福州软件职业技术学院

信息安全管理制度

目录

一、安全管理制度

1.1 信息安全总体方针及策略

第 1 章. 总则

第一条 为保障福州软件职业技术学院业务的正常持续运行，保护信息资产的安全，制定了本方针。本方针旨在为福州软件职业技术学院的信息安全管理实践提供清晰的策略方向，阐明信息安全建设和管理的重要原则，为福州软件职业技术学院的信息安全管理工作提供指引与支持，并达到“系统、科学、连贯、主动”的风险驾驭状态。

第二条 除非特别说明，本方针的管理对象包括福州软件职业技术学院拥有、控制、管理和使用的所有硬件、软件、信息、服务、人员和无形资产等信息资产。本方针的适用对象主要包括与以上信息资产相关的福州软件职业技术学院所有部门，以及与福州软件职业技术学院有关的集成商、软件开发商、产品提供商、安全顾问、商业合作伙伴、临时工作人员和其他第三方机构等关联人员。

第 2 章. 信息安全总目标

第三条 福州软件职业技术学院信息安全工作的总体目标是：建立信息系统安全保障体系，运用等级化保护理念，结合福州软件职业技术学院实际、总体规划、短板优先，以保障业务为核心，建立安全策略和制度规范、组织人员完备、技术先进实用、安全管理到位、日常运维高效的信息安全保障体系。

第 3 章. 信息安全管理原则

第四条 福州软件职业技术学院的信息安全管理推行治理、管理与技术并重原则和PDCA(“Plan：规划”—“Do：实施”—“Check：检查”—“Act：处置”)动态循环管理原则。

(一) 治理原则：信息安全管理要符合福州软件职业技术学院的治理原则。在战略层面上,信息安全决策必须由最了解福州软件职业技术学院整体目标与价值的权威部门来决定，使信息安全问题得到最高管理层的关注，并进入福州软件职业技术学院战略层的日常议题；在战术层面上，信息安全实践由国际和国内得到普遍实践与认可的治理标准（如ISO27001 等）来指导。

(二) 管理与技术并重原则：信息安全不是单纯的技术问题，在采用安全技术和产品的同时，重视采取有效的管理措施，不断积累完善针对实际情况的各类安全管理策略、规章制度，全面提高信息安全管理水平，达到成本效益最优目标。

(三) PDCA 动态循环管理原则：对信息与信息系统的建设、运行、维护、废止的全过程进行信息安全管理；在对信息资产的管理上遵循 PDCA 动态循环管理原则，针对福州软件职业技术学院内外部业务环境及技术条件的变化情况，进行周期性的风险评估，根据风险状况及时调整信息安全管理策略和方法。

第 4 章. 总体安全策略

第五条 福州软件职业技术学院的信息系统安全保障体系要按照以下安全策略进行建设和管理：

总体规划、系统工程：要总体规划福州软件职业技术学院的信息系统安全保障体系，采用系统工程的思想和方法对福州软件职业技术学院信息系统安全保障体系进行设计和建设。

政策法规、充分体现：福州软件职业技术学院信息系统安全保障体系的设计与建设必须充分体现国家政策及相关安全规章制度的要求,必须与国家政策和相关法律法规与制度的相关要求相一致，不能违背国家政策的要求。

标准规范、完整适用：安全保障体系的建设必须充分利用成熟的信息安全理论成果，参照国际和国内的安全标准和规范组织实施，具有较高的整体性、适用性和可扩展性。

风险管理、等级保护：福州软件职业技术学院信息系统安全保障体系的设计体现风险管理、等级保护思想。综合平衡安全成本与风险，合理优化信息安全资源配置，实行信息安全等级保护，正确处理安全保密与开放互联之间的关系，做到技术上可实现，组织上可执行。

纵深防御、全面防护：建立纵深防御体系，设计合理的安全防御体系和全面的防护机制。

综合防范、重点防御：按照我国信息安全保障工作“积极防御，综合防范”的基本方针，非涉密信息系统建设要符合《信息安全等级保护管理办法》（公通字（2007）43 号）、《信息系统安全保护等级定级指南》、《信息系统安全保护等级基本要求》和《信息系统安全保护等级实施指南》等文件的要求；坚持管理与技术并重，加强以安全技术为基础的信息保护和网络信任体系建设，建立和完善信息安全监控系统，建立健全信息安全应急处理协调机制。

最高防护、最小特权：按照信息系统所承载信息的最高等级和信息系统的最薄弱环节进行防护，任何实体（用户、管理员、进程、应用和系统等）仅有该主体需要完成其被指定任务所必须的最小特权，此外没有更多的特权。

第 5 章. 标准及符合性要求

第六条 福州软件职业技术学院信息系统安全保障体系过程需符合以下标准：

1. 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）；
2. 《信息系统安全等级保护基本要求》（GB/T 22239-2008）；
3. 《信息安全技术　信息系统安全等级保护定级指南》（GB/T 22240—2008）
4. 《信息系统安全等级保护安全设计技术要求》（GB/T 24856－2009）；
5. 《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）；

第 6 章. 安全教育及培训

第七条 福州软件职业技术学院信息系统安全保障体系建设的过程中，还应关注信息安全教育及培训。应定期对从事操作和维护信息系统的工作人员进行培训，包括：计算机

操作维护培训、应用软件操作培训、信息系统安全培训等，保证只有经过培训的人员才能上岗。

第八条 对于涉及安全设备操作和管理的人员，除进行上述培训外，还应由相应部门进行安全保密专门培训。

第九条 对于安全负责人要进行高级安全培训，并且取得“上岗证书”后方可任职。

第十条 人员上岗后仍需不定期接受安全教育和培训，包括听讲座，观看影片、录象资料，学习信息安全材料等，以此提高员工的信息安全防护意识。

第 7 章. 管理评审

第十一条 信息安全方针及管理制度需要根据经营环境、业务内容和技术状况的变化情况，进行定期评审（一年一次）或不定期评审（系统发生重大安全事故、出现新的安全漏洞，以及技术基础结构和组织结构等发生变更时），并根据实际情况进行修订，以适应当前最新的信息安全需要。

第十二条 信息安全方针及管理制度的变更由网络安全和信息化领导小组、福州软件职业技术学院各部门或员工提出，由网络安全和信息化领导小组进行汇总、分析研讨，并负责起草工作，由网络安全和信息化领导小组审批后发布。

第十三条 福州软件职业技术学院将通过纸质文件或电子文件方式向所有在福州软件职业技术学院工作的人员发布本方针的最新版本及相关信息。

1.2 安全管理制度制定规范

第 1 章. 总则

第一条 为了指导信息安全管理制度的制定、评审、发布、修订、废止与监督落实，建立科学、严谨的信息安全管理规章制度，根据信息安全总方针，结合福州软件职业技术学院实际特制定本规范。

第二条 本规范所述的信息安全管理制度包括为加强信息安全管理而制定的信息安全体系、安全规范、安全管理办法、安全管理指南、安全管理制度、实施细则和操作规程等各类制度文件。

第三条 福州软件职业技术学院网络安全和信息化领导小组、信息安全管理人员是信息安全管理规章制度的责任部门和责任人，负责组织信息安全管理制度的制定、并负责信息安全管理制度的发布、修订、废止与监督落实。

第 2 章. 制度文档制定格式

第四条 制度文件按照统一格式处理。每个版本制度发布时都需要标明版本编号、发布时间、签发人、批准人、使用范围、施行时间等。若制度中含有表格，请将表格单独绘制，或者以附录形式放在文档的后面。

第五条 文档编号需福州软件职业技术学院内唯一，以下提供一种格式，若该格式与单位章不符，以单位章为准。

单位代号-信息安全+文件类型-制度代码+版本号

如：FJNZ-ISO1-ZFZ1.0　信息安全总方针 1.0

- 单位代号：

FJNZ 福州软件职业技术学院

- 信息安全：

ISO1 Information Security　信息安全

01 表示方针政策

02 表示制度体系

03 表示指南手册

04 表示记录表单

- 制度代码+版本号:

ZFZ1.0 Zong Fang Zhen 总方针第 1.0 版本

第 3 章. 制度评审和修订

第六条 制度的发布需要经过论证与审订，必要时应该就制度的细则开展讨论会议，集思广益。正式发布制度需要经过各领导的审批通过，管理层签字或单位盖章，才可以正常发布执行。

第七条 网络安全和信息化领导小组应每年定期对制度进行修订，系统发生重大安全事故，出现新的安全漏洞以及技术基础结构和组织结构等发生变更时应该对安全管理制度进行及时修订，修订后亦需要各有关领导的审批同意，才能正式发布执行。

第八条 当现行规章制度有下列情形之一时，必须及时予以废止：

- 因国家政策或公安部有关规定废止，使该规章制度失去依据的；
- 因已规定的事项已经执行完毕，没有存在必要的；
- 已被新的规章制度所替代的。

第 4 章. 发布

第九条 信息安全管理制度以正式文件的形式发布到内部网站、公告栏及员工手中，需要详细登记文件收发记录。

第十条 信息安全管理制度发布后，信息安全工作小组可组织相关人员参加新的信息安全管理制度培训，详细讲解制度的内容并解答疑问。

二、安全管理机构

2.1 信息安全管理部门和岗位职责

第 1 章. 总则

第一条 为了加强福州软件职业技术学院信息系统安全的领导和管理，促进福州软件职业技术学院信息化工程的应用和发展，保障系统有序、稳定运行，我单位内部建立起自己的信息安全管理组织机构，制定了本制度。

第二条 本制度旨在指导我单位信息安全管理组织机构及其信息安全岗位的管理办法。

第 2 章. 信息安全组织与责任

第三条 网络安全和信息化领导小组是福州软件职业技术学院最高信息安全管理机构，下设网信领导小组办公室，设在现代教育技术中心，由现代教育技术中心负责日常信息安全运维事项。

第四条 网络安全和信息化领导小组由下列人员组成：

组　长：　林　　莺（书记）
　　俞发仁（执行校长）
副组长：王秋宏（副校长）
　　林艺勇（副书记）

小组成员：由福州软件职业技术学院各各学院（系、部），各部（处、室、中心、馆）负责人员组成。

第五条 网络安全和信息化领导小组定期召开会议，对有关信息安全重大问题做出决策。

第六条 信息安全办公室主任由分管学院领导兼任，副主任由党委宣传部、现代教育技术中心、安全保卫处负责人担任。

第七条 网络安全和信息化领导小组及其办公室应：

1. 负责信息安全政策和措施的宣传、贯彻和督促检查，并针对信息安全事件建立完善的响应、调查和报告机制。

2. 负责福州软件职业技术学院信息网络安全政策和措施的宣传、贯彻、督促检查、

整体建设规划、实施、管理和服务等工作。

3. 根据信息网络发展规划和信息安全建设需求，组织起草福州软件职业技术学院网络信息安全建设总体规划和实施方案，并针对信息安全事件建立完善的响应、调查和报告机制。

4. 建立有效的信息安全管理体系，定义信息资产的安全需求，持续进行信息资产的风险评估，建立并完善信息安全保护策略和程序，使福州软件职业技术学院拥有可控的风险管理架构、方法和保障落实机制，确保福州软件职业技术学院在不断变化的信息安全风险环境中，始终能够通过科学的方法和持续的改进来增强福州软件职业技术学院抵抗风险的能力。

5. 审定福州软件职业技术学院网络与信息系统的安全策略及应急预案，决定相应应急预案的启动，负责现场指挥，并组织相关人员排除故障，恢复系统。每年组织对信息安全应急策略和应急预案进行测试和演练。

6. 加强信息安全日常运维管理，保障我单位信息系统安全稳定运行；

7. 提高全体职工的信息安全意识和技能，负责制定管理员和普通职工的信息安全培训计划。

第八条 负责福州软件职业技术学院网站信息发布工作的执行与监督，严格执行国家关于信息网络安全的有关规定和要求，加强对网站信息的保护，防止非法用户对网站的攻击和破坏。

第九条 福州软件职业技术学院全体员工、承包方和第三方人员必须接受必要的信息安全教育与培训，充分理解福州软件职业技术学院制订的信息安全管理规定，明确在保护福州软件职业技术学院信息资产安全过程中所应担当的角色和责任。

第十条 根据“谁主管，谁负责；谁运行，谁负责”的原则，建立信息安全绩效考核体系。对于违反信息安全规定的部门和个人，将按有关规定进行处理。

第 3 章. 人员岗位职责

第十一条 现代教育技术中心设置主任、安全主管、系统管理员、网络管理员、数据库管理员、机房管理员、安全管理员、审计管理员等，该职位均为关键岗位，任职人员需从内部人员中选拔，任职前均需签订关键人员保密协议。

现代教育技术中心主任

现代教育技术中心主任负责全单位信息管理，并使之符合福州软件职业技术学院内部办公、行政工作的要求，其岗位职责如下：

1. 发展信息服务系统，使之达到福州软件职业技术学院的既定标准；
2. 制定现代教育技术中心业务发展规划和年度工作计划，并组织实施；
3. 在已批准的预算控制下管理好本部门；
4. 参加与数字建设有关的会议；
5. 做好现代教育技术中心人员业务考核，提出人员调整、晋升及奖励意见；
6. 安排本部门主要业务人员的发展方向和业务进修，指导他们从事专业的研究；
7. 检查各岗位任务的执行情况，并组织协调；
8. 协调与用户的关系，组织本部门人员做好用户的业务指导与咨询工作；
9. 评估现代教育技术中心各项工作，建立有关的标准及技术，必要时做出适当的修正。

安全主管

现代教育技术中心设立专职安全主管，在现代教育技术中心主任的直接领导下，协助做好信息安全相关工作，其岗位职责如下：

1. 负责福州软件职业技术学院信息安全工作的具体实施和有关信息安全问题的处理，根据信息安全事件的处理情况和对网络系统安全检测的结果，提交事件处理报告；
2. 根据信息系统安全需求，定期提出网络系统安全整改意见，上报信息安全办公室；
3. 定期对信息系统进行信息安全巡检，并在其他管理员的协助下建立完整的安全巡检报告，及时向上级提交报告，汇报信息安全现状；
4. 指导和监督其他管理员和工作人员与安全相关的工作，为信息安全工作的提供建议；
5. 监控信息系统的安全需求变化，及时获取来自其他管理员和工作人员的安全意见，必要时提交安全策略体系修订建议；
6. 负责计算机系统病毒、木马等恶意软件的防治工作；
7. 协助解决信息系统安全突发事件，负责重大事件的上报；
8. 发布信息安全通报及安全预警。

系统管理员

系统管理员确保操作系统、应用软件系统、业务应用系统安全稳定地运行，其岗位职责如下：

1. 随时观察主机系统运行情况，及时排除故障，查明故障原因；
2. 负责调整各主机的运行参数、用户注册、权限管理、作业优先级管理，确保各主机系统内运行效率；
3. 制订系统转贮及恢复方案，监督值班人员正确完成每日的数据备份工作。每月的第一天作一次全转贮，并将备份介质妥善保管；
4. 在所管理操作系统、应用软件系统、业务应用系统上发现可疑的信息安全事故或隐患现象时及时向安全管理员报告，协助安全管理员进行信息安全事故的查处。对于重大的信息安全事故，做好操作系统、应用软件系统、业务应用系统的日志保存工作；
5. 每月或定期向安全管理员提交信息安全事件记录，并对系统记录文件保存存档，以备查阅。

数据库管理员

数据库管理员负责福州软件职业技术学院数据库系统全面管理控制，制定数据库备份计划，灾难出现时对数据库信息进行恢复，其岗位职责如下：

1. 负责主机数据的应用管理，包括表空间、用户的增加、删除及修改等操作；
2. 参与应用系统中的数据结构、存贮、处理及分布等设计方案的讨论与实施，并提出协调建议；
3. 负责解决应用中，遇到的有关主机数据库使用中出现的技术问题；
4. 遇到主机数据库管理出现不能解决或较为严重问题时，负责与数据库厂商技术服务人员联系，并协助处理；
5. 负责主机数据库的性能监测与调整，每三个月至半年做一次数据整理，监测并记录有关现行性能指标，并根据应用对相应参数进行适当调整；
6. 保证主机数据安全，制订转贮计划，对系统值班人员的执行情况进行检查与监督；
7. 建立数据库管理员工作月志，详细记录主机数据库的各种状态及操作过程。

网络管理员

网络管理员负责网络的运行管理，实施网络安全策略和安全运行细则，其岗位职责如下：

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，及时修补网络设备的漏洞；
2. 监控网络关键设备、网络端口、网络物理线路，防范黑客入侵，及时向计算机安全人员通报安全事件；
3. 对负责网络管理功能的操作人员进行安全监督；
4. 协助安全管理员制定网络设备安全配置规则，并落实执行；
5. 为安全管理员提供完整、准确地记录重要网络设备和网站运行活动的运行日志；
6. 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；
7. 编制网络设备的维修、报损、报废等计划，报主管领导审核。

机房管理员

机房管理员其岗位职责如下：

1. 值班员应自觉遵守规章制度，做好防火、防盗、防潮、防尘等机房物理安全工作，确保机房内设备的正常、可靠运行；
2. 严格按照《机房管理制度》规定做好值班工作，值班期间不得擅离岗位；
3. 每天巡视机房一次，检查机房内设备的运行和供电状况；认真填写机房值班及设备运行日记和机房环境条件日志；发现设备运行异常，应立即采取有效措施，并及时上报、做好记录；
4. 爱护机房内设备及设施，严格按照设备操作规程进行操作；
5. 负责对进出机房的外来人员及进出机房的设备进行详细登记，防止丢失设备的情况发生。

安全管理员

机房管理员其岗位职责如下：

1. 贯彻和落实上级及本单位相关管理制度，开展信息安全管理
2. 组织开展信息安全体系建设，组织实施信息安全管理工作，制定和落实安全策略

3. 组织开展信息系统等级保护和安全风险管理工作，开展关键业务系统的应急演练工作
4. 落实防病毒系统等信息安全措施及日常管理工作，实施防火墙、入侵检测、审计等安全专用设备的日常维护和运行管理工作
5. 完成领导交办的其它工作

2.2 授权审批管理

第 1 章. 授权审批管理

第一条 当系统发生变更，进行重要操作，执行物理访问和系统接入时需经过现代教育技术中心或福州软件职业技术学院领导的审批。

根据各个部门和岗位的职责制定授权审批事项，各项授权与审批事项应经过指定的部门和人员进行授权和审批。

要定期对授权与审批事项列表进行修订，及时更新授权和审批的项目、审批部门和审批人等信息。

现代教育技术中心要对审批过程进行记录并保存审批文档。

系统管理员需要对不再适用的权限及时取消授权的记录。

第 2 章. 授权审批列表

系统投入使用

1. 系统安装调试场地应该受控制并由使用部门人员陪同，必须保证与在线运行的应用系统隔离或远离应用系统，避免重大问题的发生；

2. 系统安装调试无误后，使用部门人员填写授权审批表，经部门负责人批准后，报信息系统运行管理部门审批；

3. 审批同意后，系统安装调试人员、使用部门人员协同信息安全主管对系统各项安全情况进行检查。不符合福州软件职业技术学院信息安全要求的责令使用部门调整，直到符合福州软件职业技术学院安全规定才签字批准；

4. 所有审批完成，系统上线执行人员才可以进行系统上线工作。

网络接入

1. 单位内职工需加入福州软件职业技术学院内网，需填写员工入网审批表，经本部门领导审批后，提交现代教育技术中心。

2. 网络管理员应依据经过批准的访问控制策略进行网络访问控制设置和修改；

远程访问控制审批

1. 需要远程访问的人员提交策略的制定、修改应提出申请，填写审批表；

2. 经福州软件职业技术学院领导审批同意后方可按照策略制定、修改有关设备的配置，并要求做好相关的记录。

网络系统接入

1. 各应用系统部门如需要增加设置或修改网络访问控制策略必须经过授权，由需求部门填写审批表，经现代教育技术中心负责人批准后实施；

2. 网络管理员应依据经过批准的访问控制策略进行网络访问控制设置和修改；

3. 只有网络管理员和安全管理员才有权限登录网络设备，发生人员变更后，应及时更改网络设备帐户和口令设置。

重要资源访问

1、访问单位内密级文件、等级保护三级系统、机房等重要资源，需通过资产所有部门的负责人授权，由本部门人员陪同放可访问；

2、在访问过程中，如需带入或带出福州软件职业技术学院资产需在申请书中说明，并由资产所有部门人员监督下执行；

3、资产负责人应对访问时间、人员、过程进行记录。

2.3 审核与检查管理

第 1 章. 总则

第一条 为了督促福州软件职业技术学院网络与信息系统安全管理要求、技术规范良好执行，落实各项网络与信息安全工作，特制定信息安全检查制度。

第二条 本制度的目标是规范福州软件职业技术学院信息安全检查工作的具体过程，明确各相关人员的职责和工作内容，为信息安全检查工作的顺利开展提供有效的指导。

第 2 章. 安全检查概要

第三条 各管理员应定期检查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。

第四条 每次信息安全检查过程与结果都要记录并保存，每次检查后出具安全检查报告，报告中应包括检查事项、检查人员、检查数据汇总表、检查结果等内容。

第五条 对于检查过程中发现的不符合项，管理员形成书面改进意见后，经现代教育技术中心主任审核后，指派专人整改。

第六条 日常检查：机房管理员需每日对机房进行巡检，巡检内容包括但不限于机房内设备运行状态、机房温湿度等，并填写巡检记录表；

第七条 季度检查：各安全管理员需每季度对服务器、网络设备、安全设备进行扫描巡检，巡检内容包括但不限于系统风险评估、漏洞扫描、系统日志分析、数据备份情况等，并出具巡检报告；

第八条 年度巡检：网络安全和信息化领导小组应组织相关人员对福州软件职业技术学院信息系统进行一次全面的安全检查。

第 3 章. 管理规范检查列表

第九条 信息安全相关制度

检查信息安全相关制度的覆盖范围以及制度的适宜程度；信息安全相关制度管理工作的开展情况，包括制度的制定、落实、评审与修订等是否符合规范要求等。

第十条 人员安全管理

岗位设置及人员配备：包括安全相关岗位的设立以及职责的明确/落实、岗位的授权等；内部人员安全管理：包括员工的安全培训及考核、岗位授权管理等；外部组织人员安全管理：包括外部组织访问事前、事中及事后不同阶段的安全控制措施的落实情况等。

第十一条 信息资产管理

资产管理：包括信息资产识别、分类、标识；介质管理：包括介质在使用、传输、保存、清除及销毁等过程中的安全控制落实情况；设备管理：包括各类设备在使用和管理维护过程中的安全控制措施落实情况。

第十二条 系统运维管理

运维管理：包括用户账号情况、系统漏洞情况、系统审计情况；监控、恶意代码防范、变更管理等的落实情况。

第 4 章. 技术规范检查列表

第十三条 物理安全管理

物理环境安全：包括物理区域的电源、防雷、防火、防潮、防静电等周边环境安全控制措施落实情况等； 访问控制：为保护区域内信息不受非授权物理访问，机房及重要办公场所的访问控制措施（如门禁、值守等），以及防盗窃、防破坏措施的实施情况。

第十四条 系统建设安全

系统建设安全：系统建设整个生命周期，包括系统建设设计阶段、实施阶段以及验收阶段中涉及的信息安全控制措施落实情况；

第十五条 应用安全检查

应用系统安全：对于应用系统技术安全控制落实情况的检查 ，包括身份鉴别、访问控制、交易安全、数据安全、密码安全、输入输出合法性、备份恢复、日志及审计等；数据库安全：对于常用数据库（Oracle、SQLServer 等）的安全配置、访问控制、备份恢复、日志及审计情况等进行检查；中间件安全：对于中间件的安全配置、访问控制、备份恢复 、日志及审计情况等进行检查。

第十六条 网络安全检查

网络架构：对网络整体架构的安全情况，包括网络可用性、访问控制、网络管理与审计、网络防护等方面的安全控制情况进行检查；网络设备安全：包括针对网络主要设备（如路由器、交换机等）以及网络中部署的安全设备（防火墙、入侵检测、防病毒系统）等的安全配置、访问控制、备份、日志与审计等进行检查。

第十七条 服务器主机安全检查

主机操作系统的安全性，包括账号安全、系统日志、安全配置等。

第十八条 终端安全检查

终端的安全，包括终端安全配置，补丁安装情况、终端系统以及帐户情况，终端口令策略检查，终端使用安全检查，终端开启服务检查，终端防病毒检查。

三、人员安全管理

3.1 人员录用管理

第 1 章. 人员录用

第一条 福州软件职业技术学院的人员录用依据国家相关的法律和法规来执行。

第二条 福州软件职业技术学院占行政编制的工勤人员（合同工）的录用，依据《福州软件职业技术学院合同工管理办法（试行）》。

第三条 人事外负责人员录用、筛查、审核等相关事宜。

第 2 章. 人员筛选和审查

第四条 根据福州软件职业技术学院的需要确定人员审查内容，包括聘用人员履历的审查、学术和专业资格的核实、身份审查等。

第五条 录用关键工作岗位的工作人员时，应按照其申请表中的个人履历逐一审查，必要时要会见证明人，对履历进行确认。

第六条 对在职人员应进行定期审查，当工作人员婚姻、经济、身体状况等发生大的变化，或被怀疑违反了安全规章制度，或对其可靠性产生怀疑时，都应进行重新审查。

第七条 对于占据重要职权位置的人员，周期性地进行审查。

第 3 章. 签订保密协议

第八条 与福州软件职业技术学院的工作人员（长期或临时）签订工作人员保密协议，明确其对系统应尽的安全保密义务，保证在岗工作期间和离岗后一定时期内，均不得违反保密协议和泄漏系统秘密。保密协议的内容应符合国家有关规定，对违反保密合同的应设有惩处条款。

第九条 应从内部人员中选拔从事关键岗位的人员，并签署关键岗位人员安全协议。

第 4 章. 岗位责任与授权

第十条 根据分权制约和最小特权原则，建立岗位责任制度和授权制度。明确所有人员在系统中的安全职责和权限，职责和权限要文档化，并要求签字确认。所有人员的工作和活动范围应当被限制在完成其任务的最小范围内，关键岗位人员不允许兼职。

3.2 安全培训、考核及惩处

第 1 章. 安全意识教育与培训

第一条 信息安全教育培训计划由现代教育技术中心根据年度工作计划作出安排。

第二条 信息安全主管应负责对福州软件职业技术学院所有使用计算机的人员进行安全意识教育、岗位技能培训和相关安全技术培训工作。

第三条 信息安全人员每年必须参加不少于 15 个课时的专业培训。

第四条 管理层（决策层）的培训要求如下：

（1） 管理层培训目标是明确建立信息安全体系的迫切性和重要性，从而获得单位管理层（决策层）有形的支持和承诺。

（2） 管理层培训方式可以采用聘请外部培训的方式，由专业安全公司的技术专家和咨询顾问以专题讲座、研讨会等形式开展培训。

第五条 信息安全管理员的培训要求如下：

（1） 信息安全管理员培训目标是理解及掌握信息安全原理和相关技术、强化信息安全意识、支撑本单位的信息安全管理体系的建立、实施和维护。

（2）信息安全管理员培训方式可以采用多种形式，包括参与外部的信息安全专业资格认证培训、参加信息安全专业技术培训、自学信息安全管理理论及安全技术、参与单位内部学习研讨等。

第六条 网络和系统管理员的培训要求如下：

（1） 网络和系统管理员培训目标是掌握各种网络设备和系统相关专业安全技术，维护和保障网络和系统的正常、安全运行。

（2） 网络和系统管理员培训方式可以采用外部和内部相结合的培训以及自学的方式。

第七条 单位员工的培训要求如下：

（1） 单位员工培训目标是了解单位相关的信息安全管理制度和技术规范，确保能安全、高效地使用业务和办公系统。

（2） 单位员工培训方式应主要采取内部培训的方式。

第八条 新员工的上岗培训要求如下：

（1） 新员工在正式上岗前，应进行信息安全方面的培训，了解所在岗位要求遵守的信息安全管理制度和技术规范。

（2）新员工上岗培训方式应主要采取内部培训的方式。

第 2 章. 人员考核

第九条 每次培训后，需对培训人员进行当堂考核，对于重要岗位，需考核通过后才能上岗。

第十条 信息系统的维护人员和管理员应定期参与安全技术教育培训（每年至少一次），明确如何安全使用有关系统，包括各业务系统、主机操作系统、办公系统、电子邮件系统、内部网站以及普通计算机周边硬件设备。

第十一条 安全管理员、网络管理员和系统管理员应定期参与由供应商或厂家提供的专业安全技术培训，了解和掌握信息系统安装、配置及维护的正确方法和技能。

第十二条 单位应根据实际情况，挑选合适的信息安全管理及安全技术人员进行相关的认证考试培训，并参加认证考试，以提高安全管理人员对信息安全的管理理论和技术的水平。

第 3 章. 职责与惩戒

第十三条 福州软件职业技术学院内员工应严格遵守《信息安全管理部门和岗位职责》及其他相关规定履行各自的职责。

第十四条 违反本规定有下列行为之一者，由现代教育技术中心以口头警告、撤销当事人上网资格、停机或经济处罚，严重者提交福州软件职业技术学院处理，直至追究法律责任。

（1）违反信息安全管理制度，危害网络系统安全；

（2）接到网络中心人员要求改进安全状况通知后，拒不整改；

（3）擅自安装或拆卸、硬件设备；

（4）删改网络系统设置、篡改数据；

（5）私自运行非本网络提供的软件、游戏软件，或造成病毒感染、传播；

（6）进行与本职工作无关的操作；

（7）向单位外人员泄露数据信息、资料、程序、数据、口令密码；

（8）非法进入网络系统，恶意攻击或破坏网络系统的行为；

(9) 网络系统设施附近作业而危害网络系统安全，影响网络正常运行造成经济损失的，由作业单位赔偿；造成福州软件职业技术学院财产重大损失的，依法追究和承担法律责任。

（10）在主机房、维护工作区、仓库等地吸烟及陪同者；

福州软件职业技术学院各类人员有失职行为而造成后果的，由现代教育技术中心书面通知福州软件职业技术学院人事外和财务外给予经济处罚或书面通知人事外给予行政处分。

第十五条 对严格执行我单位计算机网络的各项管理规定，取得突出成绩的单位和个人，除了给予福州软件职业技术学院周会通报表扬外，还将增加部门相应的综合考评管理分，年终评比先进部门和个人及晋级晋职时，给予优先考虑，同时酌情给予适当经济奖励。

3.3 人员离岗规定

第一条 对调离人员，特别是因不适合安全管理要求被调离的人员，必须严格办理调离手续，进行调离谈话、承诺其调离后的保密义务，交回所有钥匙及证件，

退还全部技术手册、软件及有关资料，更换系统口令和机要锁。涉及福州软件职业技术学院业务核心技术的信息安全人员调离单位，必须进行离岗审计，方可调离。

第二条 立即终止由于各种原因即将离岗的员工的所有访问权限；取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备,并填写存档离岗人员安全处理记录；经机构人事部门办理严格的调离手续，承诺调离后的保密义务并签署离岗人员保密承诺书后方可离开

3.4 第三方人员管理

第 1 章. 总则

第一条 为了有效防范外部人员（非福州软件职业技术学院员工）进出重要区域所带来的安全风险，加强规范福州软件职业技术学院对外部人员的安全管理，提供外部人员访问重要区域所要遵守的行为准则，保证信息系统及网络的安全，制定了本规范。

第二条 本规范中的重要区域特指中心机房、重要服务器及设备区等区域。

第 2 章. 外部人员访问

第三条 外部人员包括软件开发商、硬件供应商、系统集成商、设备维护商和服务提供商，以及实习生和临时工作人员。

第四条 应对外部人员的物理访问和逻辑访问实施访问控制，根据其在系统中完成工作的时间、性质、范围、内容等方面的需要给予最低授权。

第五条 外部人员的现场或远程维护工作内容应在合同中明确规定，外部人员访问重要区域涉及机密或秘密信息内容，应要求其签署外来人员信息安全保密协议。

第六条 外部人员进入重要区域要填写进入机房申请表,经过了领导审批后由专人陪同才可以进行访问。值班人员需维护相关进出记录，并告知外部人员相关的安全注意事项。

第七条 外部人员接入单位受控网络访问系统前需要先填写申请表，在领导审批后由专人全程陪同才可接入网络访问。值班人员需将外部人员接入网络访问进行记录。

第八条 外部人员工作结束后，应及时清除有关账户、过程记录等信息。

第九条 需要接触涉密资料的外部服务人员需要签订保密协议，承诺遵守本单位制定的安全管理制度和规范，对于违反保密协议的外部服务人员，本单位将依法追究本人以及所属公司法律责任。外部服务人员如在保密期限内离开所属公司，所签署的保密协议依然有效。

四、系统建设管理

4.1 工程实施管理

第 1 章. 总体要求

第一条 一个项目的生命周期包括：项目申报、项目审批和立项、项目实施、项目验收和投产；从项目建设的角度来看，这些生命周期的阶段则包括以下子阶段：需求分析、总体方案设计、概要设计、详细设计、系统实施、系统测试和试运行，如下表所示：

项目管理生命周期	
项目申报	需求分析 总体方案设计
项目审批和立项	
项目实施	概要设计、详细设计、系统实施
项目验收和投产	系统测试、试运行和投产

项目建设安全管理的目标就是保证整个项目管理和建设过程中系统的安全。

第二条 项目安全管理工作应强化责任机制、规范管理程序，在项目的申报、审批、立项、实施、验收等关键环节中，必须依照规定的职能行使职权，并在规定的时限内完成各个环节的安全管理行为，否则应承担相应的行政责任。

第 2 章. 项目申报安全管理

第三条 项目申报阶段应对信息化项目及其建设的各个环节进行统一的安全管理规划，确定项目的安全需求、安全目标、安全建设方案，以及生命周期各阶段的安全需求、安全目标、安全管理措施。

第一节 系统定级

第四条 依据国家信息系统安全等级保护定级指南（GBT 22240-2008）对项目中的系统进行定级，明确信息系统的边界和安全保护等级；

第五条 以书面的形式说明确定信息系统为某个安全保护等级的方法和理由，形成信息系统定级报告；

第六条 组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定，上报上级主管单位和安全监控单位进行审定；

第七条 信息系统的定级结果向本地公安机关进行备案。

第二节 挖掘安全需求

第八条 应进行系统的安全性需求分析，应至少包括以下信息安全方面的内容：

1. 安全威胁分析报告：应分析待建计算机系统在生命周期的各个阶段中可能遭受的自然威胁或者人为威胁（故意或无意），具体包括威胁列表、威胁可能性分析、威胁严重性分析等；
2. 系统脆弱性分析报告：包括对系统造成问题的脆弱性的定性或定量的描述，这些问题是被攻击的可能性、被攻击成功的可能性；
3. 影响分析报告：描述威胁利用系统脆弱性可能导致不良影响。影响可能是有形的，例如资金的损失或收益的减少，或可能是无形的，例如声誉和信誉的损失；
4. 风险分析报告：安全风险分析的目的在于识别出一个给定环境中涉及到对某一系统有依赖关系的安全风险。它取决于上面的威胁分析、脆弱性分析和影响分析，应提供风险清单以及风险优先级列表；
5. 系统安全需求报告：针对安全风险，应提出安全需求，对于每个不可接受的安全风险，都至少有一个安全需求与其对应。

第三节 安全方案设计

第九条 根据系统的安全保护等级选择基本安全措施，设计安全标准必须达到等级保护相关等级的基本要求，并依据风险分析的结果进行补充和调整必要的安全措施；

第十条 指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

第十一条 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；

第十二条 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；

第十三条 根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

第 3 章. 方案论证与审批安全管理

第十四条 本阶段主要是项目审批单位对项目申报内容进行审批，对项目进行安全性论证，必要时可以聘请外单位的专家参与论证工作。

第十五条 安全性论证应着重对项目的安全需求分析、安全对策以及总体安全方案进行成本效益、合理性、可行性和有效性分析，并给出明确的结论。

第 4 章. 实施方案和实施过程安全管理

第一节 实施方案设计

第十六条 详细设计中应提出相应的具体安全方案，标明实现的安全功能，并应检查其技术原理；

第十七条 对系统层面上的和模块层面上的安全设计进行审查；

第十八条 完成安全测试和评估要求（通常包括完整的系统的、软件的、硬件的安全测试方案，至少是相关测试程序的一个草案）；

第十九条 确认各模块的设计，以及模块间的接口设计能满足系统层面的安全要求。

第二节 产品采购

第二十条 信息产品的采购必须由综合管理科进行统一采购；

第二十一条 网络安全设备选型应根据国家或公安部有关规定选择经过国家有关权威部门的测评或认证的产品；

第二十二条 所有安全设备购回后均需进行严格检测，凡购回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交付使用；

第二十三条 通过上述测试后，设备才能进入试运行阶段。试运行时间的长短可根据需要自行确定。通过试运行的设备，才能投入生产系统，正式运行。

第三节 软件开发或外包

第二十四条 现代教育技术中心需对软件进行质量审核；并确保开发商提供相关的设计文档及使用指南，必要时应要求开发商进行培训。

第二十五条 在软件安装之前进行恶意代码测试；对于重要的项目建设，需要求开发商提供源代码并进行代码审核检查是否存在后门。

第四节 信息技术产品选型

第二十六条 对项目实施所需的计算机及配套设备、网络设备、重要机具（如 ATM）、 计算机软件产品的购置，计算机应用系统的合作开发或者外包开发的确定，按现有制度中的相关规定执行；

第二十七条 安全专用产品应具有国家职能部分颁发的信息安全专用产品的销售许可证；

第二十八条 密码产品符合国家密码主管部门的要求，来源于国家主管部门批准的密码研制单位；

第二十九条 关键安全专用产品应获得国家相关安全认证，在选型中根据实际需要制定安全产品选型的标准；

第三十条 关键信息技术产品的安全功能模块应获得国家相关安全认证，在选型中根据实际需要制定信息技术产品选型的标准；

第三十一条 所有安全设备购回后均需进行严格检测，凡购回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交付使用；

第三十二条 通过上述测试后，设备才能进入试运行阶段。试运行时间的长短可根据需要自行确定。通过试运行的设备，才能投入生产系统，正式运行。

第五节 产品和服务供应商选择

第三十三条 系统集成商的资质要求：至少要拥有国家权威部门认可的系统一级集成资质，对于较为重要的系统应有更高级别的集成资质；

第三十四条 安全服务商资质：至少应具有国家一级安全服务资质，对于较为重要的系统应有更高级别的安全服务资质；

第三十五条 人员资质要求：系统集成人员、安全服务人员以及相关管理人员应获得国家权威部门颁发的信息安全人员资质认证；

第三十六条 其它要求：系统符合国家相关法律、法规，按照相关主管部门的技术管理规定对非法信息和恶意代码进行有效控制，按照有关规定对设备进行控制，使之不被作为非法攻击的跳板。

第三十七条 基本建设工程项目实施过程所签订的全部合同都必须按国家合同发的规定的条款进行签订。

第六节 工程质量管理和监督

第三十八条 工程质量管理在政府监督、法人管理、社会监理、企业自检的四级质量保证体系下，确定工程质量终生负责制。项目负责人对工程在设计使用年限内任何质量缺陷负全责。从分项工程到分部工程进行严格质量管理，做好各种标准性试验，以试验指导施工，保质保量，按期完成各项工程任务；

第三十九条 工程监督由工程管理领导小组负责，监督工程质量，督促工程按计划实施。对于延误工期计划、质量存在隐患、成本失控的项目部要及时进行整改，施工项目部必须及时落实整改意见，按要求采取补救措施，确保工程保质保量，按计划实施。对于不能确保工程目标的实现又不能落实整改措施的项目部，工程管理领导小组将及时撤换主要负责人及相关人员，视情节按福州软件职业技术学院有关制度进行处罚。

第 5 章. 验收与投产安全管理

第一节 安全测试

第四十条 应制定投产与验收测试大纲，在项目实施完成后，由项目应用主管单位和项目开发承担单位共同组织进行测试。在测试大纲中应至少包括以下安全性测试和评估要求：

1. 配置管理：系统开发单位应使用配置管理系统，并提供配置管理文档；
2. 安装、生成和启动程序：应制定安装、生成和启动程序，并保证最终产生了安全的配置；
3. 安全功能测试：对系统的安全功能进行测试，以保证其符合详细设计并对详细设计进行检查，保证其符合概要设计以及总体安全方案；
4. 系统管理员指南：应提供如何安全地管理系统和如何高效地利用系统安全功能的优点和保护功能等详细准确的信息；
5. 系统用户指南：必须包含两方面的内容：首先，它必须解释那些用户可见的安全功能的用途以及如何使用它们，这样用户可以持续有效地保护他们的信息；其次，它必须解释在维护系统的安全时用户所能起的作用；
6. 安全功能强度评估：功能强度分析应说明以概率或排列机制（如，口令字或哈希函数）实现的系统安全功能。例如，对口令机制的功能强度分析可以通过说明口令空间是否有足够大来指出口令字功能是否满足强度要求；
7. 脆弱性分析：应分析所采取的安全对策的完备性（安全对策是否可以满足所有的安全需求）以及安全对策之间的依赖关系。通常可以使用穿透性测试来评估上述内容，以判断它们在实际应用中是否会被利用来削弱系统的安全。

第四十一条 测试完成后，项目测试小组应提交《测试报告》，其中应包括安全性测试和评估的结果。不能通过安全性测试评估的，由测试小组及第三方测试单位综合提出修改意见，项目开发承担单位应作进一步修改。

第二节 验收测试

第四十二条 验收阶段项目开发承担单位应制定详细的测试验收方案，并对测试结果进行详细的记录，形成测试验收报告。

第四十三条 验收阶段需委托第三方测试单位对系统进行安全性测试，并出具报告，保证系统的安全性。

第四十四条 系统安全试运行半年后，项目应用主管单位可以组织由项目开发承担单位和科技部门人员参加的项目验收组对项目进行验收。验收应增加以下安全内容：

1. 项目是否已达到项目任务书中制定的总体安全目标和安全指标，实现全部安全功能；
2. 采用技术是否符合国家、海关总署有关安全技术标准及规范；
3. 是否实现验收测评的安全技术指标；
4. 项目建设过程中的各种文档资料是否规范、齐全；
5. 在验收报告中也应在以下条目中反映对系统安全性验收的情况：
6. 项目设计总体安全目标及主要内容；
7. 项目采用的关键安全技术；
8. 验收专家组中的安全专家及安全验收评价意见。

第三节 系统交付

第四十五条 系统建设完成后，项目承建方要依据项目合同的交付部分向应用主管部门进行项目交付，但交付的内容至少包括：

1. 制定的系统交付清单，对交付的设备、软件和文档进行清点；
2. 对系统运维人员进行技能培训，要求系统运维人员能进行日常的维护；
3. 提供系统建设的过程文档，包括实施方案、实施记录等；
4. 提供系统运行维护的帮助和操作手册。

4.2 产品采购

第 1 章. 采购原则及分工

第一条 设备采购原则

1. 设备采购小组应根据福州软件职业技术学院的总体发展规划和行业的技术发展趋势，结合福州软件职业技术学院实际运营状况、作业能力，有计划地实施设备采购工作；

2. 采购的设备应与福州软件职业技术学院的发展相适应,满足过程能力的要求，真正发挥投资的经济效益；

3. 设备的性能应体现和保持行业先进水平，以延长设备的技术寿命。禁止选用国家明令淘汰的设备，同时注意结合福州软件职业技术学院的实际需要，不追求脱离实际需求的技术先进；

4. 采购的信息安全产品（边界安全设备、重要服务器操作系统、数据库等）具有国家销售许可；同时，应确保密码产品采购和使用符合国家密码主管部门的要求；

5. 将“质量第一”和“经济合理”结合起来，坚持“比质比价”和“寿命周期费用最经济”的原则。经济效益好的设备不仅应安全、耐用、可靠，而且价格应合理，并且在使用过程中能耗低、维护费用低；

6. 采购小组需要对供应商产品的质量、价格、交货期、售后服务四个因素进行综合考虑，要货比三家、择优采购。

第二条 设备采购的职责划分

为进一步做好设备采购工作，福州软件职业技术学院特成立设备采购小组，采购小组由设备使用部门、设备科、现代教育技术中心、财务处及其他相关部门人员组成。

1. 小组负责人

指定现代教育技术中心领导为信息设备采购小组的负责人，根据本单位的长期经营计划制订现阶段的设备投资计划，并对采购小组的工作进行总体指挥和协调。

2. 设备使用部门

设备使用部门负责人参与设备添置或更新改造的技术经济可行性论证，向设备科采购主管提出设备更新计划，并参与新设备到位后的安装调试工作。

3. 现代教育技术中心

采购前期信息处负责参与前期的设备技术经济可行性评测、提出大众设备采购申请计划及选型建议、与供应商进行设备的技术谈判等。

采购后期，信息处负责新设备的安装布置，制定设备使用的操作规程，并在设备到位后进行安装调试，对使用设备的人员进行培训等。

4. 设备科

采购前期，设备科负责参与论证设备的技术经济可行性、编制设备采购规划、组织采购招标、谈判和签署采购合同、监督供应商对合同的执行进程，以及设备验收入库、保管和移交等。

采购后期，设备科负责参与新设备的安装、调试，并处理有关设备质量、人员培训等需要与供应商联络的事宜，同时完成供应商评价工作。

5. 财务外

财务外负责参与经济可行性论证、审核采购预算、筹措采购资金、参与设备价格谈判、核算和报销采购过程中实际发生的各项费用等。

第 2 章. 政府采购目录

第三条 使用部门根据业务需要每年底提交下年度需求计划报现代教育技术中心，申请表经科主任审批；分管领导审批；提交年度预算会议审议。

第四条 非年度预算增补项目申请流程：申请表经科主任审批；分管领导审批；按财务外有关规定审议；分管设备领导审批。

第五条 现代教育技术中心按月收集整理分析，结合年度预算和资源合理配置要求，提出经济、技术性论证报告决定是否配备的初步意见。定时汇总采购需求，报相关部门立项审核报批。

第六条 达到省级政府招标目录规定的标准的，由省政府采购办组织招标采购。具体规程如下：

a) 审核批准后，协议定点采购的项目的采购计划和招标委托书直报省采购中心办理。非定点协议采购项目的采购计划报省财政厅办理采购计划批复手续，批复后再与省招标采购中心办理招标委托手续，同时提交采购

需求包括技术、服务参数。

b） 根据省采购中心或招标代理机构发出的中标通知书及时与供应商签订销售合同。

第七条 未达到省级政府招标目录规定的标准的，委托招标代理机构或由福州软件职业技术学院采购小组组织招标采购。委托招标代理机构招标的由代理机构按法定流程执行，福州软件职业技术学院采购小组组织招标采购的具体规程如下：

a） 根据立项审核结果汇总分类，提出具体参数要求，在福州软件职业技术学院内招标公告栏

或福州软件职业技术学院网站上发布招标公告，时间五天以上。

b） 在规定时间、地点，投标人送达投标文件。

c） 现代教育技术中心，财务，审计，分管领导组成采购小组集体评标、议标、定标。

d) 现代教育技术中心根据定标结果与中标人签订供货合同,实施具体采购验货手续。

第八条 根据采购合同督促供方履行，及时验货、安装调试、投入使用。

第 3 章. 非政府采购目录

第九条 非政府采购目录的非专用配件采购，原则上应采用询价方式或竞争性谈判方式选定采购，且采购范围需在候选产品名单中，该名单中的厂商设备均需符合国家保密等相关规定。

第十条 现代教育技术中心根据部门采购需求或维修需要，进行技术诊断，市场调查。

第十一条 确定采购计划，并拟定谈判程序，审定标准，报分管领导批准。

第十二条 一次采购数量较大，预算金额超过 5 万。由福州软件职业技术学院采购小组组织招标采购。具体规程如下：

a） 根据采购计划情况张贴采购招标公告或经初审后邀请三家以上的供应商，按需求要求（技术参数，服务承诺）进行投标报价（密封）。

b） 由现代教育技术中心，财务，审计，分管领导组成的商务谈判小组进行开标评标或竞价谈判，审定推荐供应单位。

第十三条 品种单一，金额小的非专用维修配件可按询价方式比价，现代教育技术中心应书面填写询价采购确认单，由财务，审计等部门确认。

第十四条 专用设备的专门维修，经分管领导集体认定后签订定点维修协议。

第十五条 与供应商签订合同。

第十六条 现代教育技术中心应按合同要求组织采购并验货。

第 4 章. 设备选型与评价

第十七条 设备选型应考核的因素

选择设备应在确保技术上先进、经济上合理、生产上实用的基础上，综合考虑下列因素，以做好设备的技术效益、投资效益评价。

1. 设备的规格、功能、精度、效率等；
2. 设备的能源消耗情况、安全性能、环保性能、维修状况等；
3. 供应商的资质、产品质量、产品价格、交货期、售后服务及付款方式等；
4. 选购设备应符合国家保密协议相关规定。

第十八条 设备选型调查工作的实施

1. 调查时，应选择多家设备供应商，通过对比确定最佳方案，例如通过测试来检验设备供应商的产品适用性、可靠性；
2. 调查结束后，调查人员应如实填写可行性论证，并定期维护候选产品名单；

第 5 章. 测试验收

第十九条 设备到货验收

设备到现场 8 小时内，设备采购科应会同设备使用部门、现代教育技术中心共同做好开箱检查、现场清点工作。

第二十条 开箱检查的步骤及内容

1. 检查外观及包装情况；
2. 按照装箱单清点零件、部件、工具、附件、备品、说明书和其他技术资料是否齐全，有无缺损；
3. 检查设备有无锈蚀；

4. 核对实物是否符合图纸要求；

5. 开箱检查过程中做好检查记录。

第二十一条 进口设备的接运与验收

1. 进口设备到货前，采购小组应制定详细的接运方案，办理通关手续，做好接运工作；

2. 进口设备的开箱验收应按照国家海关及商检法律、法规，在规定期限内同商检部门共同验收。发现问题需向外商索赔的，采购小组应负责在合同规定的索赔期限和保证期限内办理检验、索赔工作。

第二十二条 及时处理未按合同执行的交货事宜

采购小组应及时处理未按合同执行的交货事宜，遇到由于供应商交货与合同规定不符，例如设备质量未达到要求、数量不足、未在规定期限内交货等，设备供应商应承担违约责任。

第二十三条 收集开箱资料

设备验收后，所有的供应商装箱资料（装箱清单、合格证、安装图纸、出厂证明文件等）等原始技术资料由设备科档案室负责保管。

第二十四条 质量问题的解决

1. 设备采购到位后,经安装调试发现不能满足福州软件职业技术学院的业务技术要求，或者设备本身不具有先进性、高效性，则由设备采购人员负责与设备供应商联系对设备进行更换或改进，直到达到合同约定的要求为止；

2. 如果质量问题长期得不到有效解决,设备采购人员应负责向供应商提出索赔。

4.3 自行软件开发管理

第一条 应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；

第二条 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

第三条 应制定代码编写安全规范，要求开发人员参照规范编写代码；

第四条 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；

第五条 应确保对程序资源库的修改、更新、发布进行授权和批准。

4.4 软件外包开发管理

第 1 章. 总则

第一条 为规范福州软件职业技术学院外包软件的管理工作，特制定本制度。

第二条 本制度中软件开发指新系统开发和现有系统重大改造。

第三条 本制度中外包开发是指将 IT 应用项目的设计、开发、集成、培训等任务承包给某家专业单位（可以是专业的单位或咨询单位等），由该单位（承包商）负责应用项目的实施。

第四条 软件开发遵循项目管理和软件工程的基本原则。项目管理涉及立项管理、项目计划和监控、配置管理、合作开发管理和结项管理。软件工程涉及需求管理、系统设计、系统实现、系统测试、试运行、系统验收、系统上线和数据迁移。

第 2 章. 立项管理

第五条 提出开发需求的现代教育技术中心参与立项，进行立项的技术可行性分析，编写《立项分析报告》，开展前期筹备工作，《立项分析报告》应明确项目的范围和边界。

第六条 应用系统主要使用部门将《立项分析报告》上交福州软件职业技术学院领导处进行立项审批，以保证系统项目与福州软件职业技术学院整体策略相一致。

第七条 《立项分析报告》得到批准后，成立外包商项目组，该项目组应包括业务组（由福州软件职业技术学院相关业务部门组成）和 IT 组（外包商成员）。福州软件职业技术学院委派一名员工负责监督项目的进度，进行项目管理工作，确保开发能及时完成并能满足业务需要。项目组人员的选择应满足项目对业务及技术要求，项目组人员应有足够的业务和 IT 技术方面的专业知识来胜任项目各方面的工作。

第 3 章. 需求分析

第八条 立项后，业务组对本次立项需求进行汇总整理，出具《业务需求说明书》，并确保《业务需求说明书》中包含了所有的业务需求。经系统使用部门审批确认，

作为 IT 组开发的需求基线。 若业务需求发生变更时，业务组应提交《需求变更申请》 。

第九条 需求分析过程中，项目经理组织制定详细的《项目计划书》，包括具体任务描述和项目进度表等。当项目计划需要变更时，项目经理填写《项目计划变更说明》并提福州软件职业技术学院领导审批，通过审批后交给业务组组长和 IT 组组长执行。

第 4 章. 系统设计

第十条 系统设计应分为概要设计和详细设计，系统设计要遵循完备性、一致性、扩展性、可靠性、安全性、可维护性等原则。

第十一条 在系统设计阶段中，用户应充分参与，确保系统设计能满足系统需求。

第十二条 项目组进行详细设计，出具《设计说明书》和《单元测试用例》。《设计说明书》中需要定义系统输入输出说明和接口设计说明。现代教育技术中心组织相关人员对概要设计进行评审，出具《设计评审报告》。业务组组长和 IT 组组长应参加此评审并对评审意见签字确认。

第十三条 对系统设计的修改的文档须由文档管理人员进行归档管理。

第 5 章. 系统测试

第十四条 福州软件职业技术学院需对上线前系统进行测试，在测试大纲中应至少包括以下安全性测试和评估要求，测试完成后应出具《测试报告》：

8. 配置管理：系统开发单位应使用配置管理系统，并提供配置管理文档；
9. 安装、生成和启动程序：应制定安装、生成和启动程序，并保证最终产生了安全的配置；
10. 安全测试：对系统进行源代码测试，以保证代码中无后门；对系统进行恶意代码扫描，以保证无恶意代码遗留。
11. 安全功能测试：对系统的安全功能进行测试，以保证其符合详细设计并对详细设计进行检查，保证其符合概要设计以及总体安全方案；
12. 系统管理员指南：应提供如何安全地管理系统和如何高效地利用系统安全

功能的优点和保护功能等详细准确的信息；

13. 系统用户指南：必须包含两方面的内容：首先，它必须解释那些用户可见的安全功能的用途以及如何使用它们，这样用户可以持续有效地保护他们的信息；其次，它必须解释在维护系统的安全时用户所能起的作用；
14. 安全功能强度评估：功能强度分析应说明以概率或排列机制（如，口令字或哈希函数）实现的系统安全功能。例如，对口令机制的功能强度分析可以通过说明口令空间是否有足够大来指出口令字功能是否满足强度要求；
15. 脆弱性分析：应分析所采取的安全对策的完备性（安全对策是否可以满足所有的安全需求）以及安全对策之间的依赖关系。通常可以使用穿透性测试来评估上述内容，以判断它们在实际应用中是否会被利用来削弱系统的安全。

第十五条 测试人员不可与开发人员相同；测试数据不应经过挑选，测试数据和测试结果需受到控制。

第 6 章. 试运行

第十六条 系统主要使用部门根据项目规模及影响决定试运行策略。

第十七条 项目组制定《试运行计划》，并制定试运行指标，上报主管领导审批。《试运行计划》中应包含问题应付机制，明确问题沟通渠道和职责分工。

第十八条 在试运行阶段，试运行单位应对我单位相关人员进行培训，用户培训的完成度应作为后期评估的指标之一。

第十九条 项目组根据《试运行计划》进行系统转换和数据迁移。系统转换前，检查系统环境，确保运行环境能满足新应用系统的需要。系统转换时必须详细记录原系统中的重要参数、设置等系统信息，并填写试运行报告相关内容。系统参数、设置的转换工作作为系统上线的验收的评估指标之一。

第二十条 数据迁移前，应制定详细的《数据迁移计划》，《数据迁移计划》中应包含迁移方案、测试方案、数据定义，新旧数据对照表、迁移时间、回退计划等信息。数据迁移计划需经项目经理和主管领导签字审批。

第二十一条 数据迁移后，项目组对数据迁移的完整性和准确性作出检查，出具《数据迁移报告》，其中包括数据来源、转换前状态、转换后状态，数据迁移负责人、

对完整性检查情况、对准确性检查情况等内容。各相关部门验收转换结果后在该报告上签字确认。

第二十二条 系统转换和数据迁移由试运行单位业务部门和福州软件职业技术学院内主管领导共同监督并进行验收。

第二十三条 系统转换和数据迁移验收通过后，正式启动试运行。在试运行过程中，试运行单位把系统运行情况（系统资源使用，反应速度等）记录到试运行报告中。必要时，项目组应根据系统运行情况对应用系统进行优化。

第二十四条 试运行达到试运行计划规定的终止条件时，项目组编写《试运行报告》。此报告应由项目组和试运行单位签字确认，并提交福州软件职业技术学院主管领导审阅。福州软件职业技术学院主管领导审阅试运行结果，决定试运行结束或延期。

第 7 章. 系统验收

第二十五条 系统主要使用部门及现代教育技术中心联合组成独立系统验收小组，从功能需求及技术需求层面对系统进行综合评估。

第二十六条 验收小组应根据验收情况整理形成《系统验收报告》提交系统主要使用部门和现代教育技术中心审阅。

第二十七条 系统主要使用部门和现代教育技术中心负责人根据系统测试、试运行情况签署验收意见。

第 8 章. 系统上线

第二十八条 系统上线应遵循稳妥、可控、安全的原则。

第二十九条 通常情况下，系统上线包含数据迁移工作。

第三十条 项目组制定《系统上线计划》，上报主管领导审批。在上线计划得到批准后才能开始部署上线工作，《系统上线计划》内容应包括但不限于：

1、部署方式和资源分配（包括人力资源及服务器资源）；

2、上线工作时间表；

3、上线操作步骤以及问题处理步骤；

4、项目阶段性里程碑和成果汇报（项目执行状态的审阅、进度安排等）；

5、数据迁移的需求和实施计划；

6、完整可行的应急预案和回退计划；

7、用户培训计划（包括：培训计划、培训手册、培训考核等）；

8、福州软件职业技术学院下发的系统标准参数配置。

上线部门在上线初期需加强日常运行状态监控，出现问题时应及时处理，对重大问题应启动紧急预案。

第三十一条 系统上线前，对开发单位提供软件源代码需要检测软件是否存在恶意代码，并且留存检测报告。

4.5 应用系统开发安全管理

第 1 章　总则

第一条 制度目标：为了加强信息安全保障能力，建立健全的安全管理体系，提高整体的网络与信息安全水平，保证网络通信畅通和业务系统的正常运营，提高网络服务质量，在安全体系框架下，本制度旨在提高 IT 项目信息安全建设质量，加强 IT 项目建设安全管理工作。

第二条 适用范围：本制度适用于所有 TCP/IP 网络 IT 建设项目，主要用于 IT 项目立项过程中方案设计、规划的安全要求参考。

第三条 使用人员及角色职责：本制度适用于全体人员。

第四条 制度相关性：本制度与项目立项及建设等管理制度相关，以《福州软件职业技术学院安全管理制度汇编——项目及信息系统建设管理制度》为主导，以各安全技术规范作为评测标准的参考。

第 2 章　应用系统的安全要求

第五条 为了规避应用系统中的用户数据丢失、修改和误用，应用系统应设计有适当的控制措施、审计跟踪记录或活动日志。

第六条 针对用以处理敏感、脆弱或关键资产的系统，或者对此类资产有　影响的系统，还应根据风险评估的结果确定安全要求，并采取额外的控制措施。

第七条 为了保证系统的安全性，必须在开发过程中对输入到应用系统中的数据进行严格的检查，以确保其正确性及适用性，避免无效数据对系统造成危害。

第八条 对输入数据的验证一般通过应用系统本身来实现，并应在系统开发中实现输入数据验证功能。

第九条 系统应采取有效的验证检查措施来检测故意破坏数据的行为，并在应用系统设计时引入数据处理控制，尽可能地减小破坏数据完整性的几率。可以采用的控制措施如下：

（一） 应用系统不应在程序或进程中固化帐户和口令；

（二） 系统应具备对口令猜测的防范机制和监控手段；

（三） 避免应用程序以错误的顺序运行，或者防止出现故障时后续程序以不正常的流程运行；

（四） 采用正确的故障恢复程序，确保正确处理数据；

（五） 采取会话控制或批次控制，确保更新前后数据文件的一致性；

（六） 检查执行操作前后对象的差额是否正常；

（七） 严格验证系统生成的数据；

（八） 检查文件与记录是否被篡改。例如通过计算哈希值（HASH）进行对比。

第十条 应用系统的输出数据应当被验证，以确保数据处理的正确性与合理性。

第十一条 应用系统正式上线前，需要对其数据库系统、主机操作系统、中间件进行安全加固，并在主管负责人批准后方可上线运营。

第 3 章 系统文件的安全

第十二条 为了最大限度地降低操作系统遭受破坏的风险，应考虑采取如下控制措施：

（一） 程序运行库（operational program libaries）的升级只能由指定的程序库管理员在获取授权后予以完成；

（二） 操作系统应尽可能只保留应用程序的可执行代码；

（三） 在系统测试、用户验收结束之前，及相应的程序源代码库升级之前，可执行代码不得在操作系统中运行；

（四） 程序运行库的所有更新记录都应当予以保留；

（五） 历史版本的软件应当予以保留，用作应急措施。

第十三条 应对系统测试数据加以保护和控制，并避免使用含有个人隐私或敏感信息的数据去测试系统，确保测试数据的普遍性。

第十四条 为降低系统程序遭受破坏的可能性，应严格控制对系统源代码的访问，具体控制措施如：

（一） 源代码尽量不要保留在操作系统内；

（二） 为每个系统指定程序库管理员；

（三） 控制系统支持人员对程序源代码库的访问；

（四） 处于开发和测试阶段的程序不得保留于程序源代码库中；

（五） 程序源代码库的更新及发布只能由指定的程序库管理员在经过该应用的主管领导授权后实施；

（六） 程序清单应当保存在安全环境中；

（七） 对程序源代码库的所有访问都应保留审计日志；

（八） 老版本的源程序应当归档，并清楚记录其被正式使用的确切日期和具体时间，及所有相关的支持软件、功能说明、数据定义和程序（如流程图）等；

第十五条 程序源代码库的维护和拷贝应当遵从严格的变更控制程序。

第十六条 各职能管理部门进行项目立项申请前，在进行项目规划和设计的过程中，应参照各安全技术规范中的相关技术要求进行安全建设。

第十七条 项目安全性论证对项目的安全需求分析、安全功能说明、安全设备、性能指标以及技术方案的技术可行性进行总体分析和审计。

第十八条 项目立项论证和评估过程中，信息安全工作组负责 IT 项目安全性建设的技术部分论证和评估。

第十九条 在提交项目立项申请时，应在技术方案中增加安全方面的说明和文档，内容包括：

（一） 根据安全规范中的要求，系统在建设过程中进行安全部署的说明；

（二） 根据安全规范中的要求，系统在建设过程中无法实现的安全部署的说明和论证；

（三） 系统在建设过程中具体的安全功能以及安全功能的实现方法和技术；

（四） 系统在建设过程中所采用的安全设备的品牌、型号、性能指标说明

以及对于业务系统的影响分析。

第二十条 IT 项目安全性的论证和评估主要关注以下方面的内容：

（一） IT 项目建设中网络规划中安全域的划分、网络冗余、网络传输安全、网络访问控制、网络边界安全、远程访问安全；

（二） IT 项目建设中系统的性能、容量以及系统和业务的兼容性；

（三） IT 项目建设中应用系统中身份验证、角色访问控制、数据加密、备份、日志审计等安全功能；

（四） IT 项目建设中应用系统是否有后门、漏洞和不安全的隐患。

第 4 章 开发人员安全管理

第二十一条 在系统开发过程中，应明确不同人员的身份和职责，各类人员不允许兼职。在系统开发过程中具体可分以下三种角色：

（一） 项目负责人员：确保在整个系统开发的各个阶段都实施了相关的安全措施，同时在整个系统开发的过程中负责整个项目的开发安全管理；

（二） 系统开发人员：根据业务需求确保开发的系统能够满足业务上的需求和相应的安全上的需求，同时满足系统质量上和进度上的要求；

（三） 系统审核人员：对整个开发的过程进行审核和监督，确保开发的质量和开发的安全。

第二十二条 开发人员授权，具体要求包括以下内容：

（一） 应根据该员工在整个开发项目中所负责的开发内容授予其相应的权限和所应承担的责任；

（二） 开发人员必须负责其开发内容的保密性，不得私自将开发的相关信息泄漏出去，即使对家人或开发团队中的其他开发人员也不得泄漏。但开发人员有责任将开发的相关信息告诉项目的负责人员或开发小组的负责人员；

（三） 以书面的方式将员工的权限和相应的责任提交给员工本人。必须严格规定在为企业工作期间，所有和工作相关的开发成果的所属权都归企业所有；

（四） 应根据员工权限和责任的大小确认是否需要签署相关的保密协议；

（五） 应在日常工作中记录员工与开发相关的日志信息；

（六） 员工一旦离职或调动岗位应立即收回或调整其相应的权限。

第二十三条 领导小组必须确保应用系统的开发和运作管理从组织人事和权限职责上分开，应注意以下几点：

（一） 信息技术人员可以现场修复或更改偶然或恶意的数据和软件问题；

（二） 测试代码中往往包含调试或者查错代码，大大增加了主机系统的性能负担；

（三） 开发人员不应具有很高的权限，否则将在系统运作中产生很大的风险。

第 5 章 开发过程的安全控制

第二十四条 在系统开发过程中，开发人员必须参照规范编写代码，具体要求包括但不限于以下内容：

（一） 输入验证，对于用户输入顶进行数据验证，除常见的数据格式、数据长度外，还需要对特殊的危险字符进行处理。特殊字符包括< > ″ ’ % ( ) & + \\’\″等；对于核心业务功能，除在客户端或浏览器进行数据验证外，还必须在服务器端对数据进行合法性检验，规避用户跳过客户端校验，直接将不合规的数据保存到应用中；对于浏览器重定向地址的数据，需要进行验证核实，确认重定向地址是否在可信，并且需要对换行符（\r 或\n)进行移除或者替换；

（二） 数据输出，对需要输出到用户浏览器的任何由用户创造的内容，应在输出到 浏览器之前或持久化存储之前进行转义(至少对<>转义为< >)以防止跨站攻击脚本<XSS) 。对于无法规避的 HTML 片段提交，需对<script>、<iframe>标签进行检查处理，避免应用被挂马的可能性；在程序中应尽量规避 SQL 的拼接处理，优先推荐使用 iBatis/MyBaits 框架，其次推荐使用 SQL 的参数化查询方法，在无法避免使用 SQL 拼接时，因对 SQL 参数值进行编码处理（至少对单引号进行编码)；

（三） 会话管理，不要在 URL、错误信息或日志中暴露会话标识符。会话标识符应当只出现在 HTTP cookie 头信息中。比如，不要将会话标识

符以 GET 参数进行传递。将 cookie 设置为 HttpOnly 属性，除非在应用程序中明确要求了客户端脚本程序读取或者设置 cookie 的值从 Cookie 或者 Session 中获取之前保存的数据进行应用时，须增加必要的数据检验。对于敏感的业务操作，通过在每个请求或每个会话中使用强随机令牌或参数，为高度敏感或关键的操作提供标准的会话管理；

（四） 访问控制，应用必须具备授权访问控制功能，能够限制在最小的范围内使用系统功能。同时限制只有授权的用户可以访问受保护的 URL；

（五） 文件管理，在文件上传处理中，应限制符合要求格式的文件，尽量避免用户直接上传可执行文件或在服务器端限制可执行文件的执行权限。在文件下载时，应规避直接列举服务器上的文件，同时规避将服务器端的路径作为参数进行传递，避免用户非法获取服务器端文件；

（六） 数据加密，原则上在程序代码中不能直接写入用户和密码，对于无法规避的情况，应当对使用的用户名、密码进行加解密处理，在程序中使用加密后的内容；

（七） 错误处理，不要在错误响应将服务器的信息暴露给最终用户，例如：服务器的 IP 地址、操作系统的类型和版本、会话标识符、账户信息等，从而避免增加服务器端被黑客攻击的可能性。在错误处理时，因在后台统一进行日志记录，避免显示调试或堆栈跟踪信息，建议使用通用的错误消息并使用定制的错误页面。

（八） 其他通用规范，审核应用使用的第三方开发框架、第三方代码或类库文件，以确定业务的需要，并验证功能的安全性，避免产生新的漏洞。执行安全更新，如果应用程序采用自动更新，则为你的代码使用加密签名，以确保你的下载客户端验证这些签名，使用加密的信道传输来自主机服务器的代码。

第二十五条 为了降低计算机程序被破坏的可能性，应对运作程序库的访问进行严格的控制：

（一） 严格的管理在开发设备上的存放开发运作程序的目录。如果开发运作程序没有很好的保护，则系统及其设置可能遭到未经授权的访问，

并造成系统的安全性可靠性大大下降；

（二） 只有指定的人员如程序库管理员经过适当的管理授权后，才可以访问运作程序库，对运作程序库的访问必须结合严格的访问控制技术手段和双重访问控制机制。

第二十六条 管理源程序库，源程序包含了系统及其控制如何实现的细节，为修改系统提供了很好的切入点。且如果缺少源程序代码会使得今后应用系统的维护工作十分困难甚至无法完成。因此为了降低计算机程序被破坏的可能性，应对源程序库的访问进行严格的控制：

（一） 严格管理在开发设备上的存放源程序的目录。如果源程序没有很好的保护，则系统及其设置可能会遭到未经授权的访问，并造成系统的安全性可靠性大大下降；

（二） 只有指定的人员如程序库管理员经过适当的管理授权后才可以访问源程序库，对源程序库的访问必须结合进行严格的访问控制技术手段和双重访问控制机制；

（三） 各项应用均应指定相应的管理员；

（四） 信息技术支持人员(非开发人员)不应自由访问源程序库；

（五） 源程序库和运作程序库宜分开存放并且分开管理；

（六） 源程序库和运行的应用系统宜分开存放且分开管理；

（七） 源程序库的更新和向程序员发布的源程序应由指定的管理员根据一定的 授权进行，不得私自进行更新或发放；

（八） 应保存所有对源程序库进行访问读取或修改的日志记录，以便日后审核。

第二十七条 在系统开发与运行维护的所有阶段（如：计划需求、设计、编码、测试、运行和维护）强制实施严格的变更控制，对变更的申请、审核、测试、批准、执行计划与具体实施提出明确要求，确保系统安全性与控制措施不被损害。变更控制包括以下内容：

（一） 审查变更控制措施和流程的完整性，确保未被修改和破坏；

（二） 确保操作系统的更改不会对应用系统的安全性和完整性造成不良影响；

（三） 确保系统文档在每次修改后得到及时更新，并确保旧文档被正确归

档和处置；

（四） 做好软件升级的版本控制，如保存历史版本；

（五） 保留所有变更的审计跟踪记录；

（六） 确保操作文档以及用户程序能在必要时被修改；

（七） 确保及时更新业务连续性计划。

第二十八条 应尽量避免修改厂商提供的软件包，如必须修改，应注意以下几点：

（一） 评估软件包内置的控制措施和完整性流程遭受破坏的风险；

（二） 应征得原厂商的同意，由原厂商提供标准的升级程序来实现软件包的更改。

第二十九条 在软件的原始采购、开发、使用和维护过程中，应采取如下防范控制措施：

（一） 仅从信誉卓著的厂商处购买软件；

（二） 尽量购买提供源代码的软件，以便进行检验，在投入使用之前检查所有源代码；

（三） 使用通过权威机构评估测试的软件产品；

（四） 一旦安装完毕，控制对源代码的访问和修改；

（五） 安装并正确使用有关后门、特洛伊代码的检测和查杀工具。

第三十条 在外包软件开发时，应注意以下几个方面：

（一） 选择信誉与质量保证能力好的软件承包商；

（二） 签订软件许可权协议、明确代码所有关系以及知识产权；

（三） 对外包工作质量和准确性进行检验，并保留检查权利；

（四） 明确承包方违约时应该采取的措施；

（五） 明确代码质量的合同要求，如对编程标准的要求；

（六） 在安装之前进行测试，以检测后门、逻辑炸弹和特洛伊代码。

第 6 章 应用系统维护过程安全管理

第三十一条 应用系统应该包括正式的注册、登录认证和注销模块，并且能够对不同用户的访问权限进行严格的访问控制。具体要求包括以下内容：

（一） 应用系统和操作系统账号分离；

（二） 逐步统一所有应用程序的认证，建立 PKI；

（三） 用户访问权限应得到上级领导和责任人的批准；

（四） 确保服务提供者不能在授权程序结束之前提供访问服务；

（五） 保留所有注册人员使用服务的记录；

（六） 修改或注销已经更换岗位或离开单位的用户的访问权限；

（七） 定期核查并删除多余、闲置或非法的用户 ID 和账户。

第三十二条 对系统管理帐户需要进行如下限制：

（一） 确定不同系统的超级权限以及需要获得此类特权的人员类型；

（二） 尽量对管理权限进行分割，把不同的管理权限赋予不同的账户；

（三） 应用系统应该做好管理账户登录和管理操作的记录；

（四） 定期对系统的日志进行审计，以发现异常登录、操作；

（五） 做好超级权限拥有者无法行使职责时的应急安排，如角色备份。

第三十三条 应用系统应该具有完善的日志功能，能够记录系统异常情况及其它安全事件。

4.6 代码编写安全规范

第 1 章通用编码原则

(一) 不要信任外部的用户输入或系统。

应用程序应该彻底验证所有用户输入，然后再根据用户输入执行操作。验证可能包括筛选特殊字符。针对用户意外地错误使用和某些人通过在系统中注入恶意命令蓄意进行攻击的情况，这种预防性措施对应用程序起到了保护作用。常见的例子包括 SQL 注入攻击、脚本注入和缓冲区溢出。此外，对于任何非受控的外部系统，都不要假定其安全性。

(二) 不要通过隐藏来保障安全。

尝试使用让人迷惑的变量名来隐藏机密信息或将它们存储在不常用的文件位置，这些方法都不能提供安全保障，最好使用平台功能或使用已被证实可行的技术来保护数据。

(三) 以安全的方式处理失效

如果应用程序失效（如发生严重错误等），要恰当的进行处理，一定要保护好机密数据。同时，在向最终用户返回错误消息时，不要公开任何不需要公开的信息。

也就是不要提供任何有助于攻击者发现应用程序漏洞的详细信息。

第 2 章防范常见安全编码问题

在实现应用软件的编码阶段，也较容易因缺乏严谨思考或不好的编程习惯而引入安全问题，而且这些安全问题产生的危害作用非常大，因其产生的漏洞常常会造成应用程序中其他部分构筑的安全控制措施完全失效.目前存在的相当数量系统漏洞都是由编码问题造成的.因此要想保证应用软件的安全性,必须在编码阶段继续高度贯彻安全性原则.

在编码阶段，避免安全问题的基本原则如下：

- 程序只实现指定的功能
- 永远不要信任用户输入，对用户输入数据做有效性检查
- 必须考虑意外情况并进行处理
- 不要试图在发现错误之后继续执行
- 尽可能使用安全函数进行编程
- 小心、认真、细致地编程

目前在各种应用软件中常见的安全漏洞如下所示，应对这些常见问题进行有针对性的防范。

第 3 章缓冲区溢出

如果对输入参数（字符串、整数等）处理时长度检查不严格，或对指针和数组越界访问不进行保护，就容易产生缓冲区溢出（Buffer Overflow）问题，这种问题主要出现在主要出现在 C/C++ 语言编写的系统中,它造成的漏洞是当今绝大多数安全漏洞的主要根源。在 Java / .NET 等利用虚拟机的(托管)平台上不会产生此问题。

要避免此问题，则必须对系统输入数据进行严格的长度检查，废弃或截断超长的越界数据,同时利用基础库函数中的一些更为安全的字符串处理函数来处理数据，也可以利用编译器或代码复查工具提供的检查功能来尽早发现可能会产生问题的程序。

第 4 章输入非法数据

恶意的攻击者会尝试在用户界面或接口中向系统输入恶意数据，以便期望绕过系统的安全限制，致使系统出甚至崩溃或其他非法目的，因此在编码时，须要对所有输入数据（包括用户在界面中输入的数据和其他应用系统通过接口传递的数据）进行严格的合法性检查。

第 5 章 SQL 注入式攻击

SQL 注入式（SQL Injection）攻击是一种典型的，因对输入数据不当处理而产生的非常严重的安全漏洞。其原因是基于数据库的应用程序中经常会使用动态 SQL 语句，而且在程序又没有对输入数据严格检查，致使攻击者能在界面层或接口层注入非法的 SQL 语句，从而非法访问和破坏数据、反向工程、甚至对服务器本身造成威胁。对于攻击者来说，SQL注入式攻击是一种简单有效的攻击方式，也是首选方式，尤其是在基于 Web的应用程序中，因此开发人员必须重点关注此问题。

预防 SQL注入式攻击的手段就是严格检查用户输入的数据，要使用基础系统提供的参数化查询接口，避免使用字符串来构造动态 SQL查询。同时对于数据库对象的访问权限进行严格限制，避免恶意 SQL语句破坏数据或系统。

第 6 章拒绝服务攻击

拒绝服务攻击（Denial of Services -DoS）是指通过大量并发访问，使得服务器的有限特定资源（如网络、处理器、内存等）接近枯竭，使得服务器或操作系统失效的攻击行为。

DoS攻击的一般方式有发送大量数据包造成网络阻塞、执行内存泄漏代码使得系统可用内存越来越少、执行大量消耗 CPU处理能力的代码、通过客户端发送大量的HTTP请求造成巨量 Web点击以及 SYN Flood等。DoS 攻击虽然不会直接对服务器本身带来损坏，但它使得真正的合法用户无法访问系统，从而可能带来业务上的损失。除了 DoS之外，攻击者还可能利用数量庞大的攻击源发起 DDoS（Distributed DoS，分布式拒绝服务）攻击，其破坏和危害作用更大。

在编码时要注意防范可能的 DoS攻击，具体措施包括提高软件行为的可管理性、

主动拒绝异常连接、自动锁定攻击源、提供实时监控界面，能够有效甄别攻击源、具有(异常)事件报警机制、具有审核日志等。通过这些主动或被动的防御手段，能够将 DoS/DDoS攻击行为带来的破坏和危害降到较低水平。

第 7 章敏感信息泄露

攻击者可能会通过暴力攻击、侦听、截取中间数据、反向工程、社会工程学（Social Engineering）等手段，获取访问凭据或机密信息，危及数据的私有性/安全性或者暴露敏感的商业数据，如用户名/口令、加密密钥、数据库连接串、商业敏感信息等。

因此在处理这些数据时，必须利用以密码技术为主的安全技术来进行强有力的机密性保护。在使用密码技术时，一般要利用公开的、经过广泛验证的可靠加密算法，同时加强密钥的管理和保护。

4.7 第三方服务管理制度

第 1 章. 总则

第一条 为了规范第三方安全服务商的服务行为，提高服务质量，降低我单位安全服务成本，完善信息技术服务体系，特制定本制度。

第二条 第三方安全服务包括安全咨询、等级测评、风险评估、安全审计、运维管理、安全培训等几个重点方向。

第 2 章. 细则

第三条 安全服务商应选择具有国家信息安全服务资质证书等其他符合国家的有关规定的组织机构。

第四条 第三方服务商的资质认证内容，包括但不限于第三方的技术能力、经济和财务能力以及对服务的报价。

第五条 所有第三方服务商提供的服务必须签订服务协议或者合同，第三方服务商必须经过资质认证才有签订服务协议或合同的资格。

第六条 在与第三方服务商签订的服务协议或合同中应明确规定：

- 符合福州软件职业技术学院内部控制、内部安全管理及其他相关制度的要求；
- 规定对第三方服务商服务持续性的要求；
- 符合知识产权保护法；
- 与第三方服务商签订服务规范及保密协议；
- 第三方服务商的服务范围。

4.8 等级保护测评管理制度

第 1 章. 总则

第一条 为规范福州软件职业技术学院信息安全等级保护管理工作，明确福州软件职业技术学院在信息系统安全等级保护工作方面的总体要求及相关法律法规的要求，结合福州软件职业技术学院的实际情况，特制定本制度。

第二条 本制度根据《信息系统安全等级保护基本要求》、《信息系统安全等保护定级指南》、《信息系统安全等级保护实施指南》等国家有关法律法规制定。

第 2 章. 建设设施

第三条 信息系统的安全保护等级确定后，福州软件职业技术学院现代教育技术中心应当依照《信息系统安全等级保护基本要求》中对于信息系统保护现状进行差距分析，查找现有保护措施的不足与差距。

第四条 现代教育技术中心应根据差距分析的结果明确需求，有针对性地制定符合《信息系统安全等级保护基本要求》和具体实际情况的整改方案。

第五条 福州软件职业技术学院应根据整改方案规划各项整改工作至相关责任部门，制定整改工作落实计划，切实地保障整改工作得以有效落实。整改完成后，应编写整改报告，并提交至网络安全和信息化领导小组。

第六条 应按照国家信息系统安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，制定并落实符合本系

统安全保护等级要求的安全管理制度，开展信息系统安全建设、实施保护或者改建工作。

第 3 章. 等级划分与备案

第七条 福州软件职业技术学院信息系统安全保护等级应当根据信息系统在本单位中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

第八条 福州软件职业技术学院信息系统的安全保护等级应参照《等级保护定级指南》进行等级划分。

第九条 在信息系统建设过程的需求分析阶段，福州软件职业技术学院应按照国家相关信息系统安全保护等级定级指南对新建信息系统进行等级划分。

第十条 新建或已运营（运行）的第二级以上信息系统，当在安全保护等级确定后 30 日内，现代教育技术中心应到所在地设区的市级以上公安机关办理备案手续，同时将定级备案信息报送至网络安全和信息化领导小组进行内部备案。

第十一条 办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料：

1. 系统拓扑结构及说明；
2. 系统安全组织机构和管理制度；
3. 系统安全保护设施设计实施方案或者改建实施方案；
4. 系统使用的信息安全产品清单及其认证、销售许可证明；
5. 测评后符合系统安全保护等级的技术检测评估报告；
6. 信息系统安全保护等级专家评审意见；
7. 主管部门审核批准信息系统安全保护等级的意见。

第十二条 信息系统备案后，现代教育技术中心若收到公安机关颁发信息系统安全等级保护备案证明，应进行归档；若公安机关要求重新审核确定等级，应重新确定信息系统等级，并按照本办法向网络安全和信息化领导小组和公安机关重新备案。

第十三条 网络安全和信息化领导小组应定期汇总自行建设信息系统的信息、相应的备案资料、及等级保护备案证明。

第 4 章. 系统测评

第十四条 信息系统安全整改工作完成后，选择具备等级保护测评资格的测评单位，对三级以上（含三级）的信息系统进行测评。经测评，信息系统安全状况未达到安全等保要求的，应制定整改方案并进行整改。

第十五条 应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，发现不符合相应等级保护标准要求的需及时整改。

第十六条 信息系统建设或整改完成后，应依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评。

第十七条 通过测评后，现代教育技术中心应报送测评报告至网络安全和信息化领导小组内部备案。

4.9 安全服务商选择管理

第一条 应确保安全服务商的选择符合国家的有关规定；

第二条 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；

第三条 应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

第四条 系统集成商的资质要求：至少要拥有国家权威部门认可的系统一级集成资质，对于较为重要的系统应有更高级别的集成资质；

第五条 工商要求：

a. 产品、系统或服务提供单位的营业执照和税务登记在合法期限内；

b. 产品、系统或服务提供商的产品、系统或服务的提供资格；

c. 连续赢利期限要求；

d. 连续无相关法律诉讼年限要求；

e. 没有发生重大管理、技术人员变化和流动的期限要求；

f. 没有发生主业变化期限要求。

第六条 安全服务商资质：至少应具有国家一级安全服务资质，对于较为重要的系统应有更高级别的安全服务资质；

第七条 人员资质要求：系统集成人员、安全服务人员以及相关管理人员应获得国家权威部门颁发的信息安全人员资质认证；

第八条 应定期对服务供应商提供的服务内容及质量进行评价与考核，对服务供应商提供的服务过程进行监督。

第九条 由服务供应商或业务需求导致需要变更相关服务内容的，需提供相应的说明材料至安全领导小组，经确认无误及审批后，方可执行。

第十条 其它要求：系统符合国家相关法律、法规，按照相关主管部门的技术管理规定对非法信息和恶意代码进行有效控制，按照有关规定对设备进行控制，使之不被作为非法攻击的跳板。

五、系统运维管理

5.1 办公区域环境安全管理

第一条 对重要办公区域的访问应严格限制，未经许可员工不得擅自进入福州软件职业技术学院严格限制的办公区域，如设备室和存储介质室等。

第二条 未经许可和授权，任何人员禁止将办公区域的计算机、笔记本、硬盘、存储介质以及移动介质带离福州软件职业技术学院，如需携带离开时必须开具出门单。

第三条 在员工离职或调离时，收回所有员工使用的技术资料和存储介质，以及其他访问权（例如工作证、办公室钥匙等）。

第四条 员工离开座位超过 30 分钟，桌面上不能有密级纸件文档、磁介质等。下班前，应关闭个人使用设备的电源，并对办公室内公用设备进行检查。

第五条 维护人员进入办公区域进行设备维修时，应事先和相关部门取得联系，在维修的过程中应有专人进行监督。

第六条 使用复印机等设备应按有关规定进行，对复印后作废的纸张应及时销毁。

第七条 禁止员工利用单位网络传播和散布与工作无关的文章和评论，特别是破坏社会秩序的文章或政治性评论。

第十八条 在各科工作站计算机上，除了安装福州软件职业技术学院指定的应用系统软件外，不得安装运行未经现代教育技术中心允许的任何程序及游戏，不得私自卸载任何软件，不得私自存储任何文件，不得任意外接设备（如 U 盘、移动硬盘、移动光驱、蓝牙等），不得私自更换计算机及网络设备，必须保证各工作站的单一工作姿态。

第十九条 读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

第二十条 现代教育技术中心应组织人员不定期检查。对违反管理规定的，将追究管理计算机指定人员的责任并上报福州软件职业技术学院给予行政和经济处罚。

5.2　机房安全管理

第 1 章. 总则

第一条 福州软件职业技术学院中心机房是福州软件职业技术学院网络的心脏，其关系到整个福州软件职业技术学院网络能否正常运行。为了确保福州软件职业技术学院网络中心机房的安全，特制定本制度。

第 2 章. 机房物理安全

第二条 机房应选择具有防震、防风和防雨等功能的建筑内，不得设在建筑物的高层或地下室、以及用水设备的下次或隔壁。

第三条 机房内应采取相应的措施防水、防潮、防火、防雷、防静电；机房管理员需保管好相应设施系统的安全资质材料、安装测试及验收报告。

第四条 现代教育技术中心应根据等级保护相关规定对机房进行分区域管理，重要区域应配置电子门禁系统，24 小时控制、鉴别和记录进出的人员；同时，应在各区域间设置物理隔离装置，在重要区域前设置过渡区域；

第 3 章. 机房安全规定

第五条 非工作人员不得随意进入中心机房；外来人员进入机房，应先填写《进入机房申请表》，经现代教育技术中心领导批准并在值班员处登记后，有相关人员陪同下方可进入机房。

第六条 值班人员必须坚守岗位，认真填写机房值班记录，发现重大故障应及时报告和处理。

第七条 外来人员的现场工作或远程维护工作内容应在合同中明确规定，当外来人员访问重要区域涉及机密或秘密信息内容，应要求其签署《外来人员进入重要区域申请表》。

第八条 机房管理员应履行以下责任与义务：

1、保障机房的物理环境安全，（周期）查看门禁系统、防盗系统、监控系统、消防系统等是否正常运行，保存运行、监控、报警等相关记录；

2、根据需要启动或关闭服务器系统，（周期）监视并记录服务器系统运行情况，特别是出现的异常情况；

3、监视电压、电流、湿温度等环境条件，机房温度应尽量控制在 20° C 左右，最佳相对湿度控制在 45%～50%；

4、监视空调等设备运行的作业和信息传输情况；

5、对机房巡检进行记录；

6、维护网络拓扑结构图，保障其与机房真实情况相符合；

第九条 危险品、可燃品和液体不得带入机房；不准在机房吃饭、吃零食或进行其他有害、污损服务器的行为。

第十条 机房内应经常保持整齐、清洁、有秩序，做到进门换鞋、地面清洁、设备无尘、排列有序、布线整齐、仪表准确、工具就位、资料齐全。

保证服务器 24 小时不间断正常工作，不得随意在服务器用电线路上加载用电设备，严防服务器掉电。

5.3 资产安全管理

第 1 章. 总则

第一条 为加强对福州软件职业技术学院信息资产的管理，保障信息资产安全，防止信息资产损毁、误用和非授权访问，确保信息资产的保密性、完整性和可用性，特制订本制度。

第二条 本规定适用于现代教育技术中心及其他相关部门针对信息资产进行分级分类保护以及相应的管理活动。

第 2 章. 资产分类

第三条 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、分级和实施相应的保护措施，需从安全责任划分资产所有者（或所有部门）、维护者以及使用者，并填写《信息资产登记表》。

第四条 根据信息资产的 CIA，将资产的重要程度为：重要、一般、非重要；对于新资产，资产负责人需根据资产 CIA 对每个资产进行分类，并填写《信息资产登记表》中重要程度项。

第五条 信息资产按形式不同可以分为五类：数据和文档资产、软件资产、实物资产、人员资产和服务资产。其中数据和文档资产主要包括业务数据和记录、各类管理制度、管理文档、办公文档以及外来的数据文件等。具体如下：

1. 数据和文档资产：通常包括各种电子档：业务数据、配置文件、记录数据（日志、审计记录）、管理文件（策略、流程文件、操作手册等）、商务文件（合同、协议等）以及外来数据文件等。也包括以实物方式存在的资产：各类电子数据的归档、打印件、书面管理文件、业务报表、包含重要商业成果的文件，还有胶片等；
2. 软件资产：各种系统软件、应用软件（OA、业务软件等）和工具软件（开发系统、网管软件、安全软件等），包括操作系统、数据库应用程序、网络软件、办公应用系统、业务系统程序、软件开发工具等，这些软件资产负责处理、存储或传输各类信息；
3. 实物资产：与业务相关的 IT 物理 设备，包括计算机（工作站和服务器等）和网络通信设备、磁介质（磁带和磁盘等）、装置、环境等，这些实物资产容纳着软件和数据文件；
4. 人员资产：承担某项与业务活动相关责任的角色和职位。例如普通用户、系统管理员、网络管理员、有合同约束的保安、清洁员等，这些人员与各类数据、软件和实物资产的操作直接相关；
5. 服务资产：安保（例如监控、门禁、保安等），环境服务（例如清洁），基础保障（供水、供热、供电），设备维护，通信服务（例如互联网接入）。

第 3 章. 信息使用控制

第六条 实物资产的使用

1. 实物资产的接收和发出

- 实物资产的接收和发出按固定资产管理方面的管理规定执行；
- 接收到新的信息资产后，由部门信息安全管理员对信息资产重要程度进行标识；
- 信息资产发生变化时（新增、删除、变更），部门信息安全管理员应及时更新《信息资产登记表》。

2. 新增的硬件和与 IT 相关的环境设施在经过必要的安装、配置和性能调优后，才能并入福州软件职业技术学院的网络系统。

3. 需要对主干网络、主机、网络设备、安全设备和 UPS 等重要环境设施的性能和运行状况进行日常监控和维护。

4. 控制的所有硬件类资产都应按照《办公区域安全管理规定》进行保护，机房内的设备要按照《机房安全管理制度》的规定进行保护。

5. 未经批准，资产不得随意移动位置或带出福州软件职业技术学院的物理安全区域。

第七条 软件类资产的使用

1. 福州软件职业技术学院办公计算机不得使用未经批准的软件，系统软件应根据需要及时进行补丁更新；

2. 计算机采取必要的措施防范病毒、木马和流氓软件等恶意程序；

3. 采购软件类资产，要选择软件开发商，进行软件测试，必要时要进行原代码审查，以确保采购软件安全；

4. 所有存储软件的介质应当妥善保存，并登记入册。

第八条 信息类资产的使用

1. 信息资产的保密管理

- 对重要信息资产实施严格的安全与保密管理，防止系统数据的非法生成、变更、泄露、丢失与破坏；
- 一般及以上信息资产不得泄露，禁止外传；

- 重要信息资产的处理过程中，被批准使用数据人员以外的其它人员不应进入机房工作；处理结束后，应清除不能带走的本作业数据；妥善处理打印结果，任何记有重要信息的废弃物在处理前应进行粉碎；
- 各业务数据仅用于明确规定的目的，未经批准不得它用；
- 无正当理由和有关批准手续，不得查阅重要信息资产资料；经正式批件查阅数据时必须登记，并由查阅人签字；
- 重要信息资产不得以明码形式存储和传输；

2. 信息类资产的访问控制管理

- 对信息资产的备份、恢复、转出、转入的权限都应严加控制。严禁未经授权将财务数据等拷贝出系统，转给无关的人员或单位；严禁未经授权进行数据恢复或转入操作；
- 采用实时监控机制，及时发现不良信息或破坏性数据，对其采取封堵、清除等相应安全控制措施；
- 对监控或检测到的可疑数据采用跟踪机制，并对其进行可控性操作，以便发现其最终企图。

3. 数据存储管理

- 数据库管理员负责信息资产存储设备的使用和安全，包括磁盘阵列、磁带、光盘等的安全；
- 采用专门的数据备份和容灾安全解决方案及存储设备；
- 备份数据除了备份在本地机器上外，还需准确地转储到不可更改的介质上；
- 为保证数据不被删除或修改以及能长时间保存，要求采用只读式数据记录设备。

5.4 介质安全管理规定

第 1 章. 总则

第一条 为保障福州软件职业技术学院内部存储介质的信息安全，对存储介质的使用、存储、携带、记录、清除等活动提供明确的安全管理标准，特制定本规定。

第二条 存储介质是指计算机磁盘、磁带、软盘、光盘等外部存储设备，用于存储系统软件、应用软件、数据库及其他数据信息。本规定适用于在福州软件职业技术学院对磁带、磁盘、光盘、硬盘、磁盘阵列等存储介质进行的所有安全管理活动。

第 2 章. 细则

第三条 介质的保管由现代教育技术中心指定专人负责，在介质的使用过程中，介质管理员需维护《存储介质管理记录表》

第四条 操作系统、业务应用系统的备份介质其使用权仅限于数据库管理员和系统管理员。

第五条 使用者要对介质的物理实体和数据内容负责，使用后应及时交还介质管理员，并进行登记。

第六条 超过数据保存期的介质，必须经过特殊清除后，才能视为空白介质。

第七条 对保密性较高的存储介质，未经批准使用者不得自行销毁内部数据。

第八条 使用者认为不能正常记录数据的介质，必须由使用者提出报废（或维修）介质申请《介质销毁审批单》，由现代教育技术中心责成有关人员进行测试后并提出处理意见，报批后由双人进行敏感信息清楚，并做好处理纪录。

第九条 含有涉密内容的介质一律不得外借，不得挪出机房；如有特殊需要暂借或带出工作环境的，需报批后方能执行，介质管理员需首先对敏感信息进行处理，或销毁或加密，并做好相应记录，明确归还日期。

第十条 对重要介质中的数据和软件采取加密存储，加密方法可采取身份认证、通信完整性保护、多级密钥管理模式等，同时需根据所承载数据和软件的重要程度对介质进行分类和标识管理，分类标识需符合《资产安全管理制度》等祥光制度。

第十一条 长期保存的介质，要定期进行检查，防止保存过久造成数据丢失。

第十二条 介质存放环境需采取适当的保护措施防止介质被盗、被毁、介质内存储信息被未授权修改以及非法泄漏等；

第十三条 介质管理员需根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。

第十四条 安全移动存储介质需作数据恢复的，应由各科室计算机专业技术人员进行操作;必须送外部作数据恢复的，应由现代教育技术中心负责人审核同意后，到具有保密资质的单位进行数据恢复，须填写《介质销毁(送修)审批单》

5.5 设备使用及维护管理

第 1 章. 总则

第一条 为了加强福州软件职业技术学院信息化设备管理，保障设备的安全，合理配置设备，提高设备的使用效益，制定本规定。

第二条 本规范适用于福州软件职业技术学院及下属单位配置的终端计算机、工作站、便携机、系统和网络设备等的购置、使用、维修、储存等方面。

第三条 现代教育技术中心是设备管理的职能部门，负责设备购置计划的编制，设备实物的清点、保管和调拨，报损报废设备的处置，固定资产账务的处理、报表的编制等工作。

第四条 现代教育技术中心指定一名设备管理员，负责办理设备的调拨、报废、编制报表等固定资产账务处理的工作；指定一名仓库管理员，负责办理设备的清点、库存设备保管和领取等工作。

第 2 章. 设备的购置管理

第五条 由现代教育技术中心负责对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；具体操作规程参见《产品采购管理规定》。

第 3 章. 设备维护管理

第六条 操作人员须参加现代教育技术中心组织的培训，经考核合格后方能操作电脑。操作人员必须掌握相应的计算机操作常识，工作认真负责，熟悉业务和操作规范。

第七条 设备由设备管理员负责维修相关工作，对网络系统进行维修时必须采取数据保护措施，安全设备维修时必须有安全管理员、设备管理员在场。

第八条 经检查为人为损坏的，损坏者或使用部门应支付维修费，无法维修的应照价赔偿。

第九条 对设备进行维修时必须记录维修对象、故障原因、排除方法、主要维修过程以及维修有关情况。

第十条 设备报损报废办理手续，必须由安全管理员和设备维修员共同进行鉴定和残值估价，并对设备情况进行详细登记，提出报告书和处理意见，由信息中心批准后方能进行报废处理。

第十一条 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

第十二条 符合下列条件之一的设备，可以申请报损、报废：

1. 设备损坏经确认无法修复或降级使用的；
2. 设备超过规定的使用期限（6 年）,即达到自然使用寿命或失去继续使用价值的；
3. 损坏设备的一次性修复费用超过该设备或同类设备现价 60%的；
4. 设备总体性能下降且年度维护费用超过该设备或同类设备现价 50%的；
5. 设备丢失经查找没有找回的并经有关规定处理后的；
6. 设备陈旧，主要技术性能指标不能满足使用要求的；
7. 设备长期闲置且没有调剂价值的。

第 4 章. 设备使用管理

第十三条 设备责任人应保证设备在安全环境（出厂标称环境）下运行

第十四条 计算机电源线路及网络通讯线路的布设，计算机电源、网络资源的接入，一经确定，任何人未经许可不得随意拆卸、改动。不得随意拆接、移动计算机和外围设备，以免造成损失。如确有需要，必须取得信息管理部负责人的许可后，方可由专业人员根据需要操作。

第十五条 主服务器如 Web、Mail、WWW、DNS 等服务器，其中设置参数不得随意再修改，如果不是特殊情况，不要随意关闭服务器。

第十六条 防火墙，交换机，HUB，路由器等按规定配置，一旦配置成功，不得随意修改。

第十七条 设备需设置登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

第十八条 设备的使用必须指定专人负责并建立详细的运行日志。登记内容应包括运行起止时间，累计运行时数以及运行状况等。

第十九条 由责任人负责进行设备的日常清洗及定期保养维护，做好维护记录，保证设备处于最佳状态。

第二十条 软件安装：管理员不得随意在设备上安装软件，需要安装软件时，需要更新相应设备记录表。也不得随意升级服务器上的软件，在软件更新前做好数据备份。具体备份与恢复相关操作参见《备份与恢复管理制度》。

第二十一条 访问权限设置：

1. 非福州软件职业技术学院内部使用的各类存储介质，凡未经过系统专门进行病毒扫描程序检查的，严禁在设备上使用。
2. 应对网络设备的管理员登录地址进行限制；
3. 应实现设备特权用户的权限分离。

第二十二条 口令及屏保设置：

1. 设备的口令由管理员设置，并做好登记，口令必须符合《账号与密码管理规定》
2. 所有设备在无人操作时必须进行锁定，须设置带口令的屏幕保护功能，屏保的时间不应超过 2 分钟。

第二十三条 日常监视：管理员应确保福州软件职业技术学院所有设备都能够产生记录用户活动、异常和信息安全事件的日志，具体参照《信息系统监控管理制度》相关规定。

第二十四条 故障处理：管理员应确保所有设备的故障能自动生成日志，发生故障时，由现代教育技术中心进行统一分析、记录和处理，必要时可请求技术部门协助，确定纠正措施并实施。机房设备各种连接线较多，电源管理应科学、合理，保持电脑和各种外设处于最佳状态。

第二十五条 当设备因特殊原因需带离或带入机房时，需由设备管理员填写《（人员/设备）进入机房申请表》，经有关领导审批通过后，方可将设备带离或带入机房，值班人员须做好相关记录。

第 5 章. 设备仓库管理

第二十六条 仓库管理员对仓库内设备的安全完整负责，保证设备在安全环境（出厂标称环境）下储存，保持仓库整洁。

第二十七条 仓库管理员请假时间较长时，应将仓库移交部门其他人员暂时代管。交接时，双方应对仓库内设备进行清点，并签字确认。代管期间发生的责任，均由代管人负责。

第二十八条 管理员需根据《资产安全管理制度》等规定执行好日常工作，做好设备出库入库工作、指导借用人填写办理领用或借用手续，并维护好相关记录。

第二十九条 对新采购的设备由仓库管理员负责组织设备需求部门等相关部门进行验收，对已验收的设备清点入库，并做好固定资产编号、标签打印及粘贴。入库登记等原始记录，应妥善保管，直到设备报废。若是安全产品或保密设备必须单独储存并遵守相关保护措施。

第三十条 配发的设备，如果因岗位交流或其他情况不再使用的，应当及时归还入库。

第三十一条 设备归还时，仓库管理员应检查设备完好情况，并作入库登记。归还的设备如有损坏或遗失，使用部门或者使用人应当说明原因，视情况报各队长领导处理。

5.6 网络安全管理

第 1 章. 日常维护

第一条 任何人不得进行干扰福州软件职业技术学院网络用户、破坏网络服务和破坏网络设备的操作。严禁任何人从事下列影响网络正常运转和危害网络安全的行为：

1. 未经允许，擅自将任何计算机设备接入福州软件职业技术学院信息系统网络；
2. 未经允许，擅自安装集线器、交换机、ADSL 等上网设备和软件；
3. 未经允许，私自删除、修改或增加网络协议、网络地址和网络配置等；

4. 未经允许，擅自卸载安装的各种软件和程序；

5. 故意制作、传播计算机病毒等破坏性程序；

6. 故意使用黑客软件或远程控制软件等带有攻击其它计算机性质软件；

7. 其他危害计算机信息网络安全的行为。

第二条 网络管理员应做好网络运行日的记录保存工作，以下的日志必须保存六个月。

（一） 系统网络运行日志，包括系统的SYSLOG 和MESSAGE 等信息和警告信息；

（二） 用户使用日志记录，内容包括：

1. IP 地址分配及使用情况。

2. 交互式信息发布者。

3. 主页维护者进行操作的时间和对应 IP 地址，交互式栏目的信息等。

4. 电子邮件接收到的时间，使用和拨号用户上网的起止时间和对应 IP 地址。

5. 拨号用户的用户名，上网时间及对应 IP 地址。

6. WWW 用户访问记录必须具有时间，访问的 IP 地址、访问的网页资源。

7. FTP 用户上载及下访问记录必须具有时间、访问的 IP 地址、存取的文件名。

8. 个人主页上传的登录访问时间、访问的 IP 地址、存取的文件名。

9. 电子公告服务用户登录时间、访问的 IP 地址、访问的栏目、发表文章的时间、 标题和发表的栏目名，电子公告服务中的聊天记录也包括上述的基本内容。

第三条 网络管理员通过网络监控平台，实时对福州软件职业技术学院网络系统的运行状况进行监控，对发现的网络中断和阻塞等异常情况应及时查明情况，通知相关技术人员。技术人员采取必要的技术手段和措施尽速加以解决，保证网络系统的畅通无阻。

第四条 网络管理员应对网络实时监控和故障处理情况如实做好详细记录，每月按时间顺序将书面记录装订成册，存档备查。

第五条 福州软件职业技术学院网络系统的规划设计方案、设计图纸、设备资料、资源分配表、网络设备参数配置等技术文档资料，应按有关保密规定严格管理。

第六条 应合理安排时间，开展福州软件职业技术学院信息网络设备、线路和参数的维护，尽可能不影响网络的正常运行。因网络维护需中断网络运行的，应事先请示上级领导并通知相关部门，以便提前采取相应措施，保证数据安全。相关部门应积极配合技术人员做好网络维护工作。

第七条 将基本配置信息纳入变更范畴，实施对配置信息改变的控制。

第八条 必须提交申请并经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后理解关闭接口或通道。

第 2 章. 安全配置

第九条 应确保所网络设备和软件都安装了最新的安全补丁，关键的安全补丁必须在发布的一个月内更新。

第十条 在网络上安装系统以前，必须更改供应商提供的默认设置，包括密码、简单网络管理协议（SNMP）机构字串，并删除不必要的账户。

第十一条 应明确路由器、防火墙和交换机等网络组件上用于本地管理的组、角色和权限。

第十二条 应明确路由器、防火墙和交换机等网络组件的服务、协议和端口，以及所有系统组件的服务和协议，确保只有业务需要才能开启。

第十三条 确保删除或禁用了在所有组件上不必要的功能或服务，如脚本、驱动、特性、子系统和文件等。

第十四条 应确保设备中的策略均得到有效备份。

第 3 章. 网络账户

第十五条 网络设备管理员及用户需要保护系统登录密码，杜绝账户密码有意或者无意的泄漏。

第十六条 所有网络设备的口令设置及口令更新周期需根据《账户与密码管理制度》进行设置。

第十七条 网络管理员需要根据福州软件职业技术学院业务上的需求，删除或锁定无用的帐号；账户管理员调离时，需要修改网络设备的密码。

第十八条 网络管理员及安全主管应运用网络巡查等技术手段，对网络节点的合法性和规范性进行检查，发现不规范的节点应及时予以纠正，对非法接入节点用户应予取缔，相关部门及全体员工必须予以积极配合。

第 4 章. 审计管理

第十九条 网络设备安全策略应该拒绝便携式和移动式设备的网络接入，如需接入应该经过现代教育技术中心领导授权与批准。

第二十条 安全主管与网络管理员应该定期检查违反规定拨号上网或其他违反网络安全策略的行为。

第二十一条 每季度应对福州软件职业技术学院进行内部和外部网络漏洞扫描，在网络出现任何重大变动（如安装新的系统组件、更改网络拓扑、修改防火墙规则、产品更新）后，也应进行上述扫描。

第二十二条 每一季度出具网络漏洞扫描报告，报告内容包括存在的漏洞、严重级别、原因分析、改进意见等方面。

5.7 系统安全管理

第 1 章. 系统安全策略

第一条 系统管理员应根据业务需求和系统安全分析确定系统的访问控制策略。

第二条 加强密码策略，参照《账户与密码管理制度》等相关制度，同时根据账户的权限设置密码复杂度及最大连接数等；

第三条 定期安装系统的最新补丁程序，在安装前进行安全测试，并对重要文件进行备份后，方可实施系统补丁程序的安装。

第四条 当系统功能需变更时，需求提出部门需根据《授权与审批管理》等相关制度填写需求变更申请表，由现代教育技术中心对需求进行技术分析，并督促第三方开发商完成新功能开发；开发完成后由现代教育技术中心负责完成新功能上线安全测试，出具信息系统变更验收报告，由需求部门签字验收后方可投入使用。

第五条 安全主管每月对操作系统进行安全漏洞扫描，及时发现最新安全问题，通过升级、打补丁或加固等方式解决，漏洞报告需包含存在的漏洞、严重级别、原因分析、改进意见等方面。

第六条 系统管理员定期检查系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理。

第七条 系统管理员定级检查系统运行情况，出具系统分析报告，报告中应该分析记录帐户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等非正常事件。

第 2 章. 系统账户

第八条 现代教育技术中心负责单位人员的权限分配，权限设定应遵循最小授权原则：

1. 管理员权限：维护系统，对数据库与服务器进行维护。系统管理员、数据库管理员应权限分离，不能由同一人担任；
2. 普通操作权限：对于各个系统的使用人员，针对其工作范围给予操作权限；
3. 查询权限：对于单位管理人员可以以此权限查询数据，但不能输入、修改数据；
4. 特殊操作权限：严格控制单位管理方面的特殊操作，只将权限赋予相关部门负责人，例如退费操作等。

第九条 上述权限的分配设定，需遵循《授权与审批管理》等相关制度执行，申请人需填写权限分配申请表，在通过相关人员审批通过后才能开通。

第十条 用户责任义务：

1、账号使用者有权保护账号密码不借用他人，不将账号密码记录在桌面，书本等显眼的位置。

2、发现账号使用异常或非法用户，应及时告知相关人员。

第 3 章. 系统日志管理

第十一条 对于系统重要数据和服务器配置参数的修改，需通过相关人员批准，并做好相应记录，具体参见《授权与审批管理》等相关制度。

第十二条 对各项操作均应进行日志管理，记录应包括操作人员，操作时间及操作内容等详细信息。

第十三条 审计日志应包括但不局限于以下内容：包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全事件。

第十四条 安全审计员应每日对审计日志进行审查，对异常事件及时跟进解决，并定期形成日志分析报告。

第十五条 系统审计日志应定期做好备份工作。

5.8 恶意代码防范管理

第一条 系统管理员需不定期对员工进行基本恶意代码防范意识教育。

病毒及木马防范

- 针对内部计算机病毒及其他有害数据的控制防范手段，包括计算机软硬件及管理，由现代教育技术中心统一规划、实施，任何员工必须配合执行。
- 福州软件职业技术学院信息系统的所有终端必须安装福州软件职业技术学院指定的防恶意代码软件。所有用户不得私自卸载防恶意代码软件。
- 所有用户在未清楚病毒传播特性的情况下，发生病毒发作情况，应立即断开网络连接及时清除病毒，无法清除时应向现代教育技术中心报告，请求帮助。病毒问题彻底解决后，方可重新入网。
- 凡需引入使用的移动硬盘、存储设备、软件，均须先进行病毒和木马的查杀。
- 在各种杀毒办法无效后，须重新对计算机格式化，装入正规渠道获得的无毒系统软件，如有困难向现代教育技术中心报告。
- 安全管理员负责对防病毒措施的落实情况进行监督，及时更新维护恶意代码库。

- 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

第二条 系统管理员定期检查系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理。

第三条 系统管理员需定期进行恶意代码检测，尤其是针对于刚上线的新系统，检测后应出具相应的报告并保存记录。

5.8 配置管理办法

第 1 章资产配置评估

第一条 为了加强信息安全保障能力，建立健全的安全管理体系，提高整体的网络与信息安全水平，保证网络通信畅通和业务系统的正常运营，提高网络服务质量，在安全体系框架下，本制度规范安全体系实施的监督、检查机制；是安全体系制度的建设及检查制度。

第二条 本制度适用于信息安全管理小组，信息安全实施组，部门安全管理组织及系统管理员

第三条 信息安全管理小组应每个季度对整体信息安全现状进行评估，整理评估结果，提交信息安全工作组，评估结果应能反映的整体安全状况。

第四条 各部门应每个季度对本部门的系统进行资产配置评估，整理评估结果，提交信息安全管理小组进行备案。

第五条 资产配置评估过程中各部门要对资产管理进行安全评估，根据“信息安全管理系统”中的资产管理安全要求进行核实，具体内容详见《我单位安全管理制度汇编信息资产管理办法》中的规定。

第六条 资产配置评估过程中各部门要对各业务系统中的设备弱点进行安全评估。

第七条 资产配置评估过程中各部门要对各业务系统进行安全事件审计，记录安全事件审计结果，并提交信息安全管理小组，通过网络与信息安全管理系统进行备案。

第八条 各部门资产配置评估应由各部门信息安全组织负责完成，评估结果提交信息安全工作组进行备案。

第九条 资产配置评估的标准是根据各系统在安全体系中选定的安全目标和安全要求而定，应严格按照已确定的安全要求进行评估。

第十条 资产配置评估可以根据是否按照安全要求进行执行来判断，如果按安全要求严格执行，则判定“完成”；如果按安全要求执行一部分，则判定“部分完成”，并说明完成情况；如果没有按安全要求执行，则判定“未完成”，并说明未完成原因。

第十一条 资产配置评估可以通过网络与信息安全管理系统的安全体系模块进行实现，首次评估应根据《安全体系运作流程》中的相关内容进行确认和审批，通过后可以进行安全评估。

第十二条 通过网络与信息安全管理系统进行资产配置评估后，系统会自动显示评估结果，与安全目标和安全要求之间的差距，此项信息作为后续安全工作的指南。

第十三条 资产配置评估的具体内容包括以下几个方面的内容：

（一）安全制度；

（二）安全组织；

（三）安全运作流程；

（四）网络及网络设备；

（五）主机系统；

（六）数据库系统；

（七）生产终端系统；

（八）应用系统。

第十四条 对资产配置评估结果进行审计，并把审计成果公布在网络与信息安全管理系统主页面上。

第十五条 第十五条资产配置评估成果会作为各部门、系统安全考核的指标之一。

第 2 章 补丁管理

第十六条 安全管理员负责系统安全补丁跟进、补丁分级、补丁信息通告各部门安全管理，负责提供从正式渠道获取的安全补丁软件，负责审核和监督各部门安全补丁加载情况。

第十七条 部门安全管理员负责把从安全管理员获取的补丁信息通知相关的管理员、分发系统安全补丁软件，负责监督和向安全管理员报告各业务系统的补丁加载情况。

第十八条 各业务系统管理员负责协调系统安全补丁的测试、加载、回退，负责协调制定补丁加载流程和回退计划，负责补丁加载后的监督和验证，负责向部门安全管理员报告业务系统的补丁加载情况。

第十九条 各业务系统集成商负责系统安全补丁的测试、补丁加载流程和回退计划制定、补丁加载、补丁回退等实施工作，当补丁加载后影响业务正常运行的情况下负责应用软件的修改工作。

第二十条 产品厂商负责向安全管理员及时发布系统安全补丁信息，并提供安全补丁软件。

第二十一条 安全管理员负责跟进各产品的安全漏洞信息和产品厂商发布的系统安全补丁信息。

第二十二条 系统安全补丁根据其对应漏洞的严重程度分为三个级别：紧急补丁、重要补丁和一般补丁；紧急补丁必须在 15 天内完成加载，重要补丁必须在一个月内完成加载，一般补丁要求六个月内完整加载。

第二十三条 安全管理员向部门安全管理员通告系统安全补丁信息，然后由部门安全管理员通告相关的业务系统管理员。

第二十四条 安全管理员负责从正式渠道获取系统安全补丁，正式渠道包括正式下发的和产品厂商提供的，不建议使用从网站下载的安全补丁。

第二十五条 安全管理员负责对系统安全补丁进行完整性校验，确保获取的安全补丁软件未被修改和可用。

第二十六条 补丁加载之前必须经过严格的测试，严禁未经测试直接在生产系统上加载补丁。

第二十七条 补丁测试的方式有两种：实验室测试和现网测试；实验室测试必须进行，实验室环境需要与现网环境尽可能一致，并考虑差异性带来的风险；条件允许的情况下（如有测试环境或备机）可以现网测试。

第二十八条 补丁测试的内容包括补丁安装测试、补丁功能性测试、补丁兼容性测试和补丁回退测试：

（一） 安装测试主要测试补丁安装过程是否正确无误，补丁安装后系统是否正常启动。

（二） 补丁功能性测试主要测试补丁是否对安全漏洞进行了修补。

（三） 补丁兼容性测试主要测试补丁加载后是否对应用系统带来影响，业务是否可以正常运行。

（四） 补丁回退测试主要包括补丁卸载测试、系统还原测试。

第二十九条 补丁测试的工作由系统集成商负责实施，系统管理员负责协调，必须对补丁的现场测试和现网测试限定时间，测试完成后需要编写详细的测试报告，给出明确的测试结论。

第三十条 系统管理员需要把《补丁测试报告》提交安全管理员，并提交信息安全主管领导进行审核，审核通过后可以进行补丁加载。

第三十一条 为确保系统集成商及时配合补丁的测试和安装工作，需要通过合同的方式，明确集成商的安全补丁测试和安装责任，约束条款至少应包括：实验室测试环境的答建，在规定时间内完成补丁测试，补丁的加载，补丁加载失败时的测试与分析，补丁与应用冲突时的系统改造和升级工作。

第三十二条 从安全漏洞发布到补丁加载前，网络安全管理员根据需要给出应急措施建议，例如通过加强访问控制、临时关闭服务、加强安全审计等应急措施来加强网络安全，各相关业务系统根据建议采取适当的防护措施，并加强对系统的监控，及时发现和报告安全事件。

第三十三条 补丁加载前，必须向网络安全管理员提交《安全补丁测试报告》、《安全补丁安装计划和实施方案》、《安全补丁回退实施方案》，经部门领导及主管领导审批通过后按计划执行，审批的周期为 2 个工作日。

第三十四条 在补丁安装前，必须做好数据备份工作，确保任何的操作都可回退，在到达回退时间补丁加载没有完成时，启动回退操作，保证业务的正常运行。

第三十五条 补丁加载必须安排在业务比较空闲的时间进行，对补丁加载的操作过程必须详细记录。

第三十六条 核心业务主机的补丁加载建议要求厂商工程师现场支持。

第三十七条 补丁安装完成后，业务系统管理员必需查看系统信息，确保安全补丁已经成功加载。

第三十八条 必须对加载补丁后的系统按照计划和验证方案进行严格的测试验证，确保补丁加载后不影响系统的性能，确保各项业务操作正常。

第三十九条 补丁加载后的一周内，管理员必须加强对系统性能和事件进行密切的监控，编写每天的运行监控报告。

第四十条 业务系统管理员需编写《补丁安装报告》、《补丁验证测试报告》，提交给部门安全管理员归档，然后由部门安全管理员把文档提交给安全管理员归档。

第四十一条 部门安全管理员负责对安全补丁软件进行归档，以备系统重装时需要。

第四十二条 网络与信息安全管理工作组负责对各部门补丁管理的执行情况进行考核，考核的内容包括补丁加载情况、补丁版本信息的准确性和相关文档的质量。

第四十三条 可通过安全漏洞扫描和现场人工抽查进行审计和检查，考核的方式可通过部门内部的自查和信息安全管理部门组织的巡检进行。

5.9 账号与密码管理

第 1 章. 责任与义务

第一条 现代教育技术中心安全主管，统一管理重要主机系统、核心网络设备、安全设备等用户以及重要系统中具有关键访问权限用户的密码，对于系统用户的密码初始化、重置等做好登记工作。

第二条 系统管理员应确保除匿名帐户外，所有信息系统帐户都必须设置口令；确保系统、应用和网络设备的帐户无默认口令；确保关键应用服务器启用口令强制策略；禁止管理员为所管理的帐户设置相同的口令。

第三条 系统帐号密码持有人负责所持计算机用户口令在使用过程中的保密，负责设置、保存、更换系统帐号密码，负责密码自身的安全强度，并做好更改登记工作。

第 2 章. 账户与密码设置基本要求

第四条 账户创建应满足以下几个要求：

1. 只有具备访问信息系统正当需求的用户才可以申请信息系统的用户帐户；
2. 帐户的权限应该以满足用户需要的最小权限为原则，不得授予与用户工作职责无关的权限；
3. 对于确因工作需要而必须申请系统帐户的外部用户，则必须通过有关人员批准；并且有福州软件职业技术学院正式员工作为其安全责任人；如果需要接触本单位秘密信息，应签署相应的保密协议；
4. 任何系统的帐户必须有明确的责任人，责任人必须细化到个人，不得以部门作为责任人；
5. 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；
6. 用户申请帐户前需要掌握必要的信息系统操作常识，具备必要的信息安全意识，了解本单位信息安全管理的相关规定，以确保能够正常的操作信息系统，避免对信息系统安全造成危害；
7. 系统应当严格限制开设公用帐户，一般情况下公用帐户不得具有访问敏感信息和对系统进行写操作的权限。公用帐户应该指定责任人，负责该帐户的使用、监控和维护；

第五条 帐户使用人在工作职责发生转变，所需要的信息系统访问权限与其现有的访问权限有变化时，应当由所在部门书面通知现代教育技术中心进行访问权限的变更；

第六条 用户离岗或调岗时，账户的管理需遵照《信息系统人员安全管理规定》相关规定；

第七条 账户在使用的过程中，应遵守：

1. 任何帐户仅限于申请帐户时声明的使用人使用，禁止其他人使用此帐户；

2. 帐户正式使用前，必须修改帐户的缺省口令；

3. 帐户使用人不得使用帐户访问与自己工作无关的资源；

4. 外部用户使用本单位信息系统帐户不得违反本单位与其签订的保密协议。

第八条 计算机用户密码基本要求由密码长度、密码字符复杂度、密码历史、密码最大尝试次数，密码最长有效期组成：

1. 密码最小长度：8 位；

2. 密码字符组成复杂度：密码由数字、大小写字母及特殊字符，且至少包含其中两种字符；

3. 密码历史：修改后的密码至少与前 10 次密码不同；

4. 密码最大连续尝试次数：7 次，密码错误次数超过最大连续尝试次数后，应具有限制用户登录的机制 ，主要包括锁定用户并告警等；

5. 密码最长有效期限：30/60/90 天，可根据系统重要性和用户权限采取不同的有效期；密码使用期限即将达到密码最长有效期限时，应具有提示用户修改密码的机制。

第 3 章. 信息系统密码

第九条 主机系统、网络设备、安全设备等密码的设置除满足本制度第三章外，还需满足：

1、 启动密码管理相关功能、机制。

2、 具有关键访问权限用户的密码应由专人设置与管理。

3、 应为超级用户设置密码登记簿。

第十条 如遇特殊情况需启用封存的密码，必须经过部门负责人审批，使用完毕后，须立即更换并封存，同时在密码管理登记簿中登记。

第十一条 终端系统用户密码主要是指员工用于日常办公信息处理的计算机系统的用户密码，如台式微机、笔记本电脑及其它个人计算设备的用户密码。其密码的设置除满足本制度第三章外，还需满足：

1、 应设置开机密码、系统管理员用户密码、用户登录密码、屏幕保护密码；并定期更换。

2、 对于可直接远程连接到服务区的终端系统，应该设置 BIOS 开机系统。

5.10 信息系统变更管理

第 1 章. 细则

第一条 信息系统变更需求部门明确系统中变更类型、变更原因、变更过程、变更前评估等事项，再制定变更方案，并将需求整理成《信息系统变更申请表》，由部门负责人审批后提交给现代教育技术中心。

第二条 现代教育技术中心负责接受需求并上报给信息主管主任。主管主任分析需求，并提出系统变更建议,现代教育技术中心根据变更建议审批《信息系统变更申请表》。

第三条 现代教育技术中心根据部门提供的需求与软件开发商联系协同实现信息系统变更需求，产生供发布的程序。

第四条 现代教育技术中心组织相关业务部门的信息系统最终用户对系统程序变更进行测试，系统变更前，应对系统进行备份，并确保系统变更失败后能恢复到变更前的状态。

第五条 系统运维负责人应该事先建立变更失败恢复流程并组织进行变更失败的恢复演练。

第六条 应对变更过程进行控制，对变更影响进行分析并形成文档，要对变更实施过程进行记录，并妥善保存所有文档和记录。

第七条 现代教育技术中心出具信息系统变更验收报告，需求部门签字验收。

第八条 信息系统变更程序测试完成后，由现代教育技术中心配置完善信息系统，正式发布并通知需求部门。

5.11 备份与恢复管理

第 1 章. 系统备份

第一条 福州软件职业技术学院信息系统备份一般要求：

1. 备份可以采用程序自动进行、操作系统自动进行和手动进行 3 种方式；

2. 数据备份可采用全备、增量备份、差量备份相结合的方式，其中完全数据备份至少每天一次；对于重要数据、关键数据还需进行异地备份；

3. 数据备份介质主要采用磁盘；

4. 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；

5. 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

第二条 系统备份包括：应用系统操作程序备份、应用系统配置参数备份、应用服务器备份、应用数据库备份等。具体要求如下：

1. 应用系统操作程序备份一般要求：

- 对应用系统操作程序所在目录、应用系统操作程序所在系统注册信息进行整体复制或压缩复制，所备份的数据本地或异地单独存放；
- 应用系统安装程序及补丁程序应复制 2 套以上；
- 应详细记录应用系统操作程序安装过程，并随安装程序一起保存；
- 应用系统原始录入数据及其录入工具或方法随安装程序一起保存。

2. 应用系统配置参数备份一般要求：

- 应用系统配置参数备份应于本地或异地单独存放；
- 应用系统配置参数备份应注明有效期限和相关应用系统的信息。

3. 应用服务器备份一般要求：采用冗余备份技术或双机备份，并保证冗余设备与其操作系统、补丁的一致性。

4. 应用数据库备份一般要求：

- 若应用系统操作程序提供应用数据备份工具，则优先采用此工具进行数据备份，同时还应采用数据库管理软件所带数据备份工具进行数据备份；
- 应用数据库备份应包括数据表和文件仓库内容，两者必须保持一致并共同存放；
- 应用数据库备份必须标明所用应用系统操作程序信息和所用数据库管理软件版本信息。

第三条 资源服务器（包括磁盘阵列）数据备份一般要求：采用冗余技术；首次使用前必须进行 1 次整体备份，之后可以采用增量备份方式进行。

第四条 交换设备数据备份一般要求：定期将交换机内配置文件进行手动备份，每次升级及补丁安装均进行一次整体备份，备份文件异地存放。

第五条 安全保密产品备份要求：定期将防火墙、IDS 等安全保密产品的配置文件进行手工备份，备份文件异地存放。

第六条 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

第 2 章. 备份存放及管理

第七条 关键数据和重要数据备份除采用光盘外，必须采用能长期保存的磁带进行保存。

第八条 备份介质均须标明密级，按照有关规定进行存档，并保证其完整性和数据可靠性。

第九条 保存关键和重要数据备份介质的部门应考虑到可能发生的物理环境威胁（如火灾、水灾、地震等）对介质所带来的危害，必要时将关键和重要数据备份存储介质放置在其他建筑物内，防止在异常事故发生时被破坏。

第十条 每年定期对所存放的关键和重要数据备份存储介质进行内容检查，保证备份数据的有效性。

第 3 章. 系统恢复

第十一条 信息系统恢复一般原则：

1. 在进行数据恢复时应事先确定所恢复的时间,取离其时间最近的整体备份进行整体数据恢复，然后依时间顺序进行增量数据恢复；
2. 应用系统数据恢复采用先恢复应用系统操作程序,后恢复业务数据的方式进行；
3. 数据恢复必须进行有效性验证，确保数据可用；
4. 系统恢复严格按照相关策略文档操作步骤进行，不得跳过或篡改其步骤；
5. 在系统恢复期间严格注意数据保密，防止关键或重要数据泄密；
6. 应保证在 12 小时内对系统基本功能进行恢复或重建。

5.12 安全事件处置管理

第 1 章. 总则

第一条 为了明确福州软件职业技术学院信息安全事件的管理职责，规范对信息安全事件的管理流程，特制定本制度。

第二条 本制度旨在建立有效的信息安全弱点报告和处理机制，确保能及时发现弱点，迅速采取纠正措施，防患于未然，降低信息安全事件发生的概率。

第三条 安全事件等级划分参照《信息安全技术信息安全事件分类划分指南 GB/Z20986-2007》执行。

第 2 章. 安全事件处理流程

第四条 安全事件处置流程是：事件报告→事件受理→事件处理→事后总结。

第五条 安全事件报告程序：

1、发现一般安全事件时，由现代教育技术中心受理并记录归档、安全事件处理人员进行处理，并上报相关负责人；

2、发现较大安全事件时，首先报现代教育技术中心主任，由安全事件处理人员进行事件处理，处理完毕上报相关负责人；

3、发现重大安全事件或特别重大安全事件时，应报福州软件职业技术学院领导及相关负责人，联系维护支撑单位协助处理安全事件，处理完毕上报福州软件职业技术学院领导及相关负责人。

4、发现信息泄露事件时，除根据上述三个等级进行操作外，应报网络安全和信息化领导小组，由领导小组成员根据信息泄露主体、范围及影响程度等进行判断，考虑是否向保密、国家安全或公安部门报案。

第 3 章. 应急工作组职责

第六条 我单位应建立预警、应急响应和处置快速反应机制，确保各环节的衔接，做好人力、物力、财力储备，增强应急处理能力，保证一旦出现网络信息安全事故，能够迅速启动应急处置系统。

第七条 信息安全应急处置指挥办公室

1. 负责建立福州软件职业技术学院网络与信息安全事件监测预警、应急处置和应急响应机制，发布网络与信息安全事件预防警报，组织实施网络与信息安全事件应急处置；
2. 决定启动和终止应急预案；
3. 负责福州软件职业技术学院各部门的应急协调配合，负责与外单位相关部门的及协调配合；
4. 组织应急小组的应急处置行动；
5. 研究新闻发布方案；
6. 组织日常应急演练及培训；
7. 组织善后工作和网络与信息安全事件的调查工作；
8. 负责对应急预案进行评审: 当福州软件职业技术学院发生较大变革，或根据上次应急演练（应急响应）过程中得到的经验教训不定期进行应急响应预案的评，并根据实际情况进行修订，以适应当前最新的应急响应需要。评审周期每年不得少于一次。

第 4 章. 安全事件报告

第八条 当发生安全事故后，安全管理员应负责分析和鉴定安全事件产生的原因，收集证据，记录处理过程；总结经验教训，制定防止再次发生的补救措施，同时编制安全事件报告，向网络安全和信息化领导小组说明事件前因后果，并记入安全事件汇总表。

第九条 安全事件报告的内容应包含安全事件发生的时间、地点、值班人或当事人、事故现象、事故分析、处理情况、参与人员、和恢复时间等，因事故造成损失或影响的，应写明损失或影响程度。

第 5 章. 应急处置

第十条 如出现网络故障问题，网络管理员应迅速排查问题，解决不了的问题立即上报信息安全应急处置指挥办公室。由应急处置指挥办公室决定是否启动应急预案，

第十一条 应急响应

1. 应急处置指挥办公室做出启动应急预案的决策；
2. 应急处置指挥小组进入应急状态，履行应急处置工作的统一领导、指挥、协调职责。指挥部成员保持 24 小时联络畅通，必要时应立即到达指挥场所；
3. 应急处置人员迅速集中，在最短时间内到达事发现场，集结待命。

第十二条 处置措施步骤

1. 控制事态：应急处置指挥小组应分析和鉴定事件产生的原因，控制事态，防止事件进一步扩大；及时寻求电信、厂家等服务和设备供应商或者国家信息安全技术支持队伍的紧急支援；必要时应决定启动业务应急预案；
2. 做好安全消除隐患：应急处置人员分析和鉴定事件产生的原因，有针对性的采取措施，恢复受破坏信息系统正常运行；
3. 做好处置记录：应急处置人员在应急恢复过程中应保留有关证据，做好处置记录。

第 6 章. 培训演练

第十三条 每年信息安全应急指挥办公室应至少组织一次有关人员对各应急预案及应急流程进行培训和演练，同时做好相关记录。

第十四条 将网络与信息安全事件的应急知识等列为行政管理干部和相关人员的培训内容，加强网络与信息安全特别是网络与信息安全应急预案的培训，提高防范意识及技能。

第十五条 应急演练的目的是为了熟悉应急预案的流程与环节，检测预案的有效性，应急演练应符合以下规定：

1. 应急演练应制订详细的演练方案，保证演练的顺利进行。方案包括演练项目、演练目的、演练时间、演练范围、现场指挥、参与人员及其分工职责、系统备

份、操作步骤、系统切换时间、业务验证、系统恢复等内容，并附上演练操作记录表、演练结果（目标达成情况表）、方案改进完善建议表；

2. 应急演练方案应进行风险评估，确保演练不能影响系统正常运行；

3. 应急演练应涵盖应急计划中的所有内容，这些内容可分重点、分层次、分系统、分阶段定期进行；

4. 应急演练应当从流程和技术两方面尽量接近真实；

5. 应急演练过程应有完整的记录。

第十六条 应急演练结束后，应按照以下方面对其进行总结并提交报告：

1. 对应急准备状况进行评价，评价事项包括前期安排的制度学习、系统学习等方面的落实情况，以及应急资源就绪状况等方面的评估；

2. 对应急组织情况进行评价，评价事项包括对信息系统应急工作的组织领导、机构及人力资源设置、分工职责、计划安排等方面的评价；

3. 对应急操作能力进行评价，对技术人员在进行应急演练操作和处理应急演练过程中出现问题时所表现的熟练性和准确性进行评估；

4. 对应急硬件设备状况的评价，评价设备的运行状况以及配置能否达到预期的应急效果；

5. 对应急演练进行评价，主要对在方案规定的时间点内完成流程处理和技术操作进行总体评价；对存在问题出具整改意见和改进措施。

第 7 章. 应急工作组职责

第十七条 办公室应建立预警、应急响应和处置快速反应机制，确保各环节的衔接，做好人力、物力、财力储备，增强应急处理能力，保证一旦出现网络信息安全事故，能够迅速启动应急处置系统。

第十八条 信息安全应急处置指挥办公室

1. 负责建立福州软件职业技术学院网络与信息安全事件监测预警、应急处置和应急响应机制，发布网络与信息安全事件预防警报，组织实施网络与信息安全事件应急处置；

2. 决定启动和终止应急预案；

3. 负责福州软件职业技术学院各部门的应急协调配合，负责与外单位相关部门

的及协调配合；

4. 组织应急小组的应急处置行动；

5. 研究新闻发布方案；

6. 组织日常应急演练及培训；

7. 组织善后工作和网络与信息安全事件的调查工作；

8. 参与每年针对应急预案的修改讨论。

5.13 信息安全审计管理制度

第 1 章．工作职责

第一条 安全审计员的职责是：

- 制定信息安全审计的范围和日程；
- 管理具体的审计过程；
- 应定期对运行日志和审计数据进行分析，以便及时发现异常行为；
- 分析审计结果并提出对信息安全管理体系的改进意见；
- 召开审计启动会议和审计总结会议；
- 向主管领导汇报审计的结果及建议；
- 为相关人员提供审计培训。

第二条 评审员由审计负责人指派，协助主评审员进行评审，其职责是：

- 准备审计清单；
- 实施审计过程；
- 完成审计报告；
- 提交纠正和预防措施建议；
- 审查纠正和预防措施的执行情况。

第三条 受审员来自相关部门，其职责是：

- 配合评审员的审计工作；
- 落实纠正和预防措施；
- 提交纠正和预防措施的实施报告。

第 2 章．计划及实施

第四条 审计计划应包括审计的目的、审计的范围、审计的准则、审计的时间、主要参与人员及分工情况。每年应进行至少一次涵盖所有部门的审计；当进行重大变更后（如架构、业务方向等），需要进行一次涵盖所有部门的审计。

第五条 评审员需事先了解审计范围相关的安全策略、标准和程序；准备审计清单，其内容主要包括：需要访问的人员和调查的问题，需要查看的文档和记录（包括日志），需要现场查看的安全控制措施。

第六条 在进行实际审计前，召开启动会议，其内容主要包括：评审员与受审员一起确认审计计划和所采用的审计方式，如在审计的内容上有异议，受审员应提出声明（例如：限制可访问的人员、可调查的系统等）；向受审员说明审计通过抽查的方式来进行。

第七条 审计方式包括面谈、现场检查、文档的审查、记录（包括日志）的审查。

第八条 评审员应详细记录审计过程的所有相关信息。在审计记录中应包含下列信息：审计的时间、被审计的部门和人员、审计的主题 、观察到的违规现象、相关的文档和记录(比如操作手册、备份记录、操作员日志、软件许可证、培训记录等)、审计参考的文档（比如策略、标准和程序等）、参考所涉及的标准条款和审计结果的初步总结。

第九条 如怀疑与相关安全标准有不符合项的情况，审计员应记录所观察到的详细信息（如在何处、何时，所涉及的人员、事项，和具体的情况等）并描述其为什么不符合。关于不符合的情况应与受审员达成共识。

第十条 在每项审计结束时应准备审计报告，审计报告应包括：审计的范围、审计所覆盖的安全领域、审计结果的总结、不符合项（不符合项的具体描述和相关证据）、纠正和预防措施的建议。

第十一条 不符合项是指与等级保护基本要求不一致的情况。产生不符合项可能是由于与相关的规定不一致，包括：等级保护基本要求、信息安全策略、相关标准和程序、相关法律条款及福州软件职业技术学院的相关规定。

第 3 章．汇报、纠正和预防

第十二条　　召开审计总结会议，应总结汇报以下内容：

- 审计的目标和范围；
- 审计的时间；
- 参与审计的人员；
- 审计报告（包括纠正和预防措施的建议）；
- 提交审计报告的副本供受审员参考；
- 受审员可对审计报告提出任何疑问。

第十三条　　受审员应该制定计划从而纠正和预防审计报告中发现的安全隐患，受审员应在规定时间内向评审员提交纠正和预防措施的实施报告。

第十四条　　评审员应在受审员提交报告的 3 个月内，审计纠正和预防措施的实施状况。审计纠正和预防措施应包括：面谈、现场检查、文档的审查以及记录（包括日志）的审查。

第十五条　评审员根据受审员提交的纠正和预防措施实施报告，收集、记录和审查相关证据并审阅和分析所有审计结果。

5.14 信息资产分类和标识管理规定

第 1 章．信息资产分类

第一条 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、分级和实施相应的保护措施，需从安全责任划分资产所有者（或所有部门）、维护者以及使用者，并填写《信息资产登记表》。

第二条 信息资产按形式不同可以分为五类：数据和文档资产、软件资产、实物资产、人员资产和服务资产。其中数据和文档资产主要包括业务数据和记录、各类管理制度、管理文档、办公文档以及外来的数据文件等。具体如下：

1. 数据和文档资产：通常包括各种电子档：业务数据、配置文件、记录数据（日志、审计记录）、管理文件（策略、流程文件、操作手册等）、商务文件（合同、协议等）以及外来数据文件等。也包括以实物方式存在的资产：各类电子数据

的归档、打印件、书面管理文件、业务报表、包含重要商业成果的文件，还有胶片等；

2. 软件资产：各种系统软件、应用软件（OA、业务软件等）和工具软件（开发系统、网管软件、安全软件等），包括操作系统、数据库应用程序、网络软件、办公应用系统、业务系统程序、软件开发工具等，这些软件资产负责处理、存储或传输各类信息；

3. 实物资产：与业务相关的 IT 物理 设备，包括计算机（工作站和服务器等）和网络通信设备、磁介质（磁带和磁盘等）、装置、环境等，这些实物资产容纳着软件和数据文件；

4. 人员资产：承担某项与业务活动相关责任的角色和职位。例如普通用户、系统管理员、网络管理员、有合同约束的保安、清洁员等，这些人员与各类数据、软件和实物资产的操作直接相关；

5. 服务资产：安保（例如监控、门禁、保安等），环境服务（例如清洁），基础保障（供水、供热、供电），设备维护，通信服务（例如互联网接入）。

第三条 信息资产分级，根据各类信息资产在保密性 C、完整性 I 和可用性 A 三个方面所表现出的不同的重要程度，划分为五个级别。从保密性角度，从高到低分别为：绝密、机密、秘密、内部和公开。

1. 绝密

- 保密性：其包含福州软件职业技术学院最重要的秘密，关系未来发展的前途命运，对福州软件职业技术学院根本利益有着决定性的影响，如果泄露会造成灾难性的损害；
- 完整性：完整性价值极高，未经授权的修改或破坏会对福州软件职业技术学院造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补；
- 可用性：可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度 99.9%以上，或系统不允许中断。

2. 机密

- 保密性：包含福州软件职业技术学院的重要秘密，其泄露会使福州软件职业技术学院的安全和利益受到严重损害；

- 完整性：完整性价值较高，未经授权的修改或破坏会对福州软件职业技术学院造成重大影响，对业务冲击严重，较难弥补；
- 可用性：可用性价值较高，合法使用者对信息及信息系统的可用度达到每天90%以上，或系统允许中断时间小于 10 分钟。

3. 秘密

- 保密性：福州软件职业技术学院的一般性秘密，其泄露会使福州软件职业技术学院的安全和利益受到损害；
- 完整性：完整性价值中等，未经授权的修改或破坏会对福州软件职业技术学院造成影响，对业务冲击明显，但可以弥补；
- 可用性：可用性价值中等，合法使用者对信息及信息系统的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于 30 分钟。

4. 内部

- 保密性:仅能在福州软件职业技术学院内部或在福州软件职业技术学院内某一部门内公开的信息,向外扩散有可能对福州软件职业技术学院的利益造成轻微损害；
- 完整性：完整性价值较低，未经授权的修改或破坏会对福州软件职业技术学院造成轻微影响，对业务冲击轻微，容易弥补；
- 可用性：可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60 分钟。

5. 公开

- 保密性：可对社会公开的信息，公用的信息处理设备和系统资源等；
- 完整性：完整性价值非常低，未经授权的修改或破坏会对福州软件职业技术学院造成的影响可以忽略，对业务冲击可疑忽略；
- 可用性：可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%。

第 2 章．敏感性标识

第四条 纸质文档的敏感性标识

1. 纸质文档的敏感性标识采用印章方式；

2. 纸质文档所有者或管理者负责对该文档盖章，部门信息安全管理员负责指导；

3. 印章分为“绝密”、“机密”、“秘密”、“内部”和“公开”五种；

4. 每个部门至少配备“绝密”、“机密”、“秘密”和“公开”四个印章各一个；印章由部门信息安全管理员保管；

5. 印章应盖在纸质文档封面的右上角。一份文档只需要在文档封面盖一个印章；一册记录的只需要在本册的第一页上盖一个印章；

6. 盖完章后，在“密级”栏后的空白处，手工填写保密期限（例如“1 年”、“3 年”、“5 年”、“长期”等）和生效时间；

7. 产生或接收到新的纸质文档时，要及时盖章；

8. 打印或复印的具有敏感性标识的文档，无需盖章。

第五条 电子信息的敏感性标识

1. 电子文档的敏感性级不应直接在文件模板中注明；

2. 电子文档所有者或管理者负责在文档模板中添加敏感性级别，部门信息安全管理员负责指导；

3. 电子文档敏感性级别分为“绝密”、“机密”、“秘密”、“内部”和“公开”五种；

4. 电子文档应该在文档的封面上标识其敏感性级别；

5. 电子表格模版应该在表格的页眉内标识其敏感性级别，如“密级”、“生效时间”等内容；

6. 电子表格编写人员可根据实际情况调整所编写电子表格的密级，但不能修改电子表格的生效时间。

第六条 存储了秘密级以上信息的移动介质或备份介质（如优盘 、移动存储卡、磁盘、磁带 、光盘等），在条件允许的情况下，应采用盖章或张贴敏感性标识不干贴等方式进行标识。

第七条 软件类资产在条件允许的情况下，应该在关键界面上添加敏感性标识电子标签。

第八条 针对硬件设备、环境设施等实物资产，原则上不进行敏感性标识，仅标识相应设备的基本序列等信息。

第九条 所属密级应记录在相应文档。

第 3 章．信息使用控制

第十条 实物资产的使用

1. 资产的接收和发出

- 实物资产的接收和发出按固定资产管理方面的管理规定执行；
- 接收到新的信息资产后，由部门信息安全管理员对信息资产敏感性进行标识；
- 信息资产发生变化时（新增、删除、变更），部门信息安全管理员应及时更新《信息资产登记表》。

2. 新增的硬件和与 IT 相关的环境设施在经过必要的安装、配置和性能调优后，才能并入福州软件职业技术学院的网络系统。

3. 需要对主干网络、主机、网络设备、安全设备和 UPS 等重要环境设施的性能和运行状况进行日常监控和维护。

4. 控制的所有硬件类资产都应按照《办公区域安全管理规定》进行保护，机房内的设备要按照《机房安全管理制度》的规定进行保护。

5. 未经批准，资产不得随意移动位置或带出福州软件职业技术学院的物理安全区域。

第十一条 软件类资产的使用

1. 福州软件职业技术学院办公计算机不得使用未经批准的软件，系统软件应根据需要及时进行补丁更新；

2. 计算机采取必要的措施防范病毒、木马和流氓软件等恶意程序；

3. 采购软件类资产，要选择软件开发商，进行软件测试，必要时要进行原代码审查，以确保采购软件安全；

4. 所有存储软件的介质应当妥善保存，并登记入册。

第十二条 服务资产的使用要防止资源的浪费和节约能源，如占用网络带宽进行与工作无关的下载，下班后不关电脑、照明、空调等的电源。

第十三条 严禁职工在未经允许的情况下，利用任何手段将涉密文件及内容制作成电子形式在办公自动化系统内或以其他方式进行传输。

第十四条 秘密级以上信息的使用应受到严格控制，文件的接收人应按信息的使用目的、使用范围进行正确使用，未经许可不得向他人公开和传播。

第十五条 秘密级以上文件，如无特别规定，原则上应在使用后及时进行回收、归档及保存或者实施废弃。废弃秘密级以上文件时，纸类媒体可用粉碎的方法 ，其它媒体可用初始化或破坏媒体的方法处理。

第十六条 应定期对信息资产进行风险评估，如果信息资产 CIA 各属性值发生变化。应按照新的属性值进行对应的处理和保护。

5.15 个人信息保护管理规定

第一条 为了保护福州软件职业技术学院的新 OA 系统用户的合法权益，维护网络信息安全，依据《中华人民共和国个人信息保护法》《中华人民共和国电信条例》《电信和互联网用户个人信息保护规定》等，制订本制度。

第二条 福州软件职业技术学院提供网络信息服务过程中，有收集、使用用户个人信息的网络应用平台，适用于本制度。

第三条 本制度所称用户个人信息，是指新 OA 系统在提供服务过程中收集的重要个人信息如：用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息，以及用户使用服务的时间、地点等信息。

第四条 新 OA 系统在提供信息服务过程中，收集、使用用户个人信息，应当遵循合法、正当、必要的原则。

第五条 新 OA 系统对收集、使用的用户个人信息的安全负责，应明确和落实相关人员安全管理责任，对工作人员实行权限管理，对批量导出、复制、销毁信息实行审查，并采取防泄密措施。

第六条 新 OA 系统未经用户同意，不得收集、使用用户个人信息，如确需用户提供个人信息，应明确告知用户使用的目的、方式、范围和救济渠道，并告知拒绝提供信息的后果。

第七条 新 OA 系统收集、使用用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供，不得与他人谈论用户个人信息内容。

第八条 福州软件职业技术学院对用户个人信息保护工作实施监督管理，新 OA 系统保管的用户个人信息发生泄露、毁损或者丢失，造成或者可能造成严重后果的，应及时通报福州软件职业技术学院安全领导小组进行调查和应急处置。

第九条 新 OA 系统保管的用户个人信息因泄露、篡改、毁损或者丢失，对我单位工作带来不利影响的，参照《信息公开违规违法行为责任追究制度》办理。

第十条 新 OA 系统应积极接受公民、法人和其他社会组织的批评、意见和建议。

第十一条 本制度由福州软件职业技术学院负责解释，自发布之日起开始实施。

附录

1. 福州软件职业技术学院网络安全管理评审表

申请日期：　　编号：

文件名称			
文件编号		版本	
增加、变更内容概要：			
现代教育技术中心意见	签字： 日期：		
网络安全工作领导小组审查意见	签字： 日期：		
备注			

2. 福州软件职业技术学院网络安全管理制度收发登记表

编号	制度名称	版本	发布范围	发布时间	签发部门/单位	备注

3. 福州软件职业技术学院信息系统授权审批表

<table>
<tr><td>使用部门</td><td colspan="3"></td></tr>
<tr><td>联系电话</td><td></td><td>申请日期</td><td></td></tr>
<tr><td>授 权
性 质</td><td colspan="3">☐ 系统投入使用 ☐访问控制变更 ☐管理员账户设置
☐ 策略配置变更 ☐业务账户设置 ☐内网接入
☐数据访问及拷贝 ☐其他_____</td></tr>
<tr><td>授 权
期 限</td><td colspan="3"></td></tr>
<tr><td colspan="4">申请权限要求：</td></tr>
<tr><td colspan="4">申请理由：</td></tr>
<tr><td colspan="4">现代教育技术中心意见：

签名： 日期：</td></tr>
<tr><td colspan="4">执行记录</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">其他设置</td></tr>
<tr><td>执行人</td><td></td><td>执行日期</td><td></td></tr>
</table>

4. 福州软件职业技术学院会议记录

部门： _____ **日期：** _____

会议名称			
会议时间			
会议地点			
会议主持			
出席人员：			
缺席人员： ☐ 无 ☐ 有 人员： 原因：☐因事请假 ☐出差在外 ☐无故不参加 ☐其他			
会议内容：			
遇到问题及解决方案：			
会议记录人		负责人签署	

5. 福州软件职业技术学院上网帐号、IP 地址申请表

编号：

<table>
<tr><td colspan="2">单位/部门</td><td colspan="3"></td></tr>
<tr><td rowspan="3">用户填写</td><td>姓名</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>位置(房间号)</td><td colspan="3"></td></tr>
<tr><td>墙信息端口编号</td><td></td><td>MAC 地址</td><td></td></tr>
<tr><td rowspan="4">单位网管填写</td><td>IP 地址</td><td></td><td>子网掩码</td><td></td></tr>
<tr><td>默认网关</td><td></td><td>DNS</td><td></td></tr>
<tr><td>用户名</td><td></td><td>密码</td><td></td></tr>
<tr><td>开通日期</td><td></td><td>经办人</td><td></td></tr>
<tr><td>用户入网责任书</td><td colspan="4">本人申请接入福州软件职业技术学院网，保证入网后遵守国家有关法律、法规及福州软件职业技术学院网络管理的相关规定，不在网上从事危害国家安全、泄露国家机密等违法犯罪活动；不查阅、复制和传播妨碍社会治安及淫秽黄色的信息；不向他人发送恶意的、挑衅性的文件；不利用福州软件职业技术学院网从事妨害网络正常运行、管理的活动；不盗用他人的帐号以及 IP 地址等信息。本人将妥善保管好帐号和密码，不转借他人使用，如果出现利用本人帐号从事任何违反网络规定的活动，本人将承担全部责任，接受有关单位的处罚。

用户签名：
年　　月　　日</td></tr>
<tr><td>说明</td><td colspan="4">1．用户需安装“福州软件职业技术学院网上网客户端”，经认证通过后方能使用网络。</td></tr>
</table>

本表一式两份，单位网络管理员在办理后一份交还用户，一份整理入档备查。

6. 福州软件职业技术学院邮件账号申请表（单位用户）

流水号：MD

单 位 名 称					
负 责 人		职 务		联系电话	
使用人姓名		性 别		联系电话	
帐 号★		E-mail 地址★			

用 户 责 任 书

1、遵守国家福州软件职业技术学院关于 XX 的各项法律法规和规章制度。

2、遵守所有使用电子邮箱服务的网络协议、规定、程序和惯例。

3、未经接收信件人的允许，用户不能利用电子邮箱服务作连锁邮件、分发垃圾邮件或分发任何商业、非商业电子邮件。

4、电子邮箱及网络存储空间不得作非法用途。不得利用电子邮箱进行干扰或混乱网络服务、散布谣言、传播病毒，影响其它用户正常使用。

5、用户应自行妥善保管好账号、密码，不得转借他人使用。

本单位保证自觉遵守以上条款，负责人将承担由自身行为导致的一切后果及损失。

负责人签名：　　（单位盖章）

年　月　日

注：

1、本表格用蓝黑或黑色钢笔填写，必须保证所提供信息的准确性和真实性。

2、★部分为现代教育技术中心填写。

以上表格须完整填写，否则不予受理（本表格复印有效）。

7. 福州软件职业技术学院邮件账号申请表(个人用户)

流水号：MG

姓　　名		性　别	
证件类别	□工作证　　□身份证	证件编号	
所在单位		联系电话	
帐　号★		E-mail 地址★	

用　户　责　任　书

1、遵守国家各项法律法规和福州软件职业技术学院的各项规章制度。

2、遵守所有使用电子邮箱服务的网络协议、规定、程序和惯例。

3、未经接收信件人的允许，用户不能利用电子邮箱服务作连锁邮件、分发垃圾邮件或分发任何商业、非商业电子邮件。

4、使用电子邮箱及网络存储空间不得作非法用途。不得利用电子邮箱进行干扰或混乱网络服务、散布谣言、传播病毒，影响其它用户正常使用。

5、用户应自行妥善保管好账号、密码，不得转借他人使用。

我保证自觉遵守以上条款，并承担由自身行为导致的一切后果及损失。

用户签章：

年　　月　　日

备注：

1、本表格用蓝黑或黑色钢笔填写，必须保证所提供信息的准确性和真实性。

2、★部分为现代教育技术中心确认填写。

3、以上表格须完整填写，否则不予受理（本表格复印有效）。

8. 福州软件职业技术学院外联人员联系方式

项目名称	单位/学院名称	联系人		联系电话/邮箱	备注
		岗位	姓名		

9. 福州软件职业技术学院管理人员配置表

序号	岗位名称	姓名	部门	是否专职	备注说明
1	机房管理员				
2	系统管理员				
3	数据库管理员				
4	网络管理员				
5	安全管理员				
6	资产管理员				
7					
8					
9					
10					

填表日期：

10. 福州软件职业技术学院保密协议书

根据《中华人民共和国保守国家秘密法》、《科学技术保密规定》以及《福州软件职业技术学院保密工作暂行条例》等相关规定，为保守国家秘密、技术秘密及其它不宜公开的内容等，甲方(福州软件职业技术学院)与乙方( )达成如下协议：

保密期限为____年。甲方按照相关规定负责论文的管理。甲乙双方在涉密未解密之前，不得向知悉范围外的任何单位或个人以任何方式（直接、间接、口头或书面等形式）泄露所掌握的秘密事项。

凡违反本协议规定泄露国家秘密或内部秘密者，须承担相应涉密责任，后果严重者，甲方将保留依法追究其刑事责任的权利。

本协议一式两份，双方各执一份。

本协议自双方签字之日起生效，至论文解密之日起自动终止。

甲方委托人　　乙方委托人（签字）

培养单位保密责任人：

（签字）

日期：　　年　　月　　日　　日期：　　年　　月　　日

11. 福州软件职业技术学院网络管理和网络安全责任书

为了切实加强福州软件职业技术学院各部门的网络管理和网络安全规范，增强全体人员上网的法制意识、责任意识、政治意识、自律意识和安全意识，引导开展健康、文明的网上活动，形成全体人员共同抵制网上有害信息的良好氛围，为全面推进素质教育，维护福州软件职业技术学院和社会政治稳定，实现福州软件职业技术学院网络信息内容安全状况的明显好转，推进网络精神文明建设，创造良好的福州软件职业技术学院网络环境。根据《福州软件职业技术学院计算机网络管理办法》、《福州软件职业技术学院网络安全保护管理办法》、《福州软件职业技术学院计算机网络安全管理规定》、《福州软件职业技术学院网电子公告类栏目安全管理暂行办法》、《福州软件职业技术学院互联网上网场所管理规定》和《福州软件职业技术学院关于对员工计算机网络安全违纪处理的暂行规定》等网络管理规章制度的规定，福州软件职业技术学院下属各个职能部门与福州软件职业技术学院第一责任人签订如下安全责任书：

一、福州软件职业技术学院内凡提供上网的开放或公用计算机机房、微机，只能接入福州软件职业技术学院网，纳入福州软件职业技术学院网的统一管理，并由福州软件职业技术学院网提供统一的网络出口。

二、福州软件职业技术学院内任何单位的网络机房不得擅自租用独立专线连网。如确因工作需要或特殊原因需建立上网场所或租用独立专线连网的，须经福州软件职业技术学院审批同意。

三、福州软件职业技术学院内任何单位必须自觉遵守国家法律和行政法规，不得利用福州软件职业技术学院网危害国家安全、泄露国家秘密，不得侵犯国家、社会、集体的利益和公民的合法权益，不得从事违法犯罪活动。应当服从福州软件职业技术学院保卫处和现代教育技术中心的管理和监督检查，并对上网用户违反规定的行为负有监督、举报和停止为其服务的责任。

四、福州软件职业技术学院内任何单位上网用户不得从事下列危害网络安全的行为：

1. 制作或者故意传播计算机病毒程序以及其他破坏性程序；

2. 非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序；

3. 法律、行政法规禁止的其他行为。

五、福州软件职业技术学院内任何单位上网用户不得利用福州软件职业技术学院的计算机信息系统制作、传播、查阅和复制下列信息内容：

1. 煽动抗拒、破坏宪法和法律、行政法规实施的；

2. 煽动颠覆国家政权，推翻社会主义制度的；

3. 煽动分裂国家、破坏国家统一的；

4. 煽动民族仇恨、民族歧视，破坏民族团结的；

5. 捏造或歪曲事实，散步谣言，扰乱社会秩序的;

6. 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

7. 公然侮辱他人或者捏造事实诽谤他人的；

8. 损害国家机关信誉的；

9. 其他违反宪法和法律、行政法规的。

六、 福州软件职业技术学院内任何单位必须遵守以下规定：

1. 建立健全网络安全管理制度，逐级落实责任制，设置专职人员负责网络安全管理人员，检查网络安全。

2. 开展网络信息服务的单位，要建立健全上网用户日志记录留存制度，必须做好上网实名登记，记录有关上网信息，记录备份应当保存 90 日，并在保卫处和现代教育技术中心等网络安全监察部门依法查询时主动予以提供。

3. 电子公告服务信息巡查、个人主页信息审查制度，链接网站和聊天室有害信息检查管理制度以及发现有害信息立即向主管单位报告制等。

4. 不得擅自出租、转让计算机上网场地，随意更换安全管理人员。

5. 不得使用含有色情、赌博、暴力、愚昧、迷信等不健康内容的电脑游戏。

6. 落实网络安全管理制度和措施。

7. 落实消防安全管理责任和措施。

8. 承担教育辅导上网用户的义务。让用户阅读了解有关规章制度，对用户上网过程及时监督教育，保持文明上网的良好风气。

七、 福州软件职业技术学院内任何单位必须设立专职人员负责网络安全检查，对于上网场所发生的安全事故或者违法案件，福州软件职业技术学院内任何单位和安全责任人应当在 24 小时内向现代教育技术中心报告，配合查处。

八、 福州软件职业技术学院内任何单位上网场所，应当主动接受现代教育技术

中心网络安全监察部门的安全监督、管理、检查，积极配合现代教育技术中心做好技术防范工作。

福州软件职业技术学院　　_____ 负责人

主 任（签章）：　　负责人（签章）：

年　　月　　日　　年　　月　　日

12. 福州软件职业技术学院离岗人员安全处理记录

离岗人签字：　　年　月　日

<table>
<tr><td>姓名</td><td></td><td>部门</td><td></td><td>离岗日期</td><td></td></tr>
<tr><td colspan="6">离岗类型（请在变动项目前打勾√，可以复选，如果选其他请说明情况）：
□终止劳动合同　□辞职　□解除劳动合同　□外部调动　□退休　□其他</td></tr>
<tr><td colspan="6">移交有关工作资料情况（工作内容、方法、结果及相关资源等，如空白处不够另附页）

接收人/日期：　　监交人/日期：</td></tr>
<tr><td colspan="3">借款归还情况：

出纳员/日期：</td><td colspan="3">固定资产、出入身份证件、徽章等归还情况：

安全管理员/日期：</td></tr>
<tr><td colspan="3">邮箱、FTP、支持服务平台、内部系统等变更情况：

网络管理员/日期：</td><td colspan="3">档案、钥匙及其他物品归还情况：

人事部/日期：</td></tr>
<tr><td>办理结果</td><td colspan="5">确认的项目后打勾，并写明详细情况（日期、金额、原因等），没有的项目划掉

从通讯录中删除　　人事信息系统更新
本月出勤天数　　本月工资
人事档案调出日期
户口迁移日期　　党组织关系转移日期
出具解除劳动合同证明　　其他

经办人签字/日期：　　分管领导签字/日期：</td></tr>
<tr><td colspan="6">备注</td></tr>
</table>

说明：监交人一般为移交人之直接上级。

13. 福州软件职业技术学院离岗人员保密承诺书

本人了解有关保密法规制度，知悉应当承担的保密义务和法律责任。在此庄重承诺：

一、认真遵守国家保密法律法规和福州软件职业技术学院保密规章制度，履行保密义务。

二、不以任何方式泄露所接触、知悉的国家秘密和商业秘密。

三、已全部清退不应由个人持有的各类国家秘密及商业秘密载体。

四、未经原单位审查批准，不擅自发表涉及原单位未公开工作内容的文章、著述。

五、自愿接受脱密期管理，自　　年　　月　　日至　　年　　月　　日服从有关部门的保密监管。

违反上述承诺，自愿承担党纪、政纪责任和法律后果。

承诺人签名：

年　　月　　日

14. 福州软件职业技术学院内单位网站（主页）备案表

申请日期：　　年　　月　　日

<table>
<tr><td>网站域名</td><td colspan="2"></td><td>所属单位</td><td></td></tr>
<tr><td rowspan="2">责任人</td><td>姓　　名</td><td></td><td>E—mail</td><td></td></tr>
<tr><td>办公电话</td><td></td><td>手　　机</td><td></td></tr>
<tr><td rowspan="2">网管员</td><td>姓　　名</td><td></td><td>E—mail</td><td></td></tr>
<tr><td>办公电话</td><td></td><td>手　　机</td><td></td></tr>
<tr><td>网站用途</td><td colspan="4"></td></tr>
<tr><td rowspan="8">网站链接
地　　址</td><td colspan="4">☐　存放在福州软件职业技术学院 Web 主页服务器上</td></tr>
<tr><td>目录名</td><td></td><td>操作帐号</td><td></td></tr>
<tr><td colspan="4">☐　连接至指定主机</td></tr>
<tr><td>IP 地址</td><td></td><td>开放服务端口</td><td></td></tr>
<tr><td>CPU</td><td></td><td>内存</td><td></td></tr>
<tr><td>硬盘</td><td></td><td>MAC 地址</td><td></td></tr>
<tr><td>操作系统</td><td></td><td>计算机名</td><td></td></tr>
<tr><td rowspan="2">构建方式</td><td>网页技术</td><td colspan="3">☐静态 HTML
☐动态：　☐ASP　☐PHP　☐CGI　☐PERL　☐其它 _____</td></tr>
<tr><td>数据库</td><td colspan="3">☐无　☐ACCESS　☐MYSQL　☐MSSQL　☐其它 _____</td></tr>
<tr><td>单位负责人签字
（加盖单位章）</td><td colspan="4"></td></tr>
<tr><td>福州软件职业技术学院审核意见</td><td colspan="4"></td></tr>
<tr><td colspan="5">注意事项：
1. 凡在福州软件职业技术学院网上发布的信息，必须真实可靠，内容健康，不得有其他违反规定的内容和链接，不得私自设置聊天室、论坛、广告和电子公告版(BBS)等栏目。
2. “单位负责人”为本网站（页）的内容审核人，对网站的内容负责。
3. 现代教育技术中心只提供托管服务器空间和技术支持，对网站的内容不承担任何责任。</td></tr>
</table>

填表须知：

1. 备案表应采用打印填写，字迹务必工整、清楚；填写完后，应由单位负责人签字，并加盖本单位公章；
2. 若备案表中的有关信息发生变更，需重新填写备案表。

3. 该备案表一式两份，一份交现代教育技术中心办理开通，一份本单位留存。

15. 福州软件职业技术学院信息门户平台二级网站报备表

编号：

<table>
<tr><td>部门</td><td colspan="4"></td></tr>
<tr><td rowspan="2">网络安全
责任人</td><td>姓　　名</td><td></td><td>工　　号</td><td></td></tr>
<tr><td>办公电话</td><td></td><td>联系电话（手机）</td><td></td></tr>
<tr><td rowspan="2">网络安全
管理员 1</td><td>姓　　名</td><td></td><td>工　　号</td><td></td></tr>
<tr><td>办公电话</td><td></td><td>联系电话（手机）</td><td></td></tr>
<tr><td rowspan="2">网络安全
管理员 2</td><td>姓　　名</td><td></td><td>工　　号</td><td></td></tr>
<tr><td>办公电话</td><td></td><td>联系电话（手机）</td><td></td></tr>
<tr><td colspan="5">二级网站安全责任书
本单位自愿在信息门户平台上申请二级网站，申请的网站主要用途为：发布本单位对外宣传的信息。本单位保证网站发布的信息权威与真实，并及时维护与更新网站内容，不在网站上发布违反国家、福州软件职业技术学院规定的互联网网络安全内容和商业性广告链接。门户信息平台以发布信息文档为主，不提供音乐、视频类的大型文件下载。</td></tr>
<tr><td>二级网站域名</td><td colspan="4"></td></tr>
<tr><td>单位负责人签字
（加盖单位章）</td><td colspan="4">年　　月　　日</td></tr>
<tr><td>福州软件职业技术学院
审核意见</td><td colspan="4">年　　月　　日</td></tr>
<tr><td colspan="5">注意事项：
1. 本表格填写应真实、详尽，信息门户平台上的帐号和密码与统一身份认证系统工号联动。
2. “网络安全负责人”为本网站（页）的内容审核人，对网站建设框架和信息内容负全责。
3. 二级网站域名的命名关系到本单位网站形象，请勿随意起名。
4. 若备案表中的有关信息发生变更，需重新填写备案表。
5. 该报备表一式两份，一份交现代教育技术中心备案，一份本单位留存。</td></tr>
</table>

16. 福州软件职业技术学院培训记录表

日期：

培训主题		培训教师	
培训地点		培训时间	
培训内容提要	培训内容摘要：		
参加培训人员名单			
备注：			

表格编号：

17. 福州软件职业技术学院人员考核记录

考核内容					
考核时间		考核岗位		考核人员	
考核项目（安全知识、安全技能、关键岗位特殊考核内容）：					
考核成绩（可附件）：					
综合评价：					

18. 福州软件职业技术学院外来人员进出机房申请表

<table>
<tr><td>外来人员姓名</td><td></td><td>外来单位名称</td><td></td></tr>
<tr><td>日期</td><td></td><td>进入时段</td><td></td></tr>
<tr><td>联系电话</td><td></td><td>是否携带设备</td><td></td></tr>
<tr><td colspan="4">带入/出设备情况/接入内网网情况说明：</td></tr>
<tr><td colspan="4">特殊访问需求：</td></tr>
<tr><td colspan="4">本人作为外部人员访问福州软件职业技术学院重要设备及信息系统，承诺遵守有关的各项安全管理及保密规定，包括但不限于：
一、未经福州软件职业技术学院方许可，不得将设备配置、网络拓朴、运维记录、扫描结果、项目文档、数据信息等福州软件职业技术学院内部信息、资料对外传播或泄露。
二、未经福州软件职业技术学院方许可，不得将系统帐号、密码和相关权限与他人共用，亦要防止意外泄露。
三、自觉遵守进出机房的相关管理规定。
四、自觉接受系统运维操作等相关安全审计和网络安全检查。
即日起，如因违反上述规定，造成网络安全事故或不良影响，本人愿承担相应的责任及法律后果。

申请人签字：　　日期：</td></tr>
<tr><td colspan="4">申请部门领导意见：

签字：　　日期：</td></tr>
<tr><td colspan="4">现代教育技术中心意见：

年　　月　　日</td></tr>
<tr><td>账号信息</td><td>账号</td><td></td><td>IP 地址</td><td></td></tr>
</table>

19. 福州软件职业技术学院机房设备_____操作日志登记表

日期	设备名称	操作员	操作记录	安全管理员审核签字

注：本表填写内容包括：

1、机房内重要设备配置更改，表头填写“配置更改”；

2、机房内重要设备漏洞及补丁更新，表头填写“漏洞及补丁更新”

3、机房内重要设备数据备份及恢复记录，表头填写“备份与恢复”

20. 福州软件职业技术学院机房巡检日志

<table>
<tr><td colspan="5">班内时间记录及异常情况汇总</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td rowspan="12">服务器</td><td rowspan="9">xxx 服务器</td><td>故障指示灯</td><td>正常 异常</td><td>备注</td></tr>
<tr><td>操作系统日志</td><td>正常 异常</td><td rowspan="9"></td></tr>
<tr><td>数据库日志</td><td>正常 异常</td></tr>
<tr><td>RAMN 备份情况</td><td>正常 异常</td></tr>
<tr><td>归档空间大小</td><td>G</td></tr>
<tr><td>设备使用情况</td><td>CPU 内存</td></tr>
<tr><td>数据库日志</td><td>正常 异常</td></tr>
<tr><td>归档空间大小</td><td>G</td></tr>
<tr><td>设备使用情况</td><td>CPU 内存</td></tr>
<tr><td rowspan="2">XXX 日志服务器</td><td>归档空间大小</td><td>G</td><td>备注</td></tr>
<tr><td>设备使用情况</td><td>CPU 内存</td><td rowspan="4"></td></tr>
<tr><td rowspan="2">数据库审计服务器</td><td>归档空间大小</td><td>G</td></tr>
<tr><td>设备使用情况</td><td>CPU 内存</td></tr>
<tr><td>XXX 病毒服务器</td><td>更新情况</td><td></td></tr>
<tr><td rowspan="2">交换机</td><td>核心交换机 XXX</td><td>指示灯</td><td>正常 异常</td><td>备注</td></tr>
<tr><td>汇聚层交换机</td><td>指示灯</td><td>正常 异常</td><td rowspan="5"></td></tr>
<tr><td rowspan="2">存储</td><td>EMC</td><td>指示灯</td><td>正常 异常</td></tr>
<tr><td>容灾 EMC</td><td>指示灯</td><td>正常 异常</td></tr>
<tr><td rowspan="2">防火墙</td><td>XXX 防火墙</td><td>指示灯</td><td>正常 异常</td></tr>
<tr><td>入侵检测</td><td>指示灯</td><td>正常 异常</td></tr>
<tr><td rowspan="2">门禁系统</td><td rowspan="2">XXX 门禁系统</td><td>运行情况</td><td>正常 异常</td><td rowspan="2"></td></tr>
<tr><td>日志信息</td><td>正常 异常</td></tr>
<tr><td colspan="3">检查日期： 年 月 日 时 检查者：</td><td>复查者：</td></tr>
</table>

21. 福州软件职业技术学院介质管理记录表

介质标识名	归档记录	借用人	领用时间	归还时间	备注

22. 福州软件职业技术学院介质销毁(送修)审批单

<table>
<tr><td>申请人</td><td colspan="2"></td></tr>
<tr><td rowspan="5">介质记录
信息</td><td>名　称</td><td>编　号</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">销毁（送修）原因</td><td colspan="2"></td></tr>
<tr><td colspan="2">签名：　　日期：　　年　　月　　日</td></tr>
<tr><td rowspan="2">现代教育技术中心审批意见</td><td colspan="2"></td></tr>
<tr><td colspan="2">签名：　　日期：　　年　　月　　日</td></tr>
<tr><td rowspan="2">处理办法</td><td colspan="2"></td></tr>
<tr><td colspan="2">签名：　　日期：　　年　　月　　日</td></tr>
<tr><td>备注</td><td colspan="2"></td></tr>
</table>

23. 福州软件职业技术学院物资采购审批表

<table>
<tr><td rowspan="2">请购
部门</td><td>物品名称（及个数）</td><td></td><td>存放地点</td><td></td></tr>
<tr><td>理由功能
要　求</td><td colspan="3">部门：　　主任：　　年　月　日</td></tr>
<tr><td>财务部门</td><td>预算安排情况</td><td colspan="3">主任：　　年　月　日</td></tr>
<tr><td rowspan="2">主
管
部
门</td><td>经济、技术
可行性测试
（简要）</td><td colspan="3" rowspan="2">（可靠性、安全性、节能性、耐用性等）

科长：　　年　月　日</td></tr>
<tr><td>预算
金额</td></tr>
<tr><td>审计部门</td><td colspan="4"></td></tr>
<tr><td>分管领导</td><td colspan="4"></td></tr>
<tr><td>采购小组
综合意见</td><td colspan="4"></td></tr>
<tr><td>分管领导</td><td colspan="4"></td></tr>
<tr><td colspan="5">注：1、本表适用一般的或通用设备、低值品、办公用品等采购项目。
2、大型采购项目需附专家论证报告。
3、审批完毕后，本表正本与合同一并送财务外备案，主管部门复印件备查。
4、采购单项和批量在万元以上的项目均需填报本表。</td></tr>
</table>

24. 福州软件职业技术学院设备故障处理单

故障标题			
故障描述			
设备名称		设备型号/软件版本	
故障发现人		联系电话	
故障发生时间	_____年_____月 _____ 日 _____ 时 _____ 分		
解决方法	故障原因： 处理方法： 处理结果：		
故障响应时间	_____年_____月 _____ 日 _____ 时 _____ 分		
故障解决时间	_____年_____月 _____ 日 _____ 时 _____ 分		
预防措施			
处理人员		处理人员电话	

25. 福州软件职业技术学院系统变更审批表

<table>
<tr><td>变更项目名称</td><td colspan="3"></td></tr>
<tr><td>申请人或部门</td><td colspan="3"></td></tr>
<tr><td>联系电话</td><td></td><td>申请日期</td><td></td></tr>
<tr><td colspan="4">【变更内容描述】
需求变更理由：

变更内容：

变更影响：</td></tr>
<tr><td colspan="4">【现代教育技术中心意见】

签名：　　日期：</td></tr>
<tr><td colspan="4">【执行记录】</td></tr>
<tr><td colspan="4">【其他设置】</td></tr>
<tr><td>执行人</td><td></td><td>执行日期</td><td></td></tr>
</table>

注：1、使用范围包括系统上线、功能变更、网络名称/IP 范围、访问控制、权限分配、防火墙设置等的变更申请；

2、申请内容描述及执行记录可自行增加附页。

26. 福州软件职业技术学院补丁更新表

日期		维护人员	
漏洞/补丁/恶意代码库名称			
当前版本		升级到版本	
漏洞/补丁详情			
测试及备份情况：			
操作记录：			

27. 福州软件职业技术学院（xxx）系统备份/恢复任务

记录日期：

服 务 器：

任务名称	任务说明	运行日期	运行时间	备注

记录人：

28. 福州软件职业技术学院网络安全事故报告表

报告时间		报告部门	
报告人		联系电话	
发生重大网络安全事件的网络与信息系统名称及用途：			
重大网络安全事件的简要描述（如以前出现过类似情况也应该加以说明）：			
初步判定的事故原因：			
当前采取的确应对措施：			
本次重大网络安全事件的初步影响状态：			
事件后果	□业务终端 □系统破坏 □数据丢失 □其他		
影响范围	□单台主机 □多台主机 □整个信息系统 □整个局域网		
严重程度	□极严重 □很严重 □严重 □一般 □不严重		

注：可根据需要另付页

29. 福州软件职业技术学院应急演练记录表

演练时间	
演练目的	
演练对象	
演练内容	
演练实施人员	
演练过程记录：(可另附纸记录)	
演练结果	
应急预案整改措施：	
应急领导小组负责人签字	