天津医科大学临床医学院文件

津医临政〔2017〕42号

关于印发《天津医科大学临床医学院信息技术安全管理办法（试行）》的通知

各系、部、馆、中心，机关各部门：

为加强学院信息技术安全管理，推进学院信息系统安全等级保护工作，提高信息技术安全防护能力和水平，保障学院各项事业健康有序发展，学院制定了《天津医科大学临床医学院信息技术安全管理办法》，现印发给你们，请遵照执行。

天津医科大学临床医学院

2017年7月2日

天津医科大学临床医学院
信息技术安全管理办法（试行）

第一章　总则

第一条 为加强学院信息技术安全管理，推进学院信息系统（含互联网网站）安全等级保护工作，提高信息安全防护能力和水平，保障学院各项事业健康有序发展，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》等法律法规以及《教育部关于加强教育行业网络与信息安全工作的指导意见》（教技[2014]4号）、《信息安全等级保护管理办法》等文件要求，结合我院实际，特制订本办法。

第二条 本办法所称信息技术安全工作，是指为使由学院建设、运行、维护或管理并支撑学院教学、科研和管理等各项事业的信息资产（信息系统及数据信息）的机密性、完整性、可用性得到保持、不被破坏所开展的相关管理和技术工作。本办法所指学院各单位包括各部、系、馆、中心、机关各部门。

第三条 依据《信息安全等级保护管理办法》的规定，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全信息技术安全责任体系；学院各单位、全体师生员工应依照本办法要求履行信息技术安全的义务和责任。

第二章　组织机构与职责

第四条 学院主要负责人是学院信息技术安全的第一责任人，分管信息化工作的院领导协助主要负责人履行学院信息技术安全责任。

第五条 网络信息中心是信息安全技术支撑单位，负责统筹学院网络安全与信息化建设工作，学院信息技术安全防护体系的建设、运行维护、技术指导和服务支持。具体职责包括：

1. 制定信息技术安全总体规划，并组织实施；

2. 拟定信息技术安全管理规章制度，制定信息技术安全标准规范；

3. 组织开展信息系统安全等级保护工作

4. 负责信息安全应急管理，协调处理与政府信息安全管理部门的关系

5. 负责信息技术安全监督检查工作

6. 组织信息安全宣传和教育培训工作

第六条 依据信息系统等级保护的要求，学院各单位是网络安全和信息化工作的责任主体，各单位主要负责人是本单位网络安全和信息化工作第一责任人，负责按本办法落实信息技术安全工作。

第三章　校园网管理

第七条 校园网络是指校园范围内由学院建设、运行、管理的，连接各种信息系统及信息终端，为师生在校园内提供接入服务的网络，包括校园有线网络、无线网络和各种虚

拟专网（不包括校内单位或个人直接向运营商申请开通的ADSL、无线wifi等专线服务的网络）。

第八条 网络信息中心负责制定校园网络规划，涉及网络机房、网络设备、网管系统、域名管理、安全防护、认证计费、网络接入与运维等方面，由网络信息中心负责建设、运行、维护和管理。

第九条 后勤处负责在学院地下管网统一管理的原则下，对校园网络光纤管道进行规划、建设、管理和维护。学院所有基建、修缮工程将工程范围内校园网络建设纳入工程设计、实施和竣工验收范畴。

第十条 校园网络与互联网及其他公共信息网络实行逻辑隔离，由网络信息中心统一出口、统一管理和统一防护。

第十一条 网络信息中心采取访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等措施加强校园网络边界防护。

第十二条 为了使广大教职员工和学生更加规范、科学、合理分配网络资源，提高网络使用效率，确保校园网安全、稳定运行，我院在校园网范围内实行实名制上网管理，保证校园网信息安全。IP地址由网络信息中心分配和管理，网络管理员对接入校园网的设备和使用人进行IP地址登记，任何人不得擅自更改IP地址及网络设置。网络信息中心可以对未提供真实身份信息的用户终止网络服务。

第十三条 学院非涉密信息系统接入校园网络，实行接入审批和备案登记制度。涉密信息系统不得接入校园网络。

第十四条 根据信息安全及等级保护工作的相关管理规定，校园网用户须填写《校园网使用申请表》入网申请，并签订《用户入网责任书》，分配给每名校园网用户的 IP 地址作为用户在校园网的身份标识，请妥善保存，不得转借他人使用。

第十五条 校园网的线路接入须由网络信息中心确认，个人不得私自接入路由器架设 WIFI 热点，造成网络故障和安全事故者，根据相关规定追究责任。确有需要的由网络信息中心负责对无线路由器进行接入安装，并在《校园网使用申请表》上注明（路由器的购买和日常管理由申请人负责）。

第十六条 校园网络接入单位须负责提供本单位所需的网络设备和电源保障，协助解决网络布线和设备安装所需空间，负责安防和消防安全管理。

第十七条 严禁任何单位和个人利用校园网络及设施开展经营性活动。

第四章 用户分类

第十八条 用户分类：校园网用户分为一般用户、公共服务用户、校外用户等三个类别。每类均需统一申请并填写《用户入网责任书》，由网络信息中心分配独立的校内 IP 地址上网。

第十九条 一般用户：每位教职工，可申请由网络信息中心开通一个接入校园网的专线归属本人使用，并进行上网实名登记。独立分配静态 IP 地址，用户离校地址统一收回。

第二十条 公共服务类用户：学院公共教学机房等须使

用校园网时，其主管部门应办理公共帐户的开通手续。公共教学使用的机房，经主管院领导审批同意后，为该机房办理公共帐户的开通手续，须填写《校园网使用申请表》并由主管部门签字盖章审核通过后统一接入，接入完成后不得随意更改接入配置和接入设备。公共机房的接入按照单一接入点计算，保证多台计算机同时使用为原则；根据使用方式、使用规模以及相关课程安排为依据，设定带宽和使用时间，并在开通申请时明确。

第二十一条 校外用户：非学院所属的各类公司或单位（租用校园内场所办公）中非学院在编人员以个人名义申请上网的，均纳入校外用户的管理范畴。该类用户须填写《校园网使用申请表》并由主管部门签字盖章审核通过后统一接入，接入完成后不得随意更改接入配置和接入设备。为保证校园网使用安全，校外人员在接入申请中需注明使用内容，原则上此类用户不允许接入路由器。

第五章　用户守则

第二十二条 用户必须遵守国家的有关法律、法规和学院的相关规章制度，严格执行网络安全保密制度，并对其网络行为承担独立的责任。

第二十三条 用户必须接受并配合国家安全部门依法进行的监督、检查及采取的必要措施。遵守学院的管理制度，爱护网络设备，正确使用网络设备，保证网络设备的正常运行。

第二十四条 用户不得利用校园网从事危害国家安全、

泄露国家秘密等违法、犯罪活动，不得查阅、复制和传播有碍社会治安和有伤风化的信息。

第二十五条 用户不得进行任何干扰其他网络用户、破坏网络服务或破坏网络设备的活动，如散布计算机病毒、恶意攻击网络设备等。

第二十六条 不得以代理方式（包括软硬件方式的路由器或代理服务器）向他人提供网络访问渠道；禁止将学院网络资源（包括IP、域名等）用于商业目的。

第二十七条 未得许可，不得使用校园网IP地址私自建立HTTP、FTP等网络服务。

第二十八条 不得私自改动所分配为的IP，如影响他人使用，被举报核实后，将被无限期断绝网络连接。

第二十九条 校园网内各系统上的信息和资源属于其所有者。用户必须遵守有关知识产权的法律法规，未经许可，不得私自进行拷贝和链接。

第三十条 用户有向学院报告任何违反用户管理办法行为的义务。对于违反本办法规定的用户，学院有权暂停或终止对其的网络服务，必要时将诉诸法律。

第三十一条 用于网络访问的IP地址等属个人信息，用户应妥善保管。如因用户保管不善导致相关损失或产生触犯法律法规的事实，其责任由用户自行承担。

第三十二条 网络信息中心所有工作人员使用资料时必须严格登记，对重要资料如用户密码、网络密钥等必须严格保密，不得泄漏。

第六章　数据中心和移动存储介质的管理

第三十三条 数据中心主要包括支撑学院信息系统的物理环境（其中包含网络中心机房）、软硬件设备设施等信息化基础设施和平台。网络信息中心负责数据中心的建设、运行、维护和管理。

第三十四条 网络信息中心负责数据中心物理环境、软硬件设备设施的建设和安全管理；根据信息系统安全等级的不同，对数据中心进行分区、分域管理，采取必要的技术措施对不同等级分区进行防护，对不同安全域之间实施访问控制。

第三十五条 网络信息中心负责学院信息系统数据库的安全管理工作，和软硬件设备的保障。

第三十六条 各单位负责建设、维护、备份本单位业务应用系统所配套的业务数据库，并对本单位业务数据库进行权限和安全管理。

第三十七条 网络信息中心负责制定使用数据中心的技术规范和标准，对学院数据中心的数据使用实施准入管理，在各类业务系统上线前进行安全检测。符合技术规范标准并检测通过的系统方可上线运行。

第三十八条 原则上，存储阵列、磁带库等大容量介质应托管在学院数据中心，并由网络信息中心统一运行、维护和管理。网络信息中心应采取必要技术措施防范数据泄露风险，确保存储数据安全。

第三十九条 移动存储介质在接入数据中心以及运行信

息系统终端程序的计算机之前，应当查杀病毒、木马等恶意代码。

第七章 信息系统建设、运行和维护管理

第四十条 按照同步规划、同步建设、同步运行的原则，规划、设计、建设、运行、管理信息安全设施，建立健全信息技术安全防护体系，全面实施信息系统安全等级保护制度。

第四十一条 网络信息中心负责收集整理学院信息系统安全等级保护工作，组织学院各单位开展信息系统定级、系统备案、等级测评、建设整改，具体负责信息系统台帐管理、等级评审、系统备案、监督检查工作。按照“自主定级、自主保护”的原则，信息系统建设单位是信息系统安全等级保护的责任主体，具体负责系统定级、建设整改、安全自查，协助系统备案、等级测评并接受有关部门监督检查。同时网络信息中心也是信息系统安全等级保护工作的技术支撑保障部门，负责信息技术安全防护体系建设和等级测评组织工作，参与监督检查工作，并协助学院各单位进行系统定级、建设整改。

第四十二条 为确保项目质量，网络信息中心需在立项阶段组织需求、技术、预算等方面的专家论证。网络信息中心协助建设单位在立项阶段确定安全保护等级，组织对建设方案进行单独的安全论证及等级评审等工作。对于安全等级第二级以上（含第二级）的信息系统，由网络信息中心统一办理系统备案。

第四十三条 信息系统在建设阶段应按已确定的安全保护等级，同步落实安全保护措施。信息系统投入试运行后，由建设单位初步验收，出具初步验收报告。对于安全等级第二级以上（含第二级）的信息系统，由网络信息中心组织等级测评。信息系统通过初步验收和信息安全保护等级评测后，由网络信息中心组织竣工验收。

第四十四条 信息系统建设单位应定期对信息系统运行的关键设备（服务器、安全设备、网络设备）进行安全审计，通过记录、检查系统和用户活动信息，及时发现系统漏洞，处置议程访问和操作。

第四十五条 信息系统建设单位应制定信息系统使用与维护的管理制度，包括信息系统内的使用权限管理，规范信息系统使用者和维护者的操作行为。

第四十六条 对于安全等级第二级以上（含第二级）的信息系统，网络信息中心将定期组织开展等级测评，查找、发现并及时整改安全问题、漏洞和隐患。根据国家和教育行业有关标准规范，四级系统应每年进行两次测评，三级系统每年进行一次测评，二级系统每两年进行一次测评。

第四十七条 根据《中共中央办公厅、国务院办公厅印发<关于加强重要领域密码应用的指导意见>的通知》（厅字[2015]4号）和《中共天津市委办公厅、天津市人民政府办公厅印发<关于加强重要领域密码应用的实施意见>的通知》（津党厅[2016]57号）精神，开展校园网络和信息系统建设时，应该大力支持和推进国产密码的应用，确保新建或改造

系统与国产密码推进工作同步规划、同步建设、同步运行。

第八章　信息系统数据安全管理

第四十八条 信息系统数据是指信息系统收集、存储、传输、处理和产生的各种电子数据，包括但不限于网站内容、业务数据、网络课程、图书资源、日志记录等。

第四十九条 信息系统数据的所有者是数据安全管理的责任主体，应当落实管理和技术措施，规范数据的收集、存储、传输和使用，确保数据安全。

第五十条 信息系统数据收集应遵循“最少够用”原则，不得收集与信息系统业务服务无关的个人信息。按照“谁收集，谁负责”的原则，收集个人信息的单位是个人信息保护的责任主体，应当对其收集的个人信息严格保密，并建立健全相关保护制度。

第五十一条 网络信息中心负责学院核心信息系统的备份与恢复管理，制定备份与恢复计划，信息系统建设部门负责本部门建设的系统的数据备份和恢复。

第九章　互联网网站安全管理

第五十二条 学院各单位开办网站，应使用学院教育网域名和教育网 IP 地址，并遵守《天津医科大学临床医学院网站管理办法》及相关规章制度。

第五十三条 互联网网站的内容安全由各部门负责。各部门应建立完善的网站信息发布与审核制度，确定专人担任网站管理员，负责部门网站管理、信息发布工作。

第五十四条 未经学院批准，学院网站不得开设具有交

互功能的栏目，不得发布商业广告信息。

第十章　人员安全管理

第五十五条 学院各部门应建立健全本部门的岗位信息安全责任制度，明确岗位及人员的信息安全责任。

第五十六条 学院各部门应加强人员离岗、离职管理，严格规范人员离岗、离职过程，及时中止相关人员的所有访问权限，收回各种电子身份证件、密钥以及学院提供的软硬件设备等，并签署安全保密承诺书。

第五十七条 网络信息中心定期对信息技术安全岗位的人员进行安全知识和技能的考核，并对考核结果进行记录和保存。

第五十八条 学院各单位应建立外部人员访问机房等重要区域的审批制度，外部人员须经审批后方可进入，并安排工作人员现场陪同，对访问活动进行记录和保存。

第十一章　信息安全教育培训

第五十九条 网络信息中心负责组织学院信息安全宣传和教育培训工作，建立健全相关制度。

第六十条 网络信息中心定期组织开展针对师生员工的信息安全教育，提高师生员工的安全和防范意识。

第六十一条 网络信息中心定期开展针对信息安全管理人员和技术人员的专业技能培训，提高信息安全工作能力和水平。

第十二章　信息安全检查与管理

第六十二条 学院依据《中华人民共和国网络安全法》

建立信息安全责任追究和倒查机制。

第六十三条 网络信息中心负责制定学院信息技术安全事件报告与处置流程和学院信息技术安全应急预案。

第六十四条 网络信息中心作为学院信息安全应急处置部门，完善应急情况下24小时值守制度。

第六十五条 学院各单位应定期对本单位信息系统的安全状况、安全保护制度及措施的落实情况进行自查，并配合相关部门的信息安全检查、内容检查、保密检查与审批工作。

第六十六条 网络信息中心负责对各单位的信息技术安全工作落实情况进行检查，对发现的问题，将下达安全隐患限期整改通知书。有关单位在收到安全隐患限期整改通知书后，未实施限期整改的，网络信息中心将对存在安全隐患的业务系统实施断网处理。

第六十七条 依据《网络安全法》的规定，以下行为均涉及违反网络安全：

1. 在服务器、终端计算机、移动存储设备中设置恶意程序的；

2. 对信息系统涉及的软件、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时向有关主管部门报告的；

3. 擅自终止为信息系统涉及的软件、服务提供安全维护的；

4. 其他危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安

全的活动提供技术支持、广告推广、支付结算等帮助的；

5.设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息的；

6.其他危及网络安全、信息泄露等行为。

第六十八条 学院各单位应按照信息技术安全事件报告与处置流程及时、如实地报告和妥善处置信息技术安全事件。如有瞒报、缓报、处置和整改不力等情况，学院将对相关单位责任人进行约谈或通报。

第六十九条 师生员工违反本办法规定的，由网络信息中心责令改正；拒不改正或者导致危害信息技术安全等严重后果的，根据学院相关规定给予处理。情节严重的违法行为，移交司法机关处理。

第十三章 附则

第七十条 涉及国家秘密的信息系统，严格执行国家保密工作的相关规定和标准，由学院党委监督执行。

第七十一条 本办法由网络信息中心负责解释。

第七十二条 本办法自发布之日起实施。