广 西 工 商 职 业 技 术 学 院

文 件

广商院信息〔2021〕2 号

广西工商职业技术学院关于印发《广西工商职业技术学院网络与信息安全管理办法》的通知

各部门、各单位：

现将《广西工商职业技术学院网络与信息安全管理办法》印发给你们，请遵照执行。

附件：广西工商职业技术学院网络与信息安全管理办法

广西工商职业技术学院

2021 年 7 月 6 日

广西工商职业技术学院
网络与信息安全管理办法

第一章 总则

第一条 为加强学校网络与信息安全管理，提高网络与信息安全防护能力水平，保障数据安全和信息系统稳定可靠运行，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》、《中华人民共和国计算机信息系统安全保护条例》等国家法律法规和上级有关文件精神，结合学校实际，制定本办法。

第二条 本办法适用于学校计算机网络（以下简称校园网）、校园信息化基础设施、教学、科研、管理和服务相关的网站与信息系统、新媒体、数字资源系统等所涉及的硬件、软件和信息的安全。

第三条 学校网络与信息安全管理的目标是建立健全网络安全保障体系，落实网络安全责任，提高网络安全防护能力，确保网络安全工作规范、有序进行，保障信息化工作顺利开展。

第四条 学校网络安全工作遵循“谁主管谁负责、谁建设谁负责、谁使用谁负责”的原则，明确责任主体，强化安全意识，逐级落实单位与个人安全责任制。

第二章 管理机构与职责

第五条 学校网络安全与信息化工作领导小组（以下简称网信领导小组）是学校网络与信息安全工作的领导机构，统筹指导学校网络安全建设和管理，指导重大网络安全事件的处理。

第六条 网络安全与信息化工作领导小组办公室(以下简称网信办)负责学校网络信息与安全工作的组织实施、监督检查，负责制定学校网络与信息安全相关政策，处置网络安全事件，负

责与上级网络信息安全管理部门的任务对接和工作协调，负责学校网络安全宣传教育培训。

第七条 党委宣传部负责对网络信息内容进行监督、检查，对网络舆情信息进行监控、管理和引导。对于不良或有害信息，应在第一时间联系相关部门进行处理；对涉嫌违法犯罪的信息，应立即向学校保卫处及公安机关报案。

第八条 信息技术中心负责学校网络与信息安全防护系统的规划建设、运行管理和安全等级保护；负责对网络信息安全出现的攻击和漏洞进行监控、布防、修复、整改；负责协助相关部门对网络信息安全事件进行调查取证和技术处理；负责对全校网络与信息安全工作提供技术支持和技术保障；负责对学校网络信息安全人员进行技术指导和培训。

第九条 各部门、单位是本单位网络安全工作的责任主体，负责本部门、单位网络安全工作。各部门、单位党政主要负责人是本单位的网络安全第一责任人，对本单位的网络安全负领导责任。各单位须建立本部门网络安全管理机制，设置一名网络信息安全管理员，负责本单位应用系统及网站的运行维护和网络信息安全的具体工作;负责本部门、单位的网络安全宣传教育培训，提升师生员工的网络安全防范意识。

第三章 网络运行安全

第十条 校园网包括校园有线网、无线网和一卡通、财务、安防等各类专网。校园网由学校统一规划建设，禁止私拉乱接及私自接入网络设备、服务器等各类设备。

第十一条 校园网实行出口统一管理。未经批准，不得在校园网内建设互联网出口。禁止将校园网接入延伸至校外。

第十二条 校园网实行用户统一管理，用户 IP 地址未经许可不得对校园网以外提供互联网服务。

第十三条 校园网用户使用网络应当遵守法律法规以及学校的有关规定，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。

第十四条 校园网用户不得从事或协助进行非法侵入校园网、干扰校园网正常功能、盗用用户账号等危害校园网安全的活动。校园网用户应妥善保管自己的系统账号密码，因个人账号管理不善对学校网络安全造成危害的，将追究其责任。

第十五条 未经批准，各部门、单位原则上不得单独建设机房、网络、存储资源、计算资源等基础设施。

第十六条 建立数据中心机房管理制度，明确机房消防、空调、温湿度控制、视频监控、供配电、门禁、出入人员等方面的规定，加强机房的安全管理，保障网络信息基础设施安全。

第四章 信息系统安全

第十七条 信息系统包括但不限于各部门业务信息系统（含采用移动互联技术的系统）、云计算平台（系统）、大数据应用（平台、资源）、物联网等。

第十八条 信息系统原则上应依托于学校数据中心建设，使用学校 IP 地址及域名，并进行登记备案。涉及学校基础数据、师生个人信息或敏感信息的信息系统，不得部署在校外。

第十九条 信息系统面向在校师生的用户认证应当使用学校统一身份认证，不得单独建立用户认证系统。

第二十条 各部门、单位应准确掌握本单位信息系统建设情况，加强网络安全监控，指定专人负责信息系统的日常运维和安全管理，落实网络安全责任。

第二十一条 各部门、单位在信息系统等建设中涉及的个人信息，按照国家相关法律法规及学校相关规定进行严格保护，应当采取技术措施和其他必要措施，做好个人信息、隐私等严格保护，确保信息安全，防止信息泄露、毁损、丢失。任何部门、单位及个人不得违法违规采集、存储、使用和处理校内各类个人信息。未经批准，任何部门、单位和个人不得擅自对外提供信息系统的内部数据。对于违反规定非法提供数据的部门、单位和个人，将依照相关规定予以处罚。

第二十二条 各部门、单位应做好本单位信息系统的备份和恢复管理，明确备份策略、备份存储及数据恢复流程等，定期测试备份数据的有效性。

第二十三条 各部门、单位应做好重要时期网络安全保障工作，加强网络信息系统的安全管理，做好安全处置。

第二十四条 各部门、单位要建立网站信息发布审核审查程序。严格信息发布、转载和链接管理。确保信息内容的准确性、真实性和严肃性，确保信息内容不涉及国家秘密和内部敏感信息。

第二十五条 学校杜绝出现并持续清理以下类型的“僵尸”和“双非系统”。

（一）符合如下条件之一的，视为“僵尸”网站（信息系统）：

1. 网站年访问量在 1000 人次以下的；

2. 网站 180 天以上未更新的或专题网站已完成工作使命的；

3. 网站（信息系统）每年录入信息在 100 条以下的；

4. 网站（信息系统）无人运行维护或运行维护缺乏基本保障的。

（二）符合以下条件的，视为“双非”网站（信息系统）：

各部门、单位网站（信息系统）使用的是非学校租用 IP 地址和非学校注册网络域名的。

第二十六条 对长期无人管理、内容不更新、存在安全隐患、管理制度缺失、无固定管理维护人员的信息系统，将采取暂时关闭措施并进行限期整改。整改完成后，方可恢复运行。

第五章 处置管理及责任追究

第二十七条 建立健全网络安全通报机制和应急处理机制，全力维护学校网络空间安全稳定。由网信办负责制定网络安全事件应急预案，学校各部门、单位发现网络与信息安全事件应第一时间报告网信办，采取措施处理安全漏洞、安全威胁，保存相关日志记录。

第二十八条 网信办依据网络安全监测预警信息，按照学校网络安全事件应急预案组织对校内网络安全事件的处理。相关单位及人员应积极配合，根据安全预警信息，认真查找网络安全隐患和漏洞，及时做好相应排查处置工作。为避免安全事件不良影响扩大，网信办有权直接对安全事件相关的网络及信息系统进行断网、停止服务等应急处理。

第二十九条 各部门、单位须熟悉学校网络安全事件应急处置措施，当校园网内发生网络安全事件时，应当立即响应网络安全事件应急预案，并按应急预案规定进行处置。

第三十条 各部门、单位和个人应当履行网络安全职责。对违反网络安全管理相关制度、不落实网络安全工作责任制以及未尽职责或管理不善而造成严重后果的，学校将追究该部门、单位主要负责人和直接责任者的责任。对触犯法律的，将移送公安司法机关处理。

第三十一条 有关部门、单位在收到网信办关于网络安全存在问题的限期整改通知书后，整改不力的或逾期不整改的或发生网络安全事件如有瞒报、缓报、处置和整改不力等情况，学校将对相关部门、单位责任人进行约谈或通报；对玩忽职守、失职渎

职造成严重后果的，依纪依法追究相关人员的责任；对触犯法律的，将移送公安司法机关处理。

第三十二条 对损坏校园网络系统或信息系统设备设施的个人，学校将视其情节轻重追究责任，如触犯法律应移交公安司法机关处理。

第六章 附则

第三十三条 本办法自发布之日起施行，由学校网信办（信息技术中心）负责解释。

第三十四条 以往发布的与本办法不相符的规定，按本办法执行。