临床能力培训中心信息化安全管理规定

一、总则

（一）制定依据

本制度依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《医疗卫生机构网络安全管理办法》《教育系统网络安全事件应急预案》及 ISO/IEC 27001 信息安全管理体系标准制定。

（二）适用范围

本制度适用于临床能力培训中心所有信息化系统、网络基础设施、数据资源及相关业务活动，包括教学模拟系统、患者信息数据库、远程培训平台等，覆盖在编人员、学生、进修人员、第三方服务人员及设备供应商。

（三）安全方针

坚持“零信任、全生命周期防护、动态监测”原则，构建“技术防护+流程管控+应急响应”三位一体的安全体系，确保医疗数据隐私保护与业务连续性。

二、组织架构与职责分工

（一）信息化安全管理委员会

1.组成：由中心主任任组长，分管信息化副主任任副组长，成员包括信息管理科、教学管理科、科研管理科、设备科及法律顾问。

2.职责：

- 制定信息化安全战略规划与年度工作计划。
- 审批重大信息化项目安全方案。

- 统筹协调跨部门安全事件处置。
- 每季度召开安全工作会议，研究风险防控措施。

（二）岗位安全职责

岗位	核心职责
信息管理员	总体负责信息化安全管理，制定技术方案，监督执行情况
第三方服务监管员	实施数据分类分级，监控数据访问日志，定期开展数据安全审计
	维护网络设备，部署入侵检测系统，实施零信任架构
	审核供应商安全资质，监督外包项目安全实施，定期开展合规检查
全体工作人员	遵守安全操作规范，定期参加安全培训，发现隐患及时报告

三、核心技术防护措施

（一）零信任架构实施

1.动态访问控制：

- 采用多因素认证（MFA），结合生物识别、动态令牌等技术。
- 基于角色的访问控制（RBAC），根据岗位职责分配最小权限。
- 实时监测设备状态，发现异常立即阻断访问。

2.网络微分段：

将网络划分为教学模拟区、数据存储区、公共服务区等安全域。

- 不同安全域之间通过防火墙隔离，禁止跨域直接访问。
- 重要系统采用私有云部署，与公共网络物理隔离。

（二）数据全生命周期管理

1.数据分类分级：

- 敏感数据（患者信息、科研数据）标记为最高级别，加密存储并限制访问。
- 普通教学数据采用 AES-256 加密，传输使用 TLS 1.3 协议。
- 数据销毁需经不可逆粉碎，重要数据需通过第三方认证。

2.数据备份与恢复：

- 采用“3-2-1”备份策略（3 份副本、2 种介质、1 份离线）。
- 核心系统每日增量备份，每周全量备份。
- 备份数据异地存储，定期进行恢复演练。

（三）设备与终端安全

1.医疗设备管控：

- 模拟教学设备接入专用局域网，禁止直接连接互联网。
- 设备操作系统定期更新补丁，关闭不必要的网络端口。
- 建立设备清单，记录型号、IP 地址、责任人等信息。

2.移动终端管理：

- 部署 MDM 系统，对手机、平板实施远程管控。
- 禁止在移动设备存储敏感数据，访问需通过 VPN 隧道。
- 设备丢失或被盗时，立即远程锁定并清除数据。

四、流程管控与合规要求

（一）系统建设与运维

1.开发安全：

- 采用 DevSecOps 模式，将安全测试嵌入开发全流程。
- 代码提交前需通过静态代码分析（SAST）和动态测试（DAST）。
- 第三方代码组件需经过安全评估，禁止使用已知漏洞组件。

2.运维规范：

- 实施“双人操作”制度，重要操作需双人复核。
- 运维日志保存至少 6 个月，定期进行审计分析。
- 远程运维需通过堡垒机，禁止直接访问生产环境。

（二）第三方管理

1.供应商准入：

- 签订包含安全条款的服务合同，明确数据保护责任。
- 要求供应商提供 ISO 27001 认证或等保三级证明。
- 定期开展供应商安全审计，发现问题立即整改。

2.外包项目管理：

- 对外包人员进行背景审查和安全培训。
- 限制外包人员访问权限，重要操作需全程监控。
- 项目结束后收回所有访问凭证，清除临时数据。

五、应急响应与处置

（一）事件分级与响应

1.事件分级：

- **Ⅰ级（特别重大）**：核心系统瘫痪、大规模数据泄露、国家级网络攻击。
- **Ⅱ级（重大）**：关键业务中断、敏感数据泄露、勒索病毒攻击。
- **Ⅲ级（较大）**：局部网络故障、普通数据泄露、恶意程序传播。
- **Ⅳ级（一般）**：个别设备故障、非敏感数据泄露。

2.响应机制：

- Ⅰ级事件：10 分钟内启动应急预案，1 小时内上报上级主管部门。
- Ⅱ级事件：30 分钟内处置，2 小时内报告信息化安全管理委员会。
- Ⅲ/Ⅳ级事件：责任部门 4 小时内解决，24 小时内提交书面报告。

（二）处置流程

1.快速隔离：

- 发现攻击立即切断网络连接，启用备用系统。
- 对受感染设备进行取证，保留原始日志。

2.技术溯源：

- 利用态势感知平台分析攻击路径和漏洞。
- 联合公安部门进行电子取证。

3.恢复与整改：

- 清除攻击痕迹，恢复系统至最近备份状态。
- 针对漏洞制定整改方案，72 小时内完成修复。
- 对事件进行复盘，更新应急预案。

六、教育培训与监督

（一）安全培训体系

1.新员工培训：

- 入职 1 个月内完成网络安全、数据保护等基础培训。
- 通过模拟钓鱼测试，检验安全意识水平。

2.定期培训：

- 每年组织 2 次全员安全培训，内容包括零信任架构、数据加密等。
- 技术人员每季度参加专项技能培训（如渗透测试、应急响应）。

3.考核机制：

- 安全培训纳入绩效考核，未达标者限制系统访问权限。
- 每年开展安全知识竞赛，对优秀团队给予奖励。

（二）监督检查机制

1.日常巡查：

- 信息管理科每日检查网络设备状态、系统日志。
- 数据安全管理员每周审计数据访问记录。

2.定期检查：

- 每季度开展全面安全检查，重点核查漏洞修复情况。

- 每年委托第三方进行等级测评和渗透测试。

3.专项审计：

- 对高风险操作（如数据导出）实施全程审计。
- 重要系统每半年进行一次数据安全专项审计。

七、奖惩措施

（一）奖励机制

1.对及时发现并消除重大安全隐患的人员，给予5000元专项奖励。

2.连续3年安全考核优秀的部门，优先获得信息化建设经费支持。

3.在国家级网络安全竞赛中获奖的团队，给予10000元奖励。

（二）处罚机制

1.违反安全操作规范的个人，视情节给予警告、罚款（500-2000元）或停职。

2.因失职导致安全事件的部门负责人，扣除当年绩效奖金的30%

故意泄露敏感数据的人员，依法追究法律责任并解除劳动合同。

八、附则

本制度自发布之日起施行，由信息化安全管理委员会负责解释和修订。

本制度与国家法律法规冲突时，以国家法律法规为准。

每年根据技术发展和政策变化，对制度进行1次全面修订。

临床能力培训中心

2023年12月1日