网络安全事件应急预案

1 总则

1.1 目的

为保证学校业务信息系统的连续性，必须有系统、有组织地作好应急预案的管理工作。尽量降低风险，减少损失，最大限度地降低网络安全事件给本学校工作所造成的影响，特制定本管理办法。

1.2 范围

本管理办法适应用于学校网络安全事件应急预案的管理和指导性意见，各业务部门可根据自身业务的特点制定本部门范围内的应急预案执行细则。

1.3 职责

应急预案组长： 袁洋

应急预案小组组长批准预案的实施与撤消及向上级相关部门的报告

应急预案副组长： 吴文龙

负责学校范围内人力、物力资源协调、组织、指导应急预案的实施。

成员：部门负责人

负责各自部门内部人员的协调、在各自熟悉领域内统一接收组长的指令，完成应急预案的实施。

1.4 定义

网络安全事件应急预案是在对各部门的全部业务处理功能的严格调查基础上，针对每项关键业务流程，受信息系统可能发生不同程度突发事件的影响，准备和实施的一套信息安全应急预案，其基本价值在于：在信息系统突发事件出现之前就已经制定相应措施，做好一定准备；一旦信息系统安全事件发生，可以提供和实施这些替代方案，以最大限度地争取时间，减少损失。

2 统一应急预案框架

2.1 应急预案故障分类

根据网络与信息安全突发事件可控性、严重程度和影响范围的不同，分为以下四级：

I 级（特别重大）：学校网络与信息系统发生瘫痪，对学校正常工作造成特别严重损害，且事态发展超出学校控制能力的安全事件；

II 级（重大）：学校网络与信息系统发生大规模瘫痪，对学校正常工作造成严重损害，事态发展超出学校单一部门自身控制能力，需学校各部门协同处置的安全事件；

III 级（较大）：学校某一区域的网络与信息系统瘫痪，对学校正常工作造成一定损害，但可自行处理的安全事件；

IV 级（一般）：某一局部网络或信息系统受到一定程度损坏，对学校某些工作有一定影响，但不危及学校整体工作的安全事件。

2.2 信息系统应急预案的启动

当各部门发现计算机访问数据库速度迟缓、不能进入相应程序、不能保存数据、不能访问网络、应用程序非连续性工作时，要立即报告。工作人员对各工作站提出的问题必须高度重视，做好记录，经核实后及时给各工作站反馈故障信息，同时召集有关人员及时进行讨论，如果故障原因明确，可以立刻恢复的，应尽快恢复工作；如故障原因不明、情况严重、不能在短期内排除的，应立即报告本学校领导，在网络不能运转的情况下由本学校领导协调学校各部门工作，以保障学校工作的正常运转。但是否启动应急预案需要参照以下描述执行：

1) 机房主服务器发生不可抗拒因素（不可预知的突发故障）导致学校信息系统停止运行 15 分钟以上时。

2) 突发供电系统大范围停电，供电系统不能及时修复，并且备用电源亦不能提供电源，造成全部电脑不能运行。

3) 遇地震、火灾、水灾等不可抗拒因素且对信息系统造成大面积影响，业务信息系统不能访问，或基础网络系统不能访问。

一旦发生上述情况之一，应迅速启动信息系统应急预案，但须遵守以下流程：第一时间汇报本学校领导，如遇夜间或节假日有关使用部门立即上报总值班，总值班通知技术人员，技术人员到场后作出初步结论，汇报本学校领导，由本学校负责人领导决定启动应急预案，并通知相关责任人。开展相应的处理，如发生不能自行处理的因素，立即通知签约的服务商、其他部门派人员到场处理。

2.3 应急预案响应办法

2.3.1 应急预案故障响应基本原则

1) IV 级故障由技术部完成应急响应工作；
2) III 级故障由信息安全领导小组牵头下，依靠学校自身信息技术人员、供应商完成应急响应；
3) I 级、II 级故障协调第三方服务机构、网络安全应急响应中心等完成应急响应；

2.3.2 III、IV 级故障的处置方法

III、IV 级故障的处置要根据网络与信息安全事件分类采取不同应急处置方式。

2.3.2.1 网络攻击事件处置：

判断攻击的来源与性质，关闭影响安全与稳定的网络设备和服务器设备，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 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。根据具体情况选择以下处置方式：

(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。对入侵未遂、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，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。

2.3.2.2 设备故障事件处置：

判断故障发生点和故障原因，迅速联系服务厂商尽快抢修故障设备，优先保证学校主干网络和主要应用系统的运转。

2.3.2.3 供电系统断电处置：

在通知供电系统进行检修的同时，随时观察注意 UPS 不间断电源的运行情况，停电时间接近 4 小时，必须停止服务器的运行。待电源恢复后，再按正常操作步骤恢复系统运行。

2.3.2.4 灾害性事件处置：

根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。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。

2.3.2.5 信息内容安全事件处置：

接到本学校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息的传播，根据网站相关日志记录查找信息发

布人并做好善后处理；对公安机关要求本学校协查的外网不良信息事件，根据上网相关记录查找信息发布人。

2.3.2.6 其它不确定安全事件处置：

可根据总的安全原则，结合具体情况，做出相应处理。不能处理的及时咨询信息安全学校或顾问。

2.4 信息系统应急预案的撤消与恢复

1) 确认学校信息系统恢复正常。
2) 信息系统正常运行 10 分钟以上，上报信息安全领导小组部，由领导小组组长批准撤消“信息系统应急预案”。
3) 在“信息系统应急预案” 撤消后 24 小时内，整理有关故障经过，填报《信息系统应急响应报告》，上报信息安全领导小组和本学校领导。

2.5 信息系统应急预案的善后

信息系统恢复正常，信息系统应急预案撤销后，信息系统预案应急小组还需要开展以下善后工作：

1) 查找事件发生原因，总结经验教训；
2) 如事件由人为引起，追究相关人员责任，如触犯法律，可直接报告公安机关处理；
3) 如事件因为管理疏忽引起，除追究当事人责任之外，还需要追究相关负责人领导责任；
4) 根据事件危害程度，在部门范围内或学校范围内就信息安全事件处理情况进行通报；
5) 如有必要，在相关部门或学校范围内开展教育培训，提高人员安全意识，杜绝类似事件发生。

3 应急预案演练

1) 应定期对应急计划中各种安全事件的应急恢复方案进行演练和测试，确保应急恢复方案的可行性和可靠性，锻炼应急恢复人员的应急响应速度和熟练程度，每次应急恢复演练和测试均应当作详细的记录。

2) 各部门负责组织编制应急预案演练指南，提出规范各类突发事件应急预案演练的组织与实施的方法，指导相关应急预案演练活动。

3) 应急预案应每年至少演练一次，信息安全领导小组开展演练评估工作，总结分析应急预案存在的问题。

4) 应急预案应列入应急知识宣教培训内容，其中涉及公众生命安全保障的部分应作为重点。各部门应制作有关应急预案宣传普及材料，并向公众免费发放。

4 应急资源保障

1) 资源保障是实现突发事件快速响应、高效处置的基础和先决条件，各部门应充分考虑日常与应急两个方面，范围包括人员、技术、联络协调、物资和资金保障等内容，涉及事前和事中环节。

2) 各部门应建立应急人员保障机制，配备足够的应急保障人员，包括落实主备岗并定期进行互换，配备专职灾备管理人员等，并通过应急培训和演练，确保应急处置人员具备应急工作必要的技术资质，提高人员应急处置的熟练度。

3) 应建立有效的技术保障机制，提高监测预警与应急处置的技术水平，应与通信运营商、重要设备服务商、系统集成服务商以及其他外包服务商签订服务水平协议,确保相关厂商应急处置过程中能够及时提供有效的技术服务支持。

4) 各部门应建立应急物资和资金保障机制，储备一定数量应急设备或物资，建立应急响应专项资金预算，保证应急储备。

5 附则

1) 在此统一应急预案框架下，各部门需要根据部门工作具体流程和特点制定本部门应急预案响应细则，并做好各方面储备。

2) 各部门应建立应急预案培训机制，就此统一应急预案框架和部门内部应急预案响应细则进行培训，至少每年要对部门信息应用人员进行一次应急预案培训。

3) 预案组对该应急预案框架应定期审查和根据实际情况更新，各部门对部门内部应急预案响应细则也应该根据业务信息系统变化定期进行审查和更新。