**中山大学肿瘤防治中心设备接入管理规范承诺函**

一、总则

为加强中山大学肿瘤防治中心网络安全，规范设备接入管理，根据《医疗卫生机构网络安全管理办法》《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络安全审查办法》、网络安全等级保护制度等有关法律法规标准以及中心相关安全管理制度，特制定本规范。

二、接入流程

任何设备接入中山大学肿瘤防治中心网络前，需使用科室经办人通过钉钉向信息中心提交申请，经科室负责人、信息中心负责人审批通过后方可接入。如接入设备为医疗仪器设备或非医院资产设备，还需签订安全承诺函。

科室经办人提交的审批中应注明设备型号、操作系统、数量、位置、设备供应商、MAC地址、设备用途等信息。

三、设备接入网络管理要求

1、使用科室应指定人员负责设备的使用管理工作。如有发现影响医院网络安全、数据安全等行为，应及时制止并通知信息中心处置。

2、设备系统账号不得采用弱密码，建议密码包含数字、大小写字母、特殊符号。

3、设备接入内网时，需安装信息中心提供的杀毒软件和桌面准入软件。通过以上软件实现USB、光驱、网卡等外设限制和病毒防范，避免数据泄露和病毒传播。如设备无法安装安全软件，需与信息中心沟通，协商采用其他有效的控制措施。未经信息中心同意，任何人不得禁止私自卸载杀毒软件和桌面准入软件。

4、接入外网时，须安装主流的防病毒软件，如火绒、360、小红伞等，并开启定期扫描和病毒库更新功能。

5、涉及到产生、存放医疗数据的设备，原则上需接入内网进行统一管理，不得私自接到外网或者互联网。

6、不得将接入医院内网网络的设备，通过双网卡或者5G卡等形式串接到互联网或其他存在安全威胁的网络。

7、未经批准，任何人员不得通过各种手段拷贝设备上的医疗数据。所有医疗数据的使用，请遵循《中山大学肿瘤防治中心信息数据使用管理办法》。

8、不得将接入设备作为跳板，非法探测、窃取医院信息系统数据。

9、不得通过设备做出任何危害医院网络安全的行为。

10、严禁在未授权的情况下在设备安装远程工具，如因特殊情况需要通过远程访问，须经过信息中心审批授权后，由信息中心开通远程访问权限，使用完成后及时通知信息中心关闭。

11、未经信息中心、使用科室同意，严禁任何人将设备存放的医疗数据传输到境外。如确有所需，请按照医院及国家相关数据出境管理办法进行审批。

12、如涉及医院系统对接，且需要批量获取医院生产系统数据，须提前与信息中心做好沟通工作，并提供合适的方案，经信息中心负责人审批后方可执行；保存所有应用和系统的日志，确保相应的操作可追溯可审查，日志保存期限不少于6个月。所有日志记录必须通过syslog形式发送到信息中心指定的日志服务器备查。

13、非医院资产设备在退网前，需删除与中山大学肿瘤防治中心相关的所有数据，并经信息中心确认方可撤走。

我司承诺接受以上规范条款。若我司在以上条款中未能遵守和告知，将视为我司在贵院的不诚信行为，将接受院方的处理，包括但不限于：1.院方无条件中止与我司的合作（包括购置意向和购置合同协议），2.我司在未来五年内不得参与院方的设备购置和供货服务。

特此承诺。

供应商名称（加盖公章）：

法人代表（或授权代表）：

日 期：

设备厂家名称（加盖公章）：

法人代表（或授权代表）：

日 期：