上海海关学院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

 建立健全上海海关学院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，预防和减少网络与信息安全事件对学院业务工作造成的损失和危害，保障学院正常的工作秩序。

 第二条 编制依据

 根据《国家网络与信息安全事件应急预案》和《海关网络与信息安全事件急预案》，制定本预案。

 第三条 适用范围

 本预案适用于上海海关学院网络与信息安全事件的预防预警、应急处置、应急保障、善后处理工作等。

 第四条 事件分类分级

 （一） 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、信息系统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. 信息系统故障

 信息系统故障包含软硬件自身故障、外围保障设施故障、人为破坏事故和其他信息系统故障。

 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。

 （二） 事件分级

 上海海关学院网络与信息安全事件根据危害程度和影响范围分为四级：

I级（特别重大网络与信息安全事件）、II级（重大网络与信息安全事件）、III级（较大网络与信息安全事件）和IV级（一般网络与信息安全事件）。

 1. I级网络与信息安全事件

 符合下列条件之一的，为I级网络与信息安全事件：

 （1）发生信息系统故障，导致多个业务信息系统业务中断（或运行效率明显下降）24小时以上。

 （2）信息系统数据丢失或被窃取、篡改、假冒，对学院建设和公众利益构成特别严重威胁，或对学院业务工作产生特别严重影响。

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

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

 2. II级网络与信息安全事件

 符合下列条件之一的，为II级网络与信息安全事件：

 （1）发生信息系统故障，导致多个业务中断（或运行效率明显下降）12小时以上。

 （2）学院信息系统数据丢失或被窃取、篡改、假冒，对学院建设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）通过学院网络传播反动信息、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。

3. III级网络与信息安全事件

符合下列条件之一的，为III级网络与信息安全事件：

（1）发生信息系统故障，导致某个业务中断（或运行效率明显下降）6小时以上。

（2）学校信息系统数据丢失或被窃取、篡改、假冒，对学院建设和公众利益构成比较严重威胁，或对学校业务工作产生比较严重影响。

（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比较严重危害。

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

4. IV级网络与信息安全事件

除以上情形外，对国家安全、社会秩序、经济建设和公众利益构成威胁和影响，但未达到III级事件标准的网络与信息安全事件为一般网络与信息安全事件（IV级）。

第五条 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、快速反应的原则。

 （一） 统一领导

 网络与信息安全事件应急工作启动、处置对策、对外联络、队伍调动、物资调配等均由网络与信息安全事件应急领导小组做出决策，各级部门必须坚决服从应急领导小组的指令。

 （二）快速反应

建立预警、应急响应和处置快速反应机制，确保各环节的衔接，做好人力、物力、财力储备，增强应急处理能力，保证一旦出现网络与信息安全事件，能够迅速启动应急处置。

第二章 组织指挥机制

第六条 应急指挥部组织机构

上海海关学院网络与信息安全应急领导小组：

 组 长：校长

 副组长：分管副校长、办公室主任、科技处处长

 组 员：科技处副处长 （主要负责校园网站信息安全）

 办公室网站管理员(上下传信息安全)

 请各部门出一名信息安全员

第七条 工作职责

（一）应急领导小组职责

组长负责批准启动应急方案，指导、协调、督促有关部门开展工作。副组长负责事件的具体指挥和处置工作。

负责研判事件具体原因，制定处置措施，承担应急指挥部下达的各项具体现场应急处置任务，及时通报事件处置情况。

（二）应急小组组员职责

负责学院网络与信息安全事件应急管理日常工作，包括履行值守应急、信息汇总和综合协调职责，负责接收和报送网络与信息安全事件信息，传达和督促落实上级处置网络与信息安全事件的决定和指示，组织制定、修订网络与信息安全事件应急预案，协调重大网络与信息安全事件的预警、应急演练、应急处置、检查评估、信息发布、应急保障和宣传培训工作。

第三章 预警机制

第八条 预防措施

科技处做好网络与信息安全事件的风险评估和隐患排查工作，制定完善相关应急预案，及时采取有效措施，避兔和减少网络与信息安全事件的发生及其危害。

第九条 预警信息来源

预警信息来源于：

 （一）国家有关部门发布通报的信息。

 （二）运行监控系统检测发现的信息。

 （三）巡检人员发现的信息。

 （四）企业维护、外包等外部人员发现并报告的信息。

 （五）其他信息。

第十条 预警分级

通过对预警信息进行分析研判，对可能发生的网络与信息安全事件及时进行预警。按照网络与信息安全事件发生的紧急程度、发展势态和可能造成的危害程度由高到低分为I级、II级、III级、IV级应急四个预警级别。

第十一条 预警通报内容

预警通报内容包括预警级别、预警信息、起始时间、可能造成的影响或危害、预防措施建议、发布范围和发布机关等。

第十二条 发布范围

学院网络与信息安全事件预警通报发布范围分为面向内部单位和面向社会公众两类。由网络与信息安全应急领导小组根据可能影响范围研究确定预警信息发布的范围或提出建议。

第十三条 发布、变更与解除

 I级、II级预警的发布，需由应急领导小组批准后，统一发布。III级、IV级预警，由科技处提出预警建议，并报应急领导小组批准后发布。

第四章 应急处置

第十四条 事件级别初步判断与核定

学院网络与信息安全事件级别由科技处进行初步判断，报请网络与信息安全事件应急领导小组核定。

第十五条 情况报告

（一） 报告程序

1. 科技处须在初步判断事件等级为I、II级网络与信息安全事件后30分钟内将有关情况向本部门领导报告，并在4小时内以书面形式上报应急领导小组。应急领导小组接报后，对I、II级事件进行级别复核，对于经复核确定的I、II级事件，应将事件情况连同初步处置意见向组长及副组长报告；对于经复核确定的I级事件，还应在4小时内将有关情况通报国家有关主管部门。

2. 对于III级事件，科技处须在初步判断事件等级后30分钟内，将有关情况向本部门领导报告，24小时内以书面形式报告领导小组。

3. IV级事件报告由科技处自行确定。

第十六条 应急响应

（一） 响应分级

对应学院网络与信息安全事件的四个等级将应急响应分为四个级别，I级、II级、III级和IV级应急响应。

根据不同事件核定级别，启动相应级别的应急响应。

（二） 启动程序

 I级应急响应启动程序如下：

1. 应急领导小组组员提出I级应急响应启动建议，报请组长批准；

2. 组长批准后，启动I级应急响应；

 3. I级应急响应启动后，应急领导小组成员首先到位，并通知副组长、成员单位负责人到指定地点就位，进入应急指挥状态；

4. I级应急响应宣布后，应急领导小组及相关成员单位应启动24小时值班制，根据职责分工开展应急工作。

 II级应急响应启动程序如下：

1. 应急指挥领导小组提出II级应急响应启动建议，报副组长批准，并同时报告组长；

2. 副组长批准后，启动II级应急响应；

3. II级应急响应宣布后，应急指挥领导小组成员首先到位，并通知成员单位负责人到指定地点就位，进入应急指挥状态；

4. II级应急响应启动后，应急领导小组及相关成员单位应保持24小时联系畅通，根据职责分工开展应急工作。

 III级、IV级应急响应，由科技处参照I级、II级应急响应程序，结合实际，自行处置。

第十七条 应急行动结束

应急领导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，可宣布应急行动结束。

I级、II级应急响应由应急领导小组决定结束。

III级和IV级应急响应由科技处决定结束。

第五章 附则

第十八条 本预案自发布之日起施行，原《上海海关学院网络与信息安全事件应急预案》（沪关院〔2009〕191号）废止。