成 飞 医 院

管理规章制度

医信专—025—2024

批准：张鹏

城市 LED 网络安全管理制度

修订记录：

序号	编号	名称	实施日期	修订内容
1	医信专—025—2024	城市 LED 网络安全管理制度	2024 年 7 月 16 日	新增

第一章 总 则

第一条 制定目的和范围

1、为规范和加强成飞医院城市 LED 信息安全建设和管理工作，依据国家信息安全相关法律法规政策要求，结合本院实际情况，特制定本制度。

2、本制度适用于成飞医院所有 LED、显示屏、宣传电视屏等所有显示屏设备及对应的网络和设备。

3、本制度所称网络安全是指通过采取必要措施，防范对系统的攻击、侵入、干扰、破坏和非法使用以及意外事故，使系统处于稳定可靠运行的状态，以及保障系统数据的完整性、保密性、可用性。

4、本制度规范了成飞医院安全管理、数据安全管理、供应商及外部人员安全管理、通报预警与网络安全事件管理以及检查与监督等要求。

5、坚持“顶层设计、整体防护，统筹协调”原则。立足全局，从网络安全顶层视角建立安全体系全景视图，让成飞医院全体员工共同参与网络安全工作。

6、坚持“谁主管谁负责、谁建设谁负责、谁运维谁负责、谁使用谁负责”原则。医院各部门分工负责、协同配合，依据网络安全职责分工分解落实网络安全责任制。

7、坚持“突出重点、综合防控、科学发展”原则。落实网络安全等级保护制度，并在此基础上对个人敏感信息实行重点保护，防范和遏制重大网络安全风险、事件发生。

第二条　网络安全组织与职责

业务使用部门是指系统所承载业务的管理部门及相关人员，负责系统使用过程中的业务数据安全，参与系统使用过程中的网络安全事件预警工作、个人敏感信息保护工作等。

第三条 网络安全管理策略

1、系统建设及运行过程中，应该确保各相关方及参与人员了解其安全职责，并在岗位描述文件、或合同条款和条件中明确。

2、系统账户经审批才能开通。在人员岗位变更、调离时，应确保其账户权限同步变更或消除。

3、外部人员分为短期项目实施人员、现场支撑人员。需要对内部工作人员及外部人员做好标识，以方便对第三方人员的规范化管理。

4、应对系统的所有管理、运维及使用人员进行网络安全培训，提高网络风险意识。网络安全培训内容包括但不限于：认识网络信息安全的重要性、网络攻击的方式、典型案例、注意事项及应急处置方案等。

5、梳理信息资产，确保信息资产得到妥善保护，以符合信息的保密性、完整性和可用性需求；所有信息资产必须登记入册，形成资产清单，对于有形资产必须进行标识，同时资产信息应及时更新。资产清单应包括资产类型、属性、位置、备份信息和业务价值等。

6、每项信息资产在登记入册及更新时必须指定信息资产的安全责任人，信息资产的安全责任人必须负责该信息资产的安全。

7、应采取网络隔离措施，确保医院内外网物理隔离，必要业务需使用前置机访问互联网。

8、应对用户口令和权限进行严格管理，防止对系统的非授权访问；避免未授权的用户的访问，确保信息和信息处理设施的安全。

9、用户口令管理要求如下：

系统用户口令必须不得小于 8 位，且应至少包含大写字母、小写字母、数字、特殊字符中的三种；系统用户口令不能以明文的方式通过电子邮件或者其它网络传输。

10、用户权限管理要求如下：系统特权账号（例如 root）的分配和使用应是经授权的、受限的、分隔的、可控的；系统用户授权过程必须有明确的记录，便于审计；应对系统特权账号及其访问权限进行检查；应对系统用户的权限进行分级管理，并与工作的需求相互对应。

第四条 数据安全管理

1、应采取权限控制、安全加密、安全审计、数据脱敏等技术措施，确保数据在产生、收集、传输、存储、处理、销毁等全环节的安全。

2、应按照相关法律、法规，确保用户个人信息在收集、使用、保存过程中的安全。收集个人信息应取得用户或相关部门同意，不得收集与其提供的服务无关的个人信息。应加强个人敏感信息保护，宜采用加密技术确保个人敏感信息在传输、存储过程中的机密性、完整性。

3、应提供重要数据的本地数据备份与恢复功能。

4、应加强数据活动的风险监测，及时发现数据安全缺陷、漏洞等风险并采取补救措施。

5、应对收集到的个人信息数据严格保密，未经许可不得外泄或提供给第三方使用。

6、系统停止使用时，相关部门需第一时间通知到管理部门，停止相关权限的使用。

第五条 隐私数据保护

收集个人隐私数据需征得个人同意，告知其数据收集范围、使用范围，未征得个人同意，禁止未授权收集个人隐私数据，禁止将个人隐私数据分享给第三方。

第六条 终端安全管理

1、移动医护工作站使用人员不得私自更换终端及终端配件；应对终端进行妥善保管，防止丢失；禁止将终端接入其他无线网络；禁止将终端内的数据通过拍照、拷贝等方式传播到外部网络。

2、应保证只有授权的用户可以对物联网感知节点设备上的软件应用进行配置或变更;物联网感知节点连接网关设备应具备身份标识和鉴别的能力。

3、建立城市 LED 管理台账，完善各终端标识标牌，明确使用部门和管理人员

第七条 安全运维管理

1、建立日常维护操作规程和变更控制规程，规范日常运行维护

操作，严格控制和审批任何变更行为。

2、建立信息安全运维作业计划，严格执行运维作业计划，加强对设备、操作系统、数据库、应用系统的运行监控，编写日常运行维护报告。

3、增强信息系统安全配置，应开展安全评估自查工作，包括但不限于资产核查、漏洞扫描、配置核查、渗透测试、代码审计、日志分析等内容。

4、使用远程接入（VPN）进行系统运维应妥善保存账号密码，禁止将 VPN、堡垒机、系统等运维管理账号密码以明文形式存储在终端上；通过即时通讯、邮件等方式发送 VPN、堡垒机、系统等运维管理账号密码需进行加密。

第八章 安全事件管理

1、应制定安全应急预案，对成飞医院城市 LED 进行定期的应急演练并备份有记录。

2、根据信息安全事件发生的频率和影响进行分级管理。完善信息安全事件的处置、应急响应和事后分析等流程，保证对信息安全事件及时反应，保证对信息安全事件进行事后分析以改善控制措施。

第九条 安全保障策略

1、根据医院实际情况成立安全运维团队和专项负责人，负责及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报、预警和处置。

2、各有关部门需及时接收、处置来自国家、地方监管机构网络

安全预警通报信息，按规定向备案公安机关报送网络安全运行情况、隐患整改情况、网络安全事件等内容。

3、各部门在发生网络安全事件时，应严格按照安全事件应急预案进行处置，及时向医院网络安全应急小组或信息部上报，医院按上级部门要求进行逐级上报。

第十条 检查和监督

1、医院网络安全应急领导小组应定期组织开展监督检查，检查内容包括但不限于网络安全管理情况、技术防护情况、安全运营情况、城市 LED 一键式处理等。

2、针对网络安全工作不力、重大安全问题隐患久拖不改，或存在较大网络安全风险、发生重大网络安全事件的，医院党委将对相关负责人进行约谈，情节严重、或造成明显损失的，应及时上报领导小组。构成犯罪的，应交由国家有关部门依法追究其法律责任。

第二章 附 则

第十一条 本制度经医院党委会审议批准。

第十二条 本制度自 2024 年 7 月 16 日起施行。

第十三条 本制度由信息部编制并负责解释。