

# 安徽科技学院处室函件

---

宣传〔2020〕6号

## 中共安徽科技学院委员会宣传部 安徽科技学院 网络与信息技术中心关于进一步加强网络阵地 管理工作的通知

各单位（部门）：

为进一步加强我校网络阵地管理，提高学校信息安全防护能力和水平，依据《安徽科技学院网络与信息安全管理办法》（网络〔2018〕11号）等文件规定，现就加强校园网络阵地管理、运维及网站信息审核、发布，网络群组管理等相关事宜通知如下。

### 一、提高政治站位，进一步压实网络与信息安全管理 工作责任制

要坚持用习近平新时代中国特色社会主义思想，特别是习近平总书记关于网络与信息安全工作的重要论述、批示、指示精神武装头脑、指导实践，充分认识网络与信息安全管理工作的艰巨性和复杂性，不断增强鲜明的责任意识，从思想上筑牢第一道防线。按照“谁主管谁负责，谁运维谁负责，谁使用谁

负责”的原则压实责任，明确各单位（部门）党政主要负责人为第一责任人，各单位（部门）要细化实化分管网络与信息安全管理工作的领导及网络信息管理员的具体工作职责及责任。

## 二、加强风险防范，进一步规范网站安全维护及信息审核上传工作流程

**（一）对主办的网站等信息系统开展定期检查。**一是定期开展安全性检查。各单位（部门）每季度至少进行1次安全检查，内容包括：查杀病毒，清除木马、后门等恶意程序；检查网页内容，及时清除无关网页和暗链；定期更改口令，清理不必要的管理账号，杜绝空口令和默认口令等。在技术方面需要提供支持和帮助的，可及时向网络与信息技术中心提出，必要时可在网络与信息技术中心指导下，通过购买社会服务，主动依托校外专业平台的网络监管设备和技术力量开展本单位（部门）安全检查工作。

二是强化网站信息更新工作。充分发挥校园的“窗口”作用，及时更新网站信息，除更新日常工作动态外，招生就业部门和各教学院部还要站在考生及家长的角度，及时更新诸如专业设置、师资队伍、毕业生考研及就业情况、优秀校友风采等信息。各单位（部门）每半年一次，开展对所属6个月以上未更新信息的“僵尸”网站的清理工作。

**（二）严格执行“三审三校”制度并在每一条信息中实名标注。**严格网站信息发布“三审三校”制度，自本通知印发之日起，凡在我校校园网（含二级网站）发布的信息，均须逐条

注明作者、审核领导以及网络信息管理员的姓名（作者署名原则上不超过两人。格式上采用文末标注“特约通讯员：\*\*；文：\*\*；摄影：\*\*；审核：\*\*；编辑：\*\*”的形式，若文和图为同一人，采用“特约通讯员：\*\*；文/摄影：\*\*；审核：\*\*；编辑：\*\*”的形式）。

**（三）重点审核信息中嵌入的“链接”安全性。**对拟发布在网站上的信息，除了做好文字、图片等内容的审核把关外，文中或图片中如有网址、二维码等网络链接，请务必点击查看，确认安全后，再予以上传，不能给不良网站（信息）提供任何生存空间。

**（四）定期清理过期的一般事务周知类信息。**每学期至少开展一次对过期的一般事务周知类信息的清理工作，比如一般事务性会议通知、企事业单位招聘毕业生广告等，相关信息如已经完成既定宣介功能，视情况可以卸载另行保存或直接删除；对其中含有网址、二维码等网络链接的，一律从校园网站上撤下，防止所链接的网站或信息发生改变，导致不良信息“倒灌”。

**（五）继续强化互联网群组和公众帐号申报备案工作。**各单位（部门）每年至少一次排查并据实填报30人以上（含30人）且群主为本单位（部门）师生员工的QQ群、微信群相关信息，据实填报抖音及其他等新媒体公众帐号审批（备案）信息。持续开展对全体群主及管理者的网络与信息安全教育。学校审批未通过的新媒体平台不得运行。以个人名义创建的新媒体平台，不得以“安科院\*\*\*”、“安徽科技学院\*\*\*”等学校名义运

营，且本人对所发信息负全部法律责任。

### **三、建立台账，实现本单位（部门）网络信息安全管理工 作“一本清”**

各单位（部门）要建立网络与信息安全管理专门台账，作为二级单位（部门）落实意识形态工作责任制半年报的支撑材料。

台账主要包括：

（一）本单位（部门）使用的二级域名和服务器地址审批及变更情况。

（二）本单位（部门）主管（主办）的非涉密信息系统接入校园网的审批或备案登记情况。

（三）本单位（部门）对所属网站信息系统开展安全检查中发现的问题及整改情况。

（四）本单位（部门）分管网络与信息安全管理工作的领导及网络信息管理员变更情况及工作交接详细信息。

（五）本单位（部门）有关网络与信息安全管理制度的“废、改、立”情况。

（六）其他需要记载的事项。

### **四、建立应急预案，构建网站及信息安全事件快速处理机制**

各单位（部门）如发现网站上有不良信息、网页遭篡改、网页被植入恶意代码、网站数据库被入侵、动态交互应用系统无法正常使用或用户信息被窃、服务器遭病毒或木马侵犯、网

络故障致网站无法访问以及其他严重影响网站正常运转等状况，在保存有关记录的同时，应即刻断网，并立即报告网络与信息技术中心进行处理，以防止给学校站群系统安全带来新的更大危害，相关工作要建立预案，做到安全事件早发现、早处置、早报告、早控制、早解决。

