成 飞 医 院

管理规章制度

医信专—021—2024

批准：张鹏

信息系统访问控制管理办法

修订记录：

序号	编号	名称	实施日期	修订内容
1	医信专—021—2017	信息系统访问控制管理办法	2017 年 5 月 4 日	新增
2	医信专—021—2022	信息系统访问控制管理办法	2022 年 4 月 19 日	修订部门名称
3	医信专—021—2024	信息系统访问控制管理办法	2024 年 7 月 16 日	更新生效日期

第一章 总 则

第一条 为加强对网络层和系统层的访问控制，对网络设备和安全专用设备，以及操作系统和数据库系统的安全配置和日常运行进行管理，保障信息网络的安全、稳定运行，特制订本制度。

第二条 本制度暂时适用于本单位的信息系统的所有网络设备和安全专用设备，以及操作系统和数据库系统的访问控制策略配置管理。

第二章 访问控制策略的制定

第三条 信息部负责访问控制策略的制定和组织实施工作，并指定网络管理员协同系统管理员、数据库管理员负责有关工作。

第四条 在制定本单位的网络访问控制策略、操作系统访问控制策略和数据库系统访问控制策略前，应掌握以下已形成文档的资料，并必须根据变化作出及时的更新：

局域网的详细网络结构；

各个业务应用系统的安全要求；

各个业务应用系统的数据流情况；

不同系统及网络之间的访问控制及数据传输要求；

各种连接的访问权限；

各个服务器系统及其承载应用服务的安全要求；

各个服务器操作系统的访问控制及安全要求；

各个服务器数据库系统的访问控制及安全要求；

各个终端计算机或各种用户群的访问控制及安全要求。

第五条 制定的访问控制策略要求体现以上文档的要求，并根据以上文档的更新作出相应的修改。制定的网络访问控制策略必须包含内部远程访问控制和外部远程访问控制两部分；制定的操作系统和数据库系统访问控制策略必须包含特权用户和普通用户两部分；还应制定对各种用户群的访问控制策略。

第六条 网络及安全专用设备访问控制。内部网络所使用的关键网络设备及安全专用设备的用户名和口令应由专人管理，并定期修改。用于管理有关设备的客户端软件应由专人管理，未经信息系统运行管理部门负责人同意，任何个人不得擅自安装或使用。

第七条 不同网络之间的访问控制。医院内部网络与外部网络应根据各个业务系统的安全要求，采用虚拟网等方式划分开不同的网络。不同网络之间应该有明确的边界，在边界应设置相应的网络安全设备，并根据不同网络的安全要求设置访问控制策略，在不同网络之间实现有效的流量和访问控制。

第八条 系统主机访问控制。系统主机操作系统和数据库系统的超级用户口令必须由专人保管、每月修改，注意保密。系统用户和一般用户的添加及权限的设定，需要按照系统运行安全管理制度要求填写《操作系统帐户授权审批表》或《数据库系统帐户授权审批表》，应经系统业务主管部门审批同意，由系统管理员统一处理，并建立用户资料档案。

第三章 访问控制策略的管理

第九条 访问控制策略的制定、修改、审批管理。策略的制定、修改应提出申请，并经信息部审批。审批同意后方可按照策略修改有关设备的配置，并要求做好相关的记录。

第十条 网络管理员、系统管理员、数据库管理员和网络安全审计员原则上要求由不同的人专职或兼职担任。

网络安全审计员负责每月检查各种设备的配置及日志纪录，确定网络管理员、系统管理员、数据库管理员完全按照经过审批的网络访问控制策略配置有关设备且没有做过不正常的修改。

第十一条 网络管理人员、系统管理员、数据库管理员和网络安全审计员应分别每季度向信息部的负责人报告有关设备的的运行情况及审计情况，以备检查。有关的文档应归档保存。

第四章 附 则

第十二条 本制度经医院党委会审议批准。

第十三条 原制度于 2024 年 7 月 15 日作废。

第十四条 本制度自 2024 年 7 月 16 日起施行。

第十五条 本制度由信息部编制并负责解释。