汕头职业技术学院网络与信息安全突发事件应急预案

（汕职院发〔2012〕24号）

## 第一章　总 则

**第一条** 为了有效预防、及时控制和最大限度地消除各类网络与信息安全事件的危害及影响，切实提高应急处理能力和水平，根据《信息安全事件管理指南》《信息安全事件分类分级指南》等规范，制定本应急预案。

**第二条** 本预案中网络与信息安全事件是指利用校园网发布不良信息，以及硬件、软件、数据因非法攻击或病毒入侵等安全原因，而遭到破坏、更改、泄露造成损失和不良影响的事件。

## 第二章　组织机构与职责

**第三条** 学院成立网络安全与信息化工作领导小组，统一领导、统一指挥网络与信息安全突发事件的应急处置工作，协调解决应急处置工作中的重大问题。

**第四条** 网络与信息中心负责学院网络安全事件的应急技术处理，并负责与上级网络信息安全主管部门的联动。

## 第三章 安全事件报告与处置流程

**第五条** 根据信息安全事件的分级考虑要素：系统的重要程度、系统损失和社会影响，将学院信息安全事件划分为三个级别：重大事件、较大事件和一般事件。

（一）重大事件（Ⅰ级）

会使重要系统遭受严重的系统损失，或产生较大的社会影响的信息安全事件。

（二）较大事件（Ⅱ级）

会使重要信息系统遭受较大的系统损失、一般系统遭受特别严重的系统损失，或产生较小不良社会影响的信息安全事件。

（三）一般事件（Ⅲ级）

会使重要信息系统遭受较小的系统损失、一般系统遭受不严重的系统损失，或不产生社会影响的信息安全事件。

**第六条** 事发紧急报告与处置

（一）各部门人员一旦发现安全事件，应根据实际情况第一时间采取断开网络连接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，并报告本部门第一安全责任人，同时将相关情况通报至网络与信息中心。

（二）网络与信息中心判定安全事件等级，Ⅱ级上报主管院领导，Ⅰ级报告上级网络信息安全主管部门，形成联动并启动应急处理机制，协助进行技术处理及取证工作。涉及人为主观破坏事件应同时报告当地公安机关。

**第七条** 事中情况报告与处置

（一）事中情况报告应在安全事件发现后3小时内，事件发生部门以书面报告的形式报送网络与信息中心。

（二）网络与信息中心视安全事件的严重性，及时向主管院领导进行汇报，Ⅱ级及以上应以书面形式报告。同时报送学院网络安全与信息化工作领导小组。

（三）网络与信息中心下达安全整改通知，事件发生部门应及时掌握损失情况、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。

**第八条** 事后整改报告与处置

（一）事后整改报告应在安全事件处置完毕后3个工作日内，以书面报告的形式报送网络与信息中心。

（二）如属Ⅱ级及以上事件网络与信息中心应以书面报告形式，将处理情况报送学院网络安全与信息化工作领导小组。

（三）事件发生部门应进一步总结事件教训，研判安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力。

（四）网络与信息中心详细填写事件处理记录，并存档。

## 第四章 应急响应程序

**第九条** 系统故障应急预案

（一）当发生系统故障时，发现人应在5分钟内通知业务部门信息安全员，由信息安全员报告部门第一安全责任人及网络与信息中心。

（二）网络与信息中心组织故障系统的信息安全员等相关部门和人员分析事件发生源头，查看安全审计日志，对异常事件发生源头、发生原因、影响范围做出判断，并及时控制事件范围，必要时停止系统运行。

（三）网络与信息中心针对事件原因查找系统漏洞，提出补救措施和系统安全策略调整方案，填写应急处置审批表，并报主管院领导审批。

（四）根据系统安全策略调整方案，对安全设备、应用系统等的安全控制策略做出相应调整，解决系统故障，确认无误后恢复系统运行。

**第十条** 网络攻击应急预案

（一）网络与信息中心根据安全设备的报警和审计日志，确定攻击目标和攻击源；

（二）通知被攻击系统管理员对攻击目标采取关闭或隔离措施，详细检查被攻击系统是否留有恶意代码，更改密码增强安全防范策略，必要时对系统和数据进行紧急备份；

（三）网络与信息中心对攻击来源进行隔离，分析原因，阻止攻击行为，调整安全防范策略；

（四）网络与信息中心在对被攻击系统进行安全评估后，恢复系统上线运行，对于恶意攻击上报公安部门。

**第十一条** 病毒爆发应急预案：

（一）网络与信息中心根据安全设备和网络杀毒软件的报警和日志，分析攻击来源，对攻击来源和攻击区域采取隔离措施。

（二）对重要的网络服务器和业务系统紧急备份，防止因病毒造成数据丢失，必要时可暂停系统运行。

（三）及时通知安全厂商、防病毒厂商，上报病毒爆发情况并寻求技术支持。获得处理建议后及时控制病毒进一步传播、升级病毒库、清除病毒。

（四）分析病毒产生原因，传播途径，采取补救措施，纠正违规行为。对恶意制造或传播病毒的情况上报有关部门。

（五）网络与信息中心、被感染系统管理员对系统进行安全评估后，确认病毒已得到控制或清除后，恢复系统运行。

**第十二条** 网络设备及应用服务器异常应急预案

（一）网络与信息中心对网络设备及应用服务器异常事件进行原因分析，及时发布信息对事件原因、处理措施及恢复时间进行通知公告。

（二）如属于硬件故障应及时启用备用设备，并将故障设备报修；如属于软件故障，应根据故障程度进行紧急调试或启用最近一次备份进行数据恢复。

## 第五章 应急预案管理

**第十三条** 应急预案培训。为确保应急预案有效运行，网络与信息中心应定期或不定期地举办不同层次、不同类型的培训班或研讨会，以便各部门的相关人员都能掌握网络信息安全应急处理的知识和技能。

**第十四条** 应急预案演练。为提高信息安全突发事件应急响应水平，网络与信息中心应每年至少组织一次预案演练；检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求。通过演练，进一步明确应急响应各岗位责任，对预案中存在的问题和不足及时完善。

**第十五条** 应急预案审查。网络与信息中心每年对应急预案进行一次审查，根据实际情况，如演练过程中出现的问题、已发生安全事件的处置措施等对内容进行更新，以使预案更贴合实际。

## 第六章　附 则

**第十六条** 本预案自发布之日起施行，由网络与信息中心负责解释。原网络与信息安全事件应急预案同时废止。