北 部 湾 大 学 文 件

湾大发〔2020〕103号

关于印发北部湾大学网络与信息安全管理办法的通知

校属各单位、各部门:

现将《北部湾大学网络与信息安全管理办法》印发给你们，请认真依照执行。

北部湾大学

2020年4月23日

北部湾大学校长办公室　　2020年4月23日印发

北部湾大学网络与信息安全管理办法

第一章　总则

第一条　为了保障学校网络与信息安全，维护学校权益，保护教职工、学生和其他校园网络用户的合法权益，促进学校信息化健康发展，根据《中华人民共和国网络安全法》等法律、法规和文件，结合本校实际，制定本办法。

第二条　北部湾大学网络信息系统的建设、运行、维护、使用、监督管理工作，适用本办法。

第三条　学校坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设，建立健全网络安全保障体系，提高网络安全保护能力。

第四条　学校采取措施，监测、防御、处置网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，维护学校网络空间安全和秩序。

第五条　学校网络安全与信息化建设领导小组统筹协调网络安全工作和相关监督管理工作。学校党委宣传部、网络与教育技术中心和其他有关部门依照本办法和有关法律、行政法规的规定，在各自的职责范围内负责网络安全保护和监督管理工作。

第六条　建设、运行网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应用网络安全

事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第七条 学校网络安全与信息化建设领导小组办公室指导学校各部门加强网络安全保护，提高网络安全保护水平，促进网络应用健康发展。

第八条 学校保护教职工、学生和其他网络用户依法使用网络的权利，普及网络接入，提升网络服务水平，为学校提供安全、便利的网络服务，保障网络信息依法有序自由流动。

学校网络用户应当遵守法律、行政法规，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第九条 学校任何个人和部门有权对危害网络安全的行为向学校和网信、电信、公安等部门举报。学校收到举报应当及时作出处理；不属于学校职责范围的，应当及时移送有权处理的部门。

学校应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十条 学校鼓励开发网络数据安全保护和利用技术，促进

公共数据资源开放，推动技术创新和经济社会发展。

学校支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十一条 党委宣传部、网络与教育技术中心等有关部门应当组织开展经常性的网络安全宣传教育，指导、督促学校各有关单位做好网络安全宣传教育工作。

学校各类传播媒介应当有针对性地面向全校进行网络安全宣传教育。

第十二条 学校应当经常性的组织开展网络安全培训，采取多种方式培养网络安全队伍。

第三章 网络运行安全

第一节 一般规定

第十三条 学校实行网络安全等级保护制度。学校应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改:

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任;

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月;

（四）采取数据分类、重要数据备份和加密等措施;

（五）法律、行政法规规定的其他义务。

第十四条 学校采购的网络设备、服务应当符合相关国家标准的强制性要求。发现学校的网络设备、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时向有关主管部门报告。

学校的网络设备、服务器具有收集用户信息功能的，应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守有关法律、行政法规关于个人信息保护的规定。

第十五条 学校实行实名制上网，学校在为网络用户办理网络接入服务时应当要求用户提供真实身份信息。用户不提供真实身份信息的，学校不得为其提供相关服务。

第十六条 学校应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第十七条 学校任何个人和单位不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第十八条 学校应当为公安机关、国家安全机关依法维护国

家安全和侦查犯罪活动提供技术支持和协助。

第十九条 学校应与网络运营者在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络安全保障能力。

学校应加强对网络安全风险的分析评估，定期向学校网络用户进行风险警示，支持、协助网络用户应对网络安全风险。

第二十条 学校有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第二十一条 学校对遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围由学校网络安全与信息化建设领导小组办公室参照国家有关规定制定。

第二十二条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第二十三条 除本办法第十四条的规定外，关键信息基础设施的运行部门还应当履行下列安全保护义务:

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查;

（二）定期对管理人员进行网络安全教育、技术培训和技能考核;

（三）对重要系统和数据库进行容灾备份;

（四）制定网络安全事件应急预案，并定期进行演练;

（五）法律、行政法规规定的其他义务。

第二十四条 学校任何信息系统包括关键信息基础设施在运行中收集和产生的个人信息和重要数据应当在校内存储；因业务需要，确需在境内公有云存储的，应当向学校网络安全与信息化建设领导小组办公室提出申请，由学校网络安全与信息化建设领导小组办公室会同学校有关部门进行安全评估，审核同意后才可以在境内公有云存储；学校禁止信息系统数据境外存储。

第二十五条 学校关键信息基础设施的运行部门应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关部门。

第二十六条 学校网络安全与信息化建设领导小组应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施:

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估;

（二）定期组织关键信息基础设施的运行部门进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力;

（三）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章 网络信息安全

第二十七条 学校对收集的用户信息严格保密，建立健全用户信息保护制度。

第二十八条 学校收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围并经被收集者同意。

第二十九条 学校不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供其个人信息。经过处理无法识别特定个人且不能复原的除外。

学校应当采取技术措施和其他必要措施，确保收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 学校任何个人和单位不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第三十一条 学校负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第三十二条 学校任何个人和单位应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第三十三条 学校应当加强对学校网络用户发布的信息管理，

发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录并向有关主管部门报告。

第三十四条 学校任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

第三十五条 学校应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

学校对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五章 监测预警与应急处理

第三十六条 学校建立网络安全监测预警制度。学校网络安全与信息化建设领导小组办公室统筹协调学校有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第三十七条 学校网络安全与信息化建设领导小组办公室统筹协调学校有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

第三十八条 网络安全事件发生的风险增大时，学校网络安全与信息化建设领导小组办公室统筹协调学校有关部门根据网络安全风险的特点和可能造成的危害，采取下列措施:

（一）要求有关部门和人员及时收集、报告有关信息，加强网络安全风险的监测;

（二）组织有关部门和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度;

第三十九条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大并及时向有关主管部门报告。

第四十条 由于网络安全发生突发事件的，应当依照有关法律、行政法规的规定处置。

第六章 违规责任

第四十一条 违反上述规定的，学校相关部门应及时进行处置，涉嫌违法的，移关上级主管部门处置。

第七章 附则

第四十二条 本办法解释权归属网络与教育技术中心。本办法自发布之日起施行。