常熟市卫生健康委员会文件

常卫健规信〔2021〕1号

关于做好2021年度全市卫生健康行业网络安全重点工作的通知

各医疗卫生单位：

为做好2021年度全市卫生健康行业网络安全工作及重要时期网络安全保障工作，落实网络安全工作责任制要求，进一步提升网络与信息安全保护水平，全面提高信息系统安全防护水平与应急处置能力。现就相关工作要求如下：

一、总体要求

根据《中华人民共和国网络安全法》和《信息安全等级保护管理办法》等法律规定，认真做好网络安全等级保护工作，按照“谁主管谁负责”及属地管理原则，明确网络安全工作责任，确保做好网络安全保障工作；各单位要加强网络安全保障力度，切实做好网络安全突发事件的防范和应急处理工作，进一步提高预防和控制网络安全事件的能力和水平，确保不发生重大网络安全

事件；配合做好年度网络安全检查工作，对检查发现的问题及时整改，同时做好网络安全培训、竞赛、宣传等工作。

二、重点任务

（一）积极参与“网安2021”行动

为防范化解网络安全风险，提升网络安全综合防护能力，做好庆祝中国共产党成立100周年等重要时期网络安全保障工作，确保不发生重特大网络安全事件，省卫健委和苏州市委网信办于2021年4月起组织实施“网安2021”行动。各单位根据文件要求，认真贯彻落实“责任制督查”专项行动和“规范化检查”专项行动。

（二）重要时期网络安全保障

建党100周年及国庆期间，各单位要求加强网络安全监测、信息收集及分析研判，及时预警可能的问题和隐患。加强应急值班值守，保持通信联络畅通，及时发现和处置网络安全事件。严格落实每日网络安全情况报告制度，根据上级要求报送安全情况。

（三）卫生健康行业网络安全应急演练

苏州市卫健委将组织网络安全检查服务机构，对苏州大市范围内卫生健康系统信息化资产进行抽查评估并开展模拟渗透攻击测试。对攻破的网站进行留痕，检测卫生健康系统各单位网络安全日常管理及应急反应能力。请各单位高度重视、做好准备，在发现问题后的第一时间启动应急预案进行处置。

各单位要通过应急演练，锻炼网络安全应急队伍，积累有效应对网络安全攻击和威胁的经验，锤炼应急响应能力，进一步完

善优化网络安全应急体系，为卫生健康信息化发展提供良好的网络安全支撑。

（四）卫生健康行业网络安全检查

深入贯彻落实《网络安全法》和等级保护2.0的总要求，紧紧围绕维护网络安全的总目标，以关键信息基础设施、重要信息系统、大数据、互联网资产和重点区域、重点部位的公共场所LED电子显示屏系统等为重点检查对象，通过自查自评、现场检查、技术检测、跟踪督办、复核复测相结合的方式，摸清全市卫生健康行业关键信息基础设施、重要信息系统、大数据、互联网资产的网络安全保护状况，检测排查并督促整改网络安全漏洞隐患、风险和突出问题，不断提升卫生健康行业的网络安全防护意识和综合防护水平，切实加强网络安全监测预警、信息通报和应急处置能力，坚决防范发生重大网络安全事件事故。

自2021年4月下旬至5月底开展全市卫生健康行业网络安全检查工作，本次网络安全检查采用自查与技术检测检查相结合方式，同步进行；其中4月20日到23日进行远程扫描，4月25日至5月14日进行现场检查，在现场检查前要完成自查工作。网络信息安全检查方案和现场检查时间安排见附件1、附件2。

（五）卫生健康行业网络安全培训、竞赛

为落实《网络安全法》、网络安全工作责任制及网络信息安全等级保护制度，切实增强全市卫生健康行业网络与信息安全意识与防护能力，我委将不定期开展网络与信息安全专题培训。组织参加第四届苏州市卫生健康行业网络安全知识技能竞赛等活动。

三、工作要求

1.各单位要严格落实党委（党组）网络安全工作责任制要求，强化网络安全知识、理念、技术及防范措施的宣传引导，为卫生健康行业营造良好的网络安全环境。

2.各单位要求落实网络安全主体责任，及时开展资产普查并动态管理，发现安全漏洞并及时整改，借助技术手段强化问题和整改力度。我委将对检查中发现漏洞较多，整改不到位的单位进行重点通报。

附件：

1.2021年常熟市卫健系统网络信息安全检查方案

2.2021年常熟市卫健系统网络信息安全现场检查时间安排

常熟市卫生健康委员会

2021年4月23日

（信息公开形式：主动公开）

附件 1：

2021 年常熟市卫健系统网络信息安全检查方案

为深入贯彻落实《中华人民共和国网络安全法》和党委（党组）网络安全工作责任制有关要求，防范化解网络安全风险，提升网络安全综合防护能力，做好庆祝中国共产党成立 100 周年等重要时期网络安全保障工作，确保不发生重特大网络安全事件，特制定此方案。

一、方案概述

（一）项目目标

通过开展信息安全检查，以查促建、以查促管、以查促改、以查促防，增强安全意识，落实安全责任，分析安全风险，评估安全状况，排除安全隐患，健全管理制度，完善防护措施，来提升医疗卫生单位的安全防护能力，预防和减少网络安全事件的发生，切实保障医疗卫生单位重要网络与信息系统的安全运行。

（二）实施原则

为确保信息安全检查工作高效顺利的完成，并尽量减少安全检查对被检查系统的影响，安全检查应遵循如下原则：

1.保密原则

在安全检查过程中，需严格遵循保密原则，技术服务方与各单位签订保密协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害用户利益。

2.最小影响原则

安全检查工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响(包括系统性能明显下降、网络阻塞、服务中断等)，如无法避免，则应做出说明。

3.规范性原则

信息安全检查服务的实施必须由专业的检查服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

（三）检查标准

《信息安全技术信息风险评估规范》(GB/T20984)

《信息系统安全管理评估》(GA/T713-2007)

《信息系统安全等级保护基本要求》(GB/T22239)

《计算机机房用活动地板技术条件》(GB6650－86)

《电子信息系统机房设计规范》(GB50174-2008)

《信息安全技术信息系统物理安全技术要求》(GB/T21052-2007)

《信息安全技术信息系统等级保护安全设计技术要求》(GB/T25070-2010)

《信息安全技术信息系统安全管理要求》(GB/T20269-2006)

《信息安全技术网络基础安全技术要求》(GB/T20270-2006)

《信息安全技术信息系统安全通用技术要求》(GB/T20271-2006)

《信息安全技术操作系统安全技术要求》(GB/T20272-2006)

《信息安全技术数据库管理系统安全技术》(GB/T20273-2006)

《信息安全技术信息系统安全工程管理要求》(GB/T20282-2006)

《信息安全技术服务器安全技术要求》(GB/T21028-2007)

《信息安全技术应用软件系统安全等级保护通用技术指南》(GA/T711-2007)

《信息安全管理体系规范》（ISO/IEC 27001:2005）

《信息安全管理实施指南》（ISO/IEC 27002:2007）

二、安全检查方案

1.检查方法

现场检查采用的方法包括人员访谈、人工核查、工具检测、实地察看和文档查阅等几个方面。

人员访谈是指检查人员与各单位有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。

人工核查是根据检查记录表内容，采用上机验证的方式检查主机系统、数据库系统以及网络设备的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等）。

工具检测是利用技术工具对各单位服务器和网站进行测试，包括基于网络探测和基于主机审计的漏洞扫描、工具扫描等。

实地察看是指根据各单位实际情况，检查人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况。

文档审查是指通过检查设计资料、管理文档、运行日志、登记资料等安全技术和管理相关文档是否齐备，检查重要信息系统被测安全技术的功能、策略和机制的设置和实际运行，以及被测安全管理的策略、措施的设置和实际执行情况以及文件的完整性和这些文件之间的内部一致性。

2.检查内容

（1）信息安全组织机构设置情况

建立健全信息系统安全组织机构，重点检查网络安全主管领导、系统管理员、网络管理员、信息安全管理员岗位设置及履职情况。

（2）安全管理制度建立情况

各单位应遵守国家信息安全相关制度、标准和规范，建立、完善或修订信息安全管理制度。重点检查信息安全责任制落实及事故责任追究情况，人员、安全保密、教育培训、采购、工程实施、验收交付、服务外包等相关管理制度，网络安全经费保障情况等。

（3）技术防护情况

各单位应建立健全技术防护体系及安全防护情况。重点检查机房环境、防病毒、防攻击、防篡改、防瘫痪、防泄密措施及有效性；等级保护、风险评估等保障工作落实情况；信息技术装备国产化情况；网络边界防护措施，互联网接入安全措施，无线网络安全防护策略；操作系统、数据库、应用软件、网络设备、安全设备等安全策略配置；终端计算机、移动存储介质安全防护措施；重要数据传输、存储的安全防护措施等。

（4）应急工作情况

各单位应建立健全网络安全应急工作体系。重点检查网络安全事件应急预案制定、应急演练情况；应急技术支撑队伍、灾难备份措施建设情况；重大网络安全事件处置情况等。

（5）宣传教育与技术培训情况

各单位应每年组织全员信息安全宣传教育和培训，重点检查信息安全宣传教育和培训情况等。

（6）数据备份恢复情况

各单位应根据数据重要性，制定备份和恢复策略，重点检查数据的定期备份情况，重要业务数据和系统的硬件冗余情况，重要基础数据的异地备份情况。

3.检查流程

（1）准备阶段

检查准备阶段	
项目	**内容描述**
工作内容	1.江苏安国信准备安全检查工具 2.江苏安国信编制《安全检查计划》。 3.江苏安国信与常熟卫健委签署相关合同和保密协议
工作方式	现场沟通
工作时间	1 天
参与人员	常熟卫健委项目负责人及相关技术人员,江苏安国信检查小组及项目支持人员
阶段成果	《安全检查实施方案》

（2）远程扫描阶段

远程扫描阶段	
项目	**内容描述**
工作内容	对医疗卫生单位互联网系统进行远程安全扫描
工作方式	工具扫描
工作时间	4 月 20 日-4 月 23 日

参与人员	江苏安国信渗透测试小组
阶段成果	《远程安全评估报告》

（3）现场检查阶段

现场检查阶段	
项目	**内容描述**
工作内容	对医疗卫生单位进行安全检查
工作方式	实地查看、人工核查、工具扫描、人员访谈、安全策略文档查看
工作时间	4 月 25 日-5 月 14 日
参与人员	江苏安国信检查小组、常熟卫健委项目负责人及相关技术人员
阶段成果	《安全检查记录表》

（4）整改阶段

整改阶段	
项目	**内容描述**
工作内容	对医疗卫生单位检查发现的内容进行督促整改
工作时间	5 月 17 日-5 月 21 日
参与人员	各医院信息化运维人员
阶段成果	《整改通知书》

（5）复查阶段

复查阶段	
项目	**内容描述**
工作内容	抽查部分整改后的单位
工作方式	实地查看、人工核查、工具扫描、人员访谈、安全策略文档查看

工作时间	5 月 24 日-5 月 27 日
参与人员	江苏安国信检查小组、常熟卫健委项目负责人及相关技术人员

（6）报告编制阶段

报告编制阶段	
项目	**内容描述**
工作内容	1.对现场检查结果进行汇总，描述安全现状，分析安全问题产生的安全风险； 2.确定安全风险等级，判定可接受风险与不可接受风险； 3.根据针对不可接受的风险选择适当的处理方式及控制措施； 4.总结安全检查过程，形成信息安全检查报告。
工作时间	5 月 28 日-5 月 31 日
参与人员	江苏安国信检查小组
阶段成果	《信息安全检查报告》

4.配合检查注意事项

在本次安全检查项目中需要各单位配合的工作如下：

（1）填写并反馈网络情况调查表；

（2）提供被检查设备的资产清单；

（3）提供网络拓扑和说明；

（4）提供安全管理制度、操作规程等相关文档，并配合管理检查的访谈、检查；

（5）提供合适的会议室及办公环境供交流使用。

三、现场安全检查

1.基础检查表

（1）物理机房

序号	机房名称	物理位置	重要程度
1			
2			

（2）网络和安全设备

序号	设备名称	系统及版本	品牌及型号	用途	重要程度
1					
2					

（3）服务器

序号	设备名称	所属业务应用系统/平台名称	操作系统及版本	数据库管理系统及版本	中间件及版本	重要程度
1						
2						

（4）终端

序号	设备名称	操作系统/控制软件及版本	设备类别/用途	重要程度
1				
2				

（5）应用系统

序号	业务应用系统/平台名称	主要功能	业务应用软件及版本	开发厂商	重要程度
1					
2					

2.安全管理检查表

序号	检查指标	检查内容	权重	检查记录
1	安全策略	a）应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。	1	
2	管理制度	a）应对安全管理活动中的各类管理内容建立安全管理制度；	1	
3		b）应对管理人员或操作人员执行的日常管理操作建立操作规程；	0.7	
4		c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。	1	
5	制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；	0.7	
6		b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。	0.7	
7	评审和修订	a）应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	0.7	
8	岗位设置	a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；	1	
9		b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；	0.7	
10		c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	1	
11	人员配备	a）应配备一定数量的系统管理员、审计管理员和安全管理员等；	1	
12		b）应配备专职安全管理员，不可兼任。	1	

序号	检查指标	检查内容	权重	检查记录
13	授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；	0.7	
14		b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；	0.7	
15		c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。	1	
16	沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；	0.7	
17		b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；	0.7	
18		c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	0.7	
19	审核和检查	a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；	1	
20		b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；	1	
21		c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。	1	
22	人员录用	a）应指定或授权专门的部门或人员负责人员录用；	0.7	
23		b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；	1	
24		c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。	1	
25	人员离岗	a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；	0.7	
26		b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。	1	

序号	检查指标	检查内容	权重	检查记录
27	安全意识教育和培训	a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；	0.7	
28		b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；	1	
29		c）应定期对不同岗位的人员进行技能考核。	1	
30	外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；	0.7	
31		b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；	1	
32		c）外部人员离场后应及时清除其所有的访问权限；	1	
33		d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。	1	
34	定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	0.7	
35		b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	1	
36		c）应保证定级结果经过相关部门的批准；	1	
37		d）应将备案材料报主管部门和相应公安机关备案。	1	
38	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	0.7	
39		b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；	1	
40		c）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的合理性和正确性进行论证和审定，经过批准后才能正式实施。	1	

序号	检查指标	检查内容	权重	检查记录
41	产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定；	1	
42		b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；	1	
43		c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	1	
44	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	1	
45		b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；	1	
46		c）应制定代码编写安全规范，要求开发人员参照规范编写代码；	1	
47		d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制；	1	
48		e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；	1	
49		f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；	1	
50		g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。	1	
51	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；	1	
52		b）应保证开发单位提供软件设计文档和使用指南；	0.7	
53		c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。	1	
54	工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	0.7	
55		b）应制定安全工程实施方案控制工程实施过程；	0.7	
56		c）应通过第三方工程监理控制项目的实施过程。	1	
57	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	0.7	
58		b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。	1	

序号	检查指标	检查内容	权重	检查记录
59	系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	0.7	
60		b）应对负责运行维护的技术人员进行相应的技能培训；	0.7	
61		c）应提供建设过程文档和运行维护文档。	0.7	
62	等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；	1	
63		b）应在发生重大变更或级别发生变化时进行等级测评；	1	
64		c）应确保测评机构的选择符合国家有关规定。	1	
65	服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；	1	
66		b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；	0.7	
67		c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。	1	
68	环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；	0.7	
69		b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；	0.7	
70		c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	0.7	
71	资产管理	a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；	0.7	
72		b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；	1	
73		c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	1	

序号	检查指标	检查内容	权重	检查记录
74	介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；	0.7	
75		b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。	0.7	
76	设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；	0.7	
77		b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；	0.7	
78		c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；	1	
79		d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。	1	
80	漏洞和风险管理	a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；	1	
81		b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。	1	
82	网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；	0.7	
83		b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；	0.7	
84		c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；	1	
85		d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；	1	
86		e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；	0.7	

序号	检查指标	检查内容	权重	检查记录
87	网络和系统安全管理	f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；	1	
88		g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；	1	
89		h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；	1	
90		i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；	1	
91		j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。	1	
92	恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；	0.7	
93		b）应定期验证防范恶意代码攻击的技术措施的有效性。	0.7	
94	配置管理	a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；	1	
95		b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。	1	
96	密码管理	a）应遵循密码相关国家标准和行业标准；	1	
97		b）应使用国家密码管理主管部门认证核准的密码技术和产品。	1	
98	变更管理	a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；	0.7	
99		b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；	1	

序号	检查指标	检查内容	权重	检查记录
100	变更管理	c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	1	
101	备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；	0.7	
102		b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；	0.7	
103		c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。	1	
104	安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；	0.7	
105		b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；	1	
106		c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；	1	
107		d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。	1	
108	应急预案管理	a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；	1	
109		b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；	1	
110		c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；	1	
111		d）应定期对原有的应急预案重新评估，修订完善。	1	
112	外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定；	1	
113		b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；	1	
114		c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；	1	

序号	检查指标	检查内容	权重	检查记录
115	外包运维管理	d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。	1	

3.安全技术检查表

序号	检查指标	检查内容	权重	检查记录
1	物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；	0.7	
2		b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	0.7	
3	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。	1	
4	防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；	0.7	
5		b) 应将通信线缆铺设在隐蔽安全处；	0.7	
6		c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。	1	
7	防雷击	a) 应将各类机柜、设施和设备等通过接地系统安全接地；	0.7	
8		b) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。	1	
9	防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	1	
10		b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；	0.7	
11		c) 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。	1	
12	防水和防潮	a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	1	
13		b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；	0.7	
14		c) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。	1	
15	防静电	a) 应采用防静电地板或地面并采用必要的接地防静电措施；	0.7	
16		b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。	1	

序号	检查指标	检查内容	权重	检查记录
17	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	1	
18	电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；	0.7	
19		b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；	1	
20		c）应设置冗余或并行的电力电缆线路为计算机系统供电。	1	
21	电磁防护	a）电源线和通信线缆应隔离铺设，避免互相干扰；	0.7	
22		b）应对关键设备实施电磁屏蔽。	1	
23	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要；	0.7	
24		b）应保证网络各个部分的带宽满足业务高峰期需要；	0.7	
25		c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	1	
26		d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；	1	
27		e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。	1	
28	通信传输	a）应采用校验技术或密码技术保证通信过程中数据的完整性；	0.7	
29		b）应采用密码技术保证通信过程中数据的保密性。	1	
30	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	0.4	
31	边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；	1	
32		b）应能够对非授权设备私自联到内部网络的行为进行检查或限制；	1	
33		c）应能够对内部用户非授权联到外部网络的行为进行检查或限制；	1	
34		d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。	1	

序号	检查指标	检查内容	权重	检查记录
35	访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	1	
36		b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	0.7	
37		c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	0.7	
38		d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；	0.7	
39		e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	1	
40	入侵防范	a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；	1	
41		b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；	1	
42		c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；	1	
43		d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。	1	
44	恶意代码和垃圾邮件防范	a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；	1	
45		b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	1	
46	安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	0.7	
47		b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	0.7	
48		c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	0.7	
49		d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	1	

序号	检查指标	检查内容	权重	检查记录
50	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	0.4	
51	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	1	
52		b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	0.7	
53		c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	1	
54		d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	1	
55	访问控制	a）应对登录的用户分配账户和权限；	1	
56		b）应重命名或删除默认账户，修改默认账户的默认口令；	1	
57		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	0.7	
58		d）应授予管理用户所需的最小权限，实现管理用户的权限分离；	1	
59		e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；	1	
60		f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	1	
61		g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	1	
62	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	1	
63		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	0.7	
64		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	0.7	
65		d）应对审计进程进行保护，防止未经授权的中断。	1	

序号	检查指标	检查内容	权重	检查记录
66	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	0.7	
67		b）应关闭不需要的系统服务、默认共享和高危端口；	1	
68		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	0.7	
69		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	1	
70		e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	1	
71		f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	1	
72	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	1	
73	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	0.4	
74	数据完整性	a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；	0.7	
75		b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1	
76	数据保密性	a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	1	
77		b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	1	
78	数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	1	

序号	检查指标	检查内容	权重	检查记录
79	数据备份恢复	b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	0.7	
80		c）应提供重要数据处理系统的热冗余，保证系统的高可用性。	1	
81	剩余信息保护	a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；	0.7	
82		b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。	1	
83	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	1	
84		b）应禁止未授权访问和非法使用用户个人信息。	1	
85	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	1	
86		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	0.7	
87	审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	1	
88		b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	0.7	
89	安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；	1	
90		b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	1	
91	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；	1	
92		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；	1	
93		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；	1	
94		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；	1	

序号	检查指标	检查内容	权重	检查记录
95	集中管控	e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；	1	
96		f）应能对网络中发生的各类安全事件进行识别、报警和分析。	1	

4.LED 显示安全检查表

序号	检查指标	检查内容	权重	检查记录
LED 显示后台操作系统	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	1	
		b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	0.7	
		c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	1	
		d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	1	
	访问控制	a）应对登录的用户分配账户和权限；	1	
		b）应重命名或删除默认账户，修改默认账户的默认口令；	1	
		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	0.7	
		d）应授予管理用户所需的最小权限，实现管理用户的权限分离；	1	
		e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；	1	
		f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	1	
		g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	1	

序号	检查指标	检查内容	权重	检查记录
	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	1	
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	0.7	
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	0.7	
		d）应对审计进程进行保护，防止未经授权的中断。	1	
	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	0.7	
		b）应关闭不需要的系统服务、默认共享和高危端口；	1	
		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	0.7	
		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	1	
		e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	1	
		f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	1	
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	1	
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	0.4	

序号	检查指标	检查内容	权重	检查记录
	数据完整性	a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；	0.7	
		b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1	
	数据保密性	a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	1	
		b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	1	
	数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	1	
		b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	0.7	
		c）应提供重要数据处理系统的热冗余，保证系统的高可用性。	1	

5.网络结构检查

《网络拓扑图》

网络结构存在的风险点：是否在出口部署访问控制设备、是否有恶意代码防范以及入侵防范功能，边界防护是否到位等。

四、无线安全检查

无线安全检查内容：

1.检查是否采用鉴权机制保证非法用户的识别和合法用户的正确接入；

2.检查是否采用加密机制保证合法用户的通信不受到非法的窃听、篡改或其它攻击手段的侵害。

3.检查无线接入接入加密方式是否安全。

4.检查是否建立 MAC 地址黑白名单限制访问。

5.检查是否部署上网行为管理，并且配置安全策略。

6.检查是否对上网的用户进行审计。根据公安要求日志保留 60 天以上。

7.检查内部使用无线与外部使用无线是否隔离。

五、漏洞扫描

1.主机漏洞扫描：通过扫描设备接入网络扫描主机是否存在漏洞。

2.弱密码漏洞扫描：通过扫描设备接入网络扫描网络是否存在弱密码显现。

3.通过扫描设备接入网络检测 SQL 注入、跨站脚本、文件上传、代码执行、越权、信息泄露等各类型的 web 漏洞、主机漏洞、web 服务器漏洞、CVE 编号漏洞。

附件 2：

2021 年常熟市卫健系统网络信息安全现场检查时间安排

本次网络信息安全现场检查工作分 2 组开展，共安排 4 个工程师，从 4 月 25 日开始到各医疗卫生单位进行现场安全检查，具体分组和时间安排如下：

第一组：

序号	被检查单位	检查周期	具体时间
1	常熟市卫生监督所	0.5 天	4 月 25 日
2	常熟市妇幼保健院（妇保计生中心）	0.5 天	4 月 25 日
3	常熟市中医院	1 天	4 月 26 日
4	常熟市第一人民医院	1 天	4 月 27 日
5	常熟市血站	0.5 天	4 月 28 日
6	常熟市梅李人民医院	0.5 天	4 月 28 日
7	常熟市梅李人民医院珍门分院	0.5 天	4 月 29 日
8	常熟市梅李人民医院赵市分院	0.5 天	4 月 29 日
9	常熟市碧溪卫生院	0.5 天	4 月 30 日
10	常熟市吴市卫生院	0.5 天	4 月 30 日
11	常熟市东张卫生院	0.5 天	5 月 6 日
12	常熟市古里中心卫生院	0.5 天	5 月 6 日
13	常熟市白茆卫生院	0.5 天	5 月 7 日
14	常熟市董浜卫生院	0.5 天	5 月 7 日

15	常熟市徐市卫生院	0.5 天	5 月 8 日
16	常熟市练塘中心卫生院	0.5 天	5 月 8 日
17	常熟市冶塘卫生院	0.5 天	5 月 10 日
18	常熟市辛庄中心卫生院	0.5 天	5 月 10 日
19	常熟市东南街道社区卫生服务中心	0.5 天	5 月 11 日
20	常熟市服装城社区卫生服务中心	0.5 天	5 月 11 日
21	常熟市浒浦卫生院	0.5 天	5 月 12 日
22	常熟市淼泉卫生院	0.5 天	5 月 12 日
23	常熟市虞山文化旅游度假区社区卫生服务中心	0.5 天	5 月 13 日
24	常熟王庄医院	0.5 天	5 月 13 日

第二组：

序号	被检查单位	检查周期	具体时间
1	常熟市疾病预防控制中心	1	4 月 25 日
2	常熟市第三人民医院	1	4 月 26 日
3	常熟市第五人民医院	1	4 月 28 日
4	常熟市第二人民医院	1	4 月 29 日
5	常熟市医学检验所	1	4 月 30 日
6	常熟市医疗急救中心	0.5 天	5 月 6 日
7	常熟市海虞卫生院	0.5 天	5 月 6 日
8	常熟市海虞卫生院福山分院	0.5 天	5 月 7 日
9	常熟市海虞卫生院周行分院	0.5 天	5 月 7 日
10	常熟市沙家浜卫生院	0.5 天	5 月 8 日
11	常熟市唐市中心卫生院	0.5 天	5 月 8 日
12	常熟市支塘人民医院	0.5 天	5 月 10 日

13	常熟市何市卫生院	0.5 天	5 月 10 日
14	常熟市任阳卫生院	0.5 天	5 月 11 日
15	常熟市张桥卫生院	0.5 天	5 月 11 日
16	常熟市大义卫生院	0.5 天	5 月 12 日
17	常熟市琴川街道藕渠社区卫生服务中心	0.5 天	5 月 12 日
18	常熟市琴川街道兴隆社区卫生服务中心	0.5 天	5 月 13 日
19	常熟市莫城街道社区卫生服务中心	0.5 天	5 月 13 日
20	常熟市常福街道谢桥社区卫生服务中心	0.5 天	5 月 14 日

常熟市卫生健康委员会办公室　　2021 年 4 月 23 日印发