# 中国农业大学网络安全和信息化领导小组办公室文件

中农大网信字〔2021〕1号

# 中国农业大学
# 网络安全事件应急预案

中国农业大学网络安全和信息化领导小组办公室

（信息化办公室）

2021年9月30日

## 1. 编制目的

健全完善我校网络安全事件应急工作机制，规范网络安全事件工作流程，提高我校网络安全应急处置能力，预防和减少网络安全事件造成的损失和危害，维护我校安全稳定。

## 2. 编制依据

《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》、《信息安全技术信息安全事件分类分级指南》(GB/Z 20986-2007)、《教育系统网络安全事件应急预案》等文件。

## 3. 适用范围

本预案适用于中国农业大学。按照《国家网络安全事件应急预案》规定，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、设备设施故障、灾害性事件和其他事件。信息内容安全事件的应对，参照有关规定和办法。

## 4. 工作原则

(1)统一指挥、密切协同。中国农业大学网络安全和信息化领导小组 (以下简称校网信领导小组)统筹协调我校网络安全应急指挥工作，建立学校、教育部网络安全职能部门、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，各级党组织对本单位网络安全工作负主体责任。 领导班子主要负责人是网络安全工作第一责任人。

(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。

## 5. 组织机构与职责

### 5.1 领导机构与职责

校网信领导小组统筹协调组织学校全局性网络安全事件应急工作，指导学院、管理服务机构、直属机构的网络安全事件应急处置；发生特别重大网络安全事件时，成立学校网络安全事件应急工作组(以下简称工作组)，负责组织指挥

和协调事件处置，并根据实际情况吸纳相关部门、学院和网络技术中心等参加应对工作。

## 5.2 办事机构与职责

在校网信领导小组的领导下，学校信息化办公室(以下简称“信息办”)负责网络安全应急管理的事务性工作。协调各部门网络应急处置工作，对接教育部网络安全应急办公室和网络安全职能部门，向校网信领导小组报告网络安全事件情况，提出特别重大网络安全事件应对措施建议，统筹组织网络安全监测工作，指导网络安全支撑单位做好应急处置的技术支撑工作。

## 5.3 各部门职责

党委宣传部：负责网络与信息安全事件应急处置的宣传工作和舆情监测工作。

党委保卫部（保卫处）：负责网络与信息安全事件应急处置的安全保卫工作。

党委学生工作部（学生处）：负责与本科生相关的网络与信息安全事件应急处置的协调工作。

党委研究生工作部：负责与研究生相关的网络与信息安全事件应急处置的协调工作。

网络技术中心：负责网络与信息安全事件应急处置的技术支持工作。

后勤保障处、基建处：负责网络与信息安全事件应急处置的后勤保障、基建相关工作。

学校其他各部门、各学院按照职责和权限，负责本部门、本学院网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

## 6. 事件分类和分级

### 6.1 事件分类

网络安全事件分为有害程序事件、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、灾害性事件和其他网络安全事件等。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、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。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）信息内容安全事件是指通过网络传播法律法规禁止的信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

## 6.2 事件定级

根据网络安全事件的影响范围、严重程度和可控性，学校网络安全事件分为以下四级:

（1）特别重大(Ⅰ级): 核心科研、教学、管理网络、信息系统、门户网站发生全校性大规模瘫痪，丧失业务处理能力，或重要敏感信息或关键数据丢失、泄漏或者被窃取、篡改，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大且无法承受，对学校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）重大（Ⅱ级）: 核心科研、教学、管理网络、信息系统、门户网站发生全校性长时间中断或局部瘫痪，业务处理能力受到极大影响，或重要敏感信息或关键数据丢失、泄漏或者被窃取、篡改，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大但可承受，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。

（3）较大（Ⅲ级）: 科研、教学、管理网络、信息系统、门户网站发生中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或重要信息或数据丢

失、泄漏或者被窃取、篡改，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大但是完全可以承受的，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。

（4）一般（IV 级 ）：科研、教学、管理网络、信息系统、门户网站短暂中断，影响系统效率，使系统业务处理能力受到影响，或重要信息或数据丢失、泄漏或者被窃取、篡改，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小，对全校安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

## 7. 应急报告和处置流程

网络安全事件发生后,信息办应在接到报警信息的 10 分钟内确定网络安全事件的类型和级别，并相应进行报告和处置。

### 7.1 Ⅰ级至Ⅱ级网络安全事件的报告和处置

Ⅰ级至Ⅱ级网络安全事件的报告和处置分为三个步骤: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。

### 7.1.1 事发紧急报告与处置

（1）对于网络攻击、信息破坏（篡改）等事件应第一时间通知网络技术中心，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，并保留现场。

（2）对于初判为特别重大(Ⅰ级)和重大(Ⅱ级)的网络安全事件，立即上报学校网信领导小组，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，已采取的应急措施。同时通知党委宣传部、党委保卫处、党委学生工作部、党委研究生工作部、网络技术中心、后勤保障处、基建处。学校网信领导小组根据事件级别宣布启动相关应急报告和处置流程。

（3）信息办在接到学校网信领导小组发布应急响应启动令后，立即通知网络技术中心根据网络安全事件类型采取相关抑制措施如:范围控制、渠道阻断等，同时要求网络安全事件责任部门领导、系统管理员、网络安全管理员、系统维保服务公司、设备供应商等到场进行综合判断处理，尽快恢复业务。事件处理过程要全程记录关键信息，及时汇报，需要协调外围专业力量的，及时申请。信息办负责人要全程跟踪事件处理过程，做好指挥和协调汇报工作。涉及人为主观破坏事件及严重安全事件应由保卫处联系公安部门处理。党委宣传部根据事件影响范围对校内外发布公告，避免产生舆情事件。

### 7.1.2 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 8 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《网络安全事件情况报告表》。

（2）事中情况报告由网络技术中心安全负责人组织网络安全事件责任部门、运维单位共同编写，由网络技术中心和信息办主要负责人审核后，报送学校网信领导小组，签字并加盖公章报送上级单位。

（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，填写附件 2《网络安全事件处理记录表》。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。

### 7.1.3 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 5 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 3《网络安全事件整改报告》。

2. 事后情况报告由网络技术中心的安全负责人组织网络安全事件责任部门、运维单位共同编写，由网络技术中心和信息办主要负责人审核后，报送学校网信领导小组，签字并加盖公章报送上级单位。

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。如涉及人为主观破坏的安全事件应继续配合公安部门开展调查。

### 7.2 III级至IV级网络安全事件的报告和处置

发生III级至IV级安全事件，网络安全事件责任部门应及时、自主组织应急处置工作，在事件处置完毕后7天内形成报告送网络技术中心，并归档待查。

## 8. 预防工作

### 8.1 日常管理

各部门、各学院按职责做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

### 8.2 演练

学校信息办协调有关部门定期组织演练，检验和完善预案，提高实战能力。

各部门、各学院每年至少组织一次预案演练，并将演练情况报学校信息办。

## 8.3 宣传

学校信息办、党委宣传部应充分利用各种传播媒介及其他有效的宣传形式，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，开展网络安全基本知识和技能的宣传活动。

## 8.4 培训

各部门、各学院要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应急预案的培训，提高防范意识及技能。

## 8.5 重要活动期间的预防措施

在国家和北京市重要活动、会议期间，各部门、各学院要加强网络安全事件的防范和应急响应，确保网络安全。信息办统筹协调网络安全保障工作，根据需要要求网络技术中心或有关部门启动红色预警响应。相关部门加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持 24 小时值班，及时发现和处置网络安全事件隐患。

# 9 保障措施

## 9.1 机构和人员

各部门、各学院要落实网络安全应急工作责任制，把责任落实到具体岗位和个人，建立健全应急工作机制。

## 9.2 技术支撑队伍

加强网络安全应急技术支撑队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。支持购买网络安全企业服务，提升应急处置能力，提供应急技术支援。各部门、各学院应配备必要的专兼职网络安全专业技术人员，并加强与信息办的沟通、协调，建立必要的网络安全信息共享机制。

## 9.3 专家队伍

建立网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。

## 9.4 社会资源

从学校相关院系、网络安全企业中选拔网络安全人才，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力。

## 9.5 基础平台

学校信息办要加强网络安全应急基础平台和管理平台建设，做到早发现、早预警、早响应，提高应急处置能力。

## 9.6 物资保障

加强对网络安全应急装备、工具的储备，及时调整、升级软件硬件工具，不断增强应急技术支撑能力。

## 9.7 经费保障

学校财务部门为网络安全事件应急处置提供必要的资金保障。有关部门利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、预案演练、物资保障等工作开展。各部门、各学院为网络安全应急工作提供必要的经费保障。

## 9.8 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

学校网信领导小组对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

# 10 附则

## 10.1 预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由信息办负责。

各部门、各单位要根据本预案制定或修订本部门、本单位网络安全事件应急预案。

网络意识形态相关管理参照中国农业大学《网络意识形态工作责任制实施细则》等相关规定执行。

## 10.2 预案解释

本预案由网信领导小组办公室（信息化办公室）负责解释。

## 10.3 预案实施时间

本预案自印发之日起实施。

# 附件 1:　网络安全事件情况报告表

报告时间：　年　月　日　时　分

<table>
<tr><td>部门名称</td><td colspan="2"></td><td>报 告 人</td><td></td></tr>
<tr><td>联系电话</td><td colspan="2"></td><td>邮　　箱</td><td></td></tr>
<tr><td rowspan="3">发生网络安全事件的对象名称及用途</td><td>类型</td><td colspan="3">☐网络　　☐应用系统　　☐其他</td></tr>
<tr><td>名称</td><td colspan="3"></td></tr>
<tr><td>用途</td><td colspan="3"></td></tr>
<tr><td rowspan="7">网络安全事件的简要描述（如以前出现过类似情况也应加以说明）</td><td>☐有害程序事件</td><td colspan="3">☐计算机病毒事件☐蠕虫事件☐特洛伊木马事件☐僵尸网络事件<br>☐混合程序攻击事件☐网页内嵌恶意代码事件☐其他有害程序事件</td></tr>
<tr><td>☐网络攻击事件</td><td colspan="3">☐拒绝服务攻击事件☐后门攻击事件☐漏洞攻击事件☐干扰事件<br>☐网络扫描窃听事件☐网络钓鱼事件☐其他网络攻击事件</td></tr>
<tr><td>☐信息破坏事件</td><td colspan="3">☐信息篡改事件☐信息假冒事件☐信息泄露事件☐信息窃取事件<br>☐信息丢失事件☐其他信息破坏事件</td></tr>
<tr><td>☐信息内容安全事件</td><td colspan="3">☐通过网络传播法律法规禁止信息☐组织非法串联、煽动集会游行<br>☐炒作敏感问题并危害国家安全、社会稳定和公众利益的事件</td></tr>
<tr><td>☐设备设施故障</td><td colspan="3">☐软硬件自身故障☐外围保障设施故障☐人为破坏事故<br>☐其他设备设施故障</td></tr>
<tr><td>☐灾害性事件</td><td colspan="3">☐由自然灾害等其他突发事件导致的网络与网络安全事件<br>☐其他特殊灾害事件</td></tr>
<tr><td>☐其他事件<br>（注：不能归为以上 6 个基本分类的其他网络安全事件）</td><td colspan="3"></td></tr>
</table>

<table>
<tr><td>初步判定的事故原因</td><td colspan="2"></td></tr>
<tr><td>当前采取的应对措施</td><td colspan="2"></td></tr>
<tr><td rowspan="3">本次网络安全事件的初步影响状况</td><td>事件后果</td><td>□业务中断 □系统破坏 □数据丢失 □其他</td></tr>
<tr><td>影响范围</td><td>□单台主机 □台主机 □整个信息系统 □整个局域网 □其他</td></tr>
<tr><td>事件定级</td><td>□特别重大(I 级)□重大(II 级)□较大(III 级)□一般(IV 级)</td></tr>
<tr><td>网络安全管理员建议或意见</td><td colspan="2"></td></tr>
<tr><td>应急指挥工作小组负责人建议或意见</td><td colspan="2"></td></tr>
<tr><td>应急指挥领导小组负责人建议或意见</td><td colspan="2"></td></tr>
</table>

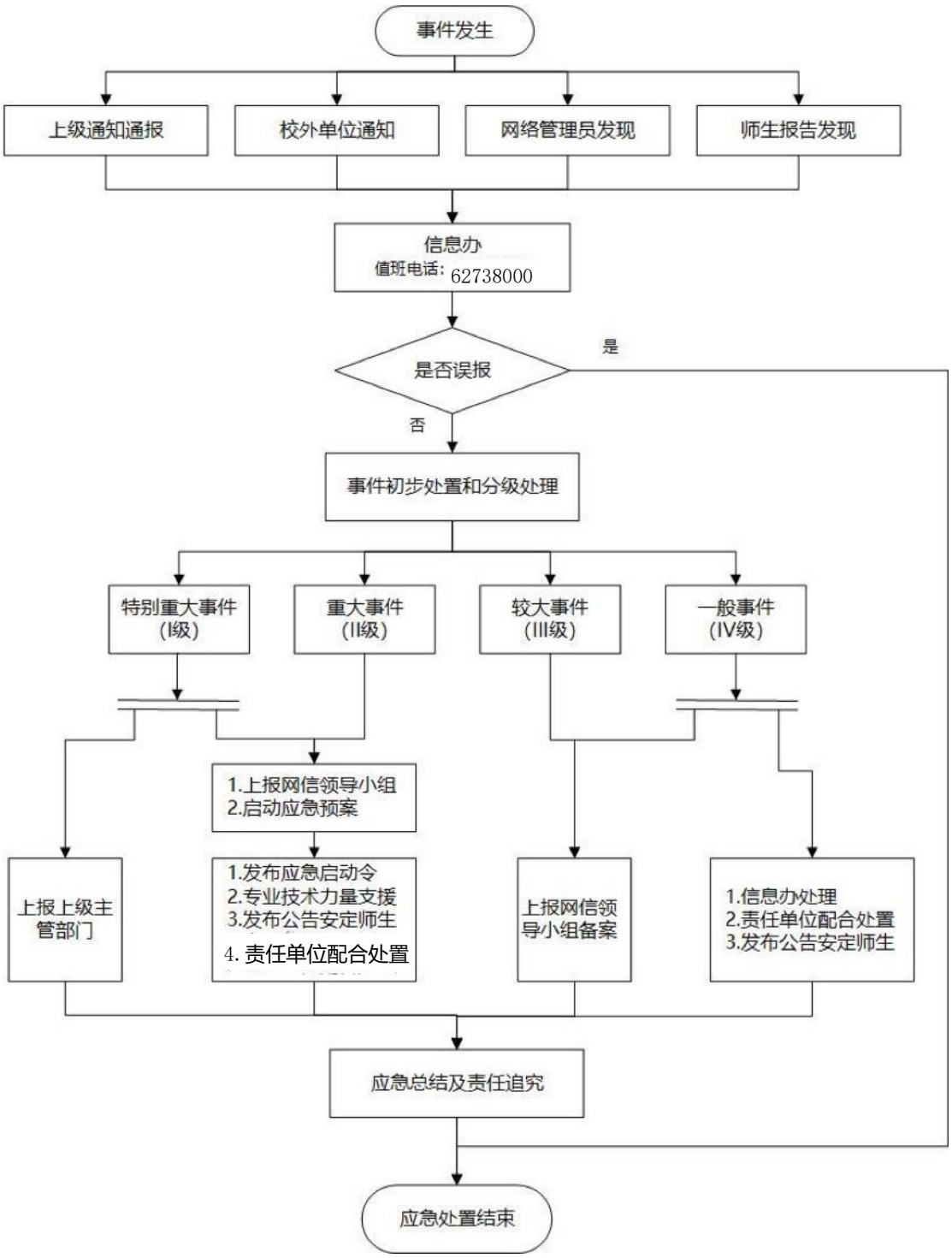
注：填写表格时根据实际情况选择相关选项，并在相应选项前的“□”中以“√”标记

# 附件 2:　网络安全事件处理记录表

<table>
<tr><td>系统名称</td><td colspan="2"></td><td>岗位</td><td></td><td>姓名</td><td></td></tr>
<tr><td>事件类型</td><td colspan="3"></td><td>事件等级</td><td colspan="2">□特别重大(I级)□重大(II级)<br>□较大(III级)□一般(IV级)</td></tr>
<tr><td>处理时间</td><td colspan="6">年　月　日　时　分</td></tr>
<tr><td>应对措施</td><td colspan="6"></td></tr>
<tr><td>处理结果</td><td colspan="6"></td></tr>
<tr><td>事件处理人<br>（签字）</td><td colspan="6"></td></tr>
</table>

# 附件 3：　　网络安全事件整改报告

<table>
<tr><td>系统名称</td><td colspan="2"></td><td>填写人</td><td></td></tr>
<tr><td>事件类型</td><td></td><td>事件等级</td><td colspan="2">□特别重大(I级)□重大(II级)<br>□较大(III级)□一般(IV级)</td></tr>
<tr><td>发现时间</td><td colspan="4">年　月　日　时　分</td></tr>
<tr><td>处理时间</td><td colspan="4">年　月　日　时　分</td></tr>
<tr><td>发生原因</td><td colspan="4"></td></tr>
<tr><td>事件影响范围</td><td colspan="4"></td></tr>
<tr><td>应对措施</td><td colspan="4"></td></tr>
</table>

| | |
|---|---|
| 处理结果 | |
| 应急指挥工作小组负责人意见<br>（签字） | |
| 应急指挥领导小组意见<br>（签字） | |

# 附件 4：应急报告和处置流程图