**平顶山学院网络与信息安全责任书**

**为进一步加强学校网络与信息安全工作，提高网络和信息系统使用人员的安全保密意识，维护校园网正常运行及学校正常的教学秩序，依照国家“谁主管，谁负责”、“谁使用，谁负责”信息安全责任落实原则，建立平顶山学院网络与信息安全责任制，凡是开通网站或部署有信息系统的单位均需签订本责任书。**

**一、严格遵守《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》和《平顶山学院校园网管理制度》及其他有关法律、法规和规章制度的有关规定。**

**二、严防本单位信息系统（网站）被利用从事危害国家安全、泄露国家秘密，侵犯国家的、社会的、集体的利益和第三方合法权益等的违法犯罪活动。**

**三、严防本单位信息系统（网站）被利用制作、复制、查阅和传播不良信息。**

**四、未经学校网络管理中心授权，不得利用属于校园网的互联网站点及各种资源从事出口代理、IP地址转让经营性或非经营性活动。**

**五、定期清理部门长期不使用、不更新的“僵尸”信息系统（网站），定期删除、禁用与系统业务无关账号（如离职人员、已毕业学生等）。**

**六、信息系统（网站）的管理后台设置只能在校园网内访问，对登录管理后台的计算机设定开机密码和屏保密码，并妥善保管和定期更改密码，密码长度设置应不少于12位，至少包含字母、数字和特殊符号三种字符，信息系统（网站）需设置登录尝试次数限制。**

**七、信息系统（网站）的部署、更新、维护不能直接远程到服务器进行，如确实需要，可由管理员向网络管理中心申请远程服务，网络管理中心不直接与公司对接提供远程。**

**八、组织、建立本单位信息采集、发布操作规范，对外发布的信息必须采用二级以上的审核机制，若有留言板，留言内容需要经过部门审核才能对外发布；确保信息发布及时、准确，不得泄露国家机密和个人敏感信息（身份证号码、银行卡、家庭住址、电话号码、工号、学号、姓名等），造成严重后果的要追究相关人员责任。**

**九、当信息系统（网站）发生重大安全事故时，立即采取应急措施，保留有关原始记录，并及时向有关领导或部门报告。**

**十、根据国家有关法律，凡因渎职导致泄密、传播非法信息、破坏信息资源和网络设备、恶意攻击、制造病毒等各类案件发生的单位，应承担相应法律责任。**

**十一、本责任书自签署之日起生效。**

**信息系统（网站）名称：**

**信息系统（网站）IP：**

**信息系统（网站）域名：**

**信息系统（网站）管理员：**

**信息系统（网站）负责人：**

**信息系统（网站）责任单位：（盖章）**

**信息系统（网站）单位负责人：**

 **日期：**