网络安全和信息化工作领导小组统筹协调全校网络安全应急指挥工作，建立与省市网络安全职能部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

（2）分级管理、强化责任。按照“谁主管谁负责、谁运维

谁负责”的原则，校内各单位（部门）对本单位（部门）网络安全工作负主体责任。

（3）预防为主、平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

2 组织机构和职责任务

2.1 领导机构与职责

学校网络安全事件防范及应急处置工作由网络安全和信息化工作领导小组统一领导、指挥和协调。负责组织Ⅰ级和Ⅱ级网络安全事件应急预案的启动，督促检查网络安全事件处置情况及校内各单位（部门）在网络安全事件处置工作中履行职责情况；负责对全校各单位（部门）贯彻执行网络安全事件报告、应急处置预案的情况进行督促检查。

2.2 办事机构与职责

学校网信办负责组织协调有关部门查处利用计算机网络泄密的违法行为；牵头组织重大敏感时期、重要活动、重要会议期间发生的网络安全事件的协调处置，完善24小时应急值守制度。

网络中心负责学校网络安全应急工作的技术支撑和保障。根据校内发生的安全事件程度，提出相应级别预案的启动，并及时收集、通报和上报安全事件处置的有关情况。定期组织网络安全应急演练，评估并适时组织安全事件应急处置管理办法修订。负责组建学校网络安全应急技术队伍。

2.3 校内相关单位与职责

学校各单位（部门）应按照网络安全事件报告与处置流程，做好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工作。做到安全事件早发现、早报告、早控制、早解决。

学校各单位（部门）应组织开展网络安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。若本网络安全事件应急预案不能满足需求，相关单位（部门）可制订本单位（部门）网络安全应急预案，制订后应及时报学校网信办备案。

3 监测与预警

3.1 预警分级

建立学校网络安全事件预警制度。按照紧急程度、发展态势和可能造成的危害程度，学校网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生的特别重大、重大、较大和一般网络安全事件。

3.2 安全监测

3.2.1 事件监测

学校网信办通过多种渠道监测、发现已经发生的学校网络安全事件，将掌握的情况立即通知校内相关单位（部门）。

校内各单位（部门）对所建网络和信息系统（网站）的运行状态进行密切监测、一旦发生网络安全事件，应当立即通过电话等方式向学校网信办报告，不得迟报、谎报、瞒报、漏报。

3.2.2 威胁监测

学校网信办组织对全校网络安全威胁进行监测，通过多种途径监测、汇聚漏洞、病毒、网络攻击等网络安全威胁信息。

校内各单位（部门）加强对所建网络和信息系统（网站）的网络安全威胁监测，对发现的威胁及时进行处置和上报学校网信办。

3.3 预警研判和发布

学校网信办对监测信息进行研判，对发生网络安全事件的可能性及其可能造成的影响进行分析评估，认为需要立即采取防范措施的及时通知有关单位；认为可能发生网络安全事件的信息，立即向学校网络安全和信息化工作领导小组报告；认为可能发生较大及以上网络安全事件的信息，经网络安全和信息化工作领导小组批准后，立即向省教育厅网络安全应急办公室报告。各单位（部门）对监测信息进行研判，认为可能发生网络安全事件的信息，应立即向学校网信办报告。

红色预警和橙色预警由教育部和省教育厅网络安全应急办公室发布。

学校网信办可根据监测研判情况，提出发布黄色预警和蓝色预警的建议，报学校网络安全和信息化工作领导小组批准后发布。对达不到预警级别但又要发布警示信息的，学校网信办可发布风险提示信息。

预警信息包括预警级别、起始时间、可能影响范围、警示事项、应采取的措施、时限要求和发布机构等。

3.4 预警响应

3.4.1 红色预警和橙色预警响应

根据《吉林省教育系统网络安全事件应急预案（试行）》精神，由教育部和省教育厅网络安全应急办公室组织红色预警和橙

色预警响应工作。

（1）学校网信办按照教育部、省教育厅网络安全应急办公室统一部署，密切关注事态发展，做好全校范围信息搜集工作，研究制定学校防范措施和应急工作方案，协调调度各种校内资源，做好校内各项准备工作。重要情况报省教育厅网络安全应急办公室。

（2）网络中心及有关单位实行24小时值班，相关人员保持通信联络畅通。

（3）网络中心技术支撑队伍进入待命状态，检查设备、软件工具等，确保其处于良好状态。

3.4.2 黄色预警响应

（1）学校网信办组织预警响应工作。联系有关部门、专业机构和专家，研究制订防范措施和应急工作方案，协调调度各种所需资源，做好各项准备工作。

（2）有关单位启动专项应急预案，开展预警响应工作，做好风险评估、应急准备和风险控制工作。

（3）学校网信办及时将事态发展情况报省教育厅网络安全应急办公室。

（4）网络中心技术支撑队伍保持联络畅通，检查应急设备、软件工具等，确保其处于良好状态。

3.4.3 蓝色预警响应

（1）学校网信办组织预警响应工作。联系有关部门、专业机构和专家，研究制订防范措施和应急工作方案，协调调度所需资源。

（2）校内有关单位（部门）启动专项应急预案，开展预警响应工作，做好风险评估、应急准备和风险控制工作。

（3）网络中心技术支撑队伍保持联络畅通，检查应急设备、软件工具等，确保其处于良好状态。

3.5 预警解除

学校网信办根据教育部、省教育厅网络安全应急办公室通知，及时转发红色预警或橙色预警解除信息。

学校网信办根据实际情况，确定是否解除黄色预警或蓝色预警，及时发布预警解除信息。

4 网络安全事件的报告与处置

4.1 Ⅰ至Ⅲ级网络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。

（1）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网络安全事件，应根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位（部门）安全责任人和主要负责人。

②本单位（部门）安全负责人接到报告后，应立即组织相关人员赶赴现场进行紧急处置，同时以口头通讯的方式将相关情况通报至学校网信办，并书面记录安全事件发现过程及口头汇报过程。涉及人为主观破坏事件应同时报告学校保卫处。

③学校网信办接到报告后，应做好书面记录，并进一步判定安全事件等级，对确认属Ⅰ至Ⅲ级安全事件的，应报告网络安全

和信息化工作领导小组相关领导，且Ⅰ、Ⅱ级安全事件应报告省教育厅和省委网信办。

④紧急报告内容包括:时间地点、简要经过、事件类型与分级、影响范围、危害程度、初步原因分析和已采取的应急措施。

⑤对确认属Ⅰ至Ⅲ级安全事件的，学校网络中心应立即组织相关技术力量赶赴现场进行协助处置工作。涉及人为主观破坏事件的，学校保卫处应组织人员赴现场协助处置，并协助省市公安机关做好相关取证和处置工作。

⑥各单位（部门）应及时跟进事件发展情况，出现新的重大情况应及时补报。

（2）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件 1。

②事中情况报告由单位（部门）安全责任人组织编写，由本单位（部门）主要负责人审核后，签字并加盖公章报送学校网信办。涉及人为主观破坏事件的，事中情况报告应抄送给学校保卫处。

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。涉及人为主观破坏的安全事件，应由学校保卫处联系、配合省市公安部门开展调查。

（3）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 3 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件 2。

②事后情况报告由单位（部门）安全责任人组织编写，由本单位（部门）主要负责人审核后，签字并加盖公章报送学校网信办。

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。涉及人为主观破坏的安全事件应继续配合省市公安部门开展调查。

4.2 一般安全事件（Ⅳ级）报告与处置

校内各单位（部门）发生一般安全事件，应及时、自主组织应急处置工作；需要网络中心协助的，应主动联系网络中心。在事件处置完毕后5日内向学校网信办报送整改报告，报告内容和格式见附件2。

5 安全事件的应急预案

5.1 预案启动

发生校园网络安全事件后，学校立即启动应急响应预案，网络中心和突发安全事件的单位（部门）应尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认突发事件的类别和等级，并按照响应机制对突发事件进行处置。

5.2 应急响应

网络安全事件应急响应分为Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级，分别对应特别重大、重大、较大和一般网络安全事件。

5.2.1 Ⅰ级响应

收到省教育厅网络安全应急办公室发布的启动Ⅰ级响应的

通知之后，进入Ⅰ级响应状态。

（1）启动指挥体系

学校网络安全和信息化工作领导小组进入应急状态，在教育部网络安全事件应急工作组的统一领导、指挥、协调下组织人员开展应急处置或支援保障工作，启动 24 小时值守，并按要求参加教育部网络安全应急办公室工作。

（2）掌握事件动态

①跟踪事态发展。若学校为事发单位，学校逐级上报，与省教育厅网络安全应急办公室保持联系，及时填写《教育系统网络安全事件情况报告》，将事态发展变化情况和处置进展情况上报省教育厅网络安全应急办公室。

②检查影响范围。当进入Ⅰ级响应状态后，学校立即全面了解学校网络与信息系统是否受到事件的波及或影响，并将有关情况及时报省教育厅网络安全应急办公室。

（3）处置实施

①控制事态防止蔓延。采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

②消除隐患恢复系统。根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患。对业务连续性要求高的受破坏网络与信息系统要及时组织恢复。

③调查取证。全校各单位（部门）应在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合省市网信部门和公安机关开展调查取证工作。

5.2.2 Ⅱ级响应

收到省教育厅发布的启动Ⅱ级响应的通知之后，进入Ⅱ级响应状态。

（1）学校网信办立即上报网络安全和信息化工作领导小组，由网络安全和信息化工作领导小组统一组织、协调指挥进行应急处置。

（2）若学校为事发单位，事发单位（部门）应及时上报学校网信办，并填写《教育系统网络安全事件情况报告》上报省教育厅网络安全应急办公室。

5.2.3 Ⅲ级响应

校内突发安全事件单位（部门）应及时将情况上报学校网信办，网信办和校内突发安全事件单位（部门）共同负责应急处置工作，并将有关情况分别报告相关分管校领导。

5.2.4 Ⅳ级响应

校内突发安全事件单位（部门）应及时将情况上报学校网信办，网信办和突发安全事件的相关单位（部门）共同负责应急处置工作。

5.3 应急处理方式

根据网络安全事件分类采取不同应急处置方式。

（1）有害程序事件。一般指病毒程序的传播，应及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助，寻找并公布病毒攻击信息，以及杀毒、防御方法。

（2）网络攻击事件。判断攻击的来源与性质，关闭影响安

全与稳定的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下措施：

①外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 IP 地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

②内部入侵：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（3）信息破坏事件。判断信息破坏的原因，尽快恢复原始信息，查找信息窃取渠道，阻断信息窃取或信息泄露的途径，避免造成进一步损失。

（4）设备故障事件。判断故障发生点和故障原因，迅速联系 IT 运维公司尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（5）灾害性事件。根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

（6）其它安全事件。可根据总的安全原则，结合具体情况，做出相应处理。

5.4 后续处理

网络安全事件进行最初的应急处置后，应及时采取行动，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。在确保安全事件解决后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

5.5 记录上报

安全事件发生时，应按照不同的安全事件等级进行上报，并在事件处置工作中作好完整的过程记录，保存各相关系统日志，直至处置工作结束。

5.6 结束响应

（1）Ⅰ级响应结束。收到省教育厅网络安全应急办公室发布的Ⅰ级响应结束通报后，Ⅰ级响应结束。

（2）Ⅱ级响应结束。收到省教育厅网络安全应急办公室发布的Ⅱ级响应结束通报后，Ⅱ级响应结束。

（3）Ⅲ、Ⅳ级响应结束。通报系统恢复运行后，学校网信办对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，组织撰写事件处理报告，Ⅲ级、Ⅳ级响应结束。

6 预防工作

6.1 日常管理

学校应做好网络安全事件日常预防工作，建立完善的应急管理体制。按照网络安全等级保护、关键信息基础设施防护等相关

要求落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强信息系统的安全保障能力。

6.2 应急演练

学校每年至少组织一次针对较大或一般网络安全事件的应急演练，每年年底前将本年度演练情况报省教育厅网络安全应急办公室。

6.3 宣传教育

学校应将网络安全教育作为国家安全教育的重要内容，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育。同时，充分利用网络安全周等各种活动形式和传播媒介，开展网络安全基本知识和技能的宣传活动，提高在校师生的网络安全意识。

6.4 工作培训

学校应定期组织网络安全培训，将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

7 配套制度与问责

7.1 人事变更报告

为保障联络通畅，各单位（部门）安全责任人、主要负责人的联络方式发生变更的，应及时向学校网信办报备。

7.2 相关配套机制

校内各单位（部门）应根据实际建立本单位（部门）的值守制度，做到安全事件早预警、早发现、早报告、早控制、早解决。

各单位（部门）应建立健全本单位（部门）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。

7.3 问责制度

校内各单位（部门）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，将对相关单位（部门）予以通报并追究相关人员的责任。

7.4 整改落实机制

发生Ⅰ至Ⅲ级安全事件后，要认真做好整改落实工作，坚持做到事故原因不查清不放过、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，尽力杜绝类似事件再次发生。

8 附 则

本预案由学校网信办负责解释，自印发之日起实施。

附件：1.长春师范大学网络安全事件情况报告

2.长春师范大学网络安全事件整改报告

长春师范大学学校办公室　　2020年10月6日印发

附件 1

长春师范大学网络安全事件情况报告

单位（部门）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　□ 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. 系统主管部门/部门： 4. 系统运维部门/部门： 5. 系统使用部门/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	
事件发生部门安全责任人意见	签名：　　年　　月　　日
事件发生部门主要负责人意见	签名：　　年　　月　　日

附件 2

长春师范大学网络安全事件整改报告

单位（部门）名称：　　（公章）　　报告时间：　年　月　日

联系人 姓　名		移动电话	
		电子邮箱	
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. 系统主管部门/部门： 4. 系统运维部门/部门： 5. 系统使用部门/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	
事件发生部门安全责任人意见	签名：　　年　　月　　日
事件发生部门主要负责人意见	签名：　　年　　月　　日