上海第二工业大学网络与信息安全事件应急预案

**第一章 总则**

**第一条 编制目的**

为了建立健全学校网络与信息安全应急工作机制，提高应对网络与信息安全事件能力，减少网络与信息安全事件造成的危害，特制定本预案。

**第二条 适用范围**

本预案适用于学校网络与信息系统安全事件的预防、通报和应急处置工作。

**第三条 编制单位**

本预案由上海第二工业大学信息化办公室负责编制。

**第四条 事件分类**

网络与信息安全事件分为**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、设备设施故障和灾害性事件**等。

（1） 有害程序事件

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

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

信息破坏事件分为信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4） 信息内容安全事件

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

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

灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

**第五条 本应急预案所处理的网络与信息安全事件**

（1） 严重影响整个学校正常教学、科研和管理秩序，造成学校各项业务中断（或运行效率明显下降）1小时以上。

（2） 学校信息系统数据丢失或被窃取、篡改、假冒，对社会和公众利益构成严重威胁，或对学校业务工作产生严重影响。

（3） 通过学校网络传播反动信息、煽动性信息、涉密信息、谣言等，对国家安全和社会稳定构成严重危害。

（4） 其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络与信息安全事件。

**第六条 工作原则**

网络与信息安全事件应急工作，应当遵循预防为主、常备不懈的方针，贯彻统一领导、快速反应、属地负责、分级处置、协同配合的原则。

**第二章 组织管理**

**第七条 组织机构**

网络与信息安全突发事件的应急指挥由信息化工作委员会下设的信息网络安全保障工作小组领导。

信息化工作委员会主任兼任信息网络安全保障工作小组组长，组员由党委办公室、校长办公室、宣传部、保卫处、后勤保障处、信息化办公室、信息技术中心负责人组成。

信息化办公室作为信息网络安全保障工作小组的执行机构，负责协调、指挥工作，信息技术中心负责具体应急预案处置工作。

**第八条 工作职责**

（1） 负责建立本级网络与信息安全事件监测预警、应急处置和应急响应机制，发布网络与信息安全事件预防警报，组织实施网络与信息安全事件应急处置。

（2） 决定启动和终止应急预案。

（3） 负责全校各部门的协调配合，负责与学校外部相关部门的协调配合。

（4） 协调应急资源指挥调配。

（5） 组织应急预备队伍的应急处置行动。

（6） 及时向学校报告应急响应的情况。

（7） 组织善后工作和网络与信息安全事件的调查工作。

**第三章 应急事件处置**

**第九条 预警信息来源**

（1） 国家有关部门发布或向学校通报的信息。

（2） 学校有关部门收集的信息。

（3） 运行监控系统检测发现的信息。

（4） 网络与信息安全巡检人员发现的信息。

（5） 学校各类工作人员发现并报告的信息。

（6） 其他信息。

**第十条 控制事态和信息初步上报**

（1）应急事件一旦发现，信息办决定启动应急预案，信息技术中心人员应进行紧急处置，停止相关的网络连接，保持相关的信息系统处于隔离状态，防止事件进一步升级。

（2） 信息化办公室在事件发现一小时内，电话上报分管校领导、同时上报校党委办公室负责人和校长办公室负责人。

（3） 信息化办公室根据事件严重程度和影响范围，电话上报上一级主管单位信息技术部门（市教委信息中心 电话 23116638）。

（4） 电话报告的“六个要素”：网络与信息安全事件发现的时间、地点、事由、现状、影响、采取的紧急处置措施。其中，时间报告要精确到分，地点要明确。

**第十一条 初步处置**

（1） 信息技术中心对于网络安全事件，应通知相关负责人、电信运营商和网络设备供应商，必要时请求上级单位信息安全技术支持。

（2） 信息技术中心对于信息系统安全事件，按照“谁使用谁负责”的原则，应通知信息系统使用部门负责人、信息系统运维厂商、必要时请求上级单位信息安全技术支持。

（3） 信息技术中心组织技术人员对事件发生的原因进行初步判断，并对可能存在的其他网络和信息系统同类安全隐患进行控制事态处理，拟定处置措施。

（4） 信息技术中心应保留事件发现时的各项日志信息、系统信息，保留能够说明事件情况的截图，在使用问题诊断工具进行事件原因诊断时，要保留诊断结果。

（5） 信息化办公室在事件发现2小时内以书面形式报告分管校领导和校党委办公室和校长办公室。经领导审核后报告上一级主管单位，相关领导来不及书面审批的，应经相关领导口头批准后直接上报。

（6） 如事件涉及到刑事犯罪的，应通知校保卫处，联系公安部门协助处理。

**第十二条 事件处理**

信息化办公室根据上级领导批复的处置措施，协调学校各个部门，指导信息技术中心对网络和信息系统进行恢复，根据事件发生原因和类别，有针对性的采取措施，恢复受破坏信息系统正常运行。

**第十三条 处理报告**

处理结束后要形成处理结果报告，通过相应渠道报送上级部门，报告要有领导签发，注明承办人全名和联系电话，缓急程度、发送时间和收（发）文编号。内容要条理清楚，语句简洁，重点突出。

（1） 网络与信息安全事件详细情况，包括事件发生的时间、地点、过程、状况、原因、影响等。

（2） 已经采取的措施及效果。

（3） 事态发展预测和下一步行动计划以及处置建议等。

**第十四条 信息发布**

信息网络安全保障工作小组研究制定信息报道方案和对外答复口径，并报校领导。经校领导授权，可由宣传部门确定对外发布形式和口径，进行信息发布工作。

**第十五条 行动解除**

（1） 信息网络安全保障工作小组确认网络与信息安全事件已得到控制或取得预期处置结果后，宣布应急行动结束。

（2） 信息网络安全保障工作小组确认和批准，所有相关人员撤离事件现场。

**第十六条 后期处置**

（1） 在应急处置工作结束后，信息化办公室应立即组织相关人员组成事件调查组，对事件发生及其处置过程进行全面的调查分析，查清事件发生的根本原因，评估损失情况和危害影响程度，总结经验教训，形成调查评估报告，以利于后期整改。

（2） 根据突发事件的性质、以及造成的后果，明确相关人员的责任，按照学校规章制度进行分级处理，对触犯法律法规的，报送司法机关处理。

**第四章 监督管理**

**第十七条 预案培训**

信息化办公室有计划的组织有关人员对预案内容及应急流程进行培训，提高网络和信息安全防范意识。

**第十八条 预案演练**

学校将每年不定期安排演练，通过演练，发现和解决应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

**第五章 附则**

**第十九条 预案更新**

本预案将结合信息网络快速发展和学校发展状况，配合相关法律法规的制定、修改和完善，适时修订本预案。

**第二十条 解释部门**

本预案由上海第二工业大学信息化办公室负责解释。

**第二十一条 本预案实施时间**

本预案自发布之日起开始实施。

附件一、

1.学校信息网络安全工作保障小组人员信息：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **职务** | **姓名** | **联系电话** | **手机** |
| 1 | 学校分管信息安全副书记 | 吴沛东 | 50216928 | 13311680393 |
| 2 | 党办主任 | 许静鸿 | 50217013 | 13916718423 |
| 3 | 校办主任 | 俞雷霖 | 50216010 | 13901891254 |
| 4 | 宣传部部长 | 殷革兰 | 50217998 | 18918321607 |
| 5 | 保卫处处长 | 黄晓峰 | 50217720 | 13636353471 |
| 6 | 后勤保障处处长 | 李琦明 | 50212353 | 18916189160 |
| 7 | 信息化办公室主任兼信息技术中心主任 | 唐黎平 | 50217735 | 13917480931 |

2、教委信息安全工作联系人

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **单位** | **姓名** | **联系电话** |
| 1 | 市教委信息中心 | 周丹 | 23116638 |
| 2 | 市教委办公室 | 杜冲 | 23117209 |

附件二、

网络与信息安全事件应急预案流程图

