四川省教育系统网络安全应急预案

（暂行）

为加强全省教育系统网络安全工作，及时处置网络安全事件，协调相关单位做好应急响应处置，降低安全事件带来的损失和不良影响，维护正常工作秩序和营造健康的网络环境，根据国家网络安全法等有关法律法规等文件，结合我省教育系统实际情况，制定本应急预案。

第一条 网络安全事件定义。根据《信息安全事件分类分级指南》（GB/T20986-2007，以下简称《指南》），本预案中所称的网络安全事件对应《指南》中的信息安全事件，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、灾害事件和其他网络相关的安全事件。

第二条 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）。

第三条 安全事件自主判定。各地各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。

第四条 I至Ⅲ级安全事件的处置与报告。处置与报告分为三个步骤：事发处置与报告、事中处置与报告和事后整改处置与报告。

（一）事发处置与报告

1．网络与信息系统一旦发现安全事件，应根据实际情况第一时间采取断网等有效处置措施，最大限度的降低安全损失和不良影响，同时保留现场，保全相关审计日志和证据，报告本单位安全责任人和主要负责人，并按规定报告有管辖权的公安机关。

2．各单位安全责任人接到报告后，应及时组织技术人员进行紧急处置，同时口头将相关情况向上级教育行政部门汇报。各市、县（区）教育行政部门、高等院校、中等职业学校和厅直属学校对属于I至Ⅲ级安全事件的，应报告教育厅。经定性为主观破坏事件的，公安机关将立案侦查，固定证据，相关人员要依法积极配合工作。

3.教育厅接到报告后，应进一步分析和研判安全事件等级，对确认属I至Ⅲ级安全事件的，指导应急处置并与教育部、省网信办、公安厅、省通信管理局等相关单位联系。教育厅按规定向教育部及省网信办等报告。

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。

（二）事中处置与报告

1．各地各单位应在安全事件发现后2小时内填写《网络与信息安全事件情况报告》（见附件，以下简称《情况报告》），并以书面形式报告教育厅。

2．《情况报告》由本单位安全负责人组织相关部门和运维单位共同编写，由本单位主要负责人审核后，签字并加盖单位公章报上级教育行政部门。各单位对属于I至Ⅲ级安全事件的应报告教育厅。

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。

4.教育厅指导事件处置，按规定向教育部及省网信办等报告情况。

（三）事后整改处置与报告

1．各地各单位应在安全事件处置完毕后5个工作日内填写《网络与信息安全事件整改报告》（见附件，以下简称《整改报告》）。

2．《整改报告》由本单位安全负责人组织相关部门和运维单位共同编写，由本单位主要负责人审核后，签字并加盖单位公章报上级教育行政部门。各地各校及时报送教育厅。

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。

4. 教育厅按规定向教育部及省网信办等报告情况。

第五条 一般安全事件（Ⅳ级）处置与报告。各地各单位发生一般安全事件，应及时自主组织应急处置工作，做好整改等善后工作。在事件处置完毕后5天内填写《整改报告》并报送教育厅。

第六条 预警类信息的报告与处置。各地各单位要按时、按要求完成国家、地方安全部门以及教育厅通报预警类信息的处置工作。

第七条 联络人变更报告。各单位网络安全工作主管领导、主管部门、联络员、联络方式发生变更的，应及时报告上级教育行政部门。各地各单位及时报告教育厅。

第八条 相关配套机制。各单位要建立本单位值守制度，建立健全本单位网络安全事件应急处置机制，制定应急预案，定期组织应急演练，做到早发现、早报告、早控制、早解决。

第九条 问责制度。各地各单位应依法依规及时处置网络安全事件并如实报告。如有处置不当、整改不力、瞒报、缓报等情况，将对相关单位进行约谈或通报。触犯法律的将依法承担法律责任。

附件

网络安全事件情况报告

单位名称：（需加盖公章） 时间： 年 月 日

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 电子邮箱 |  |
| 手机 |  | 传真 |  |
| 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 | | |
| 事发时间 | 年 月 日 时 分 | | |
| 事件概况 |  | | |
| 信息系统的基本情况（含网站） | 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：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 是否定级 □是 □否，所定级别：\_\_\_\_\_ 2. 是否备案 □是 □否，备案号：\_\_\_\_\_\_\_\_\_\_ 3. 是否测评 □是 □否 4. 是否整改 □是 □否 | | |
| 事发单位及事发网络和信息系统功能描述 |  | | |
| 事件发生时间、事态发展与处置的简要经过。 |  | | |
| 事件初步估计的危害和影响（影响程度、影响人数、紧急损失等情况） |  | | |
| 事件原因的初步分析 |  | | |
| 已采取的应急措施和效果 |  | | |
| 是否需要应急支援及需支援事项和工作建议 |  | | |
| 安全负责人意见（签字） |  | | |
| 主要负责人意见（签字） |  | | |

网络安全事件整改报告

单位名称：（需加盖公章） 时间： 年 月 日

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 手机 |  |
| 电子邮件 |  |
| 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 | | |
| 事件报告时间 |  | | |
| 事件概况 |  | | |
| 信息系统的基本情况（含网站） | 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 |  | | |
| 安全负责人意见（签字） |  | | |
| 主要负责人意见（签字） |  | | |