信息技术安全事件报告与处置流程

为加强我校网络和信息安全工作，及时掌握和处置信息技术安全事件，降低安全事件带来的损失与影响，根据国家有关法律法规和标准规范，参照教育部及公安部门有关规定，制定本流程。

第一条 适用范围。根据《信息安全技术信息安全事件分类分级指南》（GB/T20986-2007，以下简称《指南》），本流程中所称的信息技术安全事件（以下简称安全事件）是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件。涉及信息内容安全事件的报告与处置工作仍按相关规定执行。

第二条 信息技术安全事件报告与处置分为三个步骤：事发紧急报告、事件处置、事后整改报告。

（一）各单位网络信息安全管理员一旦发现发生安全事件，应根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位主要负责人及信息与教育技术中心协助处理。

（二）信息与教育技术中心接到上级有关部门安全事件通报或自主发现各单位信息系统发生安全事件后，第一时间以口头方式将相关情况通报相关单位负责人，相关单位接到通知后，应立即组织技术人员赶赴现场进行紧急处置。随后信息与教育技术中心以书面形式，将安全事件详情、要求整改内容及时限等通报给有关单位。

（三）各单位主要负责人、信息与教育技术中心根据发生安全事

件的信息系统重要程度、损失情况以及对工作和社会造成的影响判定安全事件等级。安全事件划分为四个等级：特别重大事件（Ⅰ级，如特殊敏感时期网页被篡改）、重大事件（Ⅱ级，如网页被篡改、校内重要应用系统瘫痪）、较大事件（Ⅲ级，如上级有关部门通报的安全事件）和一般事件（Ⅳ级，如自主发现系统漏洞、但尚未被利用）。对重大事件和特别重大事件，应及时上报学校网络安全和信息化领导小组，对涉及人为故意破坏事件应同时报告公安机关。

（四）事件处置过程中要及时掌握损失情况，查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为故意破坏应积极配合公安机关开展调查。

（五）事后整改报告应在安全事件处置完毕后5个工作日内，将《网络安全整改报告》及《网络安全隐患处置结果反馈表》以书面报告的形式进行报送信息与教育技术中心。相关责任单位应进一步总结事件教训，研判安全现状、排查安全隐患，加强制度建设、安全设施建设，全面提升安全防护能力。

第三条 人事变更报告。各单位负责人、网络信息安全管理员、联络方式发生变更的，应及时将变更情况报信息与教育技术中心。

第四条 相关配套机制。各单位应指定专人负责每日定时对网站、应用系统的运行情况进行检查，做到安全事件早发现、早报告、早控制、早解决。

第五条 责任追究。各单位应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况的，将对相

关单位予以通报并追究相关人员的责任。

第六条 本流程自发布之日起施行。