**校二级网站管理工作规范**

为了规范学校二级网站的管理，确保二级网站的信息安全，特制定本工作规范。

校内网站采取二级分级管理方式，基础网络信息安全机制与环境的建设维护由网络信息中心负责，网站内部安全漏洞主要由网站建设单位及归口部门联系制作单位处理，网站内容安全由网站管理员负责，网站运行维护按不同层次分别管理。

一、网站申请管理办法:

实行网站上线事前漏扫制度，网站上线的前一周内委托第三方进行安全技术扫描检测，对未通过检测的网站采取下线整改方式，修复后再上线运行。

二级网站域名及空间申请，通过网上协同办公系统办理，同时明确网站责任人（原则上为部门负责人）、网站管理员（网站日常内容管理员）、技术维护员（网站开发维护人员）。

二、在线运行网站内容管理办法：

（一）内容规范

网站内容管理由网站建设单位和归口部门负责，学校宣传部对网站内容实施监管；网站建设单位和归口部门采取领导责任制，由指定的信息管理人员定期扫描和梳理下属网站信息内容，自查并定期向校信息安全管理部门上报安全事件。

1．各二级网站内容要遵守有关法律法规，不得侵犯他人版权、署名权、肖像权、隐私权等合法权益

2．网站内容不能包含涉密信息。

3．网站内容要简洁流畅，文字和图片内容要清晰、健康。

4．网站应包括部门职能介绍或工作职责、部门管理制度、办事指南、机构设置、部门负责人简介、本部门工作动态和信息、公开信箱、办公联系方式等内容。

5．二级网站若在网页中引用学校基本情况方面的数据、提法、表述风格和宣传口径，必须与学院主页保持一致。

（二）典型问题与处理流程

预防为主，二级网站管理员通过ftp定期备份网站代码，保障网站数据安全。

二级网站管理员发现并报告的典型问题或事件如下：

终端用户不能通过国际互联网访问网页或程序服务器。

网页内容发生意外改变。

网页或应用行为异常。

从网页上下载的文件包含病毒。

网页或服务器不能使用。

网站被植入盗链。

典型问题或事件处理流程：

网站管理员处理事件

网址能由互联网访问？

网站服务器管理员处理事件

程序管理员处理事件

是病毒问题？

网络中心处理事件

YES

YES

YES

YES

NO

NO

NO

NO

结束

安全自查报告

网址反常？

网页的内容正常？

三、二级网站安全技术管理

服务器安全配置要求：

定期排查各网站可能存在的安全隐患，及时加固整改。

网站服务器根据其采用的操作系统、服务、数据库等不同的技术指标，通过用户权限规范配置，WEB访问的用户必须单独设置并按最低权限配置；实现目录分级授权，包含代码的目录严禁配置可写权限，可存放上传文档的目录严禁配置可执行权限，从而防范可能的木马植入和网页被非法篡改。

服务器安全管理则通过外围防火墙限制，VPN根据需求按IP地址、端口号授权，服务器自带防火墙设置访问地址限制等方式，规范服务器登录权限，防范校内服务器被恶意攻击。

本工作规范自发布之日起实施并有网络信息中心和宣传部负责解释。

宣传部 网络信息中心