信息技术安全事件报告与处置流程

（试行）

为加强教育部机关、直属单位和部属高等学校信息技术安全工作，及时掌握和处置信息技术安全事件，协调相关力量做好应急响应处理，降低安全事件带来的损失与影响，维护正常工作秩序和营造健康的网络环境，根据国家有关法律法规，以及相关标准文件，结合实际，制定本流程。

第一条 信息技术安全事件定义。根据《信息安全事件分类分级指南》（GB/T 20986-2007，以下简称《指南》），本流程中所称的信息技术安全事件（以下简称安全事件）是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件。

第二条 适用范围。本流程适用于教育部机关、直属单位和部属高等学校（以下简称部属单位）发生的安全事件的报告与处置工作。涉及信息内容安全事件的报告与处置工作仍按相关规定执行。

第三条 安全事件等级划分。根据《指南》将安全事件划分为四个等级：特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）和一般事件（Ⅳ级）。

第四条 安全事件自主判定。各部属单位一旦发生安全

事件，应根据《指南》，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自主判定安全事件等级。

第五条 Ⅰ至Ⅲ级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。

（一）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，并报告本单位安全责任人和主要负责人。

2. 本单位安全责任人接到报告后，应立即组织技术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教育部教育管理信息中心（以下简称信息中心）。涉及人为主观破坏事件应同时报告当地公安机关。

3. 信息中心接到报告后，应进一步判定安全事件等级，对确认属Ⅰ至Ⅲ级安全事件的，应报告教育部办公厅和科技司。办公厅负责上报有关部领导；科技司负责组织应急处置并与中央网信办、公安部等部门联系。

4. 紧急报告内容包括：（1）时间地点；（2）简要经过；（3）事件类型与分级；（4）影响范围；（5）危害程度；（6）初步原因分析；（7）已采取的应急措施。

5. 对于在京部属单位，信息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；对于京外部属单位，自主组织本单位技术力量会同当地公安机关等做好应急处置工作。涉及人为主观破坏事件应协助公安机关做好相关取证和处置工作。

6．部属单位应及时跟进事件发展情况，出现新的重大情况应及时补报。

（二） 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。

2．事中情况报告由部属单位的安全负责人组织相关部门，运维单位共同编写，由本单位主要负责人审核后，签字并加盖公章报送教育部科技司。

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。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。

（三）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 2。

2．事后情况报告由部属单位的安全负责人组织相关部门，运维单位共同编写，由本单位主要负责人审核后，签字并加盖公章报送教育部科技司。

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。

第六条 一般安全事件报告与处置。部属单位发生一般安全事件，应及时、自主组织应急处置工作，在事件处置完毕后 7 天内报送整改报告教育部科技司，报告内容和格式见附件 2。

第七条 预警类信息的报告与处置。部属单位要按时、按要求完成国家、地方有关信息安全部门以及教育部通报的预警类信息的处置工作，并按要求形成书面报告，报送教育部科技司。

第八条 人事变更报告。部属单位的信息技术安全工作主管领导、主管部门、联络员、联络方式发生变更的，应及时报送教育部科技司。

第九条 相关配套机制。教育部建立值守制度，在信息中心设立 24 小时值班电话。各部属单位应根据实际建立本单位值守制度，做到安全事件早发现、早报告、早控制、早解决。各部属单位应建立健全本单位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。

第十条 问责制度。部属单位应按照流程及时、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，将对相关单位进行约谈或通报。

本流程自发布之日起施行。

信息中心 24 小时值守电话：010-66096817

附件：1. 信息技术安全事件情况报告

2. 信息技术安全事件整改报告

附件 1

信息技术安全事件情况报告

单位名称:（需加盖公章） 事发时间: _____年___月__日__分

联系人姓名		手机	
		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. 系统主管单位/部门: _____ 4. 系统运维单位/部门: _____ 5. 系统使用单位/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	
事件原因的初步分析	
已采取的应急措施	
是否需要应急支援及需支援事项	
安全负责人意见（签字）	
主要负责人意见（签字）	

附件 2

信息技术安全事件整改报告

单位名称:（需加盖公章）　　报告时间: _____年___月__日

<table>
<tr><td rowspan="2">联系人姓名</td><td rowspan="2"></td><td>手机</td><td></td></tr>
<tr><td>电子邮件</td><td></td></tr>
<tr><td>事件分类</td><td colspan="3">☐ 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_____</td></tr>
<tr><td>事件分级</td><td colspan="3">☐Ⅰ级　☐Ⅱ级　☐Ⅲ级　☐Ⅳ级</td></tr>
<tr><td>事件概况</td><td colspan="3"></td></tr>
<tr><td>信息系统的基本情况（如涉及请填写）</td><td colspan="3">1.系统名称: _____
2.系统网址和 IP 地址: _____
3.系统主管单位/部门: _____
4.系统运维单位/部门: _____
5.系统使用单位/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</td></tr>
<tr><td>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）</td><td colspan="3"></td></tr>
</table>

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	
安全负责人意见（签字）	
主要负责人意见（签字）	