ICS 35.040
CCS L 80

DB34

安　徽　省　地　方　标　准

DB34/T 4304—2022

医院网络安全管理规范

Specification for hospital cybersecuriy management

2022－10－26 发布　　2022－11－26 实施

安徽省市场监督管理局　　发 布

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由安徽省公安厅提出并归口。

本文件起草单位：安徽医科大学第一附属医院、安徽医科大学第二附属医院、安徽省公安厅网络安全保卫总队、安徽省卫生健康委员会信息中心、中国科学技术大学第一附属医院（安徽省立医院）、皖南医学院弋矶山医院、蚌埠医学院第一附属医院、芜湖市第二人民医院、安徽国康网络安全测评有限公司、安徽溯源电子科技有限公司、安徽中医药大学第一附属医院、安徽省公共卫生临床中心、安徽医科大学、皖南医学院、合肥市公安局科技信息化支队、安徽医科大学附属安庆第一人民医院、宁国市公安局、太和县人民医院、上海安翼保信息技术服务有限公司、安徽上下数据科技有限公司、安徽安恒数智信息技术有限公司、绿盟科技集团股份有限公司、三六零数字安全科技集团有限公司、深信服科技股份有限公司、北京华誉维诚技术服务有限公司。

本文件主要起草人：周典、柴培钰、冯响林、徐红兵、杨波、葛伟、陶敏、徐兵、黄煜、汪涛、刘冬、杨爱民、张文雅、偶德俊、沈沛、史寿乐、黄盈中、张业睿、胡红雨、孙一鸣、徐礼理、张文修、张旸、黄电、郭伟、陈宗明、余福生、方成成、吕芳炉、陶晓东、马守宽、王彬、李善智、郑传统、戴博文、温长健。

医院网络安全管理规范

1 范围

本文件确定了医院安全运维管理的基本要求，并规定了医院网络安全运维的对象、安全事件处置和应急管理。

本文件适用于二级甲等以上医院网络安全运维工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 50348 安全技术防范技术标准

3 术语和定义

GB 50348 界定的以及下列术语和定义适用于本文件。

3.1

智能入网终端 intelligent network access terminal

可通过网络协议完成服务交互的设备。

3.2

感染监控 Infection monitoring

感染监控是指对管理对象被病毒、木马感染，对其它对象出现传染、攻击的现象进行实时监控，并生成感染事件进行管控

3.3

资源监控 Resource monitoring

资源监控是指对软硬件资源使用情况，如CPU、内存、存储、进程等进行监控，超过指定阈值生成资源事件进行管控。

4 基本要求

4.1 机构

4.1.1 应建立由医院主要负责人牵头，各部门参与的网络安全管理组织。

4.1.2 应设定网络安全的管理部门，负责医院网络安全管理最终裁决。

4.1.3 管理部门应牵头制定网络安全的各项制度，明确网络安全使用的各项流程及责任。

4.2 人员

4.2.1 应具备从事网络安全运维服务所必备的知识和技能。

4.2.2 应配备必备的系统管理员、审计管理员和网络安全管理员等。

4.2.3 应配备专职安全管理员，不可兼任。
4.2.4 应对各类人员进行网络安全意识教育和岗位技能培训，并签订保密承诺书。

4.3 经费

每年应有专门的网络安全管理的经费预算。

4.4 规划

4.4.1 对网络安全管理应制定规划，包括目标实现、人员培养、经费投入、制度完善等。
4.4.2 应根据保护对象制定安全整体规划，应包含密码技术等相关内容，并形成配套文件。
4.4.3 应组织相关部门和有关安全专家对安全整体规划及其配套文件进行论证，经过批准后方可实施。

4.5 制度

包括但不限于：
——安全策略管理制度；
——设备安全管理制度；
——机房安全管理制度；
——密码使用管理制度；
——系统变更管理规定；
——数据备份恢复管理制度；
——人事安全管理制度；
——员工培训管理程序；
——办公区域安全管理制度；
——产品采购管理制度；
——信息系统供应商管理制度；
——软件测试与验收管理制度；
——信息安全管理体系内审程序；
——安全审核和检查制度；
——应急预案管理制度；
——补丁管理程序；
——访问控制程序；
——信息资产管理办法。

5 对象

5.1 分类

分为终端、网络、数据中心和物理环境。

5.2 终端

5.2.1 准入要求

5.2.2 应建立审批机制，有明确的申请人、审批人、时间、原因等信息。
5.2.3 应建立责任追究机制，对终端的准入的申请、审核、批准等信息进行溯源。
5.2.4 应建立退出机制，对长期不活动、报废的终端进行清理。

5.2.5 应建立逃生机制，出现网络故障时，可以快速取消准入。

5.2.6 配置管理

5.2.6.1 明确终端配置的目标对象和要求。
5.2.6.2 对业务网内的智能入网终端等配置进行登记。
5.2.6.3 定期检查配置登记的结果。
5.2.6.4 定期组织评审。

5.2.7 感染监控

5.2.7.1 应对网内感染、攻击进行监测，并明确终端感染的管理目标和要求。
5.2.7.2 应对感染事件进行分析、汇总、及时处理，并做好处理记录。
5.2.7.3 应定期检查终端感染事件的处理过程，并做好检查记录。
5.2.7.4 应定期组织评审，并根据执行情况，对管理目标和要求、制度、流程等进行改进。

5.2.8 安全管控

5.2.8.1 应支持快速批量对无线网访问、内外网切换、文件访问、防火墙、策略、共享文件夹等进行安全设置。
5.2.8.2 应支持快速批量对业务、系统进行设置，设置过程和结果可追溯。
5.2.8.3 对终端主机进行定期杀毒，对长期无法杀毒的应进行跟踪处理。
5.2.8.4 定期核对、验证安装情况。

5.2.9 备份恢复管理

5.2.9.1 建立制度与流程，确定备份恢复时间，定期演练。
5.2.9.2 针对重要系统，应做用户终端系统备份、数据库备份、服务器系统备份，并定期演练。

5.3 网络

5.3.1 数据交换

5.3.1.1 应设立独立业务网络区域。
5.3.1.2 应设立独立的互联网访问区域，用于存放开通互联网访问的主机。
5.3.1.3 应通过中间业务逻辑层与业务网区域交换数据。
5.3.1.4 业务网区域与其他区域之间应设立防火墙，并定期对防火墙策略进行审核，应建立基于业务端口级别的策略。
5.3.1.5 应建立业务网区域与其他区域的文件安全传输管理渠道，对文件保存设定期限，定期审核。

5.3.2 配置要求

5.3.2.1 应明确配置的管理目标与要求，涵盖所有网络区域。
5.3.2.2 应包括基本信息、维保信息、线路关系、位置信息、相关负责人及其联系方式的配置数据库，并有明确责任人。
5.3.2.3 应定期对配置执行现场核验工作，并根据结果对记录进行更新。
5.3.2.4 应定期对配置信息的准确性、目标符合情况进行评估，并进行记录；
5.3.2.5 应定期对配置管理的制度、目标、流程、记录进行评审、改进。

5.3.3 资源监控

5.3.3.1 应对网络设备的运行占用资源进行监控，至少包括内存、CPU、速率、丢包率等信息。
5.3.3.2 监控方式、信息采集方式应采用安全可行方式。
5.3.3.3 应制定监控的目标，并明确监控参数与指标，报警事件的处理流程与响应速度的要求。
5.3.3.4 应定期检查资源监控的目标符合度，有监控遗漏的检测方式，并进行修正。
5.3.3.5 应定期对报警事件的完成情况进行检查，并进行记录、分析。
5.3.3.6 应定期对监控目标和要求进行评估、改进。

5.3.4 人工巡检

5.3.4.1 应明确巡检的目标与要求，包括巡检范围、种类、检查项等。
5.3.4.2 应明确巡检责任人，定期自动生成固定巡检任务，任务有明确的截止时间。
5.3.4.3 应对巡检结果检查、评估，对存在的问题进行整改，并保存整改记录。
5.3.4.4 应根据巡检执行情况，定期对巡检目标与要求，巡检流程进行改进，并保存记录。

5.3.5 变更要求

5.3.5.1 应建立变更分类分级要求，包括不同分类、分级变更的应急方式、审核流程、执行方式。
5.3.5.2 应明确变更责任人，审批人，执行人，相关通知人。
5.3.5.3 5 应有明确的备用方案，包括变更的作用、失败产生的影响、备用预案的作用，应对预案进行测试。
5.3.5.4 变更过程应做好记录。
5.3.5.5 应有变更后的检查方案，明确方案负责人。

5.3.6 备用与演练要求

5.3.6.1 应列出存在的故障隐患，并制定相应备用恢复方案，并定期演练。
5.3.6.2 应根据网络重要性，对关键交换、路由设备界定不同的级别。
5.3.6.3 根据级别，建立不同的备用方式，建立恢复目标与要求，并制定恢复管理流程。
5.3.6.4 建立变更分级管理，包括应急响应流程、申请审核流程、执行流程等。
5.3.6.5 应定期对故障处理事件、演练结果进行评审，并对相应的流程、方案进行改进，并记录。

5.4 数据中心

5.4.1 配置要求

5.4.1.1 应建立基于业务、对象种类的配置的管理目标与要求，包括信息完整率、准确率等要求。
5.4.1.2 应建立配置数据库，运维对象应有明确的运维责任人。
5.4.1.3 配置管理范围，应涵盖与业务相关的服务、操作系统以及所需的存储、计算等资源。
5.4.1.4 定期对配置执行现场核验，并根据结果对记录进行更新。
5.4.1.5 应定期对配置信息的准确性、目标符合情况进行评估，分析存在的问题，并进行记录。
5.4.1.6 定期对配置管理的制度、目标、流程、记录进行评审、改进。

5.4.2 资源监控

5.4.2.1 应建立监控管理目标与要求，包括监控参数与指标，报警事件的处理流程与响应速度。
5.4.2.2 应定期检查资源监控的目标符合度，有监控遗漏的检测方式，并进行修正。
5.4.2.3 应定期对报警事件的完成情况进行检查，并进行记录、分析。
5.4.2.4 应定期对监控目标和要求进行评估、改进。

5.4.3 感染监控

应符合5.2.3的要求。

5.4.4 人工巡检

5.4.4.1 应定期组织对风险点进行分析，并建立巡检的目标与要求，包括巡检范围、种类、检查项等。
5.4.4.2 应明确巡检责任人，定期自动生成固定巡检任务，任务有明确的截止时间。
5.4.4.3 巡检任务里，应明确具体巡检对象，并可以对每个巡检对象设立独立的巡检项。
5.4.4.4 应对巡检结果检查、评估，对存在的问题进行整改，并保存整改记录。
5.4.4.5 应根据巡检执行情况，定期对巡检目标与要求，巡检流程进行改进，并保存记录。

5.4.5 变更管理

5.4.5.1 应建立基于业务的变更分类分级，建立不同分类、分级变更的响应流程。
5.4.5.2 应明确变更责任人、审批人、执行人和相关通知人。
5.4.5.3 应有明细的变更步骤，每个步骤有专门的负责人。
5.4.5.4 应有明确的针对变更回撤方案，应对预案、回撤方案进行测试。
5.4.5.5 变更过程应做好记录。
5.4.5.6 应有变更后的检查方案，明确方案负责人。

5.4.6 备用与演练管理

5.4.6.1 应列出存在的故障隐患，并制定相应备用恢复方案，并定期演练。
5.4.6.2 应根据业务重要性，对关键服务、操作系统、设备等划分不同的级别。
5.4.6.3 应根据不同级别，建立不同的备用方式，建立恢复目标与要求，并制定恢复执行流程、响应要求。
5.4.6.4 应定期对恢复执行流程进行演练，并对比目标与要求，进行评价、记录。
5.4.6.5 应定期对故障处理事件、演练结果进行评审，并对相应的流程、方案进行改进。

5.5 物理环境

5.5.1 配置登记

5.5.1.1 应对机房运行的主要环境要求建立数据库，明确管理目标与要求，包括信息完整率、准确率等。
5.5.1.2 应建立配置数据库，应明确责任人。
5.5.1.3 应定期对配置执行现场核验，并根据结果对记录进行更新。
5.5.1.4 应定期对配置信息的准确性、目标符合情况进行评估，并记录。
5.5.1.5 应定期对配置管理的制度、目标、流程、记录进行评审、改进。

5.5.2 环境监控

5.5.2.1 应建立监控管理目标与要求，包括事件的处理流程与响应速度等。
5.5.2.2 应建立报警事件的响应流程，明确责任组织与人员。
5.5.2.3 应定期对报警事件的完成情况进行检查，并进行记录、评价。
5.5.2.4 应根据报警、巡检事件的处理与评价，定期对监控目标和要求进行评估、改进。

5.5.3 机房进出

5.5.3.1 针对不同类型的人员，应建立机房进出管理目标与要求。
5.5.3.2 应对人员进出情况进行记录，建立审批流程。
5.5.3.3 定期对人员进出情况进行审查，并记录所存在的问题。
5.5.3.4 根据存在的问题，对管理目标与审批流程进行改进。

5.5.4 备用与演练

5.5.4.1 应列出存在的故障隐患，并制定相应备用方案，并定期演练。
5.5.4.2 应对电源、空调，应有冗余措施。
5.5.4.3 建立恢复目标与要求，并制定恢复执行流程、响应要求。
5.5.4.4 应定期演练，并记录。
5.5.4.5 应定期对故障处理事件、演练结果进行评审，并记录。

6 安全事件处置

6.1 安全事件处置流程及要求

6.1.1 接收

6.1.1.1 设立接收报修、报警、安全事件的服务台组织、成员，明确负责人，定期排班。
6.1.1.2 应建立不同级别事件的受理与分配的制度与流程，设定专人负责事件请求的处理，应熟悉医院诊疗流程，熟悉诊疗相关法律，识别事件分类与定级。
6.1.1.3 定期对事件受理人员进行各类业务常见问题的培训。

6.1.2 执行

6.1.2.1 事件执行过程中，应及时对事件处理过程进行记录与反馈。
6.1.2.2 事件的处理过程中应根据不同级别事件制定明确的上报流程与期限管理要求，包括及时处理期限、完成期限等，并能及时提醒相关人员。
6.1.2.3 事件完成结果要有规范性要求，应有总结，宜与知识库关联。

6.1.3 评价

6.1.3.1 单体评价

应制定专家与用户评价管理制度与流程，包括但不限于：
——应制定专家、用户评价流程，应确定专家与用户评价的范围、内容、方式；
——制定专家与用户评价信息的采集、汇总、分析要求；
——专家与用户负面评价的核实、评估、处置、反馈、跟踪验证要求；
——专家与用户评价记录的保存要求。

6.1.3.2 阶段回顾性评价

应制定服务评审与改进管理制度与流程，包括但不限于：
——应制定不同事件评审的范围、内容、频度、方式；
——应明确事件的评审要求，包括服务评价的要求；
——评审结果应包括与目标的差距分析、原因分析与改进建议。

6.2 沟通协同管理

6.2.1 接收

6.2.1.1 有多种沟通渠道，包括电话、即时通讯、网站、邮箱等，根据不同级别的事件制定不同的通知策略。

6.2.1.2 应设立总服务台处理咨询、报修、投诉等事件。

6.2.2 执行

6.2.2.1 对事件的处理要及时记录进展情况，同时应及时共享、反馈给相关人员。

6.2.2.2 应建立与使用部门、软硬件供应商的快速信息化沟通、协同渠道。

6.2.2.3 应定期对使用部门进行调研，了解需求和问题。

6.2.3 评价

6.2.3.1 应针对不同级别的事件，建立沟通协同管理目标。

6.2.3.2 定期评价、改进协同管理制度与流程。

7 应急管理

7.1 应制定应急预案内容，包括但不限于启动预案的条件、明确预案要达到的目标、应急组织构成、应急资源保障、事后教育和培训等内容。

7.2 应定期进行应急预案的演练。

7.3 应定期对原有的应急预案、人员、组织等重新评估，修订完善。

参 考 文 献

[1]《中华人民共和国网络安全法》（中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议）

[2] GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》

[3] GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》