

武汉体育学院文件

武体院字〔2014〕73号

武汉体育学院网络信息安全管理制度

第一章 总 则

第一条 为了加强校园网和网络信息的安全管理，维护公共秩序和学校稳定，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国校园网国际联网管理暂行规定》及公安部《校园网国际联网安全保护管理办法》等相关法律法规的规定，制定本制度。

第二条 本制度适用于通过网络介质连入本校校园网的所有计算机通信设备（以下简称“设备”），以及该设备的所有者、使用者和管理者（以下统一简称“用户”）。

第二章 设备和用户

第三条 学校对连入校园网的设备和用户实行两级认证，实名注册上网。设备名与校园网网络资源使用权限对应，用户名（账号）与数字化校园应用系统使用权限对应。未通过认证的设备不能连入校园网，未通过认证的用户不能使用数字化校园共享资源。

第四条 信息化建设办公室负责对设备的网络资源和用户的上网行为实行分类管理。

第五条 学校将设备分为个人设备、公共设备、特殊设备；用户分为公共用户、特殊用户和个人用户。

1.校内各部门的业务专用设备、教学科研等场所的公用设备等公共资产属于公共设备，其资产归属部门（部门指学校内部的院、系、部、处、直属单位等，下同）属于公共用户。

2.各种服务器（包括联网机房内的相关公共资产等）属于特殊设备，其业务管理部门属于特殊用户。

3.上述之外其他所有设备（个人所有或个人专用）属于个人设备，公共资产的使用者默认为该设备的用户，私有资产的拥有者默认为该设备的用户。

4.如无特殊说明，本制度的所有条款适用于所有用户。

第六条 用户账号

校内在籍在编的师生员工和离退休人员由主管部门提供身份码，经认证注册后成为用户，其在办公区使用的公有设备按统一编码（设备名）通过认证后连入校园网。教职工住宅区和学生宿舍

舍区内师生员工的私有设备要求办理入网手续的，由用户向信息化建设办公室申请。

第七条 外籍人员要求办理入网手续的必须经外事主管部门审批，并报保卫部门备案后向信息化建设办公室提出申请。在校园内从事与学校有关工作的外部公司、商户、人员等，要求办理入网手续的，须经业务主管部门审批，并报保卫部门备案后向信息化建设办公室提出申请。

第八条 校园网用户合法的通信自由和通信秘密受法律保护。

第三章 违法违规行为

第九条 任何用户不得利用校园网从事危害国家安全、泄露国家秘密的活动，不得侵犯国家、社会、集体的利益和公民的合法权益，不得通过校园网从事其它违法犯罪活动。

第十条 任何用户不得利用或通过校园网制作、复制、查阅和传播下列信息：

- 1.煽动抗拒、破坏宪法和法律、行政法规的实施；
- 2.煽动颠覆国家政权，推翻社会主义制度；
- 3.煽动分裂国家、破坏国家统一；
- 4.煽动民族仇恨、民族歧视，破坏民族团结；
- 5.捏造或者歪曲事实，散布谣言扰乱社会秩序；
- 6.宣扬封建迷信、邪教意识、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪；

- 7.公然侮辱他人或者捏造事实诽谤他人；
- 8.发送恶意的、挑衅性的信息；
- 9.损害国家机关信誉。

第十一条 任何用户不得从事下列危害网络信息安全的活动：

- 1.未经允许进入校园网或使用校园网资源；
- 2.未经允许对校园网功能进行删除、修改；
- 3.未经允许对校园网中传输、处理的数据或应用程序进行删除、修改；
- 4.以任何理由制作和传播计算机病毒、攻击网络服务、扫描网络端口、盗用网络资源。

第十二条 任何用户不得私自转借或转让设备、账号和IP地址，不得因管理不严而造成所属设备、账号和IP地址被非法挪用、占用。

第十三条 任何用户不得私自在校园网上架设服务器并非法提供网络服务。

第十四条 任何用户不得将国家秘密文件、资料等输入联网的计算机，不得将学校科研主管部门规定密级的科研资料等输入联网的计算机。

第十五条 任何用户在校园网上发布商业信息必须通过相关部门批准，不得将校园网作为谋取不当获利的途径。

第十六条 不得从事其它违法违规、损害学校声誉和危害校

园网网络安全的活动。

第四章 安全保护责任

第十七条 学校依法实施上网行为和信息安全管理。保卫部门和信息化建设办公室共同负责校园网信息安全保护管理工作，负责对校园网用户和设备的安全监督、检查和指导。信息化建设办公室依照法律和国家规定负责外网出入口信道，负责校园网络主干链路的运行安全保护，负责建立信息安全等级保护，负责进行与上述职责有关的备案、上报、审批工作。保卫部门负责网络设备安全保卫，负责配合公安机关对违法行为追究法律责任。

第十八条 学校宣传主管部门负责建立校园网电子公告系统的用户登记和信息管理制度。科研主管部门负责对科学研究方面的文件、资料、成果确定密级。

第十九条 公共用户应明确辖内所有设备的使用者和管理者，指定1名系统管理员负责设备安全、上网行为和信息安全工作，协助学校主管部门开展信息安全和保密工作的检查与指导。

第二十条 特殊用户的部门行政负责人为该用户信息安全主管负责人，负责管理所属服务器及联网机房的安全事宜，建立健全本部门网络信息安全保护管理制度；落实安全保护技术措施，保障本部门网络设备的运行安全 and 信息安全；及时关闭因任何原因已停用的服务器；对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照第十条规定进行审核；协助学校

主管部门开展信息安全和保密工作的检查与指导。

第二十一条 学校各部门行政负责人为该部门信息安全主管负责人，负责本部门设备的网络管理和网络用户的安全教育；及时向信息化建设办公室通报人员调整或变动情况，确保用户身份受控；如发现有第十条、第十一条所列情形之一的，应当保留有关记录，并及时向信息化建设办公室报告。

第二十二条 用户有义务协助保卫部门和信息化建设办公室查处上述第十条、第十一条所列违法行为，如实反映有关情况，如实提供有关信息、资料及数据文件。

第二十三条 信息化建设办公室对联网的固定接入设备和服务器，每年清理登记一次。

第五章 责任追究

第二十四条 用户有违反网络信息安全法律法规的，有违反本制度第十条、第十一条所列行为之一的，取消其联网资格，并由保卫部门给予相应的惩罚措施；构成犯罪的，依法追究法律责任。

第二十五条 违反第十二条、十三条、十四条、十五条、十六条规定的用户，信息化建设办公室将给与关闭其账号，取消其入网资格。

第二十六条 违反第十二条、十三条、十四条、十五条、十六条规定，造成直接经济损失的，账号持有人负责赔偿；有违法行为的，保卫部门依法追究账号持有人和当事人的法律责任。

第二十七条 特殊用户未履行第二十条所列职责的，信息化建设办公室将给予警告，责令其限期整改。情节严重的，可给予停止联网处罚，直至整改合格后，方可恢复联网。如造成重大损失，应对相关责任人及主管负责人追究责任。

第六章 附 则

第二十八条 本制度自下发之日起施行，信息化建设办公室负责解释。



二〇一四年九月二十二日

主题词：网络信息 安全管理 制度

武汉体育学院办公室

2014年09月24日印发
