# 安徽科技学院处室函件

网络〔2020〕5号

## 关于开展弱密码专项治理工作的通知

各单位（部门）：

为加强网络信息安全管理及个人隐私保护，按照安徽省教育厅网络安全攻防演练工作反馈结果和我校网络安全工作总体部署，自即日起集中开展对全校各类信息系统、网站、服务器和虚拟机的管理员账户、统一身份认证账户、电子邮箱账户开展弱密码专项治理工作，避免由于弱密码被暴力破解或恶意盗取而造成的网络安全事件发生，有关要求通知如下。

一、各单位应加强对师生员工的网络安全宣传教育，尤其是所管理和负责的信息系统（网站），减少和杜绝弱密码、默认密码和通用密码的使用，养成定期更换密码的习惯，防止校园网用户的密码被恶意破解，提升学校网络信息系统的安全防护能力。

二、个人账号弱密码专项治理

师生员工须妥善保管本人的数字化校园、上网认证、电子邮箱、VPN、软件正版化平台、网站群及各类业务系统账号，加强密码复杂度设置。检查自己所属和负责的系统及账户中有无使用弱密码、默认密码和通用密码的情况，如有则必须修改，如存在使用默认密码及不符合强度要求的，请按要求即时修改。

特别提醒，各位校园网用户应妥善保管、定期更新自己的上网账号和密码，按照国家相关网络安全管理规范，实名制认证使用的各种数字资产，产生的网络安全问题，均由实名制认证的本人负责。

三、各类信息系统（网站）的弱密码专项治理

各信息系统（网站）负责人应即时对信息系统、网站和虚拟机的管理员等账号开展用户密码复杂度检查，尤其是高权限用户和管理员密码，避免账户被非法利用导致严重网络安全事件的发生，同时要求用户进行弱密码修改工作，并关闭测试账户。建议信息系统（网站）主管单位（部门）必要时要求软件提供商协助进行用户密码复杂度检查，并对弱密码、默认密码和通用密码进行强制修改，在用户管理、注册、登录、密码修改等页面处增加密码复杂度检查功能，增加用户连续登录失败后的锁定机制，从系统层面减少乃至杜绝弱密码的使用，增强系统安全性。有条件的，可考虑采用多因素验证登录方式（如密码+手机验证码等）。

学校将对重要网站和信息系统进行密码安全性检查，对于

弱密码治理不到位的，采取即刻关停措施并上报学校网络安全与信息化领导小组。

网络与信息技术中心

2020 年 12 月 23 日

安徽科技学院网络与信息技术中心　　2020 年 12 月 23 日印发