顺德职业技术学院文件

顺职院发〔2023〕95号

关于印发《顺德职业技术学院个人信息保护与密码管理规定》的通知

各党（群）政管理机构、教学机构、教辅机构:

《顺德职业技术学院个人信息保护与密码管理规定》已经学校研究同意，现印发给你们，请遵照执行。

附件：顺德职业技术学院个人信息保护与密码管理规定

顺德职业技术学院

2023年11月24日

顺德职业技术学院办公室　　2023年11月24日印发

附件

顺德职业技术学院个人信息保护与密码管理规定

第一章 总则

第一条 为规范顺德职业技术学院个人信息与密码的处置，明确对个人信息保护与密码工作的管理要求，避免个人信息、密码处置不当造成学校师生、人员利益受损，保障用户信息安全，优化用户体验，按照《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》及其他相关法律法规要求，特制定本规定。

第二条 本规定将详细说明系统在获取、管理及保护用户个人信息方面的政策与措施以及密码口令设立、维护等方面的管理要求。

第三条 本规定适用于学校系统向用户提供的所有服务，无论是通过计算机设备、移动终端或其他设备获得的系统相关服务。

第四条 本规定涉及的个人信息包括：基本信息（包括个人姓名、生日、性别、住址、个人电话号码、电子邮箱）；个人位置信息；网络身份标识信息（包括系统账号、IP 地址、邮箱地址及与前述有关的密码、密保）；个人上网记录（包括搜索记录、使用记录、点击记录）；个人常用设备信息（包

括硬件型号、设备MAC地址、操作系统类型）；其他用户个人信息。

第二章 职责与权限

第五条 网络安全和信息化工作管理委员会办公室（简称：信息化办公室）是履行个人信息保护、密码管理的主要职责部门，职责包括：

（一）全面负责学校系统数据安全管理工作，综合协调相关部门完成系统数据安全管理工作；

（二）落实国家及省、市、区有关个人信息保护安全、密码工作的法律法规、方针、政策、标准和规范，联系上级主管单位并落实个人信息数据的安全管理相关工作；

（三）组织制定信息系统数据安全管理规章制度和标准规范；

（四）指导、协调和检查学校各二级单位用户个人信息数据安全管理工作；

（五）负责系统数据安全一般事故的调查和处理，协助系统数据安全重大事故的调查和处理。

第六条 学校二级单位（含党（群）政管理机构、教学机构、教辅机构）是履行个人信息保护、负责管理密码工作的相关职责部门，职责包括：

（一）负责本部门系统数据安全管理工作；

（二）协助信息管理中心落实国家及省、市、区有关个人信息保护安全、密码工作的法律法规、方针、政策、标准和规范;

（三）组织制定本部门信息系统数据安全管理规章制度和标准规范;

（四）协助信息管理中心调查和处理系统数据安全事故。

第三章 管理要求

第七条 学校应严格遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》和《计算机信息网络国际联网安全保护管理办法》，接受并配合国家有关单位依法进行的监督检查。

第八条 定期对网站及应用系统管理人员进行网络信息安全培训并进行考核，使网站和应用系统相关管理人员充分认识到网络安全的重要性，严格遵守相应规章制度。

第九条 尊重并保护用户的个人隐私，除了在与用户签署的隐私保护协议和网站服务条款以及其他公布的准则规定的情况下，未经用户授权不随意公布和泄露用户个人身份信息。

第十条 对用户的个人信息严格保密，并承诺未经用户授权，不得编辑或透露其个人信息及保存在网站和应用系统中的非公开内容，但下列情况除外:

（一）违反相关法律法规或网站服务协议规定;

（二）按照主管单位的要求，有必要向相关法律部门提供备案的内容;

（三）因维护社会公众的权利、财产或人身安全的需要;

（四）被侵害的第三人提出合法的权利主张;

（五）为维护用户及社会公共利益、网站或应用系统的合法权益的需要;

（六）事先获得用户的明确授权或其它符合需要公开的相关要求。

第四章 工作过程

第十一条 用户应严格遵守系统用户账号使用登记和操作权限管理规定，并对自己的用户账号、密码妥善保管，定期或不定期修改登录密码，严格保密，严禁向他人泄露。

第十二条 每个用户都应对其账号中的所有活动和事件负全责；用户可随时改变用户的密码和图标，也可以结束旧的账号而重新申请注册一个新账号；用户若发现任何非法使用账号或安全漏洞的情况，有义务立即通告本系统的系统管理员。

第十三条 如用户不慎泄露登录账号和密码，应当及时与系统管理员联系，请求管理员及时锁定用户的操作权限，防止他人非法操作；在用户提供有效身份证明和有效凭据并审查核实后，重新设定密码恢复正常使用。

第十四条 用户可以注销系统账号，注销后系统不再收集用户个人信息；在用户注销账号之前，应验证用户个人身份、安全状态、账户密码等信息；注销账号的行为是不可逆的行为，一旦注销账号，系统应保留用户信息六个月，其后删除有关账户的一切信息，并保证这些信息不会泄露。

第十五条 用户信息在采集、存储、管理、传输、加工、销毁等环节，应采取加密技术和隔离技术进行加密和隔离，并且每天进行备份；对于匿名用户确保“前台匿名、后台实名”，在注册时与用户达成了用户隐私保护协议。

第十六条 个人信息使用时，例如个人信息展示、个人信息关联计算，应采用包括内容替换、加密脱敏等多种数据脱敏技术增强个人信息在使用中安全性。

第十七条 应设立严格的数据使用和访问制度，采用严格的数据访问权限控制和多重身份认证技术保护个人信息，避免数据被违规使用。

第十八条 通过建立数据分类分级制度、数据安全管理规范、数据安全开发规范来管理规范个人信息的存储和使用。

第十九条 应依照个人信息的不同等级存储不同期限，存储期限严格按照法律及相关法规规定，最低期限不少于 6 个月。

第五章 密码管理

第一节 账号设立要求

第二十条 系统要求

（一）顺德职业技术学院所使用的操作系统、业务系统、数据库、网络设备等均需要支持基于账号的访问控制功能;

（二）所有需要使用口令的应用软件、业务软件都需要对口令文件提供妥善的保护。

第二十一条 账号申请原则

（一）只有授权用户才可以申请系统账号;

（二）任何系统的账号设立必须按照规定的相应流程规定进行;

（三）员工申请账号前应该接受适当的培训，以确保能够正常的操作，避免对系统安全造成隐患;

（四）账号相应的权限应该以满足用户需要为原则，不得有与用户职责无关的权限;

（五）对于确因工作需要而必须申请系统账号的学校外部人员，则必须经部门领导批准，且学校正式员工作为安全责任人，如果需要接触学校秘密信息，必须通过信息管理中心技术部审批并且签署保密协议;

（六）任何系统的账号必须明确责任人，责任人必须细化到个人，不得以部门或个人组作为责任人;

（七）必须由申请人提出正式申请，需填写相关信息:

使用者的姓名、联系电话、职责（岗位）、MAC 地址、使用时间、申请使用的系统范围和权限等信息。由部门负责人审批后移交给网络安全和信息化工作管理委员会办公室审核后，下发至相应的管理员，管理员根据申请的内容进行赋权；操作完成后，系统管理员通过邮件或其他安全方式通知相关人员或部门。

第二十二条 公用账号

（一）系统应当严格限制开设公用账号，一般情况下公用账号不得具有访问保密信息和对系统写的权限；

（二）公用账号应该设立责任人，负责账号的正常使用及维护。

第二十三条 匿名账号

（一）匿名账号只被允许访问系统中可公开的且对学校有益的资源，不得访问任何内部公开及以上秘密等级的资源；

（二）对匿名用户对系统的访问必须有详细的记录。

第二节 口令设立要求

第二十四条 口令的生成

（一）系统账号分配时必须同时生成相应的口令，并且与账号一起传送给用户；

（二）用户在接受到账号和口令后，必须马上修改口令，任何时间都不得存在没有口令的账号，除非该账号已经失效；

（三）对于系统的账号验证只有口令作为证据的系统，如果账号名由确定的且公开的规则产生的，则口令不应当为公开的口令;

（四）管理员在传递账号和口令时，应当采取加密或其他安全的传输途径，以保证口令不会被中途截取。

第二十五条 口令设立的原则

（一）账号口令必须是具有足够的长度和复杂度，使口令难于被猜测;

（二）账号口令必须是在必要时间或次数内不循环使用;

（三）账号的各个口令之间应当是没有直接联系的，以保证不可有以前的口令推知现在的口令;

（四）账号的前后两个口令之间的相同部分应当尽量减少，减低由前一个口令分析出后一个口令的机会;

（五）账号的口令不应当取有意义的词语或其他符号，如使用者的姓名，生日或其它易于猜测的信息。口令避免使用以下选择:

1.亲戚、朋友、同事、单位等的名字，生日、车牌号、电话号码;

2.一串相同的数字或字母;

3.明显的键盘序列;

4.所有上面情况的逆序或前后加一个数字;

5.常见的词语或字典词语。

第二十六条 口令的最低标准

（一）普通用户口令长度不得低于 8 位，最近 3 个口令不可重复，口令中至少应包括以下三种：数字、大写字母、小写字母以及特殊字符（特殊符号举例如下：!@#$%^&*()_+|~-=\`{}[]:";'<>?,./）;

（二）管理员和超级管理员账号口令长度不得低于 9 位，最近 10 个口令不可重复，口令中必须包含字母和数字，口令中同一个符号出现不得多于 2 次，各个口令中相同位置的字符相同的不得多于 3 个,口令不得为有意义的单词或短语。

第三节 变更与取消要求

第二十七条 账号的使用

（一）任何账号的使用人只限于申请账号过程中声明的使用人使用，禁止其他人使用此账号;

（二）账号系统正式使用前，必须更改原来系统中的缺省账号的所有口令，以保证正式环境的安全;

（三）账号使用人在使用的过程中，不得使用账号访问与自己工作无关的资源。

第二十八条 账号的权限变更

（一）账号使用人在工作职责发生转变，造成现有职责与现有的在系统中的职责不同时，应当申请权限的修改；管理员发现用户具有工作不需要的权限，可以直接停止多余的权限;

（二）账号使用人在工作职责发生转变，而不再需要使

用系统资源的情况下，应当申请关闭账号；对不能关闭的账号则需要转移账号的责任人。

第二十九条 口令的修改

（一）账号的使用人应当定期修改账号口令，修改口令的间隔应小于本标准的相关规定，对于本标准没有规定的用户，其间隔应当小于 3 个月；

（二）账号用户必须在管理员要求更改口令时进行更改口令；如果用户拒绝配合，管理员可以在通知用户及其主管后，关闭用户的账号，以保证系统的安全；

（三）账号用户丢失或遗忘口令，必须通过规定的流程向管理员申请初试化口令，用户在接到回执后，应马上更改口令；

（四）账号用户要求口令修改的方式必须是可以确保用户身份的，且管理员必须有记录；

（五）管理员不可在没有用户申请的时候私自更改用户账号的口令，除非技术部门需要；

（六）系统的超级管理员账号的口令属于系统最高机密，应该严格限定使用范围；其他人员确因工作需要而使用超级管理员账号和口令的，应当向超级管理员账号和口令的责任人申请口令，并在完成操作后，由责任人更改口令。

第三十条 账号的取消

由于人事变动，账号的使用者发生岗位变动或者离职，

人事处发报人事变更讯息，通知至系统管理员所在小组。由系统管理员提出正式申请经系统所在部门领导审批后，立即进行相应的权限变动或账号回收，严格防止由于岗位变动，账号、权限没有进行变更的情况。

第四节 维护要求

第三十一条 密码口令的管理

（一）不能将密码口令以纸质介质或明文电子数据保存，不能通过电子邮件传输;

（二）不能使用缺省设置的密码;

（三）不能将密码告诉别人;

（四）如果系统的密码泄漏了，必须立即更改;

（五）不能共享超级用户的口令，使用用户组或适当的工具如 su;

（六）所有系统集成商在施工期间设立的缺省密码在系统投入使用之前都要删除;

（七）密码要以加密形式保存，加密算法强度要高，加密算法要不可逆;

（八）在输入时密码不能显示出来;

（九）系统应该强制指定密码的策略，包括密码的最短有效期、最长有效期、最短长度、复杂性等;

（十）除了系统管理员外，一般用户不能改变其它用户的口令;

（十一）如果需要特殊用户的口令（比如说 UNIX 下的 Oracle），要禁止通过该用户进行交互式登录;

（十二）强制用户在第一次登录后改变口令;

（十三）在要求较高的情况下可以使用强度更高的认证机制，例如：双因素认证;

（十四）如果可能的话，可以使用自己密码生成器帮助用户选择口令;

（十五）要定时运行密码检查器检查口令强度，对于保存机密和绝密信息的系统应该每周检查一次口令强度；其它系统应该每月检查一次。

第三十二条 信息系统用户的责任与义务

（一）所有用户有义务确保自己的口令的安全，系统账号与口令不泄漏给他人，同时避免使用弱口令;

（二）对于使用便携式计算机的用户，应设置开机 BIOS 口令;

（三）使用远程登陆的用户，确保不将口令保留在计算机上;

（四）不将信息系统中使用的账号和口令用于其他个人应用;

（五）任何人不得公开其本人或他人口令的全部或部分，除非这种行为不会影响系统账号的安全性;

（六）严禁任何人通过任何手段非法取得他人账号和口

令进入系统，对违反者应当进行严厉制裁，直至追究法律责任;

（七）任何人不得将其账号的口令告之无权使用此账号的人，如果用户此种行为导致其他人用此账号造成对学校信息系统的影响，账号持有人和造成影响的行为的实施人负有相同的责任;

（八）严禁任何人利用系统安全漏洞访问其权限之外的资源，一经发现，立即严惩。

第三十三条 系统管理员的责任与义务

（一）确保除匿名账号外，所有系统用户都必须有口令;

（二）定期审计，检查系统用户的数量和权限;

（三）确保系统和网络设备无默认账号和口令;

（四）确保关键应用服务器启用口令强制策略;

（五）对用户进行口令安全培训;

（六）建议同一个管理员在不同主机上使用不同的账号和口令。

第五节 流程管理要求

第三十四条 内部人员的信息系统账号的开户/权限变更流程

（一）首先由用户提出书面申请，详细列出所需权限，由其部门负责人审批其申请的权限是因为工作需要;

（二）如果用户申请系统规定的需要高级主管或其他部门主管审批的权限则需要其他部门或高级主管审批;

（三）如果有必要，由系统中业务部门的负责人员审批用户的要求是否合理;

（四）由安全负责人员审核其安全性，相应负责人员进行开户操作，在以上各审批人的审批环节中，如任何一个审批人不同意该申请，则退回用户的申请。

第三十五条 职责变动导致的销户流程

用户因职责变动，不再需要使用信息系统的资源，应当立即销户，学校内部人员的账号的销户流程如下:

（一）用户主管提出申请;

（二）安全控制人员审批并执行（离职人员的账号由信息处管理人员直接处理）。

第三十六条 例外情况

（一）安全管理人员在因系统安全原因或紧急情况下，在得到信息化办公室允许的情况下，不经过以上流程而执行账号操作;

（二）因系统升级或迁移等情况下，可以在得到信息化办公室认同的情况下，直接操作而不经过本流程。

第六章 附则

第三十七条 本规定由信息化办公室制定，并负责解释和修订。

第三十八条 本规定自发布之日起执行。

第三十九条 本规定未尽事宜，依照法律法规和上级文件要求确立的原则处理。