北京工商大学文件

北工商校发〔2017〕29号

关于印发《北京工商大学网络及信息安全管理办法》的通知

各单位:

现将《北京工商大学网络及信息安全管理办法》印发给你们，请认真学习并遵照执行。

北京工商大学

2017年5月27日

北京工商大学网络及信息安全管理办法

第一章 总则

第一条 为保障我校网络信息安全，维护师生的合法权益，规范我校网络及信息安全管理，提高我校网络信息安全保障能力和水平，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》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《信息安全等级保护管理办法》和其他法律、行政法规的规定，制定本办法。

第二条 本办法所称的网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

第三条 本办法所称的计算机信息系统，是指由计算机及其 相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第四条 本办法所称计算机信息系统的安全保护，是指保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第五条 凡使用我校所有网络和计算机信息系统及其相关和配套的设备、设施（含网络）的任何单位和个人，必

须严格遵守国家相关法律及本办法的规定。

第六条 存储、处理涉及国家秘密信息的网络运行安全保护，除应当遵守本办法外，还应当遵守保密法律、行政法规的规定。涉密信息系统须严格遵守“涉密不上网，上网不涉密”原则。

第二章 组织保障

第七条 学校网络信息安全管理工作实行统一领导和分级管理，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则逐级落实安全责任制。

第八条 学校设立“北京工商大学网络安全和信息化建设与管理委员会”统一领导学校网络及信息安全管理工作。由学校党委书记和校长担任双组长，由分管信息化工作的校领导和分管稳定工作的校领导担任副组长。

第九条 学校各部门成立网络安全与信息工作小组，由各部门一把手任部门网络安全与信息工作小组组长，并选派政治思想过硬、具有较高计算机水平的人员担任部门网络安全与信息管理员，负责本部门网络运行和信息安全管理工作。

第十条 北京工商大学网络安全和信息化建设与管理委员会职责:

（一）组织拟订网络信息化建设中长期发展规划，落实信息化项目的申报、建设与使用管理;

（二）负责审议学校重大网络信息安全计划、网络信息安全规章制度的实施和部署;

（三）组织落实上级部门网络信息安全管理规定，协调

各部门网络信息安全工作；

（四）组织落实全校各部门计算机信息系统等级保护定级备案工作；

（五）对重大信息安全项目组织专家评估；

（六）对学校信息安全管理方面的重大事项进行处理；

（七）定期组织信息安全检查、评估和培训工作。

第十一条 各部门网络安全与信息工作小组职责：

（一）部门网络安全与信息工作小组组长

1. 负责本部门计算机信息系统等级保护定级备案工作的具体实施，落实信息安全防范工作；

2. 负责贯彻执行学校重大网络信息安全计划、网络信息安全规章制度，负责监督本部门信息系统（含网站）运行状况和管理情况；

3. 负责指定一名部门网络安全与信息管理员，具体负责本部门的网络信息安全管理；

4. 负责在重要敏感时期协调本部门网络安全管理工作，服从执行学校的安全策略；

5. 完成网络安全和信息化建设与管理委员会交办的其他任务。

（二）部门网络安全与信息管理员

1. 配合学校网络信息安全管理人员工作，组织开展本部门信息安全自查工作；

2. 完成学校网络信息安全管理人员下发的本部门信息系统安全漏洞的整改工作；

3. 完成本部门上线信息系统等级保护工作；

4. 负责本部门在国家法定节假日及重大活动中的信息安全保障工作，保证24小时联络手机开机及通讯畅通，掌握所属部门领导、网络中心人员的联系方式；

5. 对本部门的各系统管理员及时传达有关网络信息安全工作规定；

6. 负责本部门二级网站的安全报送工作；

7. 部门网络安全与信息管理员需报网络中心备案。如有变更应做好交接工作，并及时通知网络中心；

8. 严格要求信息系统开发厂家履行安全责任，签署相关安全保密协议。

第十二条 网络中心负责学校网络信息安全监督和指导工作。

（一）监督网络信息安全管理办法的落实，对网络信息安全管理工作提供培训、咨询；

（二）对不符合网络信息安全管理规范的项目或行为提出整改建议，并督促、检查整改落实情况；

（三）负责制定关于网络信息安全有关的规章制度；

（四）负责组织对计算机信息系统进行安全检测工作；

（五）负责新建计算机信息系统安全性的检查评估；

（六）负责全校计算机信息系统安全等级保护工作的组织。

第三章 校园网络安全管理

第十三条 学校网络核心机房由网络中心负责运行和维护。设置消防系统、视频监控系统、防雷系统、不间断电源系统、空调系统、机房环境监控系统、门禁系统等专业子系

统。硬件故障维护需要进入机房，需由网络中心机房管理人员核对人员信息及管理设备信息后登记后进入；厂家维护人员进入机房需有设备管理人员陪同进入，不得单独进入机房操作设备。

第十四条 各部门应建立完备的网络及计算机信息系统相关设备的登记制度，严格资产管理，明确设备使用者或管理者及其安全责任。

第十五条 各部门应根据设备重要程度采取不同的安全保护措施，制定完善的访问控制策略，防止未经授权使用设备。有特殊安全要求的设备应放置在机房的特殊功能区，必要时，单独建立门禁与监控系统，并配备防电磁泄漏的屏蔽装置等。

第十六条 网络中心负责学校网络和网络安全的统一规划、建设部署、策略配置和网络资源（网络设备、通讯线路、IP地址和域名等）分配。

第十七条 学校的网络建设和改造基本安全要求：

（一）符合学校网络安全管理要求，保障网络传输与应用安全；

（二）具备必要的网络监测、跟踪和审计等管理功能；

（三）针对不同的网络安全域，采取必要的安全隔离措施。

第十八条 网络中心应严格网络接入管理。任何设备接入网络前，接入方案、设备的安全性等应经过审核与必要的检测，审核（检测）通过后方可接入并分配相应的网络资源。校园网的所有用户实行上网实名制。

第十九条 网络中心有权对全校网络及信息系统进行

安全检测、扫描和评估。检测、扫描和评估结果属敏感信息，不得向外界提供。未经网络中心授权，任何单位与人员不得检测、 扫描学校内部网络。

第二十条 各部门应严格管理远程访问控制权限。确因工作需要进行远程访问的部门和人员应向网络中心提出书面申请，提供操作人员部门授权及操作人员个人信息，并采取相应的安全防护措施。各部门须严格管理用于远程管理维护的 VPN 账号和密码，确保合法使用。

第四章 信息系统安全管理

第二十一条 信息系统(本办法所指的信息系统是北京工商大学业务系统、管理系统等，包括数据库、软件和硬件支撑环境等)建设项目应在规划与立项阶段同步考虑安全问题，建设方案应符合相关网络信息安全规定。

第二十二条 信息系统开发应符合软件工程规范，依据安全需求进行安全设计，保证安全功能的完整实现，不得在程序代码中植入后门和恶意代码程序，开发、测试和修改工作不得在生产环境中进行。

第二十三条 各部门信息系统上线运行实行安全审查制度，未通过安全审查的任何新建或改造系统不得上线运行。

第二十四条 各部门应明确各信息系统管理人员，具体负责该系统的日常运行管理，并建立系统重要运行维护档案，详细记录系统变更及操作过程。

第二十五条 业务部门负责信息系统用户和权限设定，用户根据授权进行相关操作。

第二十六条 信息系统操作人员严格按照安全操作规程进行业务操作、数据备份，并配合本部门网络安全与信息工作小组保障网络信息安全。 一旦发现系统运行异常及时向本部门领导和网络中心报告。

第五章 信息系统安全等级保护管理

第二十七条 学校信息系统安全等级保护工作由网络中心牵头，负责组织学校各级各类信息系统安全定级保护工作。全校已有或新建的各类信息系统的主管部门作为网络信息安全管理及信息系统安全等级保护的第一责任单位，应严格按照要求，认真开展信息系统安全等级保护工作。

第二十八条 信息系统建设的负责单位在进行信息系统建设规划时，应充分考虑到信息系统安全建设的重要性，应明确将信息系统安全等级保护工作作为建设内容，并按照国家信息安全等级保护管理规范和技术标准，使用满足信息系统安全等级保护需求的信息技术产品，提升信息系统的安全。

第二十九条 为掌握全校信息系统建设情况，凡属上级单位（市教委等）下发、学校自建、研发、购置或升级改造的各类信息系统（软件），均应及时到网络中心登记备案。当信息系统不再使用，应及时到网络中心登记撤销，并进行撤销登记备案手续。

第三十条 信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。我校信

息系统定级由网络中心会同有关专家、北京市公安局内部单位保卫局协商后进行定级。

第三十一条 网络中心定期组织对全校新建信息系统或升级改造后的信息系统进行等级保护测评工作，并出具测评报告。

第三十二条 信息系统负责部门要根据测评报告，研究制定整改方案并落实，促进信息系统符合安全等级保护要求。

第六章 应急处置管理

第三十三条 各部门应按照北京工商大学网络安全和信息化建设与管理委员会要求制定和不断完善网络和信息系统等方面的应急预案。

第三十四条 各部门应定期组织应急预案的演练，并指定专人管理和维护应急预案，根据人员、信息系统等变动情况以及演练情况适时予以更新和完善，确保应急预案的有效性。

第三十五条 遇有突发情况应立即启动应急预案，控制事态发展，并按要求上报。

第三十六条 网络和信息安全事件应急处理后，情况得到恢复或得到有效控制，经北京工商大学网络安全和信息化建设与管理委员会批准后结束应急状态，进入整改阶段。

第七章 附则

第三十七条 本办法由北京工商大学网络安全和信息化建设与管理委员会负责解释。

第三十八条 本办法自发布之日起施行。

北京工商大学学校办公室 2017年5月27日印发