西安文理学院

关于加强网络安全相关工作的通知

各部门、各学院:

为提升校园网络安全防护能力，全面加强学校的网络安全保障，防范网络安全风险，现将有关网络安全提示及要求通知如下。

一、网站、业务信息系统的使用

1.各部门学院网站、业务信息系统务必设置高强度密码，重要的业务系统，建议每三个月修改一次密码，且尽量在不同系统中使用不同的密码（使用学校统一身份认证的系统除外），并定期修改密码，防止遭遇“撞库”攻击（指通过收集某系统已泄露的用户和密码信息，批量尝试登录其他系统）。

2.不要将密码透露给他人，不要轻易信任以管理员名义发送的确认账户邮件，如遇特殊情况请通过可信的联系方式与管理员联系。

3.不使用浏览器自动密码保存功能保存网站、信息账号密码。

4.不在不安全的网络环境（如公共 wifi）下访问，网站、业务系统，尽量选择以 SSL 加密方式（以 https 开头的）进行登录，避免密码在传输时被劫持。

5.在使用网站、业务信息系统上传文件附件时，务必确保上传文档安全，不携带病毒。

6.做好个人数据备份，重要数据使用专用的备份存储介质如移动硬盘、NAS 等。

7.网站安全管理员要加强对负责运维的网站巡查，对存在的死链接、不良链接、暗链接进行集中排查、修复；对违规内容和错误表述进行更正；对存在的废弃网站，及时上报信息中心进行关停和域名注销。

二、安全使用电子邮箱

1.务必使用高强度密码，至少 8 为以上，以数字+大小写字母+特殊字符构成，避免暴力破解。

2.对收到的邮件及短信保持警惕，在不确定来源的情况下，不相信、不理会、不打开邮件或者短信内的链接，防止钓鱼邮件（短信）恶意攻击。

3.不利用邮件系统传输涉密的工作资料、信息，以及未经查实的信息。

三、LED 屏安全使用

各单位务必指定专人负责 LED 屏的使用，定期更换密码，检查病毒，删除无关文件。使用期间要做好监管巡查，避免宣传内容失控。

四、网络安全使用

1. 各部门学院要做好个人信息安全防护，严防泄露各种账号及密码；密码设置应使用大小写字母、特殊字符和数字混合的复杂密码，避免弱口令被破解，造成损失；避免多个系统使用同一个密码，建议定期对密码进行修改。

2. 在使用校园网过程中，如收到信息中心系统判断为“病毒、挖矿”等安全风险的提醒窗口，请使用正规杀毒软件对计算机进行查杀，避免造成损失。

3. 各二级单位加强对自建、自管信息系统的安全防护，深入排查问题隐患，并立即进行整改；各系统管理员保管好各自的账户和口令，不得向其他单位和个人提供，做好信息系统数据的保密措施。在重要时期，各单位非必要不对系统做重大改动，不上线新系统。

五、公共多媒体、智慧教室的使用

1. 互联网教室在使用过程中遵守学校网络安全要求，不打开、浏览与教学无关网站。

2. 学生机房网络由信息中心统一控制，上课教师申请使用网络后，在使用网络过程中上课教师要做好学生上网安全监管，出现问题由上课教师负责。

3. 教师在使用教室过程中发现问题请及时通过教室内讲桌上的 IP 电话向教室管理中心反应，争取做到发现问题能够第一时间进行响应处理。

信息与现代教育技术中心

2023 年 5 月 15 日