防灾科技学院信息化管理中心

信息中心〔2021〕33 号

关于印发《防灾科技学院网络安全管理制度》的通知

学校各部门、各单位：

为提高学校信息系统网络的安全性，降低网络系统存在的安全风险，确保网络系统安全可靠地运行。特制定《防灾科技学院网络安全管理制度》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 12 月 3 日

防灾科技学院网络安全管理制度

第一章　总则

第一条 为提高学校信息系统网络的安全性,降低网络系统存在的安全风险，确保网络系统安全可靠地运行，特制定本制度。

第二条 本制度适用于学校信息系统网络安全管理。

第二章　网络设备管理

第三条 网络管理员对网络设备进行维护监控等工作。

第四条 网络设备的登录口令长度需要 8 位以上,包含三种元素，保障口令难以被破译。

第五条 网络设备当前的配置文件必须进行备份,并在计算机上保存备份文件。

第六条 网络设备的拓扑结构、IP 地址等信息文档属于机密信息，应该在一定范围内予以保密。

第七条 网络整体的拓扑结构需进行严格的规划、设计和管理，一经确定，不能轻易更改。

第八条 定期每月检查网络设备的日志，及时发现攻击行为。

第九条 网络设备的软件版本应统一升级到较新版本。

第十条 网络设备的安装、配置、变更、撤销等操作必须严格按照流程执行。

第十一条 对重要网段要进行重点保护,要使用防火墙等安全设备以及 VLAN 或其他访问控制方式与技术将重要网段与其它网

段隔离开。

第十二条 网络结构要按照分层网络设计的原则来进行规划，合理清晰的层次划分和设计，可以保证网络系统骨干稳定可靠、接入安全、便于扩充和管理、易于故障隔离和排除。

第十三条 网络管理员每月对网络的性能进行一次分析，以充分了解系统资源的运行情况及通信效率情况，提出网络优化方案。

第十四条 按照最小服务原则为每台基础网络设备进行安全配置。

第三章　用户和口令管理

第十五条 需对网络设备登录帐号设置权限级别，授权要遵循最小授权原则。

第十六条 保证用户身份标志的唯一性，即不同的个人用户必须采用不同的用户名和口令登录，并且拥有不同的权限级别，不同用户的登录操作在设备日志文件上均有记录，便于追查问题。

第十七条 网络管理员拥有网络设备的超级用户权限，网络管理员不得私开用户权限给其它人员。

第十八条 用户的口令尤其是超级用户的口令必须足够强壮，保障口令难以被破译，口令设置必须严格遵循以下原则：

（一）　密码不能设置为空，不能与用户名相同；

（二）设备终端用户密码要求在 8 位以上，应至少包含字母、数字和特殊符号，常规情况下，用户至少应每隔 90 天更改一次密码，避免再次使用旧密码或循环使用旧密码。

第四章　配置文件管理

第十九条 所有的网络配置文件需有文档记录,网络设备的配置文件需要定期每90天进行一次备份。

第二十条 网络配置信息的修改要获得信息化管理中心的批准方可进行。

第五章　日志管理

第二十一条 网络管理员必须每月查看一次所管设备的日志文件，发现异常情况要及时处理和报告信息化管理中心，尽早消除网络安全隐患。

第二十二条 网络管理员要对日志文件进行备份,日志文件保存时间应在6个月以上。

第六章　设备软件管理

第二十三条 网络设备的软件版本（IOS或VRP等）较低可能会带来安全性和稳定性方面的隐患，在设备的FLASH容量许可的情况下需统一升级到较新的版本，必要情况下可升级设备的FLASH容量。

第七章　设备登录管理

第二十四条 网络设备开启远程登陆时需限定可远程登录的主机地址范围，拒绝部分潜在的攻击者，保证网络安全。

第八章　账号管理

第二十五条 网络管理员应定期更换管理员密码,及时注销无效用户；及时发现并处理网络安全问题。

第二十六条 不允许外来人员单独接触计算机网络系统资源。

第二十七条 各用户要加强安全保密意识，注意个人 ID 及密码的保密，不得与他人共用系统的账号。

第二十八条 应用系统的应设置不同的管理员帐号(系统管理员、安全管理员和安全审计员）和普通用户帐号，并按最小授权原则为其授权；

第二十九条 由安全管理员根据业务需求和系统安全分析制定应用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，系统管理员根据制定的访问控制策略进行系统日常运维管理工作；

第三十条 安全审计员通过查看审计日志和日常监控等措施，对其它管理员帐号和普通用户帐号的行为进行审计。

第九章　附则

第三十一条 本制度的解释权归信息化管理中心。

第三十二条 本制度自发布之日起生效。

防灾科技学院信息化管理中心　　2021 年 12 月 3 日印发