沈阳城市建设学院文件

城建院发〔2019〕139号　　签发人：崔景懿

关于印发《沈阳城市建设学院校园网络管理办法（修订）》的通知

各单位、部门：

现将《沈阳城市建设学院校园网络管理办法（修订）》印发给你们，请认真学习并遵照执行。

沈阳城市建设学院

2019年12月31日

沈阳城市建设学院校园网络管理办法（修订）

第一章　总　则

第一条 为加强学校计算机网络（以下简称校园网络）的管理，保证校园网络更好地为教学、科研和管理服务。根据《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国教育和科研计算机网暂行管理办法》和《中华人民共和国计算机信息系统安全保护条例》，结合我校实际情况，制定本办法。

第二条 校园网络是为学校教学、科研、管理和服务建立的计算机综合信息网络并接入互联网，实现信息的快捷传输和资源共享，是学校公共服务体系的重要组成部分。我校校园网络由学生区域部分和办公区域部分组成，本办法中提及的校园网络均为办公区域部分。

第三条 网络与信息中心是校园网络规划、建设、运行和日常管理的责任部门，负责校园网络的业务受理、故障处理和业务咨询等工作，并负责与各运营商的协调工作。

第四条 各单位、部门应明确一名负责人分管网络管理和网络安全工作。配备相应的兼职网络管理员，具体负责本单位、部门网络的管理、简单问题的处理，网络与信息中心会进行业务培训与指导。

第五条 校园网络用户应遵守本办法，对于违反本办法的用户，网络与信息中心有权停止其使用。

第二章　网络接入

第六条 办公计算机用户接入校园网络，须填写《校园网络接入申请表》，由本单位、部门领导审核并加盖公章后，交由网络与信息中心网络科配置用户信息资源。任何单位、部门和个人在未办理入网手续前不得擅自将计算机接入校园网络。开通互联网的操作，须由网络与信息中心网络科执行，任何个人不得擅自将任何一台计算机接入互联网中。接入互联网的计算机，必须由专人负责使用，原则上不得借于他人使用，出现问题由此计算机使用人负责。

第七条 网络与信息中心至各个建筑物的校园网络主干线路和建筑物内各单位、部门的新增用户接入校园网络的网络布线或局域网布线，由网络与信息中心统一设计并铺设。

第八条 学生使用办公、教学计算机或自带笔记本以局域网形式接入校园网络，需取得接入地单位、部门领导审核通过并提交《校园网络接入申请表》，加盖接入地单位、部门公章，网络与信息中心按照其批复办理接入手续。

第三章　网络设施的建设、维护和管理

第九条 网络与信息中心负责校园主干网网络线路和设备的建设、运行管理和维护。

第十条 安置在各单位、部门设备间内的网络设备由网络与信息中心负责安装、调试和系统维护，由各单位、部门负责设备的安全及清洁，并提供所必需的电源和环境条件，以保证设备

24 小时正常运行。

第十一条 各单位、部门负责本单位、部门范围内校园网络设施（包括网络设备、线路、线槽等）的安全管理。学生宿舍楼内校园网络设施的安全管理由公寓管理中心负责。由于管理不当造成的校园网络设施损坏及其它损失由负责管理的单位、部门进行修复。

第十二条 校园网络设施属学校公共资产，全校师生有义务和责任保护校园网络设施，任何损坏、拆卸、移动和侵占校园网络设施的行为必须承担赔偿责任和法律后果。

第四章　网络系统安全管理

第十三条 网络与信息中心负责校园网络的安全管理，保障校园网络设备和配套设施的安全，保障信息的安全及运行环境的安全。

第十四条 校园网络用户必须严格遵守国家有关计算机网络安全的法律法规以及学院制订的有关条例，必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受网络与信息中心进行的网络系统及信息系统的安全检查。

第十五条 在校园网络上不允许进行任何干扰其他校园网络用户、破坏网络服务和网络设备的活动，严禁利用网络从事商业活动，严禁在网络上发布未按规定程序进行审查的信息，不允许在网络上进行未经授权的活动，任何校园网络用户必须以真实身份使用网络资源。

第十六条 校园网络用户不得非法改动或盗用网络地址及用户账号。严禁输入计算机病毒及其他有害数据危害校园网络信息系统的安全。

第十七条 各部门指定专人负责计算机及其附属设备的日常管理，要有较强的病毒防范意识，定期进行病毒检测，发现病毒立即处理。

第十八条 所有连接网络的计算机均需安装杀毒软件并设置定时更新。使用人员应正确操作计算机，保证计算机处于良好的运行状态。因不安装防火墙、杀毒软件造成网络事故，导致整个网络瘫痪的，追究其使用者责任。

第十九条 未经允许，不得随意共享计算机内的各种资源，不得对局域网内共享的资源进行修改、删除。局域网网络出现问题，由网络与信息中心负责排除，各单位、部门应积极配合；各终端机因使用不当出现问题，各单位、部门先自行排查，网络与信息中心协助处理。

第五章　信息管理和服务

第二十条 校园网络信息服务主要包括内网业务系统和外网业务系统，其中，内网业务系统包括一卡通、车辆识别、消防预警系统、视频监控系统等；外网业务系统包括：办公 OA、教务系统、迎新系统、心理咨询系统等。

第二十一条 沈阳城市建设学院业务系统由校网络与信息中心负责日常管理、运行维护与系统规划、升级改造等工作。

第二十二条 校园网络信息服务统一在学院网络安全和信息化领导小组及其办公室的领导和管理下进行。

第二十三条 学院利用校园网络提供信息服务的服务器由网络与信息中心负责建立和维护，其他各单位、部门利用校园网络提供信息服务的服务器在网络与信息中心的统一安排下由各单位、部门自行建立和维护。

第二十四条 网络与信息中心负责校园网络公共信息建设，承担域名解析、电子邮件、万维网、文件传输、数据库等服务器的建设、管理和维护，保证公共信息服务器的正常运行并负责全院公共信息建设的技术支持。

第二十五条 有关在校园网络上进行图书情报检索、学术资源访问等方面的信息服务由图书馆负责。

第二十六条 校园网络信息的监控由网络与信息中心负责，有害信息的清除由网络与信息中心负责。

第六章　网络与信息系统的运行维护管理

第二十七条 网络与信息系统的维护内容在生产操作层面又分为核心机房环境维护、计算机硬件平台维护、配套网络维护、基础软件维护、应用软件维护五部分：

1.计算机硬件平台指计算机主机硬件及存储设备；

2.配套网络指保证网络与信息系统相互通信和正常运行的网络组织，包括联网所需的交换机、路由器、防火墙等网络设备和局域网内连接网络设备的网线、传输介质、光纤线路等；

3.基础软件指运行于计算机主机之上的操作系统、数据库软件、中间件等公共系统软件；

4.应用软件指运行于计算机系统之上，直接提供服务或业务的专用软件；

5.核心机房环境指保证计算机系统正常稳定运行的基础设施，包含核心机房建筑、电力供应、空气调节、灰尘过滤、静电防护、消防设施、网络布线、维护工具等子系统。

第七章　维护管理

第二十八条 网络与信息中心负责组织全网性网络优化方案的制定，逐步提高网络安全和资源利用率，积极探索网络延伸业务的新内容。

第二十九条 网络与信息中心负责解决网络设备运行中出现的热点和难点问题；研究并提出提高网络运行质量和安全的技术措施。

第三十条 网络与信息中心负责对维护作业计划执行情况、设备及网络运行情况方面的检查工作。

第三十一条 网络与信息中心协助各部门做好相关业务系统数据备份，做好相关记录，备份介质由各部门专人保管和存放。

第三十二条 网络与信息中心负责校 IP 地址的管理、分配及网络安全。

第三十三条 网络与信息中心负责校园网系统的巡查工作，做到及时发现障碍及时处理。

第三十四条 网络与信息中心做好校园网系统的基础维护工作。发现问题，及时解决，认真填写维护记录。

第三十五条 网络与信息中心负责技术支持、业务平台、部门办公、外网的网络安全管理，采取有效防范措施，保证网络系统安全。

第八章　数据共享管理

第三十六条 未经主管部门批准，任何单位、部门或个人均无权将学校信息系统数据库中的任何信息资源有偿或无偿地转移给校外用于任何目的。违反本办法的个人或单位、部门负责人将会受到相应的行政处罚直至追究法律责任。

第三十七条 学校信息系统数据库中信息资源的共享权限要根据本办法的原则制定，由网络与信息中心负责解释和实施。

第三十八条 各单位、部门对信息系统的录入必须保证其及时、准确和完整。

第九章　网络设备管理

第三十九条 网络通信设备管理：

1.网络通信设备由网络与信息中心网络科统一配置和安装，由网络技术人员负责参数设置和管理，并保存LOG记录；

2.禁止其他人员擅自改动网络配置和网卡的参数设置。如遇非法改动须及时校正，并记录在册，追查相关人员的责任；

3.路由器、交换机等网络设备由校统一规划，放置于一般人不易触及的地方，使用部门不能随意挪动；

4.网络设备的管理和定期清洁维护，全员公用设备由网络技术人员负责，各部门办公室内的由各部门指定专人负责，要保证设备的电源供给稳定，线头接插稳固；

5.无线网络设备由网络科统一维护；

6.发现不正常工作的公共设备由网络科及时更换。

第四十条 网络安全设备：

1.网络安全设备必须通过公安部门的安全认证；

2.网络安全设备由网络技术人员负责其参数的设置和管理，定期升级。

第四十一条 磁盘阵列设备：

1.磁盘阵列设备应由网络技术人员定期检测，及时发现坏区并进行维护；

2.维护记录电子版上交网络与信心中心主任，维护记录本（纸质版存于核心机房）。

第四十二条 消耗材料：

1.消耗材料包括计算机网卡、网线、网络接头等；

2.技术人员应定期检查消耗材料使用情况，保证设备正常使用；

3.网卡、网线、网络接头等应由技术人员进行更换；

4.必须配备足够数量消耗材料。

第四十三条 电源：

1.服务器必须配备断电发生后至少能支持30分钟的不间断

电源设备；

2.重要场所设备必须配备断电发生后至少能支持30分钟的不间断电源设备；

3.UPS定期放电（每三月一次）。

第四十四条 线路：

1.网络布线要尽量避免交叉，交叉处要注意防止短路；

2.易损线路须加套管保护；

3.专用线路不得挪做他用；

4.定期检测线路，保证线路的畅通；

5.主干网络及重要场所的线路应布设不同走向的备用线路。

第四十五条 设备安全：

1.凡校内、外涉及到网络线路、系统设备、停电等问题必须事先通知网络与信息中心和相关单位、部门，以便预先做好应对措施；

2.凡涉及设备搬迁、设备维修、系统升级等原因需要网络与信息系统停止运行，应在预定停机前报告。

第四十六条 运行维护管理的基本任务：

1.进行网络与信息系统的日常运行和维护管理，实时监控系统运行状态，保证系统各类运行指标符合相关规定；

2.迅速而准确地定位和排除各类故障，保证网络与信息系统正常运行，确保所承载的各类应用和业务正常；

3.进行系统安全管理，保证网络与信息系统的运行安全和网

络与信息的完整、准确；

4.在保证系统运行质量的情况下，提高维护效率，降低维护成本。

第四十七条 巡检管理：

1.网络与信息中心负责网络与信息系统相关的核心机房环境、计算机硬件、配套网络、基础软件和应用软件的运行状态巡检；

2.网络与信息中心负责网络与信息系统相关设备巡检的具体实施；

3.制定技术巡检计划，定期进行巡检工作；

4.收集设备运行故障和隐患。检查各类型设备,尤其是利用率较高的服务器、交换机等设备运行情况。对一些需要厂家解决的问题列出清单，及时与厂家沟通，制定解决方案，以供巡检过程中实施、解决。

第十章　处罚办法

第四十八条 凡违反本办法有关要求的，将由学校给予警告或暂停上网的处罚，并承担由此引起的经济损失，情节严重的，将交由学校保卫处或公安机关依法处治。

第四十九条 非法改动、盗用 IP 地址或非法将设备接入校园网络、干扰和破坏校园网络正常运行的，要承担由此引起的经济损失。情节严重的，交由保卫处或公安机关依法处治。

第五十条 对于违反国家有关法律法规规定，并构成刑事犯

罪的网络用户，将交由公安机关依法进行处理。对构成违反治安管理条例的，依照《中华人民共和国治安管理处罚条例》的有关规定处罚。对任何单位、部门或个人违反国家有关法律法规和本办法的规定，给国家、集体或他人财产造成损失的，应当依法承担民事责任。

第十一章　应急预案

第五十一条 根据网络与信息系统应急管理的要求，成立网络与信息系统应急保障领导小组（简称应急领导小组），负责领导、组织和协调全校网络与信息系统突发事件的应急保障工作。领导小组职责：

1.制定校内部网络与信息安全应急处置预案；

2.做好校网络与信息安全应急工作；

3.协调校内部各部门之间的网络与网络与信息安全应急工作，协调与软件、硬件供应商、线路运营商之间的安全应急工作；

4.组织校内部及外部的技术力量，做好应急处置工作。

第五十二条 学校网络与信息系统出现故障报告程序：

当各工作站发现计算机访问数据库速度迟缓、不能进入相应程序、不能保存数据、不能访问网络、应用程序非连续性工作时，要立即向网络与信息中心报告。网络与信息中心工作人员对各工作站提出的问题必须高度重视，做好记录，经核实后及时给各工作站反馈故障信息，同时召集有关人员及时进行讨论，如果故障原因明确，可以立刻恢复的，应尽快恢复工作；如故障原因不明、

情况严重、不能在短期内排除的，应立即报告校领导，在网络不能运转的情况下由校领导协调全校各部门工作，以保障全校部门工作的正常运转。

第五十三条 学校网络与信息系统故障根据其发生的原因和性质不同分为三类：

严重故障：由于服务器不能正常工作、光纤损坏、主服务器数据丢失、备份硬盘损坏、服务器工作不稳定、局部网络不通、重点终端故障、造成的网络瘫痪。

较大故障：由于单一终端软、硬件故障，单一数据网络与信息丢失、偶然性的数据处理错误、某些部门违反工作流程引起系统故障。

一般故障：由于各终端操作不熟练或使用不当造成的错误。

针对上述故障分类等级，处理原则如下：

严重故障——由网络与信息中心主任上报校领导，由校组织协调恢复工作。

较大故障——由网络与信息中心技术人员上报网络与信息系主任，由网络与信息中心集中解决。

一般故障——由网络与信息中心技术人员单独解决，并详细登记维护情况。

第五十四条 网络服务器故障应急处理规程：

网络服务器故障是因硬件或软件原因致使校网络与信息管理系统运行停止，一旦发生故障，按下列规程处理。

1.网络与信息中心监控网络运行。发现问题，在及时处理的同时迅速向部门领导汇报。

2.遇到较大故障，网络与信息中心工作人员应迅速集合，集体攻关。具体分为3个组做以下工作：

故障检修组：集中技术人员分析故障、查找原因、修复系统；

技术联络组：迅速与软、硬件供应商取得联系，采取有效手段获得技术支持；

校内协调组：通知全校各部门故障情况，并到关键部门协助数据保存。

第五十五条 应急保障：

（一）日常网络与网络与信息安全的防护：

1.组织管理措施：应急组织机构要进行层层把关，层层落实，对组织机构中的人员及联系方式，要做到及时更新，并进行定期的安全知识培训。

2.技术保障：一方面进行网络设备的安全加固，例如增加防火墙等，对已知的系统漏洞及时安装补丁程序，另一方面要进行技术储备，对内部技术人员定期培训。

3.在网络工程建设和规划方面，要切实加强网络安全方面考虑，设计时要考虑设备的冗余备份，网络与信息存储的异地备份等。

（二）应急预案演练：

应急小组要定期进行应急预案的演练，提高应急响应的能力

和意识。

第五十六条 管理员定期进行安全漏洞检查，及时组织、安排人员安装微软的操作系统及其它应用工具的最新补丁。

第五十七条 除打印机可以共享外，服务器与工作站的硬盘尽量不设置为共享，文件目录一般不进行网络共享。特殊情况需进行目录共享的必须设定密码，一旦使用完毕后必须立即关闭共享，或加强对该机器的病毒检查。

第五十八条 技术人员密切关注网络与信息发布部门发布的病毒疫情，并根据需要下载相应的专杀工具。

第五十九条 计算机染毒：

（一）单台计算机染毒

1.计算机仅染毒，系统未崩溃。将该计算机断开网络连接，对计算机进行杀毒处理。

2.计算机染毒，系统崩溃无法正常运行。将该计算机断开网络连接，格式化系统分区重新安装系统和杀毒软件，杀毒软件安装完毕和病毒库更新后对计算机其他分区进行杀毒处理。

（二）部分区域计算机染毒：

1.计算机仅染毒，系统未崩溃。将连接这些计算机的交换机断开，对这些计算机进行杀毒处理。

2.计算机染毒，系统无法正常运行。将连接这些计算机的交换机断开，将该计算机断开网络连接，格式化系统分区重新安装系统和杀毒软件，如有部门重要资料存放在C区先将资料备份保

存后再重做系统，杀毒软件安装完毕和病毒库更新后对计算机其他分区进行杀毒处理。

（三）网络内所有计算机染毒：

这种情况下管理员须向部门负责人报告，由部门负责人向分管领导申请停止网络内所有计算机的网络连接。如果情况紧急，网络技术人员可以决定是否断开。

1.计算机仅染毒，系统未崩溃。断开所有交换机以及与互联网的连接，为所有的计算机进行杀毒处理，杀毒完毕后打上系统补丁包。

2.计算机染毒，系统崩溃无法正常运行。断开所有交换机以及与互联网的连接，将部分C区有重要资料的计算机资料备份到移动存储设备，为所有计算机重新安装完系统，杀毒软件安装完毕和病毒库更新后对计算机其他分区进行杀毒处理，然后打上补丁包。最后给移动存储设备进行杀毒处理，将备份的文件资料恢复。

第六十条 网站上出现不良信息：

1.一旦发现网站上出现不良信息（或者被黑客攻击修改网页），立刻关闭网站。向网络应急领导小组领导汇报此事件，等待指示。

2.备份不良信息出现的目录、备份不良信息出现时间前后一个星期内的HTTP连接日志、备份防火墙中不良信息出现时间前后一个星期内的网络连接日志。打印不良信息页面留存。

3.完全隔离出现不良信息的目录，使其不能再被访问。

4.删除不良信息，并清查整个网站所有内容，确保没有任何不良信息，重新开通网站服务，并测试网站运行。

5.修改网站目录名,对目录进行安全性检测,升级安全级别，升级程序，去除不安全隐患，关闭不安全栏目，重新开放该目录的网络连接,并进行测试,正常后,重新修改该目录的上级链接。

6.全面查对 HTTP 日志，防火墙网络连接日志，确定该不良信息的源 IP 地址。

7.全面检查网站所在服务器（空间）的性能是否满足目前浏览需求，安全防护产品是否达到等级保护要求，判断是否需要进一步更新升级现有安全防护产品。

8.事件处理结束后,从事故发生到处理事件的整个过程形成文字材料向上级汇报，汇报此次事故的发生原因、发生情况、处理过程，并针对现有服务器（空间）性能及相关安全防护能力是否满足等级保护要求给与建议。

第六十一条 发现出现网络恶意攻击，立刻确定受攻击的设备及其受影响范围。并迅速推断出此次攻击的最坏结果，判断是否需要紧急切断服务器的网络连接，以保护重要数据及信息。

1.如果攻击来自校外，立刻从防火墙中查出对方 IP 地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。

2.如果攻击来自校内，立刻确定攻击源，查出该攻击出自哪

台交换机，出自哪台电脑，出自哪位教师或学生。

3.确定 IP 后，立刻关闭此 IP 所在交换机端口，将影响降至最低，此时除此端口所在房间无法上网以外，其余网络访问已恢复正常。

4.关闭端口后，立刻赶到现场，关闭该计算机网络连接，并立刻对该计算机进行分析处理，确定攻击出于无意、有意还是被利用。

5.暂时扣留该电脑。对该电脑进行分析，清除所有病毒、恶意程序、木马程序以及垃圾文件，测试运行该电脑 5 小时以上，并同时进行监控，无问题后归还该电脑。

第十二章　附　则

第六十二条 本办法由网络与信息中心负责解释。

第六十三条 本办法自印发之日起实行。原《沈阳城市建设学院校园网络管理办法（试行）》（城建院发〔2018〕58 号）及以往与此办法不一致的有关规定同日废止。

附件

校园网络接入申请表

申请时间： 年 月 日

申 请 人		部门名称	
所在位置		房间号	
机器数量		联系电话	
用途及其他说明			
所在部门意见	负责人签字： （盖章） 年 月 日		
以下由网络与信息中心填写备案			
网络与信息中心 意见及接入方案	负责人签字： （盖章） 年 月 日		
受理人		受理日期	
处理情况 （开通时间）			

主　送：各单位、部门

党政办公室　　2019 年 12 月 31 日印发