北京工业职业技术学院信息安全应急预案

为了规范学院应急响应工作内容和工作流程，提高自身的应急响应能力，完善应急响应机制，确保信息系统的安全、稳定运行和业务的连续性，根据国家有关法律、法规和政策特制定本应急预案。

1 分类分级

1.1 事件分类

依据分类参考要素，信息安全事件可分为环境灾害、常规事故、内容异常、网络或系统异常和其他事件等 5 个第一层分类，在此基础上，信息安全事件又细分成若干个第二层和第三层分类，具体类别参见信息安全事件的分类表：

第一层分类	第二层分类	第三层分类
环境灾害	自然灾害	水灾
		地震灾害
		地质灾害
		气象灾害
		自然火灾
		其他自然灾害
	人为灾害	人为火灾
		恐怖袭击
		战争
		其他人为灾害
	外围保障设施故障	电力故障
		外围网络故障
		其他外围保障设施故障
常规事故	有意事故	硬件窃取
		软件窃取
		数据窃取
		故意破坏硬件设备
		故意破坏软件
		故意破坏数据
		其他有意事故
	无意事故	硬件设备遗失
		软件遗失
		数据遗失
		误操作破坏硬件
		误操作破坏软件
		误操作破坏数据

		其他无意事故
	软硬件自身故障	软件自身故障
		硬件自身故障
内容异常	反动内容	通过邮件传播反动信息
		网页被篡改为反动页面
		通过网页传播反动信息
		通过其他方式传播反动信息
	色情内容	通过邮件传播色情信息
		网页被篡改为色情页面
		通过网页传播色情信息
		通过其他方式传播色情信息
	敏感内容	通过邮件传播敏感信息
		通过网页传播敏感信息
		通过其他方式传播敏感信息
	其他异常内容	垃圾邮件
		网页被篡改成异常信息
		通过网页传播其他异常信息
		通过其他方式传播异常信息
网络或系统异常	计算机病毒	传统计算机病毒
		邮件病毒
		脚本病毒
		蠕虫病毒
		木马程序
		其他计算机病毒
	间接攻击	扫描探测
		网络监听
		口令攻击
		网络社交攻击
		其他方式间接攻击
	直接攻击	拒绝服务攻击
		后门攻击
		漏洞攻击
		其他方式直接攻击
其他事件	不能归为以上四个第一层分类的信息安全事件。	

1.2 事件分级

信息安全事件分级的参考要素包括信息密级、公众影响和资产损失等四项。各参考要素分别说明如下：

1、 信息密级是衡量因信息失窃或泄密所造成的信息安全事件中所涉及信息的重要程度的要素；

2、 公众影响是衡量信息安全事件所造成的负面影响范围和程度的要素；

3、 业务影响是衡量信息安全事件对学校业务开展所造成的负面影响程度的要素；

4、 资产损失是衡量恢复系统正常运行和消除信息安全事件负面影响所需付出资金代价的要素。

根据突发信息安全事件所造成后果的严重程度，突发信息安全事件可划分为3个等级。各级别的突发信息安全事件具体描述如下：

一级（重大）：本级突发信息安全事件对计算机系统或网络系统所承载的业务、学校利益以及社会公共利益有极其严重的影响或破坏，业务系统中断四小时以上或者资产损失达到20万元以上的信息安全事件；

二级（严重）：本级突发信息安全事件对计算机系统或网络系统所承载的业务、学校利益以及社会公共利益有较为严重的影响或破坏，如丢失秘密信息、对学校正常工作和形象造成影响、业务系统中断四小时以内或者资产损失达到10万元以上的信息安全事件；

三级（一般）：本级突发信息安全事件对计算机系统或网络系统所承载的业务以及学校利益有一定的影响或破坏，或者基本没有影响和破坏，如丢失工作秘密、只对学校部分人员的正常工作秩序造成影响、业务系统中断二小时以内或者资产损失仅在2万元以内的信息安全事件。

2 应急指挥机构

2.1 信息安全指挥组

由网络安全和信息化领导小组组长和副组长组成，负责控制全局情况、协调各部门合作。

2.2 业务支持组

由信息中心负责人担任组长，成员由信息中心数据库管理员、应用系统管理员、业务部门系统管理员和外部单位技术人员组成。任务为：组织制定应急处理方案，报指挥组审定后实施；负责业务系统应急过程中各种信息的搜集、汇总形成书面材料向指挥组负责人报告；掌握现场应急演工作进度，及时预测发展变化趋势，并研究对策；负责联系主机支持组、网络支持组合和综合支持组，及时通知业务运行情况。同时还负责进行各项业务系统在运行不同状态下的测试，并详细记录测试数据形成测试报告上报指挥组。

2.3　主机支持组

由信息中心负责人担任组长，成员由信息中心服务器管理员和外部单位技术人员组成。任务为：组织制定应急处理方案，报指挥组审定后实施；负责主机应急过程中各种信息的搜集、汇总形成书面材料向指挥组负责人报告；掌握现场应急工作进度，及时预测发展变化趋势，并研究对策；负责联系业务支持组、网络支持组和综合支持组，及时通知主机运行情况。同时还负责进行各项主机应用系统在运行不同状态下的测试，并详细记录测试数据形成测试报告上报指挥组。

2.4　网络支持组

由信息中心负责人担任组长，成员由信息中心网络管理员、网络安全员和外部单位技术人员组成。任务为：组织制定应急处理方案，报指挥部审定后实施；负责网络应急过程中各种信息的搜集、汇总形成书面材料向指挥组负责人报告；掌握现场应急工作进度，及时预测发展变化趋势，并研究对策；负责联系主机支持组、业务支持组和综合支持组，及时通知网络运行情况。同时还负责进行各项网络应用系统在网络运行不同状态下的测试，并详细记录测试数据形成测试报告上报指挥组。

2.5　综合支持组

由学校党政办公室负责人担任组长，成员由学校各二级部门相关人员组成。任务为：负责应急演练中的车辆调度使用、应急物资准备、新闻报道工作。确保应急指挥通讯联络的畅通。

3 预防预警

预防预警是应急响应迅速启动的关键。学校利用自身的安全监控设备和工具，并结合社会其它信息源（如安全厂商的公告、各类应急响应机构的公告等），及时发现信息安全威胁或事件发生的迹象和趋势，分析导致信息安全事件的根源，为信息安全应急响应工作提供支持。

3.1 信息监测与报告

学校要进一步完善网络与信息安全突发公共事件监测、预测、预警制度。按照“早发现、早报告、早处理、早恢复”的原则，加强对各类网络与信息安全突发公共事件和可能引发突发公共事件的有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发公共事件时，信息中心在向网络安全与信息化领导小

组报告的同时，应按安全事件报送的规定及时向有关部门报告。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

1、 学校信息中心要加强信息安全监测、分析和预警工作，进一步提高信息安全监察能力和信息安全事件的防御能力。

2、 建立信息安全事故报告制度。发现信息安全突发事件发生后，立即对发生的事件进行调查核实、保存相关证据，并在事件被发现或应当被发现时起 5 小时内将有关材料报至信息安全指挥组。

3.2 预警处理与发布

信息中心接到信息安全突发事件报告后，在经初步核实后，将有关情况及时向信息安全指挥组报告。在进一步综合情况，研究分析可能造成损害程度的基础上，提出初步行动对策，视情况召集协调会，并根据信息安全指挥组的决策，实施行动方案，发布指示和命令。

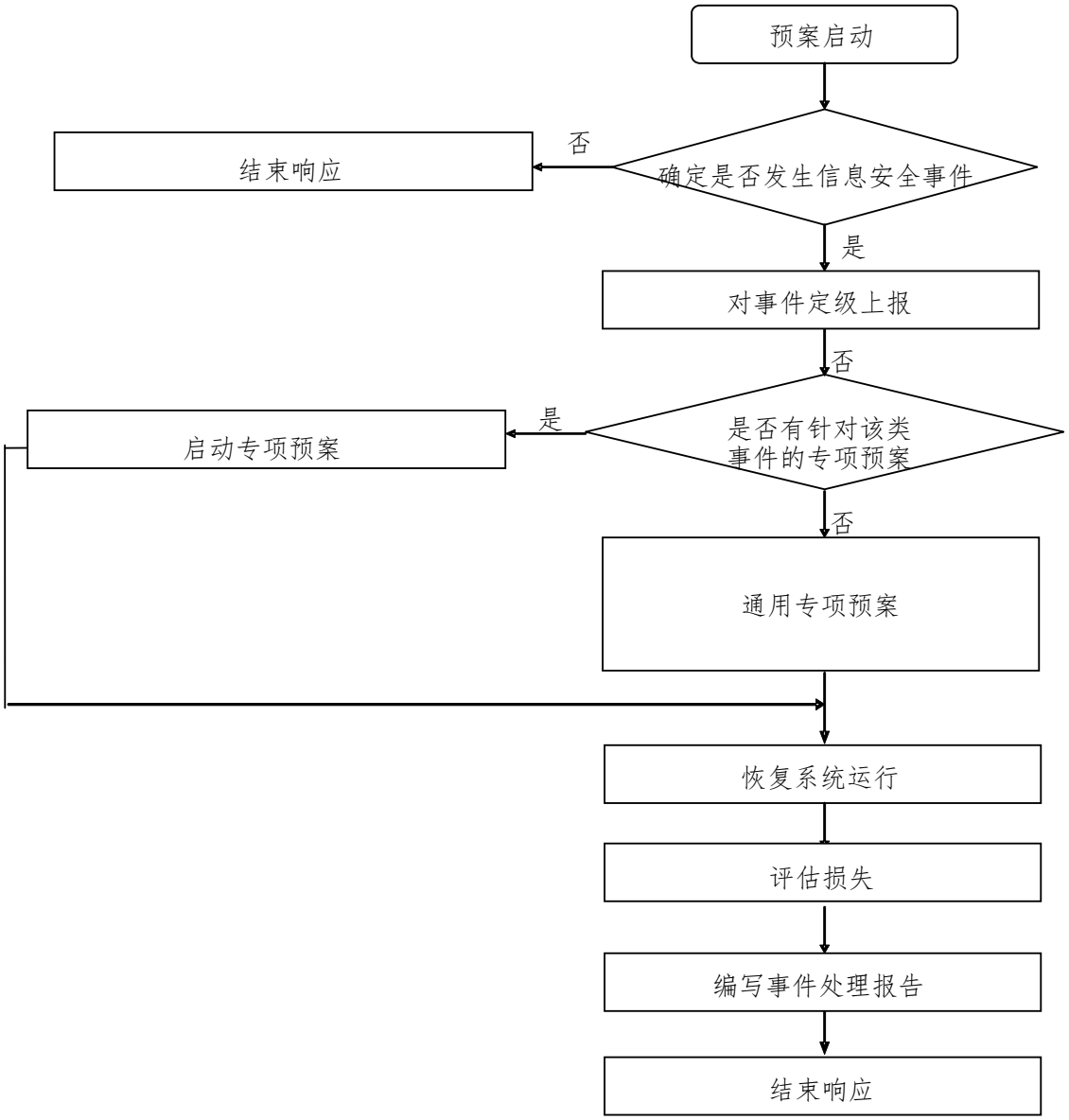
1、 对于可能发生或已经发生的网络与信息安全突发公共事件，学校应立即采取措施控制事态，并在最短的时间内进行风险评估，判定事件等级并在本系统内发布预警。必要时应启动相应的专项预案，同时向信息安全指挥组通报情况。

2、 信息安全指挥组接到报告后，应及时对信息作出判断，提出处理意见。对发生和可能发生的网络与信息安全突发公共事件时，应迅速召开应急处理工作会议，研究确定网络与信息安全突发公共事件的等级，决定启动应急预案，同时确定应急指挥人员，提出处置意见和建议，并向上级相关部门进行通报。

3、 对需要向社会发布预警的网络与信息安全突发公共事件，由信息安全指挥组根据其可能造成的危害程度、紧急程度和发展态势，及时向上级主管部门通报预警信息。由上级主管部门根据网络与信息安全事件的管理权限、危害性和紧急程度，统一发布、调整和解除预警信息，对严重、特别严重或可能衍生其他安全事件的预警信息。

4 应急响应

在发生信息安全事件时，启动下列应急响应流程，应急响应流程如下图所示。



4.1 应急响应

根据网络与信息安全事件的可控性、严重程度和影响范围，应急响应级别分为三级：一级、二级和三级，分别应对重大、严重和一般网络与信息安全事件。

1、 发生三级网络信息安全事件后，网络安全和信息化领导小组启动相应预案，并由信息安全指挥组负责应急处理工作；发生一、二级的信息安全突发事件后，应向上级主管机关报送事件情况，并由上级信息安全应急指挥组负责应急处理工作。

2、 在网络安全和信息化领导小组做出启动预案决定后，信息安全指挥组应立即启动应急处理工作。

4.2 信息报告与处理

为保证应急响应的各项资源能够得到最有效的利用，避免应急响应体系由于受到错误或虚假报警而受到干扰，学校在报告信息安全事件或请求应急支援时应确保事件信息的可靠性。

信息处理可按以下程序进行：

1、 记录与了解。接到网络与信息安全事件报警后，要先详细记录该事件的细节信息，了解事件造成的损失、影响以及现场控制情况，并尽可能全面了解与事件有关的信息。

2、 事件确认与判断。在汇总相关信息的基础上，及时判断事件性质，并根据判定结果，开展下一步的工作。

(1) 属于网络与信息安全事件的，应参考数据库对该次事件做进一步的事件验证，确认属于网络与信息安全事件的，应进入事件分析流程。

(2) 属于误报的，值班人员应对该事件进行记录和处理。

(3) 对于与网络与信息安全无关的事件，值班人员也应做好记录，并将事件转交给相关主管机构处理。

3、 事件分析。事件确认后，根据掌握的信息，分析事件已经造成的损失和预计损失、事件的严重程度和扩散性等情况。

4、 准备启动应急处置流程。

5、 确定应急处理方式。根据对事件的初步分析，确定应急处理方式，如果学校以自身力量无法处理的事件，在向上级部门报告事件的同时，提出应急支援请求。

4.3 应急处理

事件处理基本流程主要包括以下内容：

1、 确认阶段：确定应急处理方式。

2、 遏制阶段：及时采取行动遏制事件发展。

3、 根除阶段：彻底解决问题隐患。

4、 恢复和跟踪阶段。

4.4　报告和总结

网络与信息安全突发公共事件经应急处置后，得到有效控制，网络安全和信息化领导小组对事件造成的损失、事件处理流程、应急预案进行评估，对响应流程、预案提出修改意见，回顾并整理发生事件的各种相关信息，尽可能地把所有情况记录到文档中。

4.5　应急结束

根据信息安全事件的处置进展情况和网络安全和信息化领导小组意见，信息安全指挥组应组织相关部门及专家对信息安全事件处置情况进行综合评估和总结。

5　保障措施

5.1　通信与信息保障

在整合各职能部门专业通信网的基础上，加强应急通信装备准备，建立备份系统和紧急保障措施，形成跨部门、多手段、多路由，有线和无线相结合的反应快速、灵活机动、稳定可靠的通信系统。

5.2　应急装备保障

网络与各信息系统在建设系统时应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。在网络与信息安全事件发生时，由信息中心负责统一调用。

5.3　数据保障

重要信息系统均应建立异地容灾备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。各容灾备份系统应具有一定兼容性，在特殊情况下各系统间可互为备份。

5.4　应急队伍保障

按照一专多能的要求建立网络信息安全应急保障队伍。由信息中心选择若干经国家有关部门资质认可的，管理规范、服务能力较强的企业作为单位网络与信息安全的社会应急支援单位，提供技术支持与服务。

5.5 交通运输保障

各重要信息系统的主管部门均应确定信息安全事件应急交通工具，确保应急期间人员、物资、信息传递的需要，并根据应急处置工作需要，由网络安全和信息化领导小组调配。

5.6 经费保障

学校负责落实网络与信息安全事件应急管理工作的日常运作、应急处置和基础设施运维等应急管理经费预算。应列入学校年度财政预算。

学校财政和审计部门要对网络与信息安全事件应急经费的使用进行监管和评估。

6 监督管理

6.1 宣传教育

学校要加强对网络与信息安全等方面的知识培训，提高防范意识及技能，指定专人负责安全技术工作。并将网络与信息安全突发公共事件的应急管理、工作流程等列为行政管理人员的培训内容，增强应急处置工作的组织能力。

应急响应培训用于确保学校整个应急响应体系内的所有人员具备了对信息安全事件的意识和知识，确保所有人员了解了学校应急响应的策略和应急预案，并能够熟练执行应急预案。

应急响应培训应建立在日常安全培训的基础上，或作为日常安全培训的一部分，主要培训有关应急准备和应急响应的各项知识、技术、技能和经验。

应急响应培训的重点是应急预案，使所有人员了解各自在应急响应工作中的职责，明确发生信息安全事件时应采取的行动步骤。可针对不同角色的人员设置不同的培训内容，例如安全管理员应接受有关安全工具使用的培训，安全分析员应接受最新的入侵技术及攻击特征识别的培训。

应急响应培训应定期更新，并通过实际的应急响应演练过程，帮助所有人员不断更新应急响应相关的知识和技能，同时有助于促进人员的安全意识和应急响应的熟练程度，提高突发事件时应急响应的效率。应强调培训效果的反馈机制和培训计划的更新机制，通过考核、应急响应演练等及时发现培训计划中存在的问题，依据这些反馈结果调整培训的课程设置、培训的时间计划以及培训的重点。

由于关键岗位的人力资源同样需要备份，对于各关键岗位均必须培训多个能胜任该岗位应急工作的人员，保证人员的连续性。

6.2 演练

学校应建立应急预案定期演练制度。通过演练，发现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。应急响应演练是模拟突发信息安全事件，各有关部门和人员按照应急预案所进行的一系列活动和措施。每隔一定时间，或更新应急预案后，或遇有可预见的安全事件时，要开展应急响应演练，以检验应急预案的正确性，不断加强人员的应急安全意识和应急响应的熟练程度。

应急响应演练以应急预案为基础，在每次演练前应首先确定演练的目标和范围，制定详细、严谨的应急响应演练方案，避免对正常业务造成不必要影响。

应急响应演练过程中如需涉及上级主管部门或其他相关部门，应事先做好协调沟通工作，避免由于协调工作不到位而导致对这些部门的正常工作的干扰。如果应急响应演练过程涉及到社会网络服务机构，需要事先与其进行协商，并明确服务范围、服务级别及相关费用等事项。

在每次应急响应过程结束之后，应针对应急响应工作过程中遇到的问题，分析应急响应预案的科学性和合理性，针对预案中的问题进行修改。修改后的预案应经评估通过后，发布实施。

6.3 预案执行监督

发生重大信息安全事件时应当按照规定及时如实地报告事件的有关信息，不得瞒报、缓报或者授意他人瞒报、缓报。任何单位或个人发现有瞒报、缓报、谎报重大信息安全事件情况时，有权直接向信息安全委举报。

应急行动结束后，信息安全事件响应组对相关成员单位采取的应急行动的及时性、有效性进行评估。

附件 1 重大信息安全事故报告表

<table>
<tr><td colspan="4">报告时间 ：　　年　　月　　日　　时　　分</td></tr>
<tr><td>单位名称</td><td></td><td>报告人</td><td></td></tr>
<tr><td>联系电话</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="4">发生重大信息安全事件的网络与信息系统名称及用途</td></tr>
<tr><td>负责部门</td><td></td><td>负责人</td><td></td></tr>
<tr><td colspan="4">重大信息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></tr>
<tr><td colspan="4">初步判定的事故原因</td></tr>
<tr><td colspan="4">当前采取的确应对措施</td></tr>
<tr><td colspan="4">本次重大信息安全事件的初步影响状况、事件后果：
口业务中断　口系统破坏　口数据丢失　口其他</td></tr>
<tr><td colspan="4">影响范围
口单台主机　口 台主机　口整个信息系统　口整个局域网</td></tr>
<tr><td colspan="4">严重程度
口极严重　口很严重　口严重　口一般　口不严重口</td></tr>
<tr><td colspan="4">值班电话：</td></tr>
</table>

附件 2 重大信息安全事件处理结果报告表

原事件报告时间：_____ 年 _____月_____日_____时_____分

备案编号：　　年　　月　　日 第　　号　总第　　号

<table>
<tr><td>单位名称</td><td></td><td>联系人</td><td colspan="3"></td></tr>
<tr><td>联系电话</td><td></td><td>电子邮件</td><td colspan="3"></td></tr>
<tr><td rowspan="3">发生突发信息安全事件的网络与信息系统基本信息</td><td>名称</td><td colspan="4"></td></tr>
<tr><td>类别</td><td colspan="4">☐ 网络基础设施　　☐ 信息系统　　☐ 信息内容</td></tr>
<tr><td>用途</td><td>操作系统</td><td>数据库</td><td>安全测评</td><td>安全措施</td></tr>
<tr><td></td><td>☐ Sun 系列
☐ Irix
☐ Aix
☐ HP-UX
☐ Windows
☐ BSD 系列
☐ Linux
☐ _____</td><td>☐ 无
☐ Oracle
☐ MS SQL
☐ Informix
☐ Sybase
☐ MySQL
_____
_____</td><td>☐通过安全测评
☐已安全测评，未通过
☐未经过安全测评</td><td>☐ 防火墙
☐入侵检测系统
_____
_____
_____
_____
_____</td></tr>
<tr><td>信息
安全事件的补充描述及最后判定的事件原因</td><td colspan="5"></td></tr>
<tr><td>对本次突发信息安全事</td><td>事件后果</td><td colspan="4">☐业务中断　☐系统破坏　☐数据破坏
☐其他_____</td></tr>
</table>

件的事后影响状况	影响范围	□单台主机 □_____台主机 □ 整个信息系统 □整个局域网 □_____	
突发信息安全事件的类别	事件一层类别		□ 环境灾害 □ 常规事故 □ 内容异常 □ 网络或系统异常 □ 其他事件
	事件二层类别		
	事件三层类别		
突发信息安全事件定级结果	信息密级要素定级结果		□ 1 级 □ 2 级 □ 3 级 □ 4 级
	公众影响要素定级结果		□ 1 级 □ 2 级 □ 3 级 □ 4 级
	业务影响要素定级结果		□ 1 级 □ 2 级 □ 3 级 □ 4 级
	资产损失要素定级结果		□ 1 级 □ 2 级 □ 3 级 □ 4 级
	事件最终综合定级结果		□ 1 级 □ 2 级 □ 3 级 □ 4 级
本次突发信息安全事件的主要处理过程与结果（必要时可附文字、图片等材料）	（可增页）		
针对此类事件应采取的保障网络与信息系统安全的措施和建议	（可增页） 报告人签章_____		