上海工商外国语职业学院

信息管理制度汇编

2024 年 6 月

目　录

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，经有实训中心批准，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。

上海工商外国语职业学院

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，经有实训中心批准，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。

上海工商外国语职业学院

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）应急预案程序及

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。

上海工商外国语职业学院

信息资产管理制度

第一章　总则

第一条　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。

第二条　本规定适用于工商外信息资产的管理。

第三条　工商外实训中心是本部门信息资产的管理部门。

第二章　信息产品及设备采购

第四条　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。

第五条　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。

第六条　信息产品及设备的选型选购，应符合以下要求：

（一）设备选购过程坚持公开、公平、公正的原则；

（二）符合工商外业务应用需求，适应业务发展需要；

（三）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；

（四）符合专款专用、勤俭节约、追踪问效等财务、审计管理要求。

第七条　信息产品及设备到货后，实训中心相关技术人员完成到货验收并填写《到货验收单》（详见附件）。

第八条　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。

第三章　信息产品及设备入库

第九条　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。

第四章　信息资产分类和标识

第十条　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。

第十一条　实训中心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。

第十二条　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）。

第十三条　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。

第十四条　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。

第五章　信息资产的日常使用与维护

第十五条　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。

第十六条　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。

第十七条　　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。

第十八条　　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。

第十九条　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。

第六章　信息资产报废

第二十条　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。

第二十一条　　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：

（一）磁盘、磁带等设备应进行消磁处理；

（二）光盘、纸质介质采用碎纸机进行销毁；

（三）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；

（四）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。

第二十二条　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。

第七章　附则

第二十三条　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。

第二十四条　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

第一章　总则

第一条　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。

第二条　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。

第三条　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。

第四条　网络与信息安全工作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。

第五条　实训中心负责工商外信息系统帐号及密码的分配和统一管理。

第二章　帐号管理

第六条　帐号名

（一）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。

（二）不允许共享帐号身份或帐号组身份。

（三）内部人员帐号名基本规则为员工的工号。

第七条　帐号的权限申请

（一）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。

（二）帐号的权限申请必须得到实训中心负责人及所在

部门领导的关于访问该系统设备或服务的批准。

（三）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，并得到实训中心负责人的批准。

（四）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。

（五）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。

第八条　帐号的使用

（一）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。

（二）所有在一定预期内未使用的帐号应被废除或更变其状态。

（三）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。

（四）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。

（五）不允许在没用通过验证的情况下，访问信息系统设备、平台。

（六）系统中帐号产生的操作均视为申请人本人所为。

第九条　帐号权限的变更

（一）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。

（二）实训中心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。

（三）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。

第十条　帐号的删除

（一）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。

（二）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。

（三）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。

第三章　密码管理

第十一条　在相关系统的技术支持下，工商外密码的标准为：

（一）至少六位。

（二）至少包含一个字母、一个数字。

（三）至少每 90 天更换一次密码。

（四）禁止使用上一次的密码。

（五）禁止把帐号名、生日、电话号码作为密码或其一部分。

（六）在首次登陆后修改临时或缺省得密码。

（七）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。

第十二条　密码在使用过程中需注意以下几点：

（一）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。

（二）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。

（三）如果怀疑密码可能存在泄漏的问题，应立刻改变这些密码。

（四）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。

（五）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。

（六）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。

（七）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。

（八）保持密码的保密性，密码如无必要不能被共享和泄露出去。

（九）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。

第四章　附则

第十三条　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。

第十四条　本规定自颁布之日起实行。

信息安全检查管理规定制度

第一章　总则

第一条　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。

第二条　本规定适用于工商外内部或外部的信息安全检查活动。

第三条　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。

第四条　信息安全管理员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。

第五条　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。

第二章　检查方式和程序

第六条　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。

第七条　内部检查以网络与信息安全领导小组办公室为主导，信息安全管理员牵头，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。

第八条　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级保护测评、监管机构专项安全检查等。

第九条　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。

第十条　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。

第三章　安全检查的准备

第十一条　信息安全管理员应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。

第十二条　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。

第十三条　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。

第十四条　各种形式的内外部检查，都应获得网络与信息安全领导小组的授权，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。

第四章安全检查的实施

第十五条　信息安全管理员应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。

第十六条　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。

第十七条　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。

第十八条　检查过程中应做好检查结果的记录工作。

第十九条　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。

第五章 检查报告及整改

第二十条　内部检查由信息安全管理员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。

第二十一条　经与被检查部分确认后，信息安全管理员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。

第二十二条　针对外部信息安全检查，信息安全管理员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。

第二十三条　信息安全管理员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。

第二十四条　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。

第二十五条　信息安全管理员定期对整改工作进行跟踪，只至问题关闭。

第二十六条　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

第一章　总则

第一条　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。

第二条　本规定适用于工商外信息安全的组织建设。

第二章　岗位设置原则

第三条　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。

第四条　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。

第五条　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。

第六条　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。

第三章　信息安全组织架构与职责

第七条　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。

第八条　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：

（一）负责工商外信息安全决策和管理工作；

（二）负责审批学校层面信息安全管理体系建设规划；

（三）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；

（四）负责信息安全重大事宜的决策与监督；

（五）负责信息安全方针策略和管理制度文件的审批。

第九条　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：

（一）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；

（二）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；

（三）负责组织相关部门和人员制订或修订信息安全管理制度文件；

（四）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。

（五）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；

（六）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。

（七）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。

第十条　信息安全执行层为网络与信息安全工作执行小组，由信息安全管理员、机房管理员、系统管理员、网络管理员、应用管理员和各部门安全协调员组成，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。

（一）信息安全管理员

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。

（二）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。

（三）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；

（四）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。

（五）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，提交实训中心审定。

（六）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工作，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。

第四章　附则

第十一条　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。

第十二条　本规定自颁布之日起实行。

信息安全管理体系文件控制管理规定制度

第一章　总则

第一条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。

第二条　本规定适用于工商外信息安全管理体系文件控制过程和活动。

第三条　信息安全管理体系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。

第四条　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。

第二章　细则

第五条体系文件的类别

信息安全管理体系文件可分为以下四级：

（一）一级文件：管理策略；

（二）二级文件：管理规定；

（三）三级文件：管理规范、实施细则、操作手册等；

（四）四级文件：运行记录、表单、工单、记录模板等。

第六条　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。

第七条　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。

第八条　体系文件的拟稿

体系文件的拟稿应符合以下要求

（一）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。

（二）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。

（三）文件的文种应当根据行文目的、行文方向、文件内容确定。

（四）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。

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

第九条　体系文件的审核

体系文件在学校领导签发前，应由实训中心主任审核。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：

（一）是否确需行文。

（二）行文方式及级别是否妥当，是否符合行文规则。

（三）是否符合党和国家的方针政策，是否符合国家法律法规。

（四）是否符合体系文件拟制的有关要求。

（五）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。

（六）是否符合体系文件处理程序和体系文件格式规定。

（七）密级的确定是否合乎规定，紧急程度的设定是否合乎情理。

（八）主送、抄送、内部发送范围是否恰当。

（九）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，实训中心主动与主办部门协商，直接退回主办部门修改。

第十条　体系文件的签批

体系文件经核稿后，由实训中心送分管领导签发。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。

第十一条　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。

第十二条　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。

第十三条　体系文件的发送

（一）正式体系文件由院长办公室负责登记后发送。

（二）保密文件的发送应符合保密规定。

第十四条体系文件的管理

（一）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。

（二）公开发布工商外体系文件，必须经学校领导批准。

（三）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。

（四）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。

（五）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。

（六）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。

（七）实训中心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。

第十五条　体系文件的评审与修订

（一）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。

（二）文件修订后应重新提交进行发文流程。

（三）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。

（四）文件的更新应严格遵守规章制度。

第十六条　体系文件的归档

（一）体系文件原件由实训中心相关人员负责归档，个人不得保存应当归档的体系文件。

（二）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。

（三）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。

第十七条　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。

第三章　附则

第十八条　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。

第十九条　本规定自颁布之日起实行。