上海震旦职业学院

信息管理中心工作制度汇编

（2019）

目　录

上海震旦职业学院校园网络管理办法

（2015 年 6 月　沪震职〔2015〕71 号）

一、总则

1. 上海震旦职业学院校园网（以下简称校园网）是学校重要的基础设施，是学校管理、教学和科研的重要工作平台。为了加强校园网的管理，保护校园网的安全、促进学校数字化应用、保障校园网络的正常运行和学校用户的权益，特制定本办法。

2. 本管理办法所称的校园网络系统，是指由学校投资购买、由信息中心负责维护和管理、由校园网络主、辅节点设备、配套的网络线缆设施及网络服务器等设备所构成的，为学校教育教学、管理等各类活动提供网络与信息化服务的硬件、软件的集成系统。

3. 校园网使用者（以下简称“用户”）必须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国教育和科研计算机网管理办法》和国家有关法律、法规，以及中国教育和科研计算机网制定的其他制度。

4. 用户不得利用校园网从事危害国家安全、泄露国家秘密、颠覆国家政权、破坏国家统一等犯罪活动；不得损害国家荣誉和利益；不得煽动民族仇恨、民族歧视，破坏民族团结；不得破坏国家宗教政策，宣扬邪教和封建迷信；不得散布谣言，扰乱社会秩序，破坏社会稳定；不得散布淫秽、色情、赌博、暴力、凶杀、

恐怖或者教唆犯罪；不侮辱或者诽谤他人，侵害他人合法权益；以及其他政府法律、行政法规禁止的其他内容。

二、安全管理

1.校园网络系统的安全运行和系统设备的管理维护工作由信息中心负责,信息中心可以委托相关单位指定人员代为管理子节点设备。任何单位和个人,未经信息中心同意均不得擅自安装、拆卸网络设备或改变其配置，也不得私自铺设网络线缆、改变网络拓扑结构。

2.用户必须接受国家安全部门依法进行的监督检查以及所采取的必要措施；接受学校信息中心必要的管理。

3.用户不允许进行任何干扰其它网络用户,破坏网络服务和网络设施的活动。这些活动包括（但并不局限于）商业广告，散布计算机病毒，使用网络联入未经授权使用的计算机系统。

4.学校信息中心设有网络安全管理人员，负责监察、检查网络信息的使用,防止危害网络安全的事故和非法使用网络资源的情况发生。校园网主、辅节点设备及服务器等发生案件、以及遭到黑客攻击后,网络管理人员必须在二十四小时内向校保卫部门及公安机关报告。

5.学校中心机房须安装防盗安保设施并进行定期检查,发现问题须立即向有关部门汇报并及时解决。

6.任何单位和个人、不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动,不得危害或侵入未授权的(包括 CERNET 或其它互联网在内的)服务器、工作站。

7.除信息中心外,其他单位或个人在未经允许的情况下不得以任何方式试图登录校园网主、辅节点、服务器等设备进行修改、设置、删除等操作;任何单位和个人不得以任何借口盗窃、破坏校园网设施,这些行为将被视为对校园网安全运行的破坏。

8.所有联网计算机应安装使用计算机病毒防治软件,严禁在校园网上使用来历不明、引发病毒传染的软件。

9.所有联网计算机应及时升级操作系统的补丁软件。同时必须按一定的安全标准要求,设置超级用户口令。对没有安装杀毒软件或没有及时更新系统升级补丁以及不设置系统超级用户口令的部门或个人用户,校园网负责单位有权进行抽查和督促用户改正,以免引发大面积的网络拥塞和侵害其它用户的安全。

10.经信息中心批准开设的服务器必须保持日志记录功能,历史记录保持时间不低于 3 个月。服务器上开设的用户必须按照上海市公安局计算机监察处要求登记的内容,并妥善保管、备查。信息中心要按照上海市公安局计算机监察处的要求规定,不定期地检查各开通服务器的计算机日志。

三、网络管理

1. 用户的 IP 地址和电子邮件帐号分别由信息中心授权使用，未经信息中心书面同意，不得更改和转让 IP 地址和电子邮件帐号。

2. 网络使用者不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动，该活动被认为是对学校网络用户权益的侵犯。

3. 用户利用校园网获取和使用网络上的软件应遵守知识产权的有关法律。

4. 校园网工作人员和用户在网络上发现有碍社会治安和不健康的信息有义务及时上报学校有关部门按照有关规定进行处理。

5. 校园网的用户有义务向网络管理人员报告任何违反本办法的行为。

四、网络基础设施管理

1. 网络基础设施包括各校园之间的光纤通信线路/链路、各校园内各楼宇之间的室外通讯光缆、各楼宇内的计算机网络综合布线系统、室内信息插座、各楼宇配线间内的网络机柜、配线架、跳线和网络设备等。

2. 未经信息中心同意，任何单位和个人不得擅自安装、拆卸或改变网络设备；不得以任何借口盗窃、破坏网络基础设施。除信息中心，其他部门或个人不得以任何方式试图登陆进入校园网

主、辅节点、服务器等设备进行修改、设置、删除等操作，这些行为被视为对校园网安全运行的破坏行为。

3.任何部门或个人都有义务保护校园网网络基础设施，发现校园网网络基础设施的破坏行为或事件应及时通知学校信息中心或保卫处，信息中心将会同公安部门进行处理。对校园网网络基础设施造成破坏的单位或个人，将按国家和学校有关法规和规定进行处理，严重的移交公安机关处理。

4.对于新建楼宇或旧楼大修改造，信息中心应配合学校基建部门和后勤部门做好项目相关的校园网网络基础设施规划和设计工作，包括楼内布线要求、配线间位置、室外光缆路由等，根据要求做好有关技术支持和监理等工作。

5.对道路施工、暖气沟施工等凡涉及到地下网络通讯光缆的工程，主管单位应提前通知信息中心，施工过程中应采取必要的措施保护网络通讯光缆。对新建道路应将校园网通信管道纳入规划建设范畴。

五、其它

1.信息中心对违反本规定的接入部门和个人用户将给予警告、停止使用网络、行政处理等处罚，涉及违法的将由司法机关依法追究责任。

2.本管理办法自发布之日起执行，由信息中心解释。

上海震旦职业学院校园网有害信息事件及重大网络故障应急预案

（2015 年 6 月　沪震职〔2015〕73 号）

校园网是学校整个基础建设的重要组成部分，随着网络基础建设的不断拓展和完善，网络应用的不断丰富，校园网在学校教学科研、行政管理等工作中发挥着越来越重要的作用。但是也必须清醒地意识到，境外敌对势力和邪教组织等利用国际互联网进行有害信息传播和煽动的企图不断，网上大规模“黑客”攻击、计算机病毒危害的风险不断，对正常的网上教学、办公、通讯等活动构成了严重威胁。为了快速、准确、妥善地处理校园网上出现有害信息及网络链路上出现故障的紧急情况，特制定本应急预案，以确保能做好应急处置的组织工作，以最快速度恢复校园网络正常运作，最大限度地减小网络事故所造成的影响和损失。

一、应急预案

1. 网站、网页出现非法言论时的应急预案

（1）网站、网页由负责网站维护的管理员随时监控信息内容。

（2）发现在网上出现非法信息时，网站管理员立即向信息中心领导通报情况，并作好记录。清理非法信息，采取必要的安全防范措施，将网站、网页重新投入使用；情况紧急的，应先及时采取删除等处理措施，再按程序报告。

（3）网站管理员应妥善保存有关记录、日志或审计记录，将有关情况向信息中心领导汇报，并及时追查非法信息来源。

（4）事态严重的，信息中心立即上报分管校领导由分管领导统一组织、协调指挥进行应急处置。

2.黑客攻击或软件系统遭破坏性攻击时的应急预案

（1）重要的软件系统平时必须要备份，与软件系统相对应的数据必须至少有3个月的备份，并将它们保存于安全处。

（2）当管理员通过入侵监测系统发现有黑客正在进行攻击时，应立即向信息中心领导报告。软件遭破坏性攻击（包括严重病毒）时要将系统停止运行。

（3）当主机遭受病毒感染或黑客攻击时，应将主机从网络中隔离出来再行处置。但须注意，在将主机从网络中隔离出来之前，管理员须判断该主机的隔离是否会对其他正在运行的系统造成影响。如可能会造成影响，则须先安全断开与其他系统的联系，再将该主机从网络中隔离出来。遭受病毒感染或黑客攻击的主机从网络中成功隔离出来后，在对其进行处置之前，应先备份该主机中的重要数据或系统，以免在处置过程中破坏或误删该主机中原有的重要数据。

3.设备安全发生故障时的应急预案

服务器等关键设备损坏后，管理员应立即向信息中心领导报告，并立即查明原因。如果能够自行恢复，应立即用备件替换受

损部件。如不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修。

4.内部局域网故障中断时的应急预案

（1）信息中心平时应准备好相关的网络备用设备，存放在指定的位置。

（2）局域网中断后，网络管理人员应立即判断故障节点，查明故障原因，并向信息中心领导汇报。

（3）如属线路故障，应重新安装线路。

（4）如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。

（5）如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。

5.外部网络中断时的应急预案

（1）外部网络中断后，管理员应向信息中心领导报告，并应迅速判断故障节点，查明故障原因。

（2）如属可即时恢复范围，由网络管理人员立即恢复。

（3）如属电信运营商管辖范围，应立即与电信运营商的维护部门联系，要求尽快修复。

6.电源中断后的应急预案

（1）外部电中断后，管理员应立即向信息中心领导汇报情况。

（2）如因校内线路故障，由信息中心通知维修人员迅速恢复。

（3）如果是外部的原因供电局告知需长时间停电，应做如下安排:

预计停电 2 小时以内，由 UPS 供电;

预计停电 2-4 小时，关掉非关键设备，确保各主机、路由器、交换机供电;

预计停电超过 4 小时，白天工作时间关键设备运行，晚上所有设备停机。

7.机房发生火灾时的应急预案

（1）一旦机房发生火灾，应遵循下列原则：首先保证人员安全；其次保证关键设备、数据安全；三是保证一般设备安全。

（2）人员灭火和疏散的程序是：管理员应首先切断所有电源，同时通过 119 电话报警。

二、后续处理

1.安全事件进行最初的应急处置后，应及时采取行动，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

2.安全事件被处理后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。

3.在确保安全事件解决后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

三、记录上报

网络与信息系统安全事件发生时，应及时向校领导和信息中心领导汇报，并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

四、结束响应

系统恢复运行后，信息中心对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料；属于重大事件或存在非法犯罪行为的，第一时间向公安机关网络监察部门报案。

上海震旦职业学院邮箱管理办法

（2015 年 6 月　沪震职〔2015〕74 号）

为了让全院师生更好地利用网络进行教学、科研、学习、对外交流等活动，学院免费提供邮件服务(http://exmail.qq.com/login)。为确保学院邮件系统安全、正常运行，维护学院和师生的利益，根据国家有关法规和学院网络管理办法，特制定本办法。

一、 邮件系统管理

1. 信息中心作为学院授权的网络管理部门，负责电子邮件系统的所有管理和维护工作，中心指定专人负责邮件系统的日常运行管理与维护，定期作好邮件备份，及时恢复故障，确保电子邮件系统的正常运行(不可抗拒因素除外)。

2. 因邮件服务器维护而必须暂时停止服务时，信息中心应提前以网站公告、群发信件等方式通知用户。

3. 尊重用户的注册信息和电子邮件内容的隐私权，不得向第三方提供用户的注册信息，任何人不得在未经用户本人许可的情况下阅读其电子邮件内容。但应公安机关要求查阅除外。

4. 对于违反有关规定的用户，信息中心有权做出相应处理。如发现用户有下列任何一种情形，中心有权随时中断或终止该用户的邮箱使用权，而无需通知用户。

(1) 利用网络故意传播不健康信息;

(2)违反信息安全保密条例造成失密;

(3) 利用电子邮箱对他人进行骚扰;

(4) 盗用、破坏他人帐号;

(5)利用电子邮箱进行商业广告活动和传送“垃圾邮件”;

(6) 其它违犯学校有关规定的行为;

以上各项一经查实,将立即清除该用户帐号并按有关规定对其进行处理。

5. 信息中心根据需要有权调整用户邮箱存储空间的大小。

二、邮件帐号的申请、开通、注销

1. 教工邮箱（后缀为@aurora-college.cn），用户名为:“名字首字母”+“.”+“姓氏全拼”，如帐号重复，则根据先后次序在后面加上阿拉伯数字序号。新教工邮箱根据人事处提供的新进教职工名单进行开通。一个教工只能申请一个邮箱帐号。

2. 学生邮箱（后缀为@stu.aurora-college.cn），用户名为:“名字首字母”+“.”+“姓氏全拼”，如帐号重复，则根据先后次序在后面加上阿拉伯数字序号。学生用户根据教务处提供的学生信息，由信息中心统一开通帐号，不允许单独申请。

3. 部门邮箱（后缀名为@aurora-college.cn）用户名为部门名称首字母。校内部门用户由部门提出申请，到信息中心办理邮箱设置或开设邮件群组。

上海震旦职业学院中心机房管理办法

（2015 年 6 月　沪震职〔2015〕75 号）

中心机房的正常运行必须做到确保供电正常，空调，网络和服务器等所有设备运行正常。为实现中心机房的正常运行，特制订校园网中心机房办法。

一、中心机房出入管理

1.内间房门常态应是关闭。特别是在作业完毕不再需要出入内间的时候，当事人需要确保内间房门的关闭。

2.持卡员工要妥善保管门禁卡，不得随意将门禁卡借予他人使用。

3.如发现门禁卡丢失须立即向信息中心领导报告。接到挂失通知后，应采取紧急应对措施，确保机房安全。

4.作业人员离开机房的时候，必须确认中心机房的房门是关闭的，不能让房门处于虚掩状态。

5.任何无授权人员不可在没有授权人员陪同的场合单独留在中心机房内。

6.任何非授权人员进入机房后，不能打开外间的文件柜。

7.当软件媒体，资料等不再需要的时候，授权人员必须把它们放回原存放处，不能把它们遗放在桌面上。

8.信息中心网络管理人员或设备厂商技术支持人员进入机房实施操作时，应明确操作目的和操作的对象设备，不得对无关

设备进行非必要操作。

9.机房内应注意用电安全，注意 PDU 功率负荷。因为功率太大会引起电线过热，是造成起火事故的隐患。

10.任何被授权人员认为是无关的设备不能放在机房内。

二、设备定期保养

中心机房内的设备需要定期保养，确保正常运行。

三、安全消防管理

1.机房内配备的灭火器不管是否使用过,超过出厂的保质期限时，必须通知后保处进行水压试验。

2.机房内不得堆放易燃物品，如纸箱和废纸等。

3.机房内的电源和插座为机房设备专用,非机房设备不得使用机房电源。

4.机房内要经常检查有无鼠患,一旦发现,应立即采取措施。

四、环境卫生管理

1.任何进入中心机房内间的人员，必须换鞋或穿上鞋套，以保持内间的清洁。

2.机房应定期由信息中心网络管理工作人员实施保洁。

3.中心机房内严禁吸烟，就餐。

4.严格禁止携带与工作无关的物品进入机房，特别是危险、易燃和易爆物品。

5.机房内严禁存放任何食品。

五、保密管理

1.中心机房内的服务器备份，需要存放在指定的外存设备，不能存放在任何个人的电脑或存储设备上。

2.各类密码不能与非相关人员共享。写在纸上的密码不能存放机房内，必须有相关个人持有。所有设备、系统的密码应放在学校保密室保存，以备特殊情况使用。

3.中心机房内的服务器上有关个人信息的数据，不能以任何方式泄露给非授权人员，不能以任何方式在公共环境上传播。

4.各类打印的资料不得乱丢乱放。

六、软件与文档资料管理

1.具有使用许可的软件光盘必须存放在中心机房内的指定场所。

2.授权软件在任何情况下不可被用于其它学校、公司或个人。因工作需要，须要使用这些软件，须要征得部门负责人的认可。

3.使用软件媒体必须小心，以防损坏。

4.为了软件激活而获取的密钥，不能泄露给其它学校或公司或个人。

5.密钥的管理必须做到随时可以查询。

6.中心机房内存放的设备采购需求书，厂方提供的各类技术资料，产品使用说明书等不能擅自废弃。

7.机房授权人员可以借阅上述资料，但阅读完毕后必须归还。

上海震旦职业学院校园网 VPN 使用管理办法

（2015 年 6 月　沪震职〔2015〕76 号）

为更好地为我校老师创造学习、教学、科研和办公条件，方便大家在校园网以外充分使用校内网络资源，我中心搭建了 VPN(虚拟专用拨号网络)服务平台。根据《中华人民共和国计算机信息系统安全保护条例》、《上海震旦职业学院校园网络管理办法》，为了保证上海震旦职业学院校园网内部系统和信息资源的安全，规范使用 VPN 服务安全访问校内网络资源，制定本使用管理办法。

一、VPN 系统主要用于用户在校外访问原本仅限于在校园网内部才能访问的资源和应用系统。例如我院图书馆的数字资源仅允许在校园网内部访问，但通过 VPN 可以在校外访问。

二、VPN 账户由信息中心统一管理，只提供给我院教职工使用。需要使用 VNP 帐号的人员可填写“上海震旦职业学院 VPN 用户申请表”向信息中心申请，信息网络管理部门将根据工作需要审批后开通 VPN 账户。对不再使用的用户，可以携带个人身份证明到信息中心办理销户手续。

三、使用 VPN 服务接入校园网时，必须遵守国家相关法律法规及学校校园网的有关规定，不得通过 VPN 服务从事网络违纪、违法活动。

四、VPN 用户必须保管好自己的账号与密码，帐号仅限本人使用，VPN 帐号在网上的行为由帐号所有人负责。若 VPN 用户的账号和密码被盗、不慎丢失、工作调离，用户有责任及时与信息中心联系，以便注销帐户或者更改用户信息。

五、VPN 用户不得利用 VPN 服务把校内资源提供给他人使用，或利用 VPN 账号进行牟利，否则构成侵权，由此引发的法律纠纷由 VPN 账号持有者承担。

六、对故意泄露 VPN 账号密码或将 VPN 账号借给他人使用者，或其 VPN 账号被其他人控制出现异常登录者，信息网络管理部门有权停止其账号的使用并追究该用户责任，直至移交有关部门追究法律责任。第一次被发现有上述情况的用户，其帐号将立即被封闭三个月。封闭期满后若要重新开通，需本人提交书面检查和重新开通帐号的书面申请，经用户所在部门领导签字同意，并经信息网络管理部门审核批准后，方可重新开通。若同一用户第二次被发现此类情况，该用户将被永久禁止接入我院 VPN 系统。

七、VPN 专用于在校外访问校内资源，在接入后禁止使用迅雷、BT 等 P2P 下载软件下载校外资源，以免浪费 VPN 带宽，影响他人使用。

八、本办法由信息网络管理部门负责解释。

九、本办法自发布之日起实施。

上海震旦职业学院网站管理办法

（2019 年 6 月 19 日　沪震职〔2019〕48 号）

一、总则

1.为加强上海震旦职业学院网站（以下简称学院网站）的管理，推动学院网站建设，根据国家有关法律法规和学校的有关规定，结合学校实际，制定本办法。

2.学院网站是信息公开和展示学校建设成果的重要窗口，也是学院为师生和社会提供相关服务的重要平台，以公开、高效、服务、亲和为建设目标，以校务公开、校园新闻、信息服务和互动交流为主要内容。

3.学院网站是唯一以“震旦职业学院”冠名的网站，各职能部门和二级学院(部)不得另外建设独立于学院网站的自有网站。学院网站一般不提供子站栏目和内容的链接，经批准的快速通道和特殊内容除外。

二、职责分工

1.学院网站采用网站群模式构建和管理，即由学院主站和各职能部门、二级学院等子站组成。学院网站群由信息中心提供技术支持和统一的网络安全管理，学院各职能部门和二级学院(部)负责提供学院网站和各子站的建设内容。

2.在网站建设中，信息中心的主要职责是:

（1）组织制定学院网站的总体发展规划。

（2）组织学院网站工作会议，推动各职能部门、二级学院（部）贯彻落实学院关于网站工作的决策部署。

（3）决定学院网站建设、运行的年度预算，并检查执行情况。

（4）组织学院网站绩效评估或考核。

（5）协调和解决学院网站建设和运行中的重大问题。

（6）负责制定学院网站相关的技术标准与规范。

（7）负责学院网站建设和运行的技术保障和运行分析。

（8）梳理主站各栏目与相关子站栏目之间的关系，使信息发布和维护在技术上更为简便和高效。提出跨部门、跨单位应用系统与信息资源整合的建议方案。

（9）负责学院网站信息安全与应急保障。

（10）根据需要为职能部门、二级学院（部）提供子站的设计和制作。

（11）按照统一管理的要求，负责学院主站各栏目的内容更新和实施网站栏目的设置、调整。

3.各职能部门、二级学院（部）的主要职责是:

（1）在学校网站上建立各职能部门、二级学院（部）子站，围绕本部门的主要工作、师生及社会关注的内容设置和调整子站栏目。

（2）承担主站相关栏目和子站各栏目的内容保障工作，做到对应子站各栏目有计划、及时地发布本部门的各种信息。

（3）落实网站工作机构，指定一名分管领导负责网站工作，指定一名网络信息员承担相关具体工作。

（4）建立各职能部门、二级学院（部）网站工作机制和管理制度，规范栏目设置与调整、内容组织、审核把关、信息巡检等工作。

（5）负责本部门子站内容的安全检查，保证子站各种信息和内容符合国家有关法律和学院有关规定。

4.党委宣传部的主要职责是:

（1）按照学院网站总体规划和建设目标，对学院网站页面、主站及子站的内容及栏目设置和调整提出建议，经分管校领导审批后实施。

（2）按照统一管理的要求，负责提出学院主站各栏目的设置、调整的要求。

（3）对学院网站主站和子站各栏目的内容进行定期检查，并根据检查情况提出改进建议。

（4）负责组织和提供学院网站新闻网（或新闻中心）的稿件，提交给校办或党办进行审核。

5.党委办公室和校长办公室的主要职责是:

（1）党委办公室负责审核有关党务工作的新闻稿件，并交宣传部上传网站。

（2）校长办公室负责审核有关行政工作的新闻稿件，并交宣传部上传网站。

三、网站安全

1.学院各级网站应建立网站安全责任制。对于网站安全，各级党政正职是第一责任人，分管网站工作负责人为直接责任人。网站内容维护人员需要签署有关用户名和密码的安全保密承诺书。

2.各职能部门、二级学院（部）要增强保密意识，遵守国家和学校有关保密要求，严格信息审核把关，确保涉密信息不上网。不能确定信息是否涉密时，应报送学院党委办公室和校长办公室审核。

3.信息中心作为学院网站信息安全的责任单位，应建立健全信息安全工作制度，加强日常巡检和节假日、重大政治活动、重要敏感时期的应急值守与实时监控；要加强技术防护手段，健全安全防范体系，提高学院网站安全防护能力。