吉林农业科技学院
网络和信息安全事件应急预案

为提高我校处置网络和信息安全突发事件的能力，形成科学、有效、反应迅速的应急工作机制，确保我校机房、数据中心、信息系统等的安全，最大程度地预防和减少网络和信息安全突发事件及其造成的损害，保障信息资产安全，根据《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《互联网信息服务管理办法》《互联网新闻信息服务管理规定》及相关法律法规，结合学校网络和信息安全的实际情况，制定本预案。

一、组织机构及职责

学校网络和信息安全事件防范及应急处置工作由吉林农业科技学院网络安全和信息化领导小组统一领导、指挥和协调。负责组织Ⅰ级和Ⅱ级网络和信息安全事件应急预案的启动，督促检查网络和信息安全事件处置情况及校内各单位在网络和信息安全事件处置工作中履行职责情况。

学校网络安全和信息化领导小组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。

信息化管理中心负责学校网络和信息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。定期组织网络和信息安全应急演练。

二、网络和信息安全事件分类

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。

（一）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。

（二）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。

（三）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。

（四）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。

（五）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。

（六）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。

三、网络和信息安全事件等级划分

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）。

（一）符合下列情形之一的，为特别重大网络安全事件（Ⅰ级）：

1.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.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。

（二）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.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。

（三）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.校园网两个校区大量用户无法正常上网。

2.学校重要信息系统（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。

（四）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。

四、网络和信息安全事件判定

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领导小组办公室在接到报告后，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领导小组判定。

五、应急响应

（一）预案启动

发生校园网络和信息安全事件后，学校立即启动应急响应预案，信息化管理中心和突发安全事件的单位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。

（二）应急响应

网络和信息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。

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领导小组进入应急状态，在教育厅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，并按要求参加教育厅网络安全应急办公室工作。

（2）掌握事件动态

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。

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和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

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。

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和信息系统要及时组织恢复。

调查取证，全校各单位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。

2. Ⅱ级响应

收到省教育厅网络安全应急办公室发布的启动Ⅱ级响应的通知之后，进入Ⅱ级响应状态。

（1）学校网络安全和信息化领导小组办公室立即上报网络

安全和信息化领导小组，由网络安全和信息化领导小组统一组织、协调指挥进行应急处置。

（2）若学校为事发单位，事发单位应及时上报学校网络安全和信息化领导小组办公室，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。

3.Ⅲ级响应

校内突发安全事件单位应及时将情况上报学校网络安全和信息化领导小组办公室，学校网络安全和信息化领导小组办公室和校内突发安全事件单位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。

4.Ⅳ级响应

校内突发安全事件单位应及时将情况上报学校网络安全和信息化领导小组办公室，办公室和突发安全事件的相关单位共同负责应急处置工作。

（三）应急处理方式

根据网络和信息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。

（四）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。

（五）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。

（六）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，学校网络安全

和信息化领导小组办公室对事件造成的损失、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。

六、附则

本预案由学校网络安全和信息化领导小组办公室负责解释，自发布之日起实施。

吉林农业科技学院

2021 年 6 月 18 日