包头医学院网络安全管理规定(修订)

第一章 总 则

第一条 为加强学校网络安全管理，保护校园网用户的合法权益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国计算机信息系统安全保护条例》和网络安全等级保护等相关法律法规，制定本规定。

第二条 学校网络安全工作的目标是建立健全网络安全工作体系和责任体系，提高网络安全防护能力，保障校园网络安全稳定运行。

第三条 本规定所称网络是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

第四条 学校网络安全工作遵循“谁管理谁负责、谁使用谁负责、谁维护谁负责”的原则，突出“依法管理、统筹规划、分工负责、积极预防”的工作方针。

第二章 管理监督职责

第五条 学校成立国家安全、校园安全综合治理委员会与安全生产工作领导小组，下设信息网络安全工作组，统筹学校网络

安全管理和监督工作，领导小组办公室设在网络信息中心。

第六条 学校网络安全管理和监督工作主要包括但不限于以下内容：

(一) 统筹规划网络安全建设工作；

(二) 建立健全网络安全监测预警、应急处置、防护措施等方面的工作机制及技术规范并贯彻落实；

(三) 开展网络安全通报工作，及时向相关单位和部门通报安全信息；

(四) 组织落实网络安全等级保护相关工作；

(五) 督促各单位、各部门落实网络安全责任；

(六) 做好网络安全宣教工作；

(七) 组织开展网络安全应急演练；

(八) 组织开展校内网络安全检查，并指导、督促发现安全隐患的单位和部门在期限内落实整改工作，必要时进行复查；

(九) 组织开展舆情监测与防控；

(十) 做好网络安全事件应急处置工作。

第三章 责任和义务

第七条 学校实行网络安全管理工作责任制。各单位、各部门主要负责人作为第一责任人，负责其职责范围内的网络安全管理工作。

第八条 各单位、各部门须设置网络安全工作岗位，并配备相应工作人员，在学校信息网络安全工作组领导下，配合领导小组办公室开展工作，加强本单位、本部门网络安全管理。岗位人

员实施规范管理，上岗、离岗均须按流程向领导小组办公室报备。

第九条 除网络主管部门，其他单位、部门或个人不得以任

何方式试图登录进入网络节点、服务器、存储等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施。

第十条 任何单位和个人不得从事校园网账户及口令的侦听、盗用活动。

第十一条 校园内从事工程、维修等活动不得危害网络系统安全。

第十二条 严禁任何单位和个人在校园网上使用来历不明、易引发病毒传染的软件。各单位、各部门业务系统及工作计算机须做好防病毒技术措施。

第十三条 任何单位和个人不得利用校园网及其联网计算机发布(包括转发)危害国家安全、社会稳定的信息(包括多媒体信息)、录阅传送淫秽、色情资料。

第十四条 学校公共机房一律不允许对社会开放，落实实名认证管理，相关记录须保留一年以上。

第十五条 确因工作需要，由厂家或第三方提供信息服务，须单位或部门负责人与服务提供方签署信息服务保密协议。

第十六条 各单位、各部门须加强存储介质使用管理，重点岗位计算机及业务系统服务器须使用专用存储介质，使用前须完成病毒检测。

第十七条 各单位、各部门须加强业务系统及工作计算机的密码、密钥安全管理，设置符合安全保密策略的密码并定期进行更换。

第十八条 各单位、各部门工作人员须对在其职责中知悉

的国家秘密、工作秘密、商业秘密、重要数据、个人信息和隐私严格保密，不得泄露、出售或者非法向他人提供。

第十九条 确认发生重大网络安全事件，相关单位、部门人员须立即报告学校国家安全、校园安全综合治理委员会与安全生产工作领导小组，同时上报信息网络安全工作组，并采取有效措施控制事件扩大，积极协助有关人员对安全事件的调查并配合做好善后处理工作。

第四章 督查与问责

第二十条 网络安全工作纳入年度工作目标考核，网络信息中心在职责范围内依法依规对各单位、各部门开展日常检查及年度考核。

第二十一条 对网络安全责任落实不到位的单位、部门责令限期整改；存在重大安全隐患或发生网络安全事件的，对单位、部门主要负责人进行约谈、口头警告或通报批评，情节严重的依据国家有关法律法规予以处理。

第五章 附 则

第二十二条 本规定由网络信息中心负责解释。

第二十三条 本规定自印发之日起施行，原《关于印发〈包头医学院网络安全责任制度(2019年修订)〉的通知》(包医党发〔2019〕21号)、《关于印发〈包头医学院网络安全管理办法〉的通知》(包医党发〔2019〕22号)同时废止。