关于在全校开展弱密码问题专项治理工作的通知

各部门、二级学院：

根据合肥市数字资源局《关于开展弱密码问题专项治理工作的通知》，为做好迎接中国共产党成立100周年网络安全工作，增强网络安全防护能力及个人隐私保护，维护良好的网络环境，我校将于近期对全校各类信息系统（网站）、服务器（虚拟机）的管理员账号、统一身份认证账户、VPN账号、电子邮箱账户开展弱密码专项治理工作。

一、工作目标

通过本次专项治理，排查我校师生在信息系统、统一门户、电子邮箱等系统中使用弱密码、默认密码和通用密码的现象，加以整改；常态化开展网络安全宣传教育，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。

二、检查对象

1、服务器（虚拟机）的管理员账号，责任部门：自管服务器为相应服务器管理部门，托管服务器为现教中心；

2、各类信息系统的管理员账号，责任部门：各系统对应的管理部门；

3、全校师生的个人电脑登录密码、OA登录密码、统一门户、电子邮箱账户密码，责任人：全体师生。

三、工作阶段

此次集中整治工作时间4月25日至5月10日。重点排查网站、统一门户、OA、VPN、教务、学工、科研和财务等系统的管理员账号密码强度，是否存在信息泄露、内容安全等风险。

各部门和二级学院仔细梳理管理的服务器和涉及的信息系统（网站），形成清单，于4月30日前将**附件2**表格提交到现教中心汤老师邮箱（tyj@htc.edu.cn）；5月8日前各单位对管理的服务器、涉及的信息系统（网站）用户密码复杂度、最高权限用户和管理员密码开展检查，避免账户被非法利用导致严重网络安全事件发生；5月9日－5月10日，现教中心抽查各单位的信息系统和服务器，形成专项检查报告；5月11日－5月25日市数据资源局对我

校弱密码问题专项整治工作进行检查，发现弱密码治理不到位，责令关停并上报市网信办。

各单位要持续开展对教职工和学生的安全教育，加强对弱密码危害的宣传，重视弱密码等安全隐患，切实提高网络安全防范能力，有针对性地采取相应措施，常抓不懈。

四、工作要求

1、提高站位，压实责任。要充分认识弱密码专项治理工作的重要性，提前部署，集中资源，扎实细致抓好建党100周年等重要时期网络安全工作。进一步压实工作责任。认真落实网络安全总要求，紧盯关键信息基础设施、数据安全和个人信息保护等关键环节，严格制度执行，落实工作部署，构建全方位、立体化网络安全保障体系。

2、检查到位，不留死角。对本单位弱密码问题自检到位，加强所有信息系统（网站）弱密码的管理，做到不遗漏，确保基本无弱密码问题。

3、加强措施，提高能力。各单位要持续开展对师生的安全教育，加强对弱密码危害的宣传，重视弱密码等安全隐患，切实提高网络安全防范能力，有针对性地采取相应措施，常抓不懈。

附件：1、关于避免使用弱密码的安全提示

2、弱密码专项检查涉及服务器（虚拟）和信息系统统计表

现代教育技术中心

2021年4月23日

附件 1

关于避免使用弱密码的安全提示

一、什么是弱密码

弱密码(Weak passwords)即容易破译的密码，多为简单的数字组合、账号相同的数字组合、键盘上的临近键或常见姓名、终端设备出厂配置的通用密码等都属于弱密码范畴。弱密码很容易被他人猜到或破解，所以如果你使用弱密码，就像把家门钥匙放在家门口的垫子下面，这种行为是非常危险的。

二、常见弱密码

有关公司曾分析了 2018 年在互联网上泄漏的 500 多万个用户密码，最后统计出 TOP100 的结果。前 25 个最弱密码分别是：

序号	弱密码	序号	弱密码	序号	弱密码
1	123456	10	ILOVEYOU	19	654321
2	PASSWORD	11	PRINCESS	20	!@#$%八&*
3	123456789	12	ADMIN	21	CHARLIE
4	12345678	13	WELCOME	22	AA123456
5	12345	14	666666	23	DONALD
6	min	15	ABC 123	24	PAS SWORD 1
7	1234567	16	FOOTBALL	25	QWERTY123
8	SUNSHINE	17	123123		
9	QWERTY	18	MONKEY		

三、弱密码的危害

2015 年春运前夕震惊全国的 12306 数据泄露事件,传闻称黑客利用“撞库”手段获取 131653 条用户数据。通过对 网络公开的泄露数据进行分析发现，弱密码无论在任何泄密 事件中都具有举足轻重的地位，以下是安全爱好者对 12306 泄露密码的统计结果：

其中，密码中包含有 123 数字的，出现 11213 次；密码中包含有 520 数字的，

出现 4549 次；密码中包含 有 123456 数字的，出现 3236 次；密码中包含有 1314 数字 的，出现 3113 次；密码中包含有 aini 的，出现 877 次。

以上只是众所周知的帐号泄漏事件，实际弱密码的危害性比想象中要大得多，对于实体银行卡被盗，弱口令被猜测，损失大量的钱财；对于个人电脑或工业主机，弱密码意味着容易成为黑客的肉鸡，轻则成为他们进行不法行为的跳板或僵尸网络的一部分，重则电脑资料泄露，感染病毒，造成严重损失；信息系统、网站和虚拟机的管理员采用弱密码、默认密码和通用密码，或者长期不进行修改，容易被黑客使用暴力破解软件直接破解本地密码，导致服务器被黑客控制， 成为他们进行不法行为的跳板或僵尸网络的一部分，以及服务器内部资料泄露，造成群体性危害事件。

四、密码设置原则

1、不使用空密码或系统默认的密码，因为这些密码众所周知，为典型的弱密码。

2、密码长度不小于 8 位。

3、密码不应该为连续的某个字符（例如：AAAAAAAA） 或重复某些字符的组合（例如：tzf.tzf.）。

4、密码应该为以下四类字符的组合，大写字母（A-Z）、小写字母（a-z）、数字（0-9）和特殊字符。每类字符至少包含 一个。

5、密码中不应包含本人、父母、子女和配偶的姓名和出生日期、纪念日期、登录名、E-mail 地址等等与本人有关的 信息，以及字典中的单词。

6、不要长期使用固定密码，定期或者不定期修改密码，防止未被发现的入侵者继续使用该密码。

7、不要在多个场合使用同一个密码：为不同应用场合设置不同密码，特别是有关财务的网银及网购账户，避免一个帐户密码被盗，其它帐户密码也被轻易破解。

8、不把密码保存在电脑、U 盘、笔记本、书籍等上面。

五、密码设置建议

推荐使用自己喜欢的单词-喜欢的数字排列-网站名称的前三个大写字母或者后三个大写字母，也可以找到一个生僻但又容易记住的短语、句子、歌词、书名或者电影台词都可以摘录，并创建它的缩写形式，其中可包括大写字母、数字和标点符号等。

附件 2

弱密码专项检查涉及服务器（虚拟）和信息系统统计表

部门/二级学院：　　填表人：　　联系电话：　　填表日期：

序号	服务器				信息系统					当前各部门/二级学院网站		
	服务器（虚拟）名称	服务器地址	服务器管理人员	服务器管理员账号	信息系统名称	IP 地址或域名	是否外网访问	信息系统管理人员	系统管理员账号	网站地址	通讯员（新闻发布者）	网站审核人员