上海工商外国语职业学院
网络与信息安全应急预案

一、总 则

（一）编制目的

为提高我校处置网络与信息安全突发事件的能力，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大程度地预防和减少网络与信息安全突发事件及其造成的损害，保障信息资产安全，特制定本预案。

（二）编制依据

根据《中华人民共和国计算机信息系统安全保护条例》，制定本预案。

（三）分类分级

本预案所称网络与信息安全突发事件，是指我校信息系统突然遭受不可预知外力的破坏、毁损、故障，发生对国家、社会、公众造成或者可能造成重大危害，危及公共安全的紧急事件。

1．事件分类

根据网络与信息安全突发事件的性质、机理和发生过程，网络与信息安全突发事件主要分为以下三类：

（1）自然灾害。指地震、台风、雷电、火灾、洪水等引起

的网络与信息系统的损坏。

（2）事故灾难。指电力中断、网络损坏或是软件、硬件设备故障等引起的网络与信息系统的损坏。

（3）人为破坏。指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏。

2．事件分级

根据网络与信息安全突发事件的可控性、严重程度和影响范围，一般分为四级：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）和Ⅳ级（一般）。

（1）Ⅰ级（特别重大）、Ⅱ级（重大）。重要网络与信息系统发生全局大规模瘫痪，事态发展超出我校的控制能力，需要由上级主管单位协调解决，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的信息安全突发事件。

（2）Ⅲ级（较大）。某一部分的重要网络与信息系统瘫痪，对国家安全、社会秩序、经济建设和公共利益造成一定损害，但在我校控制之内的信息安全突发事件。

（3）Ⅳ级（一般）。重要网络与信息系统使用效率上受到一定程度的损坏，对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益的信息安全突发事件。

（四）适用范围

本预案是我校网络与信息安全的专项预案，适用于本校发

生或可能导致发生网络与信息安全突发事件的应急处置工作。

（五）工作原则

1．居安思危，预防为主。立足安全防护，加强预警，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统，从预防、监控、应急处理、应急保障和打击犯罪等环节，在法律、管理、技术、人才等方面，采取多种措施，充分发挥各方面的作用，共同构筑网络与信息安全保障体系。

2．提高素质，快速反应。加强网络与信息安全科学研究和技术开发，采用先进的监测、预测、预警、预防和应急处置技术及设施，充分发挥专业人员的作用，在网络与信息安全突发事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

3．以人为本，减少损害。把保障公共利益以及公民、法人和其他组织的合法权益的安全作为首要任务，及时采取措施，最大限度地避免公共财产、信息资产遭受损失。

4．加强管理，分级负责。按照 “条块结合，以条为主”的原则，建立和完善安全责任制及联动工作机制。根据部门职能，各司其职，加强部门间协调与配合，形成合力，共同履行应急处置工作的管理职责。

5．定期演练，常备不懈。加强技术储备，规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发事件应急处置的科学化、程序化与规范化。

二、组织指挥机构与职责

（一）组织体系

网络与信息安全应急处理工作由学校党委领导，党办、院办和信息办共同负责执行。

（二）工作职责

1．研究制订我校网络与信息安全应急处置工作的规划、计划和政策，协调推进我校网络与信息安全应急机制和工作体系建设。

2．发生Ⅰ级、Ⅱ级、Ⅲ级网络与信息安全突发事件后，决定启动本预案，组织应急处置工作。如网络与信息安全突发事件属于Ⅰ级、Ⅱ级的，向教委有关部门通报并协调上级有关部门配合处理。

3．研究提出网络与信息安全应急机制建设规划，检查、指导和督促网络与信息安全应急机制建设。指导督促重要信息系统应急预案的修订和完善，检查落实预案执行情况。

4．指导应对网络与信息安全突发事件的科学研究、预案演习、宣传培训，督促应急保障体系建设。

5．及时收集网络与信息安全突发事件相关信息，分析重

要信息并提出处置建议。对可能演变为Ⅰ级、Ⅱ级、Ⅲ级的网络与信息安全突发事件，应及时向校领导提出启动本预案的建议。

6．负责提供技术咨询、技术支持，参与重要信息的研判、网络与信息安全突发事件的调查和总结评估工作，进行应急处置工作。

三、监测、预警和先期处置

（一）信息监测与报告

1．要进一步完善各重要信息系统网络与信息安全突发事件监测、预测、预警制度。按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全突发事件和可能引发网络与信息安全突发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事件时，在按规定向有关部门报告的同时，按紧急信息报送的规定及时向校领导汇报。初次报告最迟不得超过4小时，较大、重大和特别重大的网络与信息安全突发事件实行态势进程报告和日报告制度。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。

2．重要信息系统管理人员应确立2个以上的即时联系方式，避免因信息网络突发事件发生后，必要的信息通报与指挥协调通信渠道中断。

3．信息安全定期汇报。每月应向教委信息中心报告我校

网络与信息安全自查工作进展情况：

（1）恶意人士利用我校网络从事违法犯罪活动的情况。

（2）网络或信息系统通信和资源使用异常，网络和信息系统瘫痪、应用服务中断或数据篡改、丢失等情况。

（3）网络恐怖活动的嫌疑情况和预警信息。

（4）网络安全状况、安全形势分析预测等信息。

（5）其他影响网络与信息安全的信息。

（二）预警处理与预警发布

1．对于可能发生或已经发生的网络与信息安全突发事件，系统管理员应立即采取措施控制事态，并在 2 小时内进行风险评估，判定事件等级并发布预警。必要时应启动相应的预案，同时上报上级领导。

2．领导接到汇报后应立即组织现场救援，查明事件状态及原因，技术人员应及时对信息进行技术分析、研判，根据问题的性质、危害程度，提出安全警报级别。

（三）先期处置

1．当发生网络与信息安全突发事件时，及时请技术人员做好先期应急处置工作并立即采取措施控制事态，必要时采用断网、关闭服务器等方式防止事态进一步扩大，同时向上级信息安全领导小组通报。

2．相关领导在接到网络与信息安全突发事件发生或可能发生的信息后，应加强与有关方面的联系，掌握最新发展态

势。对有可能演变为III级网络与信息安全突发事件，技术人员处置工作提出建议方案，并作好启动本预案的各项准备工作。信息安全领导小组根据网络与信息安全突发事件发展态势，视情况决定现场指导、组织设备厂商或者系统开发商应急支援力量，做好应急处置工作。对有可能演变为II级或I级的网络与信息安全突发事件，要根据教委要求，上报教委有关部门，赶赴现场指挥、组织应急支援力量，积极做好应急处置工作。

四、应急处置

（一）应急指挥

1．本预案启动后，各级领导要迅速建立与现场通讯联系。抓紧收集相关信息，掌握现场处置工作状态，分析事件发展趋势，研究提出处置方案，调集和配置应急处置所需要的人、财、物等资源，统一指挥网络与信息安全应急处置工作。

2．需要成立现场指挥部的，立即在现场开设指挥部，并提供现场指挥运作的相关保障。现场指挥部要根据事件性质迅速组建各类应急工作组，开展应急处置工作。

（二）应急支援

本预案启动后，可根据事态的发展和处置工作需要，及时向上级主管单位申请增派专家小组和应急支援单位，调动必需的物资、设备，支援应急工作。参加现场处置工作的有关人员要在现场指挥部统一指挥下，协助开展处置行动。

（三）信息处理

现场信息收集、分析和上报。技术人员应对事件进行动态监测、评估，及时将事件的性质、危害程度和损失情况及处置工作等情况及时报领导小组，不得隐瞒、缓报、谎报。符合紧急信息报送规定的，属于Ⅰ级、Ⅱ级信息安全事件的，同时报教委相关网络与信息安全部门。

（四）扩大应急

经应急处置后，事态难以控制或有扩大发展趋势时，应实施扩大应急行动。要迅速召开会议，根据事态情况，研究采取有利于控制事态的非常措施，并向上级主管部门请求支援。

（五）应急结束

网络与信息安全突发事件经应急处置后，得到有效控制，将各监测统计数据报信息安全工作领导小组，提出应急结束的建议，经领导批准后实施。

五、后期处置

（一）善后处置

在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作，统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，认真制定恢复重建计划，迅速组织实施。

（二）调查和评估

在应急处置工作结束后，应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及财产损失状况和总结经验教训，写出调查评估报告。

六、应急保障

（一）通信与信息保障

相关人员应保证电话24小时开机，以确保发生信息安全事故时能及时联系到位。

（二）应急装备保障

各重要信息系统在建设系统时应事先预留出一定的应急设备，做好信息网络硬件、软件、应急救援设备等应急物资储备工作。在网络与信息安全突发事件发生时，统一调用。

（三）数据保障

重要信息系统应建立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。

（四）应急队伍保障

按照一专多能的要求建立网络与信息安全应急保障队伍。选择若干经国家有关部门资质认可的，具有管理规范、服务能力较强的企业作为我校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；必要时能够有效调动相关单位的保障力量，进行技术支援。

（五）交通运输保障

应确定网络与信息安全突发事件应急交通工具，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，统一调配。

（六）经费保障

网络与信息系统突发公共事件应急处置资金，应列入年度工作经费预算，切实予以保障。

七、监督管理

（一）宣传教育和培训

要充分利用各种传播媒介，采取多种形式，加强有关网络与信息安全突发事件应急处置的法律法规和政策的宣传，开展预防、预警、自救、互救和减灾等知识的宣讲活动，普及应急救援的基本知识，提高我校信息安全防范意识和应急处置能力。

将网络与信息安全突发事件的应急管理、工作流程等列入院系部门的培训内容，增强应急处置工作中的组织能力。加强对网络与信息安全突发事件的技术准备培训，提高工作人员的防范意识及技能。

（二）预案演练

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。

（三）责任与奖惩

要认真贯彻落实预案的各项要求与任务，建立分级布置、监督检查和奖惩机制。

八、附则

（一）预案管理与更新

本预案由实训中心制订，报校领导批准后实施。

结合信息网络快速发展的特点和我校实际状况，及时修订本预案。

（二）解释部门

本预案由实训中心负责解释。

（三）实施时间

本预案自发布之日起实施。