防灾科技学院信息化管理中心

信息中心〔2021〕13 号

关于印发《防灾科技学院信息系统安全管理规定》的通知

学校各部门、各单位：

为加强学校信息系统安全管理，明确岗位职责，规范操作流程，维护系统正常运行，确保计算机信息系统的安全，特制定《防灾科技学院信息系统安全管理规定》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 10 月 7 日

防灾科技学院信息系统安全管理规定

第一章 总则

第一条 为加强防灾科技学院（以下简称“学院”）信息系统安全管理，明确岗位职责，规范操作流程，维护系统正常运行，确保计算机信息系统的安全，特制定本规定。

第二条 本规定适用于学院所有信息系统。

第二章 安全策略

第三条 由系统管理员根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、文件及服务的访问权限。

第四条 对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定遵循最小授权原则。

第五条 由安全管理员每月对系统进行一次漏洞扫描，及时通知系统管理员对发现的系统安全漏洞进行修补，并形成漏洞扫描报告，内容包含系统存在的漏洞、严重级别和结果处理等方面。

第六条 系统管理员应对服务器进行安全配置并安装防火墙或杀毒软件，每周对服务器系统、杀毒软件等进行一次升级和更新，并进行病毒清查，不允许下载和使用未经测试和来历不明的软件，不要随意使用U盘等移动存储介质。

第七条 任何员工不得制造或者故意输入、传播计算机病毒和其他有害数据，不得利用非法手段复制、截收、篡改计算机信息系统中的数据。

第三章　安全配置

第八条　系统安全配置由系统管理员、安全管理员负责，其余任何人不得随意更改配置。

第九条　安全配置的更改应保留相关记录，由安全审计员负责审计。

第四章　补丁管理

第十条　补丁管理原则：

及时性原则：对于必要的安全补丁的发布和安装流程，必须及时准确，把安全漏洞所造成的对信息系统的潜在威胁降到最低。

严密性原则：补丁的测试和分发流程都需要严密的计划，在保障安全行的同时不影响生产和应用系统的正常运行。

持续性原则：补丁管理工作是一个长期持续性的工作，安全管理人员应时刻跟踪厂商的补丁公告和安全公司的安全公告。

适应性原则：分场景执行安全补丁管理要求。

第十一条　各系统管理员、网络管理员、数据库管理员应确保从安全可靠的地方获取补丁程序，推荐直接从厂商网站上下载，如果补丁支持校验，必须进行安全校验，以验证补丁的可靠性，防止补丁被恶意用户篡改。

第十二条　在安装系统补丁前，首先在测试环境中测试通过，方可实施系统补丁程序的安装。严禁未经测试直接在生产系统上加载补丁。

第十三条　完成补丁测试后，所属管理员如果未发现问题，则

要根据漏洞威胁的紧急程度，与管理员制定补丁分发计划，根据实际情况在所属系统中分批安装。

第十四条 安全管理员应根据最新的补丁通告信息，指导和组织各进行安全补丁的安装工作。

第十五条 如无特殊原因，办公网环境、各的计算机应优先安装系统安全补丁安全管理员应督促本职责范围内计算机安全补丁的安装工作。

第十六条 对重要的业务系统安装系统安全补丁，系统管理员应事先做好系统和数据的备份工作，以便在补丁安装失败后可以尽快恢复系统。

第十七条 对补丁安装过程中出现且能解决的问题，尽快进行总结，以便为解决同类问题提供借鉴。

第十八条 对于一些不能解决的补丁安装问题，需采用应急方案，使用备份系统或者卸载补丁，同时需确定一个临时的解决办法消除漏洞的潜在威胁，并尽快向补丁厂商寻求技术支持。

第五章 账号安全

第十九条 用户账号的申请、删除、禁用、密码重置以及权限复审等变更须提交变更申请，审批通过后，系统管理员负责执行，相关记录保存留档。

第二十条 每半年对用户账号使用情况进行一次检查，及时禁用、删除系统中的空账号、临时账号等存在安全隐患的账号。

第二十一条 每年对用户账号权限进行一次检查，根据用户的

安全责任和工作要求对其身份以及相应的权限进行变更。

第二十二条 做好对特殊用户和用户组的管理，包括超级用户、Guest 用户、匿名用户以及系统或应用缺省帐户的安全管理。

第二十三条 多个用户不得共用同一账号访问系统。

第二十四条 用户应保管好自己的帐号和密码，严禁随意向他人泄露、借用自己的帐号和密码，严禁不以真实身份登录系统，避免在纸上记录密码，或避免将密码以明文方式记录计算机内。

第二十五条 为便于操作，系统用户划分为 5 类用户：系统运维人员使用的操作系统普通用户、操作系统管理员用户、应用使用的数据库普通用户、管理员使用的数据库普通用户、数据库特权用户；具体密码管理：每一类用户的密码应由不少于 8 位的大小写字母、数字以及标点符号等字符组成，更换周期根据用户的不同，有如下要求：

系统运维人员使用的操作系统普通用户：密码的位数不少于 8 位，由数字，字母和特殊符号组成；密码每一年更换一次。

操作系统管理员用户：密码的位数不少于 10 位，由数字，大小写字母和特殊符号组成；密码每半年更换一次。

应用使用的数据库普通用户：密码的位数不少于 10 位，由数字，大小写字母和特殊符号组成。

管理员使用的数据库普通用户：密码的位数不少于 8 位，由数字，字母和特殊符号组成；密码每一年更换一次。

数据库特权用户：密码的位数不少于 10 位，由数字，大小写

字母和特殊符号组成；密码每半年更换一次。

第二十六条 各级密码保管落实到人，密码所有人须妥善保存，各级密码不得以任何形式明文存放于可公共访问的设备中。

第二十七条 采取有效措施，保证用户密码在传输和存储时的安全，例如对密码进行加密传输和保存。

第二十八条 及时更改系统或者应用的默认厂商口令。

第二十九条 当出现以下情况时，必须立即更改密码并做好相关记录：

（一）掌握密码的网络管理人员离开岗位；

（二）因工作需要，由相关厂家或第三方公司人员使用过的帐号及密码；

（三）一旦有迹象表明密码可能被泄露。

第三十条 当发生以下情况时，系统管理员应立即取消帐号或修改账号的相应权限，并做好相关记录：

（一）帐号使用者已经离职；

（二）帐号使用者由于工作的变动不再需要访问权限；

（三）由于工作需要开通的临时帐号已到期

（四）帐号使用者违背了有关密码管理规定；

（五）发生其他情况，上级主管人员认为不应再具有访问权限的；

第三十一条 系统管理员修改帐号密码时，应提前（或同时）通知帐号使用人，以免影响其正常使用。

第三十二条 系统的超级管理员帐号的密码属于系统最高机密，应该严格限定使用范围。

第三十三条 由于工作需要，给第三方人员开通的临时帐号同样需要遵守“最小权限原则”。

第六章 日志管理

第三十四条 系统管理员对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。

第三十五条 安全审计员每月对运行日志和审计结果进行一次分析，并形成分析报告，报告内容包括帐户的连续多次登录失败、访问受限系统或文件的失败尝试、系统错误等非正常事件。

第七章 日常操作流程

第三十六条 各应用系统的操作流程由各应用系统开发厂商提供，经办公室进行确认，运维人员在日常工作中按照操作流程执行。

第八章 附则

第三十七条 本规定由信息化管理中心负责解释。

第三十八条 本规定自发布之日起生效。

附表 1

账户变更申请表

申请人姓名		**部门**		**分机**	
申请业务	□新账户申请□账户停用□账号删除□账户权限变更				
申请理由： 年　月　日					
主管领导签名： 年　月　日					
网络办公室意见： **签名：**年　月　日					
说明： **1、 申请人需严格遵守密码管理制度，保持密码复杂度，保证账号安全；** **2、 申请人不得向他人透露个人帐号信息。** 申请人签名：年　月　日					