

上海工商外国语职业学院

信息管理制度汇编



2025年6月

目 录

网上信息发布与管理办法	3
多媒体新闻中心管理办法	41
实验实训室管理制度	43
机房安全责任公告	46
实验实训场所安全应急预案	49
信息安全管理办法	52
信息资产管理制度	54
信息系统用户和密码管理规定制度	59
信息安全检查管理规定制度	65
信息安全组织建设管理规定制度	69
信息安全管理体系建设文件控制管理规定制度	76

网上信息发布与管理办法

一、网站设立

学校网站设学校主页和各单位二级子页。学校主页由学校党政综合办、宣传处、信息化办公室负责建设和管理。各二级单位的子页由单位自行建设和管理，建立网页的单位必须承担安全保密管理责任。

二、网站信息资源建设

1、学校网站主页

（1）主页上所有信息的发布与审核采用实名制，用户登录采用学校统一身份认证系统。

（2）学校网站主页新闻和公告栏目一般发布全校性的新闻信息和公开的通知，各二级单位信息一般发布在各单位页面上。

（3）学校主页校园新闻信息由学校宣传处负责收集、登记、编审、上传、存档和信息反馈，学校各二级单位有责任和义务提供反映学校发展和建设的重要信息。

（4）二级学院网站页面的建设、管理和维护由各二级单位负责组织、采集、制作。其页面或站点设计可根据本部门的工作特点和需要自行设计。自行设计的二级单位页面应避免出现和学校主页栏目相交叉的栏目，同时必须在各级子页面的导航栏给出到学校主页的链接，不得设置游戏娱乐类网站的外部链接，不得提供FTP及类似FTP的服务。版面、栏目的修改变更应向学校党政综合办提出申请，说明变更内容并提交设计方案，经学校党政综合办审核同意后方可发布。

（5）党政综合办负责“学校概况”内容发布，校部通知、主页弹出窗口也由党政综合办审核后发布；各二级学院及职能部门分别负责“院系导航”、“管理机构”、“教学科研”、“招生就业”等栏目所对应的二级子页网站的维护与更新。

（6）学校主页上栏目分类的增加、删除、变更、专题网站链接的设置必须由相关部门向党政综合办提交书面申请，经学校领导审核同意后，通知信息化办公室进行修改。

（7）党政综合办对网上信息定期进行巡查，对于失效、错误的栏目分类、专题网站、信息内容进行处理，处理结果必须告知相关部门。
。

2、学校门户子站

（1）学校门户子站用于各学院（部门）的信息发布、服务引导，本身不得包含任何业务系统应用。原则上必须采用上海工商外国语职业学院主页内容管理系统（CMS）建设，对于当前CMS系统不能满足其建站需求并短期内无法解决的，经学校同意，可以自行建设门户子站。
。

（2）各学院（部门）建立门户子站必须填写《校园网（互联网）网站建设申请表》，经学校校长给办公室审核通过后，可建立门户子站。

（3）各学院（部门）应专门指定信息管理人员负责门户子站架构的建设和内容管理。

3、专题网站

（1）专题网站是指学校或各学院（部门）由于某项活动或某个项目建设的，围绕该活动或项目发布各类相关信息的网站。

（2）专题网站必须采用上海工商外国语职业学院主页内容管理系统（CMS）建设。

（3）各学院（部门）建立专题网站必须填写《上海工商外国语职业学院自助建站申请表》，经党政综合办审核同意后允许建立专题网站。

（4）各学院（部门）应专门指定信息管理人员负责专题网站架构的建设和内容管理。

（5）在门户子站上设立专题网站的链接须经学院（部门）领导同意。

（6）在学校主页上设立专题网站的链接必须向校办提出书面申请，经党政综合办审核同意。

4、网上交互系统

（1）上海工商外国语职业学院易班网上交互社区及公共资源平台，采用严格的实名制认证方式，论坛发帖采取先审核后发帖，论坛内容由党政综合办、学生管理处、信息化办公室及相关部门共同管理。

（2）任何学院（部门）不得在校内建立网上交互式系统，如有需要，可以在易班中申请建立相关的交互式板块。

5、自行建站

学院（部门）自行建站是指各学院（部门）自行建设门户子站或专题网站。对自行建站将从安全、资源有效利用、建站经费、维护、成效等多方面进行评估。

（1）学院（部门）自行建站必须向学校提交书面申请，并附有完整的建站方案、成效分析、管理办法、人员配置，经专家论证确有自行建站的必要性，并有完善的保障措施、经信息化办公室审核同意后，可以自行建设门户子站或专题网站。

（2）网站必须由建站学院（部门）信息管理员登录信息化办公室网站下载并填写《校园网（互联网）网站建设申请表》申请域名，不得直接用IP地址对外发布。申请表由该申请学院（部门）主管信息领导签字同意后提交信息化办公室。

（3）网站必须根据《互联网信息服务管理办法》自行申请ICP备案号。

（4）网站不得提供网上论坛、留言板、公共FTP等具有交互式功能的服务。

（5）网站所用服务器必须自备，且放置到学校服务器托管机房。
。

（6）服务器操作系统、应用软件、防火墙、杀毒软件必须使用正版软件。系统、应用软件维护由学院（部门）信息管理人员自行维护，一旦发现网站服务器中病毒或有异常流量，信息化办公室有权立刻中断服务器与校园网的连接，并告知相关学院（部门）。相关学院

（部门）要及时处理服务器故障，在确保服务器运行正常以后，才可联入校园网。

（7）网站必须支持后台管理功能，保证非计算机专业人员也可以方便的对信息进行维护与管理，即有后台程序可以对页面内容进行更新。

（8）网站必须保留自建站之日起的所有信息发布内容。

（9）网站必须保留至少六个月以上的访问记录。

（10）网站必须有备份恢复机制。

（11）网站如因故障或维护等原因中断服务，需要及时告知信息化办公室，并在相关主页上发布通知。

6、网站架构及内容

（1）二级网站建设（含CMS建站及自行建站）必须拥有良好的用户界面，网站主页有的校徽标志、学校名称必须采用学校统一标准。

（2）每个分页都含有返回本部门主页的选项。所有网站首页必须在醒目的位置加入上海工商外国语职业学院门户网站的链接，在网站下部添加上海工商外国语职业学院网站ICP备案号。

（3）网页要保证800×600及1024×768分辨率下都能正常浏览，能够支持W3C标准。各网页页面之间链接明确、导航清晰，易于浏览。

（4）图片采用jpg或者gif格式压缩，单个大小不得超过300k。动画统一采用flash标准版本，单个大小不得超过500k。为提高网页

的访问速度，对图片、动画、视频、音频等多媒体内容的使用要适量，对这些内容应该进行合理的压缩处理。

（5）网站内容应保证准确性及时效性，网页上所有链接必须正确。

（6）为确保国家秘密、工作秘密和商业秘密安全，网站信息内容发布必须遵守学校相关规定，确保所发布的信息均经过保密审查、审批，绝对不涉及国家秘密、工作秘密和商业秘密。

（7）各类网站不准发布含有下列内容的信息：反对宪法所确定的基本原则的；危害国家安全，泄漏国家秘密，颠覆国家政权，破坏国家统一的；损害国家荣誉和利益的；煽动民族仇恨、民族歧视，破坏民族团结的；破坏国家宗教政策，宣扬邪教和封建迷信的；散布谣言、扰乱社会秩序、破坏社会稳定的；散布淫秽、色情、赌博、暴力、凶杀、恐怖或者唆使犯罪的；侮辱或者诽谤他人，侵害他人合法权益的；法律、行政法规禁止的其他内容；学校内容监管部门发现网站内容含有以上信息之一的，有权立即备份后删除，并报告相关部门。

三、附则

1、学校将根据互联网的发展和中华人民共和国有关法律、法规的变化，不断地完善和修改本办法的任何条款，一旦条款内容发生变动，学校将会在上海工商外国语职业学院主页进行通知。

2、本管理制度由信息化办公室负责起草、解释、修改和归口管理。

3、本管理制度自校领导签发之日起实施。

四、附件

附件编号	标题	页数
1	上海工商外国语职业学院 《校园网（互联网）网站建设申请表》	1

校园网（互联网）网站建设申请表

申请单位			所属部院系	
网站负责领导		职务		电子邮箱
		办公电话		移动电话
网站管理员		职务		电子邮箱
		办公电话		移动电话
网站基本信息	网站名称			
	网站域名			
	网站服务范围	<input type="checkbox"/> 部院系内部 <input type="checkbox"/> 校内 <input type="checkbox"/> 公开		
	网站服务功能	<input type="checkbox"/> WWW <input type="checkbox"/> BBS <input type="checkbox"/> VOD <input type="checkbox"/> FTP <input type="checkbox"/> 其它		
	网站运行方式	<input type="checkbox"/> 学校网络中心虚拟空间 <input type="checkbox"/> 学校站群管理平台 <input type="checkbox"/> 托管服务器 <input type="checkbox"/> 其它		
申请学校网络中心虚拟空间				
空间申请	拟申请空间	<input type="checkbox"/> 100MB <input type="checkbox"/> 200MB <input type="checkbox"/> 500MB <input type="checkbox"/> 更多		
	动态网页技术	<input type="checkbox"/> 无 <input type="checkbox"/> PHP <input type="checkbox"/> ASP <input type="checkbox"/> ASP. NET <input type="checkbox"/> JSP <input type="checkbox"/> 其它		
	数据库类型	<input type="checkbox"/> Access <input type="checkbox"/> SQLServer <input type="checkbox"/> Oracle <input type="checkbox"/> MySQL <input type="checkbox"/> 其它		

网站申请要求

- 1、认真阅读网站安全保密责任书（见背面）并严格执行。
- 2、建设单位必须认真履行管理义务，妥善保管网站帐号，及时对网站信息进行更新，至少每月对网站进行一次安全检查，及时对网站漏洞进行修复升级。
- 3、网站开通前必须进行严格的安全测试，制订并向学校信息化办公室提供完整详细的资料，包括：网站管理办法、网站应急预案、网站测试报告和网站技术说明。人员变动或变更服务应及时通知信息化办公室进行备案。
- 4、因网站管理不善造成的一切后果由网站建设单位承担全部责任。
- 5、由于网站安全问题、各种故障而影响其它网站或网络系统正常运行时，学校信息化办公室有权暂时关闭该网站。
- 6、由于网络运营商、设备故障等不可抗拒因素引起的网站无法正常访问或数据丢失，学校信息化办公室不承担任何责任。

网站负责领导签字:

年月日

所属部、院、系领导意见

签字：（盖章）

年月日

学校信息化办公室意见

签字：（盖章）

年月日

学校党政综合办意见

签字：（盖章）

年月日

以下由信息化办公室填写

网站管理方式	<input type="checkbox"/> 网站后台 <input type="checkbox"/> FTP <input type="checkbox"/> 学校站群管理平台	网站IP地址	
管理账号/管理IP		申请编号	
受理日期	年月日	受理人	
开通日期	年月日		
备注			

上海工商外国语职业学院校园网（互联网）网站

安全保密责任书

一、严格遵守国家、学校有关网络管理和信息安全保密法规制度

。

二、不在网站上存储、传播有损国家、学校声誉及有伤风化的信息，不利用网站从事非法盈利活动。

三、严禁通过网站存储和传播涉密信息。

四、未经学校批准，严禁以学校名义在校外注册和建立网站。

五、严禁未经审批变更网站主要功能，私自开设BBS、留言板等具有实时信息发布的功能。

六、自觉做好网站安全管理工作，根据实际情况，安装防病毒软件和防火墙，及时升级病毒库、操作系统补丁，及时修复网站存在的漏洞。

七、严禁通过网站存储、传播计算机病毒和其它恶意程序，严禁对网站系统进行探测、扫描。

八、结合本单位实际情况，制定网站信息发布审核、数据备份、安全检查和应急预案等各项管理制度，并严格执行。

九、做到专人管理，严禁随意将网站管理帐号透露他人或让不相关的人员进行操作。

十、网站改建、停用，负责领导、管理员发生变动，应及时在学校网络中心重新进行备案。

十一、自觉接受学校信息安全保密检查，因管理不善造成的一切后果由网站建设单位承担全部责任。

十二、单位领导应教育、督促所属人员认真贯彻落实信息安全保密法规制度，确保不发生信息安全事件。

十三、对违反上述规定者，一经查实，由学校党政综合办对网站建设单位给予警告和通报批评；对发生失泄密事件的，依据《中国人民解放军纪律条令》和有关法律法规，对网站主管领导和直接责任人给予处分；构成犯罪的，移交司法机关依法追究其刑事责任。

校园网络管理办法

一、组织管理

校园网的建设管理必须符合国家规划，实行统一领导、统一组织、分步实施的原则。校园网管理委员会和信息化办公室、各二级学院兼职网络工作信息员队伍作为校园网络建设的三个重要组成。

设立以主管副校长为首的学校信息化工作领导小组，作为校园网络建设的领导机构。其成员由信息化办公室负责人和学校有关职能部门负责人组成。

二、入网管理

1、遵守国家保密法规。

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络管理办法》、《上海教育与科研计算机网络管理办法》和国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。用户不得利用计算机网络从事危害国密、破坏社会安定的违法犯罪活动，不得查阅、会的各种有害信息。

2、校园网网络地址、信箱地址管理。

校园网网络地址、信箱地址由信息化办公室统一管理，网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改IP及网络设置，不得盗用IP地址及用户账号。

3、单位用户入网管理。

校内各单位的办公室和各系的教研室、实验室、以公共用户方式入网。入网前需填写“校园网用户申请表”，由网络中心统一开设账

号，确定使用权限，分配信箱地址。经网络中心批准后，方可按照操作说明使用网络。对个别操作复杂的信息服务系统，要通过网络中心组织培训后才能入网。

各部门的子网，必须以子网方式入网，由各部门网络管理小组填写入网申请表报知网络中心，由网络中心根据子网的规模分配网络地址。

4、个人用户入网管理。学校教职工原则上均可申请作为个人用户入网，但学校有权根据网络发展的过程，在不同时期对入网范围加以限制。教职工以个人用户方式入网根据学校人事相关办法执行，经信息化办公室核实后开设个人账户，给予电子邮箱地址后方可进网。

①用户都有义务配合国家安全部门依法对网络使用情况等进行监督检查，采取必要措施。

②任何用户未经许可不得开通Email、Web、Newsgroup等服务。不得在网上随意发布公共信息。

③任何用户未经许可不得在网上进行商业和其他任何盈利性活动。

④用户不得进行任何干扰其他网络用户，破坏网络设施的活动。这些活动包括(但并不限于)商业公告、散布计算机病毒、进入未经授权的计算机系统、盗用非法的IP地址入网等等。

⑤用户有义务向网络管理员报告任何违反用户守则的行为，并对自己在网络使用中的行为负责。

⑥对于违反计算机网络政策的用户，网络管理员有权停止对其的服务，必要时将诉诸法律。

5、校外单位和个人入网管理。与我校有密切协作关系的单位和个人，要进入我校校园网，必须遵守本暂行管理办法和填写入网申请表，并经信息化办公室审核通过后，方可办理入网手续。

6、注销管理。

①个人用户调离我校时，需到网络中心申报注销后，方可办理离校手续。

②如果机构调整或单位撤销，需报网络中心对单位用户账号和使用权限进行调整或注销。

③联入校园网的个人微电脑或公共设备因故撤掉，需向网络中心申报，予以注销。

④不按时缴费的用户，网络中心有权注销其账号。

⑤对违反本管理办法的用户，网络中心有权注销其账号。

三、运行管理

1、经费投入。校园网的主干工程建设经费由学校投入，各使用单位的建设经费由该单位投入。学校保证每年投入一定的经费用于校园网的运行维护。

2、项目管理。网络工程建设项目的实施采用工程项目管理办法，承担项目的单位负责人对学校信息化工作领导小组负责。

3、主干网连结管理、设备管理。校园网主干的所有设备，包括光缆及其附属配件、路由器和交换机等属于学校的固定资产，由信息化办公室负责管理，设备的连结与使用由信息化办公室统筹安排与调配。未经信息化办公室许可，任何人不得改变主干网络设备的连接关系

，及拆卸、拔插网络设备及其连线、电源线。安装在各部门的主干网设备，各部门应由二级学院兼职网络工作信息员妥善管理与维护，如因人为因素造成设备损坏，由各单位自己负责。为保证校园网运行畅通，各部门应为校园网设备安装专门电源，一般情况下不得断电。

4、上网信息管理。

（1）校内公共信息管理。各部门、各单位在校园网上发布信息实行“谁发布、谁负责”的管理原则。校园网上发布的信息应按程序和职责分工经严格审核，未经审核的信息不得上网发布。凡是将未经批准的信息进行发布的单位，将追究分管领导人和具体责任人的责任；对国家和学校造成损失和不良影响的，按国家法律和学校有关规定处理。

①网络新闻信息，由各采写单位录入后通过校园网传送给宣传处电子信箱，宣传处根据事件性质及实际需要或向全校发布，或送校领导和上级领导，或予取消。

②各部门、各单位负责学校门户网站有关栏目和本部门、单位二级网站信息的发布和及时更新。信息发布单位应当对所发布的信息记录备案，规范对本单位上网信息的管理。各部门内部通知信息，在本部门信箱地址内发布。

③学校职能部门告知全校信息，需按学校发文程序办理后，方可由职能部门名义向全校发布。以学校名义发布信息，应按学校发文报批程序，经主管校领导批准。

④可利用网络电子公告牌刊登教学、科研和管理方面的信息。但不得发布与国家法律、学校规定相违背的信息。

（2）对外信息管理

通过校园网向INTERNET提供的查询信息，需报信息化办公室，并经学校有关部门或学校领导批准后方可发布。

5、上网软件管理。根据知识产权法规规定，须使用合法软件。各职能部门研制开发的软件必须符合校园网管理信息系统的标准，需要在校园网上运行的软件，必须经由信息化办公室审查批准后方可安装使用。

6、安全管理。

（1）遵照国务院发布的《互联网信息服务管理办法》第十四条规定，网络与教育技术部应保留用户上网活动最近60天的原始记录，以备公安、安全部门检查。

（2）未经授权的计算机用户不得上网。校园网用户上网只能按授权口令、账号入网、不许擅自盗用他人账号。不允许散布计算机病毒。

（3）学校从技术、行政上加强过滤不健康的信息。对于利用计算机进行犯罪者，予以重罚并诉诸法律，对于有效防止犯罪的技术和软件予以鼓励和表彰。

(4) 校园网用户必须遵守国家法律和校规，服从网络中心的管理。不允许通过校园网发送商业广告信息，更不允许查找和散播黄色信息等非法活动。违者将酌情罚款并给予行政处分。

(5) 学校信息化工作领导小组办公室要经常对学校网站信息、部门网站信息进行巡查，发现不良信息应及时作好记录，网络与教育技术部在作好相关记录和备份后，应立即删除。对于一些重大事件，上报学校信息化工作领导小组。

(6) 因停电、线路故障、设备检修或其它不可抗因素造成校园网中断的，网络与教育技术部不承担其损失责任。

7、流量管理。为防止网络上流量不均匀造成流量拥塞，必要时网络中心有权采取措施进行流量控制。

四、其他管理。

1、培训工作。

(1) 校园网的使用培训工作，由信息化办公室统一管理和组织实施。信息化办公室将根据需要编写有关我校校园网建设规划、网络结构方案、信息服务和应用系统等宣传和培训材料。在校园网的不同发展阶段，根据人员的不同情况，分批组织培训。

(2) 为避免网络信息流量拥挤或因盲目操作出现意外故障，校内其他单位不得通过校园网进行以盈利为目的的计算机和网络的培训或其他培训。

(3) 校内其他单位和个人未经批准不得擅自使用校园网络的名义对外揽接工程。

2、关于利用校园网进行实验活动。

禁止任何单位和个人直接利用校园网进行设备、环境测试，光或电、雷电实验等可能危害、影响网络正常运行的实验。

五、附则

1、本管理制度由信息化办公室负责起草、解释、修改和归口管理。

2、本管理制度自校领导签发之日起实施。

校园一卡通管理实施细则

一、校园卡“应急工作小组”

由校长办公室牵头成立校园卡“应急工作小组”，负责制定校园一卡通系统的应急实施方案和处理校园一卡通系统的紧急故障。“应急工作小组”由校长办公室、财务处、信息化办公室等职能部门组成，并由各职能部门负责人作为相关责任人。

校园卡系统发生紧急情况时，相关人员应及时向“应急工作小组”汇报，并由信息化办公室统一组织、部署故障排除实施方案；重大事故应及时向校领导汇报，最终出具事故分析报告。对于由此对用户所造成的经济损失，学校应酌情予以补偿。

二、校园卡分类及使用范围

1、校园卡分类。

根据持卡人的身份，校园卡分为学生证卡、工作证卡、临时卡（分为记名临时卡和不记名临时卡）、教师卡，所有校园卡仅限校园内使用。
。

2、校园卡使用范围。

包括但不限于餐饮消费系统、图书借阅系统、楼门和宿舍门禁查验系统、学生报到注册系统、毕业离校系统、网络计费转帐系统、水电控管理系统、上课考勤系统、会议考勤系统、教职工考勤系统等。
。

三、校园卡管理

1、校园卡申请

（1）校园卡可办理人员为学校在职教职工、外聘教师、物业人员、在校学生等。

（2）各类人员申请办理校园卡，须由相关职能部门负责审核：在校学生，由学生工作办公室负责；继续教育学生由继续教育学院负责；教职工（含离退休）和学校聘用各类人员由人事处负责，按人事处相关制卡规则办理。

2、校园卡办理

校园卡初次开卡工作由信息化办公室负责，地点4号楼底楼校园卡中心。

凡需办理校园卡换卡、补卡、充值、挂失与解挂、停用与注销以及卡片维护等事宜，由校园卡中心统一负责，地点4号楼底楼校园卡中心。

（1）校园卡初办

新生入学报到时，由学校统一办理校园卡；学校教职工（含离退休及各类聘用人员）、物业人员校园卡办理由校园卡中心处负责核准并制卡和发放。

在职教职工、外聘教师、物业人员、新生的首次办卡均免工本费。

。

（2）校园卡挂失及解挂

持卡人发现校园卡丢失后，应及时通过服务电话、校园网络以及校园卡中心处现场等方式进行挂失。

持卡人解挂可在校园卡中心充值处现场办理，现场办理需本人带身份证件原件。

如持卡人在已进行挂失但未制作新卡情况下找回原卡，请及时进行现场或网上校园卡解挂；挂失前以及挂失后24小时内非联网设备上造成的经济损失由持卡人自行承担。。

（3）校园卡补卡或换卡

校园卡补卡指持卡人丢失校园卡后，申请重新补办新卡。**校园卡换卡**指校园卡遭到损坏，或因校园卡自身存在质量缺陷（申领的新卡无法正常使用等）而申请重新办理新卡。

校园卡补卡或换卡（除申请替换无法正常使用的新卡外）须交纳相应的制卡工本费，按20元/张收取工本费。新卡补办后，原卡内金额自动转入新卡内，同时原卡宣告作废并永久置入黑名单。

3、校园卡终止及销户

（1）**校园卡持卡人离校**（如离职、毕业等）时需办理相关的离校手续，否则将被冻结处理，由此造成的一切损失均由持卡人自己承担。

（2）校园卡批量销户

学生毕业时，持卡人凭离校手续单先至图书馆办理图书清退借用，再凭离校手续单至校园卡现金充值点办理卡内余额退还手续。持卡人无需至校园卡管理中心办理学生证卡销户手续，校园卡管理中心系统操作员将根据学生工作办公室同步的毕业离校学生的数据信息，在后台对学生证卡进行销户处理。对于正常毕业的学生该卡可留作纪念。

（3）校园卡零星销户

持卡人办理学生证卡销户手续时，需持本人的学生证卡及离校手续单，先至校图书馆办理图书清退借用，再至校园卡现金充值点办理卡内余额退还，最后前往校园卡管理中心办理校园卡销户手续，校园卡管理中心系统操作员将卡销户后收回校园卡。

持卡人办理记名临时卡销户时，先至校园卡现金充值点办理卡内余额退还，再持卡前往校园卡管理中心办理销户手续，校园卡管理中心系统操作员将卡销户后收回卡，制卡成本费不作退还。校园卡现金充值点可办理不记名临时卡的退卡手续。

四、校园卡使用

1、校园卡充值

（1）现金充值。

现金充值是指通过交纳现金的方式对校园卡进行充值。现金充值仅可在4号楼底楼校园卡中心的现金充值点由充值员完成。

（2）网上充值。

网上充值是指持卡人通过微信公众号方式进行校园卡充值。

（3）其他。

校园卡的专用钱包（如水控、电控等）不计流水、不可挂失，请务必小金额充值。

2、校园卡消费

（1）校园卡消费指南。

①POS机消费方式。POS机操作员键入金额，按“确定”，消费者确认消费金额无误后，将校园卡平行贴近读卡器上的读卡区域，直至确认消费完成后，将卡取走，当次消费结束。

②POS机消费补充内容。当日消费满50元，POS机会提示键入校园卡密码，若输入密码正确，则确认消费完成。若输入密码错误，则消费失败。

③消费故障。如果将校园卡平行贴近读卡器上的读卡区域，听到连续的“滴滴”报警声，说明您的校园卡出现了卡内金额不足、卡片损坏、卡片已冻结等异常情况，请您立即与校园卡管理中心联系，咨询有关情况。

④消费查询。后台系统保存校园卡通用钱包的消费流水，持卡人可通过统一身份认证平台，进入一卡通自助查询，或通过自助终端（网站等）查询，也可至4号楼底楼校园卡中心的现金充值点进行人工查询。

⑤消费纠纷。消费纠纷原则上以当场纠正为主，服务中心纠正为辅。POS机具有对前一笔交易撤销的功能，如出现错扣可当场撤销。若无法撤销，需要出具商务负责人签字的证明，由校园卡管理中心纠正。如在校园卡使用消费时，出现刷卡金额与实际消费金额不符时，请相关人员一同至一卡通充值处进行现场处理，经核实后，一卡通充值人员将立即处理。

⑥消费信息异常。个人出现消费流水信息异常，可持本人校园卡至校园卡管理中心查询、处理。如出现异常大额交易信息，校园卡管理中心有权对帐户进行冻结，并进行调查。

3、其他

（1）校园卡由持卡人随身携带、妥善保管，正确使用，校园卡损坏或者不能辨认时，应当及时更换新卡，丢失校园卡的应当及时挂失，并补办新卡。

（2）作为在校师生的个人身份识别证件和消费卡，校园卡仅限本人使用，不得转借。如果转借，学校校园卡中心有权停止该校园卡的使用，所产生的后果由出借者本人负责。

（3）师生在校内各单位办理相关事务时，任何单位不得以任何理由扣留校园卡或者要求作为抵押，否则因此造成的经济纠纷、侵权使用等责任将由扣押单位承担。

（4）由于校园卡是非接触式智能IC卡，在卡片的夹层中含有天线和集成电路，因此在日常使用时有以下要求：不能弯曲、挤压、摔打和抛丢卡片；不能将卡片放置在强磁、强电、高温的环境中；不能将卡片接触带电物品；不能将卡片接触有腐蚀的物品。

五、校园卡其他管理内容

1、校园卡应用子系统管理部门指的是以校园卡系统为依托，进行业务管理、数据收集和信息管理的学校职能部门和有关单位。各应用子系统管理部门应根据本单位的职责和业务对校园卡系统提出明确的

管理要求和权限界定，一卡通充值处将严格依据用户单位的要求做好系统的初始化和相应的参数设定。

2、校园卡各应用子系统管理部门及商户应自觉遵守校园卡管理的有关规定和学校的规章制度。各类人员管理部门（后勤保卫处、学生处）应履行向持卡人的告知义务，规范人员管理流程，配合学校做好持卡人的有效身份注册（注销）等管理工作。

3、校园卡领导小组有权检查和监督经营商户的交易活动。发现违反有关规定或其它非正常的行为，可及时采取措施，予以控制。对违规情节严重者可中止其业务，追究其责任并取消经营商户资格。

4、校园卡如有连续一个月未使用时(各类假期期间除外)，学校将视为该卡为遗弃卡，校园卡中心有权将该作停用处置，停用三个月后，仍无人认领，将注销该校园卡，并将校园卡内金额作为呆账，上缴学校。

5、拾获他人校园卡，应及时联系并归还对方，或交送至一卡通充值处，不得恶意使用他们校园卡进行各项活动，对他人造成损失者则将按有关部门规定追究其相关的法律责任，触犯刑律的将移送司法机关追究刑事责任。

6、严禁破解、仿冒、伪造校园卡。此类行为一经查实，按破坏计算机信息系统和电子金融系统的行为交学校有关部门严肃处理。若触犯法律的，则移送司法机关处理。

7、校园卡系统及设备为学校财产，各使用单位和个人应自觉爱护，按照要求加强管理和保养。凡故意破坏校园卡系统和设备，影响校

园卡系统正常运行的行为，一经查实，移交学校有关部门严肃处理，触犯法律的，将移送司法机关处理。

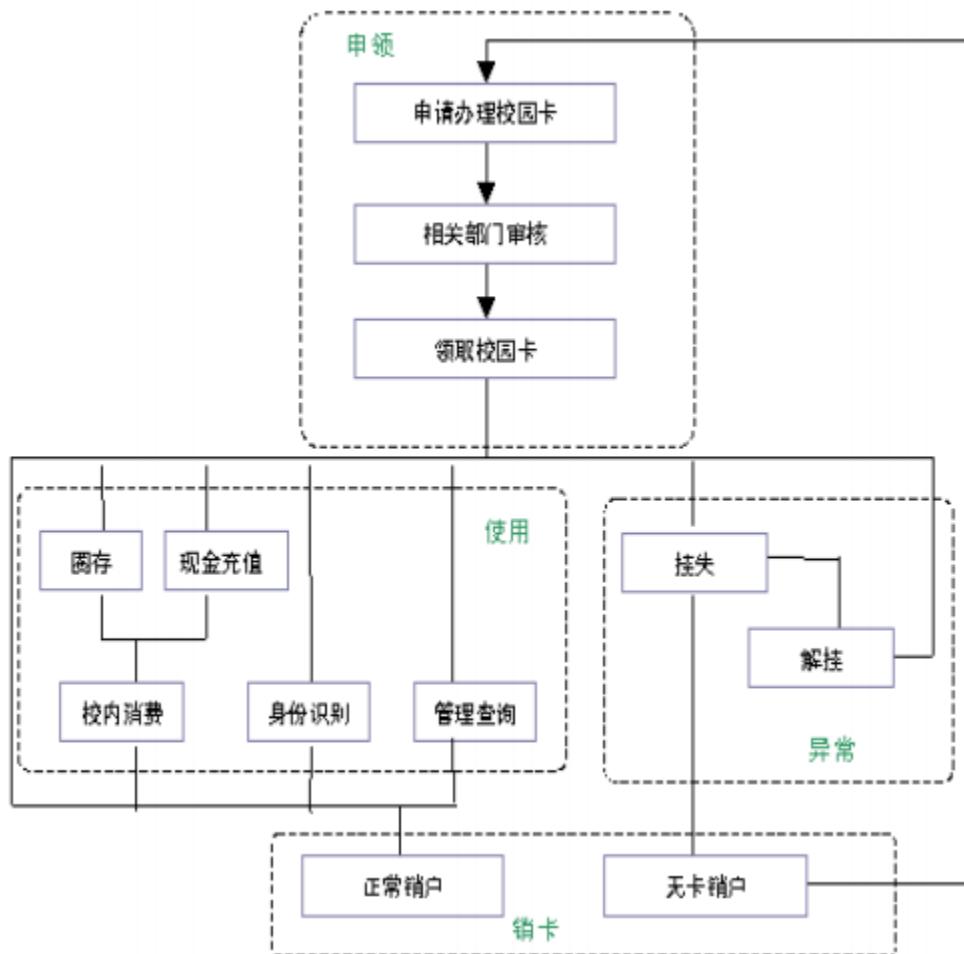
六、附则

- 1、本管理制度由信息化办公室负责起草、解释、修改和归口管理
- 2、本管理制度自校领导签发之日起实施。

七、附件

附件编号	标题	页数
1	校园卡申领、使用、注销流程	1

校园卡申领、使用、注销流程



- 1、学校信息化办公室、校园卡管理中心，负责校园卡的卡务、各消费子系统的管理与维护。
- 2、校园卡管理中心地址：4号楼底楼校园卡中心；
- 3、校园卡办理时间：周一至周四
中午11:30-12:50、下午16:00-17:30

网络故障管理、处理实施细则

一、成立网络故障处理工作小组

成立学校网络故障处理工作小组，由校主管信息副校长任小组组长；党政综合办负责人、信息化办公室负责人及校相关部门负责人任小组成员；外部支持人员包括电信运营商、设备供应商以及系统集成商，协助做好学校网络故障处理。

二、校网络故障处理原则

统一领导，综合协调，重点突出，集中备份，快速恢复，防范为主，加强监控。

1、**统一领导**。遇到重大网络异常情况，应及时向有关领导报告，以便于统一调度、减少损失。

2、**综合协调**。明确综合协调的职能机构和人员，做到职能间的相互衔接。

3、**重点突出**。应急处理的重点放在运行着重要业务系统或可能导致严重事故后果的关键网络系统上。

4、**集中备份**。通过网络设备备份和配置参数备份等措施，提高通信网络系统的安全系数。应以必要的投资，购置必要的备用设备，并在备用设备上按要求预先配置好各种参数，当发生故障时能直接上线运行。

5、**快速恢复**。网络管理人员在坚持快速恢复系统的原则下，根据职责分工，加强团结协作，必要情况下与设备供应商以及系统集成商共同谋求问题的快速解决。

6、及时反应，积极应对。出现网络故障时，网络维护人员应及时发现、及时报告、及时抢修、及时控制，积极对业务网络突发事件进行防范、监测、预警、报告、响应。

7、防范为主，加强监控。经常性地做好应对网络突发事件的思想准备、预案准备、机制准备和工作准备，提高基础网络和重要信息系统的综合保障水平。加强对网络应用的日常监视，及时发现网络突发性事件并采取有效措施，迅速控制事件影响范围，力争将损失降到最低程度。

三、校网络故障管理及处理

1、校网络故障分类

网络故障指互联网网络系统因计算机软硬件故障、人为误操作等导致业务中断、系统宕机、网络瘫痪等情况。分为：校园网故障、外网故障、域名服务器故障、宿舍区网络故障、邮件服务器故障及其他。

2、校网络故障处理

(1) 网络故障应急预案

①信息化办公室网络管理人员从故障申告、网管系统的故障告警中得知网络异常事件后，应在第一时间赶赴网络故障现场，控制事态发展，防控蔓延，采取各种技术措施，及时控制事态发展，最大限度地防止事件蔓延。

②信息化办公室网络管理人员应快速判断事件性质和危害程度，尽快分析事件发生原因。若是电源接触不好、物理连线松动或者能在最短时间内自行解决的网络问题，及时按照有关操作规程进行故障处理，并报学校网络故障处理工作小组备案；否则，网络管理人员应根据网络与信息系统运行和承载业务情况，初步判断事件的影响、危害和可能波及的范围，提出应对措施建议，及时告知学校网络故障处理工作小组。

③网络管理人员向学校网络故障处理工作小组报告，在学校网络故障处理工作小组的授权后启动相应的应急预案。针对灾难事件和影响重要业务运行的重大事件，还要及时向学校主要领导进行报告。

④网络管理人员根据故障类型及时与外部支持人员取得联系。其中，设备故障的，可与设备供应商和集成商联系；软件故障的，可与系统集成商联系，由系统集成商进行现场或远程技术支持；线路故障的，可与电信运营商联系，三方密切协作力求通信线路在短时间内恢复正常。

⑤网络管理人员在上级机构或外部支持人员的配合下，充分利用应急预案的资源准备，采取有力措施进行故障处理，及时恢复网络的正常通信状态。

⑥网络管理人员通知业务部门网络恢复正常，并向学校网络故障处理工作小组报告故障处理的基本情况。在事件处理过程中，网络管理人员应做好事件发生、发展、处置的记录和证据留存。重大事件应形成文字资料，以书面形式向上级报告。

⑦总结整个处理过程中出现的问题，并及时改进应急预案。

（2）现场应急处理

①校园网络如遇突然中断，信息化办公室应组织及时抢修，待网络修复后，在校园网主页上予以通报说明。

②在外网突然中断，上海工商外国语职业学院内网不断的情况下，信息化办公室与外网主要出口管理单位取得联系，证实情况后，在校园网主页重要栏目予以通报说明，并协助外网及时修复。

③对于放置于托管机房的域名服务器如遇故障，信息化办公室应协助排查，排查结果由相应部门网络管理员以书面报告说明故障缘由、处理结果，并交信息化办公室托管机房管理员。

④对于宿舍区出现的网络故障，信息化办公室在组织排除后，在信息化办公室网站中予以说明。

⑤对于邮件服务器出现的故障，信息化办公室修复后时应尽量保证用户邮件正常收发，并在信息化办公室网站中予以说明。

⑥发生自然灾害后的紧急处置措施。一旦发生自然灾害，导致设备损坏，由灾害发生单位向信息化办公室进行报备，信息化办公室寻找安全可靠的地点，重新构建新的系统和网络，并将相关数据予以恢复，经测试符合要求后，技术人员才能撤离。

⑦人员疏散与机房灭火预案。一旦机房发生火灾，应遵照下列原则：首先保人员安全；其次保关键设备、数据安全；三是保一般设备安全。人员疏散的程序是：机房工作人员立即按响火警警报，并通过119电话向公安消防请求支援，所有人员戴上防毒面具，所有不参与

灭火的人员按照预先确定的线路，迅速从机房中撤出。人员灭火的程序是：首先切断所有电源，启动自动喷淋系统，灭火值班人员戴好防毒面具，从指定位置取出泡沫灭火器进行灭火。

四、校网络故障通报

凡发生各类校网络故障事宜，须在故障排除后，及时在校主页予以通报说明。

信息化办公室如进行网络线路调整，须提前3天在上海工商外国语职业学院主页热点信息栏目予以通报说明，使用户及时调整上网时间。

五、其他

对于关键岗位平时应做好人员储备，确保一项工作有两人能操作。一旦发生关键人员不在岗的情况，由备用人员上岗操作，并向领导汇报情况。

六、附则

1、本管理制度由信息化办公室负责起草、解释、修改和归口管理

。

2、本管理制度自校领导签发之日起实施。

网络管理员管理办法

一、学校按照“统一领导，分级管理”的管理体制，实行校和分院、部、处、室、馆（以下简称各单位）两级管理的网络管理员制度。

二、各级领导要高度重视网络的管理工作，各单位应有一名领导分工负责本单位的网络信息建设和管理，对本单位网上信息的真实性、安全性负责，并配备一名精通计算机网络知识的技术人员担任本单位的网络管理员兼网络安全员，具体负责本单位网络的使用和管理。

三、网络管理员、网络安全员的组成

1、校内各单位设一名网络管理员兼网络安全员，由在职工作人员兼任，网络管理员行政上归所在单位领导，业务上接受信息化办公室的指导和培训。

2、各单位网络管理员由本单位指定，报信息化办公室审核备案；网络管理员的变动，须报信息化办公室备案，并及时办理新老管理员的交接工作。

四、网络管理人员工作职责

1、信息化办公室网络管理人员

（1）负责学校主页制作、更新和维护；负责学校信息发布、上传和接收，保证所提供的信息的准确、及时、全面性，建立本校网络信息数据库。

(2) 负责学校网络信息管理工作，包括指导二级学院兼职网络管理人员所属单位的网络线路设备的管理、用户技术支持，负责用户数据的收集、统计、备案、上报、违规事件的处理等。

(3) 及时了解、掌握所管辖网络线路设备的连接及运行情况，可以根据需要采取监视、记录、检测、制止等措施，防止所管辖的部门网络及连网的计算机进行违反有关规定的活动。

(4) 自觉参加网络技能培训，不断提高网络应用和操作技能，了解最新的网络技术发展动态。

(5) 学习、遵守国家有关部门颁布的有关计算机互联网络的各种管理法律法规，宣传、教育和监督用户在网络操作和应用中自觉遵守国家有关部门的有关法律法规。

2、各二级学院兼职网络工作信息员

(1) 兼职网络工作信息员在做好本职工作的同时，关心本学院和部门的重要事情、重大活动、主要教育教学改革内容，并及时告知学校宣传处。

(2) 负责本部门信息网络的规划、建设和管理；保管使用校园计算机主干网设置在各部门的设备，保证其正常运行；向网络中心报告网络使用情况、收集并反映用户意见；

(3) 对本部门申请入校园网的设备、子网、用户进行登记和管理，并及时报网络中心登记、分配地址和开设账号；做好本部门网络信息安全，数据备份；

(4) 参加信息化办公室组织的各类培训，不断提高业务水平；

（5）学生信息员要配合老师了解学生的思想动态和关注焦点，积极服务于学校大型活动，并做好简报、网站的宣传工作。

五、附则

1、本管理制度由信息化办公室负责起草、解释、修改和归口管理。

2、本管理制度自校领导签发之日起实施。

信息化办公室机房管理办法

一、管理人员按操作规程使用机房内设备，并负责日常维护及机房卫生工作，做到一天一小扫，一周一大扫；

二、如发现机器故障应及时向信息化办公室网管中心主任及上级领导报告，并负责计算机及外设的日常维护与排除故障，在遇到电脑公司三包范围内的故障时，应及时督促公司上门或将机器送公司维修；

三、对相关应用软件的购置、安装及使用提出意见和建议；

四、设备不得用于私事，谢绝外单位人员进入机房，杜绝外来计算机软盘进入机房；

五、如其他人员需使用机房内设备应征得管理人员许可，应遵循以下内容：

1、外部人员因工作需要进出机房，经信息部领导同意后，信息部人员应根据操作内容，确定进入人员，选择进出时间，填写《外部人员出入机房登记表》，整个工作过程需由信息部工作人员陪同进行，严禁从事非业务范围内的任何操作。如遇信息部领导不在，而又必须紧急处理的，需向其电话报告，并准予进入，待领导回来后补办相关手续。

2、外部参观人员出入机房，由单位领导或信息部人员陪同进行参观，需做好登记工作。

3、机房配备监控设施，未按规定进入者，如造成损失和泄密等不安全后果的，由本单位依照有关规定进行处理；如触犯国家有关法

律、法规者，移交公安、司法机关处理。违反本规定，给国家、集体或者他人财产或人身安全造成损失的，应当依法承担民事或刑事责任。

4、做好防火、防雨、防湿、防盗工作，注意用电安全；

5、要对机房内网络与设备的运行、应用、维护等情况，建立档案，做好系统日志。要对发生的故障（隐患）以及排除故障情况做好详细记录；

6、要统一管理机房内的设备，计算机及其相关设备的驱动程序、保修卡等随机文件与资料要保存完整。要明确专人负责计算机文档、信息化等资料的保管，要做到资料齐全，存放安全；

7、机房内的交换机和服务器系关键设备，任何人不得自行配置或更改系统参数；

8、机房内的环境由专人负责管理和维护(包括温度、湿度、电力系统、网络设备等)，要满足机房相关的标准要求；

9、严禁将易燃易爆和强磁物品及其它与机房工作无关的物品带入机房；

10、要做好机房的安全工作，对服务器的各种帐号、密码严格保密。对网络运行做好监控、做好记录；

11、要及时做好各服务器系统的补丁修正与升级工作；

12、管理人员要有较强的病毒防范意识，要定期对病毒库进行检测，并做好病毒库系统的定时升级工作。发现病毒应及时处理，并做好记录；

13、未经许可，不得在各服务器上安装新软件。如确实工作需要安装的，要经过信息化办公室领导批准；

14、应及时做好数据的备份工作，保证在系统发生故障时，数据能够快速、安全的恢复。所有备份数据不得更改，并要求做到本地和异地双备份保存；

15、机房内所有设备应妥善保管，任何人不得擅自开关、移动或者使用机房中的任何设备，如有此方面需要，需有信息化办公室主管领导的批示。

六、附则

1、本管理制度由信息化办公室负责起草、解释、修改和归口管理。
。

2、本管理制度自校领导签发之日起实施。

七、附件

附件编号	标题	页数
1	《机房等重要区域出入审批登记表》	1

机房等重要区域出入审批登记表

多媒体新闻中心管理办法

一、多媒体新闻中心使用申请

- 1、申请使用单位填写《校多媒体新闻中心使用申请表》，报部门负责人签字确认后，提交信息化办公室。
- 2、紧急临时使用多媒体新闻中心的，经信息化办公室负责人同意后，事后补气使用申请手续。

二、多媒体新闻中心日常管理

- 1、信息化办公室为校多媒体新闻中心日常管理部门。
- 2、做好使用情况登记记录，印制《多媒体新闻中心设备使用操作步骤》，粘贴在多媒体设备控制台上；印制《多媒体新闻中心运行日志》置于控制台内；印制《多媒体新闻中心使用登记册》并留存备案。
- 3、负责多媒体设备和操作系统的管理和维护。对现场无法解决的问题，及时进行报修，并尽快予以解决。
- 4、负责组织多媒体设备使用者和管理人员的培训，指导其正确使用设备。

三、多媒体新闻中心使用准则

- 1、使用前，应按规定办理相关使用登记手续。使用过程中严格按照粘贴在控制台上的《多媒体新闻中心设备使用操作步骤》操作，不得将设备自行移动、拆卸、带走、随意调整，遇到异常情况或疑难问

题，应当及时拨打控制台上标注的报修电话报告故障。使用完毕后，认真填写《多媒体新闻中心运行日志》，锁好控制柜并及时归还钥匙等物品。

2、凡造成设备损坏或丢失的，对责任人按照学校关于仪器设备损坏丢失赔偿处理办法处理。

3、未经信息化办公室许可擅自使用多媒体设备，由值班室人员承担全部责任。

四、附则

1、本管理制度由信息化办公室负责起草、解释、修改和归口管理。

2、本管理制度自校领导签发之日起实施。

实验实训室管理制度

为规范实验实训室管理，提高计算机使用效率，保证计算机设备安全和教学工作的正常运转，特制定本制度。

一、实验实训室财产设备管理

1、教学使用者要爱护实验实训室的各类设备，发现损坏和丢失要立即向实验实训室管理员办公室报告，配合调查原因，并追查责任。

二、实验实训室软硬件维护办法

1、实验实训室当值教师为实验实训室计算机软硬件管理的具体负责人。

2、在计算机资源相对紧张的情况下，各实验实训室软件安装首先满足各专业教学大纲规定的要求，在有余力的情况下，再考虑安装其他软件。对专业教师和学生提出的其他软件安装要求，在不影响正常教学的前提下，经有信息化办公室批准，可由实验实训室教师统一组织安装。未经许可私自从网上下载、安装任何软件的师生，如引起系统故障，视为严重违纪，一经查实，由当事人承担相关责任。

三、教师岗位职责

1、设备使用过程中要保证出口畅通，指挥学生打开门窗，并在课程结束后，关好门窗。

2、加强防火防漏电意识。

3、上课时间要在实验实训室中巡查，认真负责地指导学生设备使用操作，不得中途离开实验实训室。

4、教育、监督学生不得随意挪动实验实训室设备，并督促学生保持实验实训室清洁。

5、发现计算机故障应做好记录并及时通知实验实训室管理人员，和管理员一道重新调整和安排设备使用。

四、学生设备使用守则

1、设备使用时要求在教师指导下安静、认真地设备使用，不得喧哗吵闹，更不准随意走动。

2、爱护实验实训室卫生，雨具、仪器等不得带入实验实训室，不得乱扔果皮、纸屑等，实习用纸学生要自行带走。

3、不得在实验实训室的任何位置涂抹乱画，否则予以严惩。

4、开机时如发现计算机故障，应立即报告指导教师，重新调整机位；如果发现故障而未及时上报的，涉及到的一切责任由该生负责。

5、严禁修改客户机系统设置和入侵服务器，若练习需要，在教师的许可下修改必须改回，否则视作人为破坏，一经查实将给予严厉处分。

6、严禁随意安装、删除、卸载机器内已经安装的各种软件；严禁设备使用时间不按指导老师要求操作；严禁设备使用时打游戏、上网聊天、浏览有不健康内容的网站；

7、违犯上述规定且不听教育劝导者，取消设备使用资格，并由学校按校规进行处理。

机房安全责任公告

为规范机房管理，提高计算机使用效率，保证计算机设备安全和教学工作的正常运转，特制定本制度。

一、机房财产设备管理

1、教学使用者要爱护机房的各类设备，发现损坏和丢失要立即向机房管理员办公室报告，配合调查原因，并追查责任。

二、机房软硬件维护办法

1、机房当值教师为机房计算机软硬件管理的具体负责人。

2、在计算机资源相对紧张的情况下，各机房软件安装首先满足各专业教学大纲规定的要求，在有余力的情况下，再考虑安装其他软件。对专业教师和学生提出的其他软件安装要求，在不影响正常教学的前提下，经有信息化办公室批准，可由机房教师统一组织安装。未经许可私自从网上下载、安装任何软件的师生，如引起系统故障，视为严重违纪，一经查实，由当事人承担相关责任。

三、教师岗位职责

1、上机过程中要保证出口畅通，指挥学生打开门窗，并在课程结束后，关好门窗。

2、加强防火防漏电意识。

3、上课时间要在机房中巡查，认真负责地指导学生上机操作，不得中途离开机房。

4、教育、监督学生不得随意挪动机房设备，并督促学生保持机房清洁。

5、发现计算机故障应做好记录并及时通知机房管理人员，和管理员一道重新调整和安排上机。

四、学生上机守则

1、上机时要求在教师指导下安静、认真地上机，不得喧哗吵闹，更不准随意走动。

2、爱护机房卫生，雨具、仪器等不得带入机房，不得乱扔果皮、纸屑等，实习用纸学生要自行带走。

3、不得在机房的任何位置涂抹乱画，否则予以严惩。

4、开机时如发现计算机故障，应立即报告指导教师，重新调整机位；如果发现故障而未及时上报的，涉及到的一切责任由该生负责。

5、严禁修改客户机系统设置和入侵服务器，若练习需要，在教师的许可下修改必须改回，否则视作人为破坏，一经查实将给予严厉处分。

6、严禁随意安装、删除、卸载机器内已经安装的各种软件；严禁上机时间不按指导老师要求操作；严禁上机时打游戏、上网聊天、浏览有不健康内容的网站；

7、违犯上述规定且不听教育劝导者，取消上机资格，并由学校按校规进行处理。

实验实训场所安全应急预案

为有效预防、及时控制和妥善处置实验室突发安全事件，维护师生生命和学校财产安全，保障教学和科研工作的正常秩序，上海工商外国语职业学院结合实验室的具体情况，制定了实验实训室安全应急预案。

一、应急预案程序

1. 首次报告

发生突发事件后，应立即向中心突发事件应急处置实验实训管理委员会组长报告。

报告的内容必须包括：事件名称、发生地点和时间、报告时间、涉及人群或潜在的威胁和影响、报告单位、报告人、联系人及通讯方式；尽可能报告的信息内容包括：事件初步性质、严重程度及发展趋势、可能的原因、已采取的措施等。

2. 进程报告

进程报告内容为突发事件的发展与变化、处置进程、事件的原因或可能因素、已经或准备采取的整改措施等。对于重大或特别重大突发事件的进程报告除了向应急处置实验实训管理委员会组长报告外，还应将事件发展变化情况及时报告学校及相关部门。

3. 结案报告

在事件处理结束后，事件应急处置实验实训管理委员会应及时向学校提交结案报告。

结案报告的内容包括事件的基本情况、事件产生的原因、应急处置的过程（包括各阶段采取的主要措施及其效果）、处置过程中存在的问题及整改情况，并提出责任追究及今后对类似事件的防范和处置建议等。

二、应急处置措施

1. 突发事件发生后，实验室负责人应立即启动突发事件应急预案，同时将有关情况报告中心应急处置实验实训管理委员会组长，实验实训管理委员会组长接到报告后，根据职责和规定的权限启动本应急预案，对突发事件进行及时、有效处置，控制事态进一步发展。

2. 在实验实训管理委员会统一部署下，按照分级响应的原则，快速作出应急反应。根据实际情况可采取下列措施：组织营救和救治受害人员，疏散、撤离、安置受到威胁的人员；迅速消除突发事件的危害和危险源，划定危害区域并加强巡逻；针对突发事件可能造成的损害，封闭、隔离有关场所，中止可能导致损害扩大的活动；抢修被损坏的供水、供电、供气等基础设施。

3. 突发事件应急处置要采取边调查、边处理、边抢救、边核实的方式，以有效控制事态发展。

4. 事后，要对其他实验室和相关人员及学生进行教育，要及时部署和落实学院的预防控制措施，防止类似突发事件在本单位再次发生。

三、应急响应

对于先期处置未能有效控制事态发展的，或超出事件发生单位处置能力需要学校协调处置的，由中心及时联系上报学校，再由学校主要领导直接指挥和指导，协同开展处置工作。

四、善后处理

直接应急处置和救助活动结束后，工作重点应马上从应急处置转向补救和善后工作，争取在最短时间内恢复正常秩序。

1. 做好事故中受伤人员的医疗救助工作，对有各种保险的伤亡人员要帮助联系保险公司赔付。
2. 及时查明事故原因，严格信息发布制度，确保信息及时、准确、客观、全面，做好稳定中心正常教学和生活的秩序工作。
3. 全面检查设备、设施安全性能，检查安全管理漏洞，对安全隐患及时整改，避免事故再次发生。
4. 总结经验教训，引以为鉴，对因玩忽职守、渎职等原因而导致事故发生的，要追究有关人员的责任。
5. 配合公安机关做好事件侦察工作。

信息安全管理方法

一、学校各类信息化设备、系统申请后须至学校信息化办公室备案。

二、计算机的使用部门要保持清洁、安全、良好的计算机设备工作环境，禁止在计算机的应用环境中放置易燃、易爆、强腐蚀、强磁性等有害计算机设备安全的物品。

三、非信息化办公室本部门人员对信息设备、系统等进行维修、维护时，必须有本部门人员进行现场监督。计算机设备送外维系时，须有本部门负责人批准。

四、非信息化办公室本部门人员在借用计算机等设备时，需在借用情况登记单上签字记录。

五、各部门负责本部门内的网络安全和信息安全，对本部门内所属信息化设备进行定期巡检，一旦发现问题需及时上报信息化办公室处理，不允许私自处理或找非本部门人员进行维修及操作。

六、信息化平台的相关密码设置应具有安全性、保密性，有关人员不得将密码外泄。

七、注意计算机重要信息资料和数据的存储和归类整理，定期进行清点归纳。保证储存的安全性和完整性。

八、信息化办公室将于每年6月、12月，对备案的信息系统、设备进行年检，并将测试结果整理为报告存档。如有违反以上管理要求，并造成不良影响的，信息化办公室有权责令其停止行为，并追究责任。

九、附则

- 1、本管理制度由信息化办公室负责起草、解释、修改和归口管理。
- 2、本管理制度自校领导签发之日起实施。

信息资产管理制度

一、总则

- 1、为有利于上海工商外国语职业学院（以下简称“工商外”）信息资产的采购、分类、识别、维护和使用，加强信息资产的安全管理，特制订本规定。
- 2、本规定适用于工商外信息资产的管理。
- 3、工商外信息化办公室是本部门信息资产的管理部门。

二、信息产品及设备采购

- 1、信息产品及设备需求部门制定产品需求的技术参数，采购过程参照学校财务资产处的设备招标采购流程，将采购申请提交到资产办审核汇总，审批后成立招标小组，由专人负责产品招标。
- 2、招标小组依据信息产品及设备选购原则完成招标并确定服务商。
- 3、信息产品及设备的选型选购，应符合以下要求：
 - (1) 设备选购过程坚持公开、公平、公正的原则；
 - (2) 符合工商外业务应用需求，适应业务发展需要；
 - (3) 符合事业单位国有资产管理办法、工商外技术标准、安全标准和设备配备定额标准，与现有工商外设备兼容，著名品牌、质量好、价格和使用成本合理，售后服务良好，优先考虑选购国家

政策扶持采购的产品；安全产品应符合国家有关规定，密码技术产品应符合国家密码主管部门的要求；

（4）符合专款专用、勤俭节约、追踪问效等财务、审计管理要求。

4、信息产品及设备到货后，信息化办公室相关技术人员完成到货验收并填写《到货验收单》（详见附件）。

5、所有设备到货后均需进行严格检测，凡购置的设备均应在测试环境下经过连续72小时以上的单机运行测试和联机48小时的应用系统兼容性运行测试。严禁将未经测试验收或验收不合格的设备上线。

三、信息产品及设备入库

1、到货验收完成后，资产管理负责人将设备编码、用标签打印机打印贴签、入库登记，并更新库房资产清单。

四、信息资产分类和标识

1、所有信息资产都应指定资产责任人，并由资产责任人负责进行相关资产的识别、统计、分类、分级，以便相关人员采取相应的保护措施。

2、信息化办公室纳入信息资产管理范畴的信息资产类别划分为：数据资产、软件资产、实物资产、人员资产、服务资产、其他资产。

3、根据各类信息资产在保密性、完整性和可用性三个方面所表现出的重要程度，各划分为五个级别，对应取值范围从“5”到“1”（5为很高，1为很低）。

4、信息资产标识应建立统一的命名规则，便于资产识别和日常管理。

5、资产分类分级信息应在资产清单中进行标注，伴随每年的资产盘点更新相关信息。

五、信息资产的日常使用与维护

1、资产日常使用中的管理依据“谁使用，谁负责”原则。工商外内部所有用户日常资产使用中都应遵守本制度相关要求，结合其他管理要求，采取对应的措施手段进行资产保护。

2、存储介质(含磁盘、磁带、光盘和优盘)的管理应遵循相应的保存及使用要求。

3、需要机房上线的信息产品及设备必须经过测试后，设备才能进入试运行阶段。试运行时间的长短可根据需要确定。通过试运行的设备，才能投入生产系统，正式运行。

4、资产管理负责人应至少每年进行一次管辖范围内的资产盘点。确保资产清单及资产状态与资产实际使用情况保持一致。

5、在信息资产生命周期的不同阶段，信息资产保密性(C)、完整性(I)、可用性(A)属性值会因各种原因发生变化，此时资

产责任人及相关人员应按照新的属性值采取适当的处理和保护措施。
。

六、信息资产报废

1、信息资产需要报废的部门应填写《设备报废申请》，经本部门领导审批后，提交到资产管理负责人审批。审批通过后，统一由资产管理负责人对资产进行回收处理。资产报废部门应做好报废设备的信息及数据备份工作。

2、资产管理负责人对报废设备应进行信息处理，处置措施参考如下：

- (1) 磁盘、磁带等设备应进行消磁处理；
- (2) 光盘、纸质介质采用碎纸机进行销毁；
- (3) 其它报废不再使用的设备可考虑不可恢复的物理损坏操作；
- (4) 无法采用上述处置措施的，电子类信息可考虑三次以上低格操作。

3、报废后的设备，按照学校相关规定统一处理。资产管理负责人更改资产清单及设备状态。

七、附则

1、本规定由网络与信息安全工作领导小组办公室负责制定、解释和更新。

2、本规定自颁布之日起实行。

信息系统用户和密码管理规定制度

一、总则

1、为保障上海工商外国语职业学院（以下简称“工商外”）信息系统的安全，确保合理访问和修改工商外数据资源，根据《信息系统安全等级保护实施指南》（GBT 25058-2010），结合工商外实际，制定本规定。

2、本管理规定确立了包括建立、监控、修改、注销和删除工商外信息系统帐号的规则。

3、本管理规定适用于工商外信息系统的设备、平台等，适用对象是工商外内部人员、第三方人员以及其他任何授权使用工商外信息系统资源的人员。

4、网络与信息安全管理领导小组办公室负责制定信息系统用户帐号名策略和密码策略。

5、信息化办公室负责工商外信息系统帐号及密码的分配和统一管理。

二、帐号管理

1、帐号名

（1）每个系统的帐号名需能代表某个系统或应用的用户。每个帐号需要有一个所属人。

（2）不允许共享帐号身份或帐号组身份。

(3) 内部人员帐号名基本规则为员工的工号。

2、帐号的权限申请

(1) 应根据业务的需求申请帐号权限，并根据所属人的权限开通相关帐号的功能。

(2) 帐号的权限申请必须得到信息化办公室负责人及所在部门领导的关于访问该系统设备或服务的批准。

(3) 帐号的权限应被严格控制。帐号尤其是特别权限的帐号应被限制在职责范围内所需工作的最低权限。超过普通用户的权限，必须基于业务需求，并得到信息化办公室负责人的批准。

(4) 帐号和密码提供给员工之前，需要确认用户的身份。推荐使用较严格的方式来提供拥有特权的帐号信息。

(5) 第三方人员申请信息系统帐号时由接口的内部员工代为办理，并需明确其责任和义务。

3、帐号的使用

(1) 各类信息系统的帐号权限应定期进行检查，检查的间隔时间和方式应在相关信息系统设备或服务的文档中阐述。

(2) 所有在一定预期内未使用的帐号应被废除或更变其状态。

(3) 当员工被调动到其他部门或者不再具有相应的角色和使用需要，那么所有相关的帐号权限都应被立刻中止。

(4) 系统管理员的权限须得到明确的区分：

①操作系统管理和维护的人员，需要得到操作系统管理员的权限。

②安全管理工作的人员，需要得到安全管理员的权限。

(5) 不允许在没用通过验证的情况下，访问信息系统设备、平台。

(6) 系统中帐号产生的操作均视为申请人本人所为。

4、帐号权限的变更

(1) 员工因工作职责发生转变，造成现有权限与在系统中的职责不同时，应当申请权限的修改。

(2) 信息化办公室发现用户具有工作不需要的权限，可以直接停止多余的权限。

(3) 帐号使用人在工作职责发生转变，而不再需要使用系统资源的情况下，应当申请关闭帐号，对不能关闭的帐号则需要转移帐号的责任人。

5、帐号的删除

(1) 当员工离开学校时，管理员根据员工所在部门的通知变更帐号的状态。

(2) 作为工商外员工，当根据其工作性质不再需要拥有的帐号时，应有责任通知管理员把相关帐号权限删除并更变状态。

(3) 非学校人员的帐号停止使用后，接口的工商外员工应当负责提出删除帐户权限。

三、密码管理

1、在相关系统的技术支持下，工商外密码的标准为：

(1) 至少六位。

(2) 至少包含一个字母、一个数字。

(3) 至少每90天更换一次密码。

(4) 禁止使用上一次的密码。

(5) 禁止把帐号名、生日、电话号码作为密码或其一部分。

(6) 在首次登陆后修改临时或缺省得密码。

(7) 如果需要访问不在学校控制下的计算机系统，禁止选择在学校内部使用的密码作为外部系统的密码。

2、密码在使用过程中需注意以下几点：

(1) 即使系统没有使用技术控制措施强制更换密码，同样需要遵守密码更换要求。当更换密码时，必须选择一个新的密码，禁止使用前两次的密码。

(2) 在任何系统付诸操作之前，所有由卖方所提供的缺省密码应被改变。

(3) 如果怀疑密码可能存在泄漏的问题，应立刻改变这些密码。

(4) 当密码被存储或者在网络上传输时，尽可能先通过加密变为密文的形式。如果无法采用加密功能，必须保证只有授权的系统安全管理员才能够访问这些文件和数据库的密码部分。

(5) 密码在输入时的显示必须使用星号或方框等符号进行替代。

(6) 帐号和密码信息尽可能不通过Email发送给使用者。若使用Email进行发送，则Email必须进行加密并将帐号和密码分开发送给使用者。

(7) 硬件设备、应用系统的密码若长时间无法进行更改，则需要满足以下密码标准：

① 密码长度至少八位。

② 必须包含大写字母、小写字母、数字和特殊字符。

③ 不能在多台设备或多个应用系统中使用相同的密码。

(9) 保持密码的保密性，密码如无必要不能被共享和泄露出去。

(9) 如果密码必须被共享，那么立刻在共享需要不再存在之后改变密码。如果技术允许，改变的密码与原密码不能有原来密码的部分内容。

四、附则

- 1、本规定由网络与信息安全工作领导小组办公室负责制定、解释和修改。
- 2、本规定自颁布之日起实行。

信息安全检查管理规定制度

一、总则

1、为了加强上海工商外国语职业学院（以下简称“工商外”）信息安全检查工作，及时发现管理和技术层面存在的薄弱环节和安全隐患，有效保障网络和信息系统的稳定可靠运行，减少或防止信息安全事件的发生，根据《信息系统安全等级保护实施指南》（GBT 25058-2010），结合工商外实际，制定本规定。

2、本规定适用于工商外内部或外部的信息安全检查活动。

3、网络与信息安全工作领导小组办公室负责为信息安全检查工作提供资源保证和授权；负责组织协调各部门配合信息安全检查工作。

4、信息安全管理員负责编制信息系安全检查内容及评分表，对各部门信息安全要求的落实情况进行检查和评价，并负责外部信息安全检查的接待工作。

5、被检查部门应全力配合安全检查，如实提供所需材料和信息，对发现的问题制定整改措施，并按计划实施整改。

二、检查方式和程序

1、信息安全检查按照执行方式的不同可分为内部检查和外部检查。

2、内部检查以网络与信息安全领导小组办公室为主导，信息安全管理员认领，检查内容应包括安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

3、外部检查主要以合规为驱动，检查内容主要包括信息系统等級保护测评、监管机构专项安全检查等。

4、外部安全检查频率按照监管机构要求执行，内部安全检查频率每年不低于1次，如果发生下列情况，需及时进行安全检查：

- (1) 发生重大安全事件；
- (2) 学校组织架构变更；
- (3) 学校业务发生重大变化；
- (4) 信息技术发生重大变革。

5、安全检查工作程序分为四个阶段：准备阶段、实施阶段、报告编制阶段和整改阶段。

三、安全检查的准备

1、信息安全管理员认领建立信息安全检查机制，制订年度检查计划，检查计划应根据实际情况及时进行补充和调整。

2、在进行制度执行检查前，应根据检查时间、人员安排等实际情况，以信息安全检查提纲为主要依据，及国内外其他信息安全法律法规和标准，最终确定本次信息安全检查指标内容。

3、在进行技术类检查前，应制定检查方案，确保其可行性和合理性，检查方案应事先通过测试，必要时应进行安全检查的风险论证。

4、各种形式的内外部检查，都应获得网络与信息安全管理小组的授权，信息安全检查工具的采购、实施应符合学校相关采购管理规定要求。

四、安全检查的实施

1、信息安全管理员认按照年度检查计划进行安全例行检查，必要时可组织安全专项检查。

2、安全检查应按照所规定的检查要点及检查方式，使用学校指定的检查工具进行检查。

3、应选择对信息系统运行影响最小的方式和时间进行检查。安全检查后，被检查系统的责任部门应对被检查系统的运行情况进行确认，确保系统无异常。

4、检查过程中应做好检查结果的记录工作。

5、在外部安全检查现场实施阶段，安全管理员应全程进行接待和陪同，确保检查工作不能超出预定的范围，对检查实施单位人员进行管理。

五、检查报告及整改

1、内部检查由信息安全管理员认为进行现场评分并记录检查发现结果，在检查结束后整理安全检查报告，检查报告应至少包括信息安全检查内容、存在问题（不符合项）描述、分析总结等内容。

2、经与被检查部分确认后，信息安全管理员认为将信息安全检查报告提交网络与信息安全工作领导小组办公室。

3、针对外部信息安全检查，信息安全管理员认为和相关被检查部门确认检查结果，并将检查方出具的检查记录和报告，提交网络与信息安全工作领导小组办公室。

4、信息安全管理员认为应对信息安全中发现的问题，向问题部门开具整改通知和整改建议。

5、问题部门按照整改通知和整改建议要求制定整改方案，并按计划实施整改。

6、信息安全管理员认为定期对整改工作进行跟踪，直至问题关闭。

7、信息安全相关检查（内部检查、外部检查）结果作为部门或人员绩效考核与奖惩参考。

信息安全组织建设管理规定制度

一、总则

- 1、本文件的目的在于建立上海工商外国语职业学院（以下简称“工商外”）信息安全管理组织框架，规范信息安全岗位的职责，明确信息安全管理责任，为工商外信息安全工作的深入开展提供保障。
- 2、本规定适用于工商外信息安全的组织建设。

二、岗位设置原则

- 1、职责分离原则：应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。
- 2、多人负责原则：对一些有较高密级的与安全有关的活动，都必须有两人或多人在场。工作人员必须由系统主管领导指派，且忠诚可靠，能胜任工作；工作人员应该认真记录签署工作情况，以证明安全工作已得到保障。
- 3、任期有限原则：决不能由一人长期担任安全管理职务。对一些重要安全岗位的工作人员应该不定期循环任职，强制实行轮换、休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

4、权限随岗原则：根据岗位变动情况及时调整相应的授权，做到在岗有权、离岗失权。上述所指与安全有关的活动包括：硬件和软件的维护、系统软件的设计和维护、系统用媒介的发放与回收、重要程序和数据的删除和销毁等。

三、信息安全组织架构与职责

1、工商外信息安全管理组织架构划分为“决策层、管理层、执行层”三个层面，并实现“信息安全管理、信息安全执行、信息安全审计”人员角色职责的分离。

2、信息安全决策层为网络与信息安全工作领导小组，其主要职责包括：

（1）负责工商外信息安全管理决策和管理工作；

（2）负责审批学校层面信息安全管理体系建设规划；

（3）负责工商外信息安全管理组织的整体规划与建设，并批准和任命信息安全相关人员的角色与职责；

（4）负责信息安全重大事宜的决策与监督；

（5）负责信息安全方针策略和管理制度文件的审批。

3、信息安全管理层为网络与信息安全工作领导小组办公室，其主要职责包括：

- (1) 统一协调和落实工商外各项网络与信息安全规划、建设、监督管理和检查工作；
- (2) 负责组织、发起信息安全相关会议，部署和跟踪会议决议的执行情况；
- (3) 负责组织相关部门和人员制订或修订信息安全管理规章制度文件；
- (4) 负责指导和督促各部门依据网络与信息安全工作领导小组的决议及相关要求落实信息安全建设各项具体工作。
- (5) 负责组织信息安全事件的应急演练和处置工作，以及信息安全教育、培训工作；
- (6) 负责保持与政府部门、监管机构、公安机关、合作伙伴及其他安全专家组和专业协会的适当联系。
- (7) 负责聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审。

4、信息安全执行层为网络与信息安全工作执行小组，由信息安全管理員、机房管理員、系统管理員、网络管理員、应用管理員和各部門安全协调員组成，负责信息安全各项具体工作的开展，承担相应的信息安全职责。

- (1) 信息安全管理員

- ①负责信息安全相关的日常管理及部门之间的沟通协调工作；
- ②协助业务需求部门对新建业务系统提出安全需求，并在上线前进行安全检查；
- ③负责定期进行安全检查活动，并将每次安全检查报告和整改落实情况向网络与信息安全工作领导小组办公室汇报；
- ④负责外部信息安全检查的接待工作（如等级保护测评）；
- ⑤负责牵头处理信息安全事件，总结安全事件的发生和解决情况，并编制分析报告，及时向网络与信息安全工作领导小组办公室汇报。
- ⑥制定病毒防范操作规程；
- ⑦负责执行和监督整个系统全面的杀毒工作；
- ⑧定时升级网络杀毒软件的病毒库，监督个人杀毒软件的升级工作；
- ⑨实时监控重要业务系统和数据的安全，杜绝非法开放的病毒入侵途径，降低病毒侵害的影响；
- ⑩及时报告上级部门病毒入侵和感染情况，提供感染频率高和严重性强的病毒的有效解决方案。

（2）机房管理员

- ①负责机房的整体管理和日常管理事务；

- ②负责机房设备出入库及借用的记录；
- ③负责机房出入人员的登记、并全程陪同来访人员；
- ④负责机房环境的监控和巡检，并做好记录，发现异常情况及时上报。

（3）系统管理员

- ①负责主机操作系统的安全配置和日常审计，从系统层面实现对用户与资源的访问控制；
- ②制定主机操作系统的安全配置规则，并落实执行；负责主机设备的日常管理与维护，保持系统处于良好的运行状态；
- ③提供完整、准确的主机系统运行活动的日志记录；在主机系统异常或故障发生时，详细记载发生异常时的现象、时间和处理方式，并及时上报；
- ④编制主机设备的维修、报损、报废计划，报主管领导审核；

（4）网络管理员

- ①负责网络的部署以及网络产品、网络安全产品的配置、管理与监控，并对关键网络配置文件进行备份；
- ②制定网络设备安全配置规则，并落实执行；提供完整、准确地记录重要网络设备和网站运行活动的运行日志；

③在网络及设备异常或故障发生时，详细记载发生异常时的现象、时间和处理方式，并及时上报；

④编制网络设备的维修、报损、报废等计划，报主管领导审核。

（5）应用管理员

①对业务应用系统进行安全配置；

②督促软件开发商提供补丁来修补已发现的漏洞；

③对业务应用系统的用户、口令的安全性进行管理；

④对业务应用系统的登录用户进行监测和分析；

⑤和业务部门沟通数据的备份要求、和数据库管理员沟通备份策略，督促数据库管理员按照备份方案按时完成，并恢复所需数据；实施系统软件版本管理，应用软件备份和恢复管理；

⑥根据应用系统运行的实际情况，制定应急处理预案，提交信息化办公室审定。

（6）各部门安全协调员

①负责组织与协调本部门内的各项信息安全管理，为工作的开展提供支持；

②对本部门信息安全事件进行协调处理并及时通知相关部门。

四、附则

1、本规定由网络与信息安全工作领导小组办公室负责制定、解释和修改。

2、本规定自颁布之日起实行。

信息安全管理体系建设文件控制管理规定制度

一、总则

1、为规范上海工商外国语职业学院（以下简称“工商外”）信息安全管理体系建设文件的审批、发布、分发、更改、保管和作废等活动，根据《信息系统安全等级保护实施指南》（GBT 25058-2010），结合工商外实际，制定本规定。

2、本规定适用于工商外信息安全管理体系建设过程和活动。

3、信息安全管理体系建设文件是确保工商外信息系统正常运转形成的文书，用于阐述需保护的资产、风险管理的方法、控制目标及方式和所需的保护程度。

4、网络与信息安全工作领导小组办公室负责组织工商外信息安全管理体系建设各级文件的编写、审核和归档；负责组织体系各级文件的宣传推广。

二、细则

1、体系文件的类别

信息安全管理体系建设文件可分为以下四级：

（1）一级文件：管理策略；

（2）二级文件：管理规定；

- (3) 三级文件：管理规范、实施细则、操作手册等；
- (4) 四级文件：运行记录、表单、工单、记录模板等。

2、体系文件的编写

体系文件的封皮、目录、正文、附件等的编写格式遵从统一规范要求。

3、体系文件的发文流程

发文流程是指制发文件的过程，包括拟稿、会签、审核、签发、校对、用印、登记、分发等程序。

4、体系文件的拟稿

体系文件的拟稿应符合以下要求

- (1) 体系文件内容应符合国家的法律、法规及其他相关规定，拟稿人应主动查询有关法律法规以及其他相关规定。
- (2) 体系文件的内容应该情况属实，观点明确，表述准确，结构严谨，条理清楚，直述不曲，字词规范，标点正确，篇幅力求简短。
- (3) 文件的文种应当根据行文目的、行文方向、文件内容确定。
- (4) 文件中人名、地名、机构名、数字、日期、引文以及简称的使用要准确、规范。

①引用文件应当先引标题、后引发文字号。引用文件一般应原文引用，引用的原文部分应标注引号；不便原文引用的，必须准确引用原意，不标注引号。引用外文应当注明中文含义。

②文件中，同一人员、机构、地点的称谓要前后一致。使用简称应该规范，一般应当先使用全称并注明简称，注明简称后应统一使用简称。文件中的外文名称或其缩写形式，第一次出现时应注明中文译名。

③结构层次序号，分两种：

- 1) 第一层为“第一章”，第二层为“第一条”，第三层为“（一）”，以后自行标注其他层次。
- 2) 第一层为“一”，第二层为“（一）”，第三层为“1.”，第四层为（1），以后自行标注其他层次。

④文件中使用国家法定计量单位。

⑤文件中的数字，除成文时间、部分结构层次序数和词、词组、惯用词、缩略词、在具有修辞色彩的词句中作为词素的数字必须使用汉字外，应当使用阿拉伯数字。

⑥日期应当写具体的年、月、日。

（5）拟稿一律使用A4纸，并按规定填写发文稿纸相关内容，首页各项签名应用钢笔或签字笔书写。

5、体系文件的审核

体系文件在学校领导签发前，应由信息化办公室主任审核。文件审核实行分级负责制。主办部门要有专人对本部门拟写的体系文件进行初审；主办部门负责人要严格把关，对文件内容、数字的真实性和准确性负责。

体系文件审核的主要内容包括：

- (1) 是否确需行文。
- (2) 行文方式及级别是否妥当，是否符合行文规则。
- (3) 是否符合党和国家的方针政策，是否符合国家法律法规。
- (4) 是否符合体系文件拟制的有关要求。
- (5) 内容涉及其他部门的文件，是否经过协商、会签，意见是否一致。
- (6) 是否符合体系文件处理程序和体系文件格式规定。
- (7) 密级的确定是否合乎规定，紧急程度的设定是否合乎情理。
- (8) 主送、抄送、内部发送范围是否恰当。
- (9) 发文稿纸及版面是否整洁。

体系文件经审核如需进一步明确政策、调整结构或修改较大需清稿、会签、文中内容要做说明、补充附件、或者发现不需要发文等，信息化办公室主动与主办部门协商，直接退回主办部门修改。

6、体系文件的签批

体系文件经核稿后，由信息化办公室送分管领导签发。签批体系文件，应使用钢笔或签字笔。各级经办人和领导签批体系文件必须写上姓名和审批日期。凡经学校领导签发的发文，如文字需要更改，应得到签发领导的认可同意。

7、体系文件的校对

体系文件打印后，由院长办公室校对，主办部门审读，每份体系文件做到文字、格式正确，发文手续完备，文字整洁，装订规范，附件无遗漏，发送份数、对象、密级程度准确无误。

8、体系文件的印制

领导签批后的体系文件，原则上应当天或次日送印，学校领导改动较大或另有要求的除外。

9、体系文件的发送

- (1) 正式体系文件由院长办公室负责登记后发送。
- (2) 保密文件的发送应符合保密规定。

10、体系文件的管理

- (1) 体系文件应由院长办公室专职人员统一收发、审核、用印、归档和销毁。
- (2) 公开发布工商外体系文件，必须经学校领导批准。
- (3) 体系文件复印件作为正式体系文件使用时，应加盖工商外公章。
- (4) 体系文件被撤销，自撤销之日起不生效力；体系文件被废止，自作废之日起不生效力。
- (5) 工商外工作人员调离工作岗位时，应当将本人暂存、借用的体系文件按照有关规定移交、清退。
- (6) 不具备归档和存查价值的体系文件，经过鉴别并经院长办公室负责人批准，可以销毁，实行定点收集、集中销毁的管理办法，不得随便弃置、不得交给清洁工、不得私自按废品出卖。
- (7) 信息化办公室主任负责组织工商外的体系文件销毁。参加体系文件销毁的人员要认真负责、确保销毁的文件安全。销毁涉密体系文件应当到指定场所由2人以上监销，保证不丢失、不漏销。其中销毁涉密体系文件的，应当进行登记，经部门负责人审核后报学校院长办公室备案。

11、体系文件的评审与修订

- (1) 网络与信息安全工作领导小组应定期组织对体系文件进行评审和修订，文件的评审至少每年进行一次。

- (2) 文件修订后应重新提交进行发文流程。
- (3) 当业务发生重大变化、组织架构出现重大调整或法律法规发生变化时，也应酌情进行文件评审，并根据需要对文件进行修订与更新。
- (4) 文件的更新应严格遵守规章制度。

12、体系文件的归档

- (1) 体系文件原件由信息化办公室相关人员负责归档，个人不得保存应当归档的体系文件。
- (2) 工商外体系文件的具体归档范围、立卷整理、归档、接收等具体事宜参考工商外档案管理工作办法。
- (3) 拟制、修改和签批体系文件，书写及所用纸张和字迹材料必须符合存档要求。

13、外来体系文件的管控

外来体系文件的管控由引入部门负责，需报备网络与信息安全工作领导小组。

三、附则

- 1、本规定由网络与信息安全工作领导小组办公室负责制定、解释和更新。
- 2、本规定自颁布之日起实行。