上海市商贸旅游学校网络与信息安全应急预案

随着国际互联网的普及与发展，计算机网络在人们的工作和生活中正发挥着日益重要的作用，同时，针对计算机网络的各种攻击、入侵等各类安全事件也越来越多，为了建立健全我校校园网络与信息安全应急响应工作机制，科学应对网络与信息安全突发事件，有效预防、及时处置校园网信息网络安全事件，保障校园网作用的正常发挥，结合我校实际情况特制定本预案。

本预案适用于校园网突发网络与信息安全事件的应急处置。应急处置工作原则：统一领导、规范管理；快速反应，协同应对；预防为主，加强监控；依靠科技，资源整合。

网络与信息安全事件发现和处置主要由信息宣传中心负责，同时聘请上海心通信息技术有限公司专业技术人员专家作为顾问，协助制定应急处置方案并为应急处置过程和重建工作提供咨询和技术支持。

一、网络与信息安全事件定义

根据网络与信息安全事件的发生原因、性质和机理，网络与信息安全事件主要分为以下三类：

1．攻击类事件：指网络与信息系统因计算机病毒感染、非法入侵等造成校园网网站主页被恶意篡改、交互式栏目里发表不良信息；应用服务器（如办公系统、财务系统等）被非法入侵，应用服务器上的数据被非法拷贝、修改、删除；在网站上发布的内容违反国家的法律法规、侵犯知识版权并已造成严重后果等，由此导致的业务中断、系统宕机、网络瘫痪等情况。

2．故障类事件：指网络与信息系统因计算机软硬件故障、人为误操作等导致业务中断、系统宕机、网络瘫痪等情况。

3．灾害类事件：指因洪水、火灾、雷击、地震、台风等外力因素导致网络与信息系统损毁，造成业务中断、系统宕机、网络瘫痪等情况。

二、预防措施

1．对我校校园网络现有信息系统和今后新建设的信息系统，参照国家有关信息安全等级保护的要求，按照最终确定的保护等级采取相应的安全保障措施。

2．建设安全事件预警预报体系和校园网络管理规定，专人负责对校园网络和重点信息系统的监测、监控，加强安全管理，对可能引发网络与信息安全事件的有关信息，要认真收集、分析判断，发现有异常情况时，及时处理并逐级报告。

3．一旦发生网络与信息安全事件，立即启动应急预案，采取应急处置措施，判定事件危害程度，并立即将情况向有关领导报告，在处置过程中，应及时报告处置工作进展情况，直至处置工作结束。属于重大事件或存在非法犯罪行为的，还应向公安机关报告。

4．特殊时期，可根据学校的统一要求和部署，由信息宣传中心进行统一安排，组织专业技术人员对网络和信息数据采取加强保护措施，对网络进行不间断的监控。

三、处置程序

1．预案启动

在发生网络与信息安全事件后，信息宣传中心网络室应尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，以确定事件范围和评估事件带来的影响和损害，确认为网络与信息安全事件后，对事件进行处置和上报。

2．应急处置

初步确定应急处置方式，根据事件引发原因分为灾害类、故障或攻击类两种情况，区别对待。

灾害类：根据实际情况，在保障人身安全的前提下，首先保障数据安全，然后是设备安

全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

故障或攻击类：判断故障或攻击的来源与性质，断开影响安全与稳定的信息网络设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质分别采用以下方案：

（1）病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助，寻找并公布病毒攻击信息，以及杀毒、防御方法。

（2）外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵不成功、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 IP 地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和带来恶劣影响。

（3）内部入侵：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口。然后针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（4）网络故障：判断故障发生点和故障原因，能够迅速解决的尽快排除故障；必要时向计算机网络公司求助技术援助，并优先保证主要应用系统的运转。

（5）其它没有列出的不确定因素造成的事件，可根据总的安全原则，结合具体的情况，做出相应的处理。不能处理的及时咨询信息安全顾问。

3．应急处置后续处理

（1）在进行最初的应急处置以后，应及时采取行动，抑制安全事件影响的进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

在发生网络故障时，优先保证学校校党总支、校长室及各行政处室等要害部门的网络畅通。

（2）在事件被抑制之后，通过对有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。

（3）在确保安全事件解决后，要及时清理系统、恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

4．记录和上报

网络与信息安全事件发生时，应及时向校领导汇报，并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

5．结束响应

系统恢复运行后，信息宣传中心对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料；根据情况需要上报公安部门的由办公室协调解决。

四、保障措施

网络与信息安全应急处置是一项长期的、持续的、跟踪式的、不断发展变化的工作，是有组织的科学与社会行为，必须做好各项应急保障工作。

1．人员保障

重视信息安全队伍的建设，并不断提高工作人员的信息安全防范意识和技术水平，确保安全事件应急处置过程和重建工作中人员的在岗与战斗力。

2．技术保障

重视网络信息系统的建设和升级换代，重视网络安全整体方案的不断完善，加强技术管理，确保网络信息系统的稳定与安全，聘请信息安全技术人员为应急处置过程和重建工作提

供咨询和技术支持。

3．资金保障

信息宣传中心应根据网络与信息系统安全预防和应急处置工作的实际需要，提出本年度应急处置工作相关设备和工具软件所需经费，并上报财务处纳入年度财政预算，给予资金保障。

4．培训

举办学校教职工网络与信息安全知识培训，加强教职工和学员的计算机操作、网络和信息安全等相关知识的宣传普及，增强预防意识和简单应急处置能力。

校办公室

信息宣传中心

2015 年 1 月