天津城建大学文件

天城大政〔2020〕57号

关于印发《天津城建大学网络信息安全管理办法》的通知

各单位、部门:

《天津城建大学网络信息安全管理办法》已经2020年7月9日第21次校长办公会审议通过,现印发给你们,请遵照执行。

天津城建大学

2020年7月14日

天津城建大学网络信息安全管理办法

（经2020年7月9日第21次校长办公会审议通过）

第一章　总则

第一条　为深入贯彻习近平总书记网络强国战略思想，进一步加强校园网络信息安全的管理，规范学校各级网络信息平台建设，保证网络信息安全，把校园网建设成为宣传党和国家事业、学校发展和改革创新的窗口；成为广大师生进行交流的平台、教育和学习的阵地；成为联系学校党政部门和广大师生的桥梁，根据《中华人民共和国网络安全法》、《计算机信息网络国际联网安全保护管理办法》和《互联网新闻信息服务管理规定》等法律法规和相关文件精神，结合学校实际，制定本管理办法。

第二条　校园网及信息系统(含网站)是由学校投资建设，为学校教学、科研、管理、生活服务的现代化信息基础设施。校园网及信息系统(含网站)的服务对象是学校各单位、部门，全校教职工和学生，以及其他经学校授权的单位和个人。

第二章　管理机构与职责

第三条　学校网络安全和信息化领导小组（以下简称网信领导小组）是学校网络安全和信息化建设及管理的领导机构，

负责学校网络信息安全工作的统筹、组织、协调和重大问题的决策。网络安全和信息化办公室（以下简称网信办）是网络信息安全的审查和管理部门，负责校园网日常运行、管理和维护，同时为校园网络和信息安全提供技术支持和保障。

第四条 各单位、部门的党政主要负责同志是本单位、部门网络信息安全的第一责任人，各单位、部门要明确网络信息安全工作分管负责同志和信息管理员，按照“谁建设谁负责、谁主管谁监督”的原则对本单位、部门建设使用的应用系统、网站、APP、交互式栏目等进行管理和检查，并制定本单位、部门的网络信息安全管理措施，报送网信办备案。

第五条 未经批准，任何单位、部门或个人不得将校园网延伸至校外或将校外网络引入至校园内。未经批准，任何数据业务运营商或电信代理商不得擅自进入校园内进行工程施工，开展互联网业务。

第三章 信息系统（含网站）管理

第六条 各单位、部门应按照国家信息系统等级保护制度的相关法律法规、标准规范以及《市教委关于印发加强天津市教育行业网络与信息安全工作的指导意见的通知》（津教委〔2016〕21号）要求，加强对信息系统（含网站）的日常管理，制定信息安全事件应急预案，切实落实信息技术安全工作责任制和信息系统安全等级保护制度。

第七条 学校各单位、部门开办信息系统（含网站），应使用学校互联网域名和互联网 IP 地址，信息系统（含网站）内一律不得开设交互式栏目（如论坛、贴吧等）。各单位、部门要准确掌握本单位、部门信息系统（含网站）建设情况，规范信息维护、信息管理、运行维护等方面的工作流程和机制，指定专人负责系统运行的日常工作，及时补充和更新管理系统的业务数据，确保数据的完整性、时效性和准确性，并做好用户授权等管理服务工作。

第八条 各单位、部门要保证信息系统（含网站）安全，制定重要数据库和系统主要设备的容灾备案措施；记录并保留至少 180 天系统维护日志；妥善保管好账号和密码，定期更新密码，防止密码外泄。

第九条 网信办负责对学校信息系统使用情况进行监督、检查。对存在安全隐患的信息系统，网信办将停止其对外服务。

第十条 学校信息安全事件等级分为四级：IV 级（一般信息安全事件）、III 级（较大信息安全事件）、II 级（重大信息安全事件）、I 级（特别重大的信息安全事件）。I 级为最高级别。

（一）IV 级：一般信息安全事件，包括信息系统（含网站）遭受系统损失，产生一般的工作和社会影响。

（二）III 级：导致较严重影响或破坏的信息安全事件，包括信息系统（含网站）遭受严重的系统损失，产生较大的工作和社会影响。

（三）II 级:导致严重影响或破坏的信息安全事件，包括信息系统（含网站）遭受严重的系统损失产生重大的工作和社会影响。

（四） I 级：导致特别严重影响或破坏的信息安全事件，包括信息系统（含网站）遭受特别严重的系统损失，产生特别重大的工作和社会影响。

第十一条 对 IV 级信息安全事件，由信息系统(含网站）所属部门负责应急处置，并将有关情况向网信办报告。对 III 级、II 级、I 级的信息安全事件，由网信办调配应急资源，协助信息系统（含网站）所属部门进行处置。发生 II 级、I 级的信息安全事件，由学校网信领导小组向上级主管部门报告。

第十二条 将信息收集、记录和分析贯穿于信息安全事件应急处置全过程。校园网络与信息安全事件发生报警后，信息系统（含网站）所属部门要协助网信办全面、准确收集与事件相关信息，如采取现场快照或设备日志快照等，详细记录事件细节信息，了解事件造成的损失和影响；对安全事件的起因、性质、影响、责任、经验教训和恢复重建等问题进行调查评估；根据暴露的问题和调查评估结果，对信息安全事件应急预案进行相应的调整。

第四章 数据中心管理

第十三条 数据中心主要包括支撑学校信息系统的物理环

境（其中包含机房）、软硬件设备设施、云计算平台、学校中心数据库（其中包含基础数据库）、数据共享交换平台、统一身份认证平台及统一信息门户等信息化基础设施和平台。网信办负责数据中心的建设、运行、维护和管理。

第十四条 网信办负责数据中心物理环境、软硬件设备设施和云计算平台的建设和安全管理；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。

第十五条 网信办负责学校中心数据库、数据共享交换平台的建设和安全管理，负责基础数据库与各单位业务数据库之间完成数据交换和共享。各单位、部门负责建设、维护本单位、部门业务应用系统所配套的业务数据库，并对本单位、部门业务数据库及所申请的共享数据的安全负责。

第十六条 统一身份认证平台为学校信息系统提供统一的身份管理、安全的认证机制、审计及标准接口。各单位、部门建设面向师生服务的应用系统时，应使用统一身份认证平台进行身份认证。网信办负责统一身份认证平台的安全，各单位、部门负责本单位应用系统的权限管理及安全。

第十七条 原则上，各单位、部门应依托学校数据中心开展信息系统（含网站）建设。需使用校外数据中心的，须报网信办审批。涉及学校基础数据、师生员工个人信息或敏感信息的信息系统（含网站），不得部署在校外数据中心。未经批准，严禁使用境外数据中心。

第十八条 网信办对学校数据中心的使用实施准入管理，负责制定使用数据中心的技术规范和标准，在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。

第十九条 数据中心的使用单位应遵循数据中心相关管理制度和技术标准，按需申请、有序使用，不得利用数据中心资源从事任何与申请项目无关或危害信息技术安全的活动。

第五章 信息管理

第二十条 校园网所有用户必须遵守《中华人民共和国计算机信息网络国际互联网络管理办法》、《中华人民共和国保守国家秘密法》及国家有关法律法规和学校管理规定，严格执行信息安全保密制度，对所提供和发布的信息负责。

第二十一条 任何单位及个人不得利用校园网危害国家安全、泄露国家秘密；不得侵犯国家、社会、集体利益和个人的合法权益；不得从事违法犯罪活动；不得利用校园网制作、复制、传播和查阅下列信息:

（一）煽动抗拒、破坏宪法和法律、法规实施的;

（二）煽动颠覆国家政权、推翻社会主义制度的;

（三）煽动分裂国家、破坏国家统一的;

（四）煽动民族仇恨、民族歧视，破坏民族团结的;

（五）煽动非法集会、结社、游行、示威、聚众扰乱社会秩序的;

（六）捏造或者歪曲事实，散布谣言，扰乱社会秩序的;

（七）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的;

（八）公然侮辱他人或者捏造事实诽谤他人的;

（九）损害国家荣誉和利益的;

（十）以非法民间组织名义组织活动的;

（十一）其它违反宪法和法律、行政法规的。

第二十二条 各单位、部门要按照国家及学校有关规定，严格信息发布审核制度，未经审核的信息内容不得发布。凡涉及国家秘密和工作秘密的信息严禁上网。

第二十三条 校园网用户须自觉配合上级有关部门和学校的监督、检查。用户若发现违法有害信息，应及时向网信办报告。

第六章 电子邮件管理

第二十四条 电子邮箱开户实行实名制，在校教职工均可申请邮箱帐户。一个用户只能开设一个电子邮箱帐户。帐户不再使用时，须通知网信办进行注销。

第二十五条 电子邮箱用户须自觉配合上级有关部门和学校的监督、检查，并认真履行电子邮件操作的安全规定:

（一）用户须对帐户和密码的安全负责，对以其帐户进行的所有活动负责，应定期修改密码，加强密码强度，不得将账户和密码借与他人使用;

（二）用户若发现任何非法使用其帐户或存在安全漏洞的情况，应立即报告网信办;

（三）用户不要阅读和传播来历不明的电子邮件及其附件，提高对电子邮件病毒的防范意识，避免传播电子邮件病毒;

（四）用户传送日常办公文件时，应采取压缩加密等有效安全保护措施，并以附件的形式传送;

（五）用户应避免使用邮箱及密码注册第三方网站、论坛或在线服务等平台，如因此导致邮箱帐户和密码的泄露风险由用户承担。

第二十六条 网信办负责对校园网电子邮件系统使用情况进行监督、检查。有违反本办法第二十二条规定及发送垃圾广告邮件、存在安全漏洞情况的帐户，或连续两年没有登录电子邮件系统的账户，网信办将停止该帐户使用。

第七章 终端计算机安全管理

第二十七条 终端计算机是指由学校师生员工使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括台式电脑、笔记本电脑及其他移动终端。

第二十八条 终端计算机使用人按照“谁使用，谁负责”

的原则，对其终端计算机负有保管和安全使用的责任。

第二十九条 终端计算机设备上安装、运行的软件须为正版软件。在终端计算机上使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第三十条 终端计算机应当设置系统登录账号和密码，禁止自动登录，登录密码应具有一定强度并定期更改。

第三十一条 终端计算机使用人应做好数据日常管理和保护，定期进行数据备份。非涉密计算机不得存储和处理涉密信息。

第三十二条 终端计算机使用人应做好终端计算机的安全防范，如发现终端计算机出现可能由病毒或攻击导致的异常系统行为或其他安全问题，应立即断网后进行处置。

第三十三条 终端计算机使用人应对终端计算机妥善保管。若发生损坏丢失，按学校仪器设备相关管理规定处理。

第八章 存储介质安全管理

第三十四条 存储介质是指存储数据的载体，主要包括硬盘、存储阵列、磁带库等不可移动存储介质，以及移动硬盘、U盘等可移动存储介质。

第三十五条 原则上，存储阵列、磁带库等大容量介质应托管在学校数据中心。

第三十六条 各单位、部门应建立移动介质管理制度，记录介质领用、交回、维修、报废、损毁等情况。介质使用人按

照“谁使用，谁负责”的原则，对其移动介质负有保管和安全使用的责任。

第三十七条 非涉密移动存储介质不得用于存储涉密信息，不得在涉密计算机上使用。

第三十八条 移动存储介质在接入终端计算机和信息系统前，应当查杀病毒、木马等恶意代码。

第三十九条 介质使用人应注意移动存储介质的内容管理，对送出维修或销毁的介质应事先清除敏感信息。

第九章 人员安全管理

第四十条 各单位、部门应建立健全本单位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。关键岗位的计算机使用和管理人员应签订信息安全与保密协议，明确信息安全与保密要求和责任。

第四十一条 各单位、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，及时终止相关人员的所有访问权限，收回各种身份证件、钥匙、徽章以及学校提供的软硬件设备，并签署安全保密承诺书。

第四十二条 各单位、部门应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。

第四十三条 各单位、部门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。

第十章　外包服务安全管理

第四十四条 信息技术外包服务是指信息系统的开发和运维的外包。

第四十五条 外包服务需求各单位、部门应与信息技术外包服务提供商签订服务合同和信息安全与保密协议，明确信息安全与保密责任，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的任何信息资产，不得以服务为由强制要求委托方购买、使用指定产品。

第四十六条 信息技术现场服务过程中，外包服务需求单位应安排专人陪同，并详细记录服务过程。

第四十七条 外包开发的系统、软件上线应用前，外包服务需求单位应组织安全检查，要求开发方及时提供系统、软件的升级、漏洞等信息和相应服务。

第四十八条 网信办负责远程在线运维管理设备的统一购置、运维和管理。信息系统运维如需采用远程方式进行，必须通过远程在线运维管理设备统一进行管理。

第十一章　　信息安全应急管理

第四十九条 网信办负责制订学校信息技术安全应急预案，

若学校信息技术安全应急预案不能满足需求,相关单位、部门可制订本单位、部门信息技术安全应急预案。信息技术安全应急预案制修订后应及时报网信办备案。

第五十条 网信办定期组织信息技术安全应急演练,评估并适时组织信息技术安全应急预案修订。各单位、部门应组织开展信息技术安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第五十一条 各单位、部门应按照学校信息技术安全事件报告与处置流程，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作。做到安全事件早发现、早报告、早控制、早解决。

第五十二条 各单位、部门和师生员工均有义务及时向网信办报告信息安全事件，不得在未授权情况下对外公布、尝试或利用所发现的安全漏洞或安全问题。

第十二章　信息安全教育培训

第五十三条 网信办负责组织学校信息安全宣传和教育培训工作，建立健全相关制度。

第五十四条 网信办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。

第五十五条 网信办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。

第十三章　信息安全检查监督

第五十六条　各单位、部门定期对本单位、部门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，并配合有关部门的信息安全检查、信息内容检查、保密检查与审批等工作。

第五十七条　网信办对各单位、部门的信息技术安全工作落实情况进行检查，对发现的问题下达限期整改通知书，责成相关单位、部门制订整改方案并落实到位。

第五十八条　网信领导小组对年度安全检查情况进行全面总结，按照要求完成检查报告并报有关信息安全主管部门。

第十四章　信息安全责任追究

第五十九条　学校建立信息安全责任追究和倒查机制。

第六十条　有关单位、部门在收到网络信息安全限期整改通知书后，整改不力的，学校给予通报批评；玩忽职守、失职渎职造成严重后果的，依纪依法追究相关人员的责任。

第六十一条　各单位、部门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，学校将对相关单位责任人进行约谈或通报。

第六十二条 本校师生员工在交互式栏目（如论坛、贴吧等）中制作、复制、发布不良信息，造成严重后果者，学校将依据相关规定给予责任人相应的纪律处分，违反法律的承担相应的法律责任。

第六十三条 对违反本管理办法的，学校将予以警告、限期整改、封帐户（端口）直至安全问题排除；拒不改正或者导致危害信息技术安全等严重后果的，将追究相关单位、部门人员的责任；对违反有关法律、法规的，将依法追究法律责任。

第十五章 附则

第六十四条 各单位、部门要经常性地开展互联网信息安全和文明上网的宣传，加强对广大师生的教育和引导，增强政治意识、法制意识、责任意识、自律意识和安全意识，形成共同抵制网上有害信息的良好氛围。

第六十五条 本办法由网络安全和信息化办公室负责解释。

第六十六条 本办法自发布之日起施行，原《天津城建大学网络信息安全管理办法》（天城大政（2016）90号）同时废止。