

中国矿业大学处室文件

矿大网信〔2022〕1号

关于开展信息系统账号弱密码整治工作的 通 知

各有关单位：

为加强我校信息系统网络安全防护能力，经研究决定，开展信息系统账号弱密码整治工作，对全校各类信息系统（网站）和虚拟机的管理员账号弱密码问题进行全面排查和整改，具体工作要求如下：

一、信息系统账号排查

从即日起至5月13日，各单位信息系统（网站）管理员及虚拟机负责人检查所管理的登录账号，梳理账号清单。落实账号实名制，确保账号对应到人。对无人负责的账号应及时采取停用、删除等措施，避免无人管理的账号被非法利用造成网络安全事件。

检查账号的密码强度，尤其要重点核验系统管理员和高权限用户的密码。各系统管理人员应检查所负责的信息系统（网站）和虚拟机账号中是否有弱密码、默认密码和通用密码的情况，弱密码类型说明见附件 1。

二、信息系统弱密码整改

各单位根据自查情况及信息化处下发的信息系统弱密码账号清单(附件 2)，组织弱密码整改工作。

对于本次梳理的信息系统管理员账号，各单位应参照附件 1 中的密码设置策略，统一更换不符合要求的密码，提升系统管理人员网络安全意识，减少和杜绝使用弱密码、默认密码及通用密码，建立密码定期更换机制。

对于排查出的信息系统普通用户账号弱密码问题，各单位应联系信息系统软件开发商协助设定用户密码强度检查，对存在的弱密码、默认密码和通用密码进行强制修改并及时通知相关用户，确保用户服务不中断。

三、整改反馈和持续改进

请各单位在 5 月 13 日下班前反馈整改情况，将已完成整改的信息系统管理员账号清单发送至工作联系人邮箱。各单位后续应要求所管理的信息系统（网站）软件开发商在用户管理、注册、登录及密码修改等页面增加密码强度检查功能，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，可考虑采用多因素认

证登录方式（如密码+手机验证码核验）。

网信工作领导小组办公室将根据各单位反馈情况持续进行网络安全定期复查，对重要信息系统（网站）及虚拟机进行密码安全性检查，对于弱密码整治工作不到位的，将扣减年度网络安全综治考核得分，并上报学校网络安全和信息化工作领导小组。

工作联系人：苏昕

电话：83592178 邮箱：xsu@cumt.edu.cn

附件：1. 弱密码类型提示及密码策略参考
2. 信息系统弱密码账号清单

网络安全和信息化工作领导小组办公室

2022年5月9日

中国矿业大学网络安全和信息化工作领导小组办公室 2022年5月10日印发