四 川 农 业 大 学

信息与教育技术中心文件

信教发〔2022〕 9 号

四川农业大学账号密码管理细则

（试行）

第一章 总 则

第一条 按照《网络安全法》《个人信息保护法》、《互联网用户账号信息管理规定》等要求，为规范学校各类信息系统个人用户、管理用户账号、密码的管理，防范个人信息、学校业务数据泄露、被篡改、信息系统被破坏等安全事件发生，保障信息系统安全运行，根据网络安全管理相关规定，结合学校实际，特制定本细则。

第二条 按照“谁使用，谁负责”的原则，账号使用人负责所申请账号的安全管理。账号使用人应确保所申请账号、密码的安全，并为使用所申请账号执行的全部操作负责。

第三条 学校上网认证、统一信息门户、电子邮箱等公用信息服务系统、各学院、各单位业务信息系统（网站）所开设的师生个人账号、一般工作人员的管理账号，服务器、业

务信息系统、数据库系统的超级管理员账号，适用本管理细则。

第二章　账号开设与授权

第四条 学校各类信息系统的账号原则使用学校统一身份认证系统进行统一接入，管理由系统的主管单位负总责，系统的运维单位具体实施。账号管理应贯穿账号申请、开设、授权、权限变更、账号冻结或注销全过程。

第五条 师生个人账号一般依本人申请而开设。对在一定范围内全员使用的业务系统，可批量开设个人账号，主管部门须采取有效手段通知到每位用户，确保其明了对相关账号应承担的安全责任。

第六条 对一般工作人员所使用的管理账号，其设置应与岗位职责相匹配，坚持最小授权原则，严格按需授权。信息系统主管部门应拟定并定期更新账号、权限划分表，明确管理账号使用人，规定操作对象范围、操作权限，并对管理账号的使用情况定期进行检查。

第七条 各业务信息系统必须明确每个账号责任人，不得开设共享账号，不得以部门或用户组作为最终责任人。

第八条 服务器、业务信息系统、数据库系统的超级管理员账号须在系统验收投入正式运行后收回，由学校正式教职工保管，不得随意交给临时人员、厂商人员使用。

第九条 在特定任务需要校外人员配合时，可开设堡垒机账号。任务完成后，系统管理员应立即收回相关账号。

第十条 单位自建信息系统确需由公司定期进行维护的，需由系统建设单位与维护公司签订保密协议，并交信息与教育技术中心备案后，申请开通期限为 6 个月的堡垒机账号，系统建设单位为账号管理责任单位。

第十一条 学校各类信息系统在建设时，原则上应与学校统一身份认证系统对接，并明确对账号认证、授权、操作日志记录的明确要求，在验收环节重点考察。系统正式运行期间，用户登录、操作日志应留存不少于 180 天。

第三章 密码管理

第十二条 在账号申请审批完成并创建后，账号使用人应对密码进行定期修改。因工作交接，管理账号需要赋予另一个人时，接管人应及时修改密码。

第十三条 一般管理用户、超级管理员密码设置应使用强密码策略。密码长度至少 8 位，其中需包括数字、小写字母、大写字母、特殊符号 4 类中至少 3 类。

第十四条 师生个人账户密码应有一定强度。密码长度至少 6 位，其中需包括数字、小写字母、大写字母、特殊符号 4 类中至少 2 类。

第十五条 师生个人账户密码分发应以点到点方式进行，禁止通过网络批量分发师生个人账户初始密码或在网站上公布初始密码生成规则。

第十六条 有初始账号、密码设置的软件系统与硬件设备，在联网前应修改系统默认密码，并禁用初始的无关账户。

第十七条 网络安全等级保护级别确定为第三级及以上的信息系统，主管部门在系统规划、建设和运行阶段，应按照国家密码应用安全性评估管理办法和相关标准，落实密码安全防护要求，并在网络安全等级测评中同步开展密码应用安全性评估。

第四章　账号注销或冻结

第十八条 以下情况下，信息系统管理员应及时注销相应账号:

1. 教职工调离、辞职、离校的，需及时到信息与教育技术中心销户。已毕业学生网络用户在毕业当年九月统一作销户处理。

2. 临时性或阶段性使用的账号，在使用时限结束后。

第十九条 以下情况下，信息系统管理员有权先行冻结用户账号，暂时禁止用户访问:

1. 账号使用者违反了信息系统有关操作规定，可能或已经给系统运行安全、数据安全带来危害。

2. 用户私自转借、转让上网账号；盗用他人账号上网；未经网络安全和信息化办公室批准，利用校园网内各级接入设备进行各类网络技术实验；从事与国家法律法规和学校有关规定相抵触的上网活动；阻挠学校有关部门就可疑事件或网络运行状况进行调查、检查。

3. 有迹象表明用户密码可能已经泄露等。

第五章　网络安全责任

第二十条 师生个人用户应及时关注个人账户的使用情况，因密码被盗用而造成的个人信息泄露、丢失、被篡改及因此造成损失或不良影响，相关责任自负。

第二十一条 各类管理用户应关注账户的使用情况、定期修改密码、应用强密码策略，因使用弱密码、默认密码，造成系统被攻击，引发系统正常运行收到影响、数据被破坏或师生个人信息泄露等网络安全事件的，应认定为责任事故，视情节轻重，按照学校相关管理办法进行追责。

第六章　附　则

第二十二条 本细则自发布之日起施行，由信息与教育技术中心负责解释和修订。

信息与教育技术中心

2022 年 4 月 26 日