浙江大学宁波理工学院商学院文件

理工商[2017]10号

商学院关于印发《浙江大学宁波理工学院商学院网络与信息安全管理办法》的通知

各研究所、实验中心、各部门：

经研究决定，现将《浙江大学宁波理工学院商学院网络与信息安全管理办法》印发给你们，请遵照执行。

商学院

2017年10月20日

浙江大学宁波理工学院商学院网络与信息安全管理办法

根据浙江大学宁波理工学院《校园网络与信息安全条例》和国家有关法律规定，为保证商学院网络的正常运行和健康发展，结合我院实际情况，特制定本管理办法。

一、商学院网络信息安全管理实施工作责任制，学院党政主要负责人中有一人为网络信息安全责任人，并配备信息员，负责本学院内网络的信息安全管理工作。

二、学院根据各内容模块安排具体的信息员，负责所在模块的账户密码安全、内容维护及审核等工作，账户密码由各负责人专人保管，不得外泄。

三、各学科平台、专业创建的网站及公众危险号由各平台、各专业负责人负责，并选派安全责任人及信息员负责日常维护、审核工作，并提前向商学院党政办公室报备。

四、凡在商学院网站及微信公众号上发布的内容需要做好信息发布的审核工作，做好信息监视保存、清除和备份工作。

五、不允许在商学院网站及微信公众号上进行任何干扰网络用户、破坏网络服务和网络设备的活动；不允许在网络上发布不真实的信息或散布计算机病毒；不允许通过网络进入未经授权使用的计算机系统；不得以不真实身份使用网络

资源；不得窃取他人帐号、口令使用网络资源；不得盗用未经合法申请的IP地址入网。若发现以上行为，将进行追责。

六、商学院网络所有工作人员及用户必须对所提供的信息负责，严禁在商学院网站及微信公众号上进行下列行为：

1.查阅、复制或传播下列信息：

（1）煽动抗拒、破坏宪法和国家法律、行政法规实施；

（2）煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度；

（3）捏造或者歪曲事实，散布谣言扰乱社会秩序；

（4）侮辱他人或者捏造事实诽谤他人；

（5）宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

2.破坏、盗用计算机网络中的信息资源和危害计算机网络安全的活动。

3.盗用他人帐号、盗用他人IP地址。

4.私自转借、转让用户帐号造成危害。

5.故意制作、传播计算机病毒等破坏性程序。

6.不按国家和学校有关规定擅自开设二级代理接纳网络用户。

7.上网信息审查不严，造成严重后果。

8.以端口扫描等方式，破坏网络正常运行。

发现有上述行为者，商学院党政办公室可对其提出警告乃至停止其网络使用。情节严重者，由学校有关部门依照校纪、校规及法律、法规进行处理；如触 犯国家有关法律、法规者，移交公安、司法部门处理。

附件 1 商学院网络工作具体工作人员名单

附件 2 商学院网站应急预案

浙江大学宁波理工学院商学院

二０一七年十月二十日

附件 1

商学院网络工作具体负责人名单

具体内容	负责人
商学院网站建设；实验室建设	陆　泳
商学院网站新闻等信息、学院人事及师资信息	许　菁
学院党政、对外联络及各研究所信息	陈　恩
学院学工及校友信息	袁彦鹏、马双龙、董俊娜
学院分工会信息	肖　玮
学院教务教学及招生信息	王一程
学院学科建设、科研信息	潘　锋

附件 2

商学院网站应急预案

（一）网站、网页及公众微信号出现非法言论时的紧急处置措施

1、网站、网页及公众微信号由具体工作人员人员对所负责模块进行日常监视信息内容。

2、发现网上出现非法信息时，负责人员应立即向学院党政办公室负责人及分管领导通报情况，情况紧急时应先及时采取删除等处理措施，再按程序报告；并由学校信息中心负责技术指导与支持。

3、具体负责人员应在接到通知后要立刻采取行动，作好必要的记录，清理非法信息，强化安全防范措施，并联系学校信息中心，确保网站网页重新投入使用。

（二）黑客攻击时的紧急处置措施

1、当网站负责人或其他人员发现网页内容被篡改或系统检测到有黑客正在进行攻击时，应立即向信息中心相关工作人员通报。

2、信息中心工作人员应立即赶到现场，并首先将被攻击的服务器等设备从网络中隔离出来，并保护现场，同时向信息中心负责人汇报情况。

3、网站、网页各具体负责人员负责被破坏系统数据的恢复

与重建工作。

4、网站、网页具体负责人员协同有关部门共同追查非法信息来源。

5、如情况严重，应立即向公安部门或上级机关报警。

（三）病毒安全紧急处置措施

1、当发现计算机感染有病毒后，应立即将该机从网络上隔离出来。

2、对该设备的硬盘进行数据备份。

3、启用反病毒软件对该机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作。

4、如发现反病毒软件无法清除该病毒，应立即向信息中心工作人员人员报告。

5、信息中心工作人员在接到通报后，应立即赶到现场。

6、经信息中心工作人员确认无法查杀该病毒后，应作好相关记录，同时立即向信息中心主任报告，并迅速联系有关产品厂商研究解决。

7、情况特别严重的，应立即向公安部门或上级机关报告。

8、如果感染病毒的设备是服务器或主机系统，经信息安全领导小组负责人同意，应立即告知各负责单位做好相应的清查工作。

（四）软件系统遭受破坏性攻击的紧急处置措施

1、重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日备份，并将它们保存于安全处。

2、一旦软件遭到破坏性攻击，应立即向信息中心工作人员报告，并将系统停止运行。

3、网站、网页具体负责人员负责软件系统和数据的恢复。、

4、网站、网页具体负责人员、信息中心工作人员检查日志等资料，确认攻击来源。

5、情况特别严重的，应立即向公安部门或上级机关报告。

浙江大学宁波理工学院商学院

二０一七年十月二十日

抄送：毛才盛副院长，学院领导，学院党委，分工会、团委。

商学院党政办公室　　主动公开　　2017 年 10 月 20 日印发