附件 1：

《XXXXXXXXXX 信息平安管理制度》

《XXXXXXXXXX 计算机网络信息平安保密制度》

《XXXXXXXXXX 用户密码平安保密管理规定》

《XXXXXXXXXX 电子文件保密管理规定》

《XXXXXXXXXX 涉密计算机系统病毒防治管理规定》

《XXXXXXXXXX 数字复印机多功能一体机保密管理规定》

《XXXXXXXXXX 计算机信息发布、传递保密管理制度》

《XXXXXXXXXX 互联网发布信息保密管理制度》

《XXXXXXXXXX 计算机维修、更换及报废保密管理规定》

《XXXXXXXXXX 移动存储介质管理制度》

《XXXXXXXXXX 计算机保密管理制度》

《XXXXXXXXXX 网络管理方法》

《XXXXXXXXXX 系统数据备份与恢复管理制度》

《XXXXXXXXXX 网络信息平安应急预案》

《XXXXXXXXXX 机房平安管理制度》

《XXXXXXXXXX 信息化平安管理方法》

《XXXXXXXXXX 信息系统变更管理制度》

《XXXXXXXXXX 信息平安事件报告和处置管理制度》

《XXXXXXXXXX 信息平安系统平安建设工作方案》

信息平安管理制度

近年来， 随着计算机技术和信息技术的飞速开展，社会的需求不断进步，企业传统的手工生产模式和管理模式迈入了一个全新的时代——信息化时代。随着信息化程度的日益推进，企业信息的脆弱性也日益暴露。如何标准日趋复杂的信息平安保障体系建设，如何进行信息风险评估保护企业的信息资产不受侵害，已成为当前行业实现信息化运作亟待解决的问题。

一、前言：企业的信息及其平安隐患。

在我公司，我部门对信息平安做出整体规划：通过从外到内、从广义到狭义、从总体到细化、从战术到战略，从公司的整体到局部的各个部门相结合一一剖析，并针对信息平安提出解决方案。涉及到企业平安的信息包括以下方面：

A 效劳器信息。主要存在于信管部。

B 密码信息。存在于各部门所有员工。

针对以上涉及到平安的信息，在企业中存在如下风险：

1 来自企业外的风险

①病毒和木马风险。互联网上到处流窜着不同类型的病毒和木马，有些病毒在感染企业用户电脑后，会篡改电脑系统文件，使系统文件损坏，导致用户电脑最终彻底崩溃，严重影响员工的工作效率；有些木马在用户访问网络的时候，不小心被植入电脑中，轻那么丧失工作文件，重那么泄露机密信息。

②不法分子等黑客风险。计算机网络的飞速开展也导致一些不法分子利用网络行窃、行骗等，他们利用所学的计算机编程语言编译有特定功能的木马插件，经过层层加壳封装技术，用扫描工具找到互联网上某电脑存在的漏洞，绕过杀毒软件的追击和防火墙的阻挠，从漏洞进入电脑，然后在电脑中潜伏，依照不法分子设置的特定时间运行，开启远程终端等常用访问端口，那么这台就能被不法分子为所欲为而不被用户觉察，尤其是技术部、工程部和财务部电脑假设被黑客植入后门，留下监视类木马查件，将有可能造成技术图纸被拷贝泄露、财务网银密码被窃取。还有些黑客纯粹为显示自己的能力以攻击为乐，他们在用以上方法在网络上绑架了成千上万的电脑，让这些电脑成为自己傀儡，在网络上同时发布大量的数据包，前几年流行的洪水攻击及 DDoS 分布式拒绝效劳攻击都由此而来，它会导致受攻击方效劳器资源耗尽，最终彻底崩溃，同时整个网络彻底瘫痪。

2、来自企业内的风险

①

文件的传输风险。假设有员工将公司重要文件以 QQ、MSN 发送出去，将会造成企业信息资源的外泄，甚至被竞争对手掌握，危害到企业的生存开展。

② 文件的打印风险。假设员工将公司技术资料或商业信息打印到纸张带出公司，会使企业信息资料外泄。

③ 文件的　风险。假设员工将纸质重要资料或技术图纸　出去，以及将其他单位　给公司的技术文

件和重要资料带走，会造成企业信息的外泄。

④　存储设备的风险。假设员工通过光盘或移动硬盘等存储介质将文件资料拷贝出公司，可能会泄露企业机

密信息。假设有动机不良的员工，私自拆开电脑机箱，将硬盘偷偷带出公司，将会造成企业信息的泄露。

⑤　上网行为风险。员工可能会在电脑上访问不良网站，会将大量的病毒和顽固性插件带到企业网络中来，造成电脑及企业网络的破坏，更甚者，在电脑中运行一些破坏性的程序，导致电脑系统的崩溃。

⑥ 用户密码风险。主要包括用户密码和管理员密码。假设用户的开机密码、业务系统登陆密码被他人掌握，

可能会窃取此用户权限内的信息资料和业务数据；假设管理员的密码被窃取，可能会被不法分子破坏应用系统的正常运行，甚至会被窃取整个效劳器数据。

⑦ 机房设备风险。主要包括效劳器、UPS 电源、网络交换机、　交换机、光端机等。这些风险来自防

盗、防雷、防火、防水。假设这些自然灾害发生，可能会损坏机房设施，造成业务中断。

⑧ 办公/区域风险。主要包括办公区域敏感信息的平安。有些员工缺乏平安意识，在办公区域随意堆放本

部门的重要文件或是在办公区域毫不避嫌谈论工作内容，假设不小心被其他人拿走或听到，可能会泄露部门工作机密，甚至是公司机密。

为了保证企业信息的平安保密，公司所有人员必须严格遵守企业信息平安管理总那么，以平安总那么为根底，各部门具体细那么为平安管理行为标准，从各个层面杜绝信息平安隐患。

二、总那么：从整个公司层出发，针对这些信息隐患制订平安防范措施。

1.计算机设备平安管理。

1〕 公司所有人员应保持清洁、平安、良好的计算机设备工作环境，禁止在计算机应用环

境中放置易燃、易爆、强腐蚀、强磁性等有害计算机设备平安的物品。

2〕 严格遵守计算机设备使用、开机、关机等平安操作规程和正确的使用方法。任何人不允许私自拆卸计算机组件，计算机出现故障时应及时向信息管理部报告，不允许私自处理和维修。

3〕发现由以下等个人原因造成硬件的损坏或丧失的，其损失由当事人如数赔偿：违章作业；保管不当；擅自安装、使用硬件和电气装置。公司每位员工对自己的工作电脑既有使用的权利又有保护的义务。任何的硬件损坏必须给出损坏报告，说明损坏原因，不得擅自更换。公司会视实际情况进行处理。

4〕下班后所有不再使用的计算机，应关闭主机电源，以防止意外，对于共同使用的计算机，原那么上由最后一个退出系统的使用人员关机，并关闭电源。外人未经公司领导批准不得操作公司计算机设备。

2.部门资料平安管理。

1〕 外接存储设备平安管理。

严禁所有人员以个人介质光盘、U 盘、移动硬盘等存储设备拷贝公司的文件资料并带出公司。假设因出差等原因需要拷贝文件资料到存储设备中，需要向上级请示此行为，并以公司存储设备做文件拷贝。为确保硬盘的平安，严禁任何人私自拆开电脑机箱：①将用户主机贴上封条标签，除信管部人员外，任何人不得私自拆开机箱，假设信管部进行电脑硬件故障排查时，撤除封条标签后，在故障排查结束及时更换新的封条标签。信管部将定期检查，假设发现有封条拆开痕迹，将查看视频监控记录，追查相关人责任。②给每台电脑主机配备锁柜，将所有用户主机存放在锁柜内，锁柜钥匙统一由信管部保管，假设需要为用户处理电脑故障时，信管部在翻开锁柜处理完电脑故障时，一定要锁好主机柜，确保主机内硬盘的平安。

2〕 文件　平安管理。

所有人员对外发送　，必须经上级核实后，统一在综合部登记，由综合部发送，严禁个人私自在未经许可的情况下对外发送任何类型的　文件，一经发现，所有后果将由个人承当。在对内　文件时，应即刻通知　接收人接收并取走　件，在　结束时，应马上取走　原件。假设因　时没有取走　件，导致　件丧失，造本钱部门信息外泄，那么由本人承当一切后果。

3〕 文件打印平安管理。

所有人员不得私自将公司文件打印带出公司，一经发现，严肃处理。假设在上班时间，打印工作文件时，需要即刻在打印机处等候文件的打印，文件打印完成后马上取走，假设因文件打印时有其他紧急事件，应该通知本部门人员代为领取打印文件。禁止一切打印后未及时取走打印文件的行为，一经发现，将对本人警告，假设因打印后，文件丧失，造成信息资料外泄，那么由本人承当相关责任。

4〕 文件的存储平安管理。

所有部门人员应每周清理计算机中的文件，去除不需要的垃圾文件，将重要的文件和工作资料保存在特定的文件夹里，每月末应将电脑中的文件资料做一次备份，将文件资料备份到部门专用U盘或移动硬盘上，确保个人工作资料的文件归档，在电脑突发性故障或硬盘损坏时，能够及时恢复最近的工作资料；电脑桌面上的文件应每周末拷贝到非系统盘符中或不要在桌面存放任何工作性文件资料。假设因个人原因未执行备份，造成数据资料丧失时，将由本人承当相关后果。假设员工离职，在办完离职手续后，所在部门负责人应联系信管部协助将此员工工作资料拷贝到部门U盘或移动硬盘上，假设没有执行此平安过程，离职员工损失的文件资料由该部门承当。

5〕 办公区域的平安管理。

所有部门人员每天下班时应保证办公桌的整洁，将部门重要文件资料存放在个人抽屉柜中，并检查确保办公桌上没有存放重要文件或其他有可能泄露本部门工作内容的信息源。假设因资料没有存放好，被他人取走，造成的后果将由本人承当。

3.帐号密码平安管理。

使用者须妥善保管好自己的帐户和密码。严防被窃取而导致泄密。帐户及密码由网络管理员设置后通知员工，员工不得随意更改密码。所有员工必须在所使用的计算机中设置开机密码和屏幕保护密码。为了保护公司的信息资产，设置密码时应注意：密码至少有8个字符长；密码必须包含以下任一局部：字母A-Z或a-z，数字0-9，特殊字符，例如 $ ，-等。

1〕 电脑密码管理：每个员工拥有一个公司内部计算机登录帐户。新员工申请帐户时需要向网络管理员提供姓名、部门、职位等信息，网络管理员将在一天内将账户信息通知其本人。公司所有用户在分配到工作电脑时,应首先更改自己的电脑登录密码,并将个人登录密码在信息管理部登记，假设更改密码后，未进行登记，一经信管部发现，将对该用户进行口头警告。同时，因没有及时向信管部备案造成的电脑故障问题或文件丧失等问题，信管部不承当责任。

2〕

应用系统密码管理：所有 ERP 用户及 OA 用户都将分配到一个帐号密码，帐号是不变的，用户可以更改自己的系统密码，密码尽可能设置为高平安性的复杂密码，严禁用户将密码设置为如 123456 等傻瓜式密码，假设密码设置过于简单，被其他用户非法登陆后，在 ERP 中将会非法编制篡改单据，在 OA 中非法冒用流程管理权限，假设产生此情况，将会导致严重的后果；严禁将 ERP 帐号或 OA 帐号密码透露给他人，让他人代己做 ERP 单据或办理 OA 流程；员工调离岗位或离职，所在部门负责人应及时通知信管部注销该员工的应用系统帐户。假设因以上原因造成的信息平安后果将由本人承当。

3〕 采用用户身份认证系统：目前我公司登陆效劳器采取的是静态密码认证，这种密码保护技术是最低层次的。在企业内，容易被其他部门人员注意到效劳器登陆密码，从而可能会被动机不良的员工登陆到效劳器，破坏效劳器数据；在企业外，容易遭到黑客字典扫描破解密码，从而攻击各应用效劳器，破坏或盗取商业数据等。因此，我部门在未来的开展规划中，要将用户身份认证当作平安的一个重大隐患，想方法解决这个问题。

这里，我们可以采取动态口令牌或 USBKEY 认证技术，并选择其中一种技术与公司现有的静态密码技术相结合，动态口令牌随机生成动态密码，并于 60 秒内自动刷新密码，无法采用数据字典扫描破解密码，让黑客攻击行为束手无策；而 USB KEY 采用 USB 密钥，存储特定的加密算法，只有将 USB 钥匙接上电脑，与电脑中存储的认证软件验证通过后，才能进入。我们通过〔动态+静态〕混合身份认证，或〔硬件+软件〕混合身份认证，保证效劳器的登陆基于网内的行为、网外的行为都是平安的。

4..杀毒软件平安管理。

用户使用的杀毒软件和防火墙已经设置好自动调度更新和病毒库升级，每日定时杀毒，使用者也应经常手动扫描杀毒。

5.各类软件平安管理。

软件原始盘片应交综合部保管，软、硬件设备的原始资料〔软盘、光盘、说明书及保修卡、许可证协议等〕交综合部保管。保管应做到防水、防磁、防火、防盗。使用者必需的操作守册由使用者长借、保管。

6.邮件平安管理。

所有因公对外联系的电子邮件一律通过公司邮箱 info@163 在指定的电脑上进行收发。〔参考邮箱管理制度〕

综上所述，使用者应该具有一定的平安防范意识，具体应做到：

日常工作信息平安：

1〕员工应对在自己公司电脑内公司机密信息的平安负责，当需暂时离开座位时必须立即启

动屏幕保护程序并带有密码。

2.〕员工有责任正确地保护分配给本人的所有计算机帐户。

3.〕各部门经理及人事部应及时向信息管理部提供本部门及公司员工的人事及职位变动信息。

4〕每台公司电脑内必须安装反病毒软件并启动实时扫描程序。信息管理部可以提供最新杀毒软件。

5〕不得安装有可能危及公司计算机网络的任何软件，假设实在有需要进行软件测试的必须将计算机脱离公司计算机网络进行单机操作。

6〕任何对公司内部计算机网络的黑客行为是绝对禁止的，一经查实将按公司有关规定严肃处理。

假期时间办公室的平安： 确保工作电脑的平安，在你离开之前的一周内备份你的文件。在你即将离开之际确保你的电脑关机并设有开机密码，其它信息管理部设备的电源也必须切断。

确保数据的平安：确保你的软盘，备份数据源和所有机密文件被妥善锁好。公司高度秘密和秘密信息在不用时必须总是被保存在设有密码锁或钥匙的柜中。公司的机密信息必须存放在锁上的办公桌或文件柜中。

当你在外的时候：不要在任何地方谈论公司的机密信息。公司的竞争对手成员也可能在休假，而且总在探听我们公司的消息。任何小小的信息都可能是他们所需要的。

当你回来的时候：如果你发现在平安方面有任何可疑之处都要向公司有关方面进行汇报。报告任何意外对于正确调查和阻止任何更进一步错误的行为是很重要的。

常规考前须知

1〕任何外来盘片(包括 CD、VCD 碟片及软盘)，只有经过系统管理员确认不带病毒后，才可在公司计算机上使用.否那么造成病毒感染或其他破坏的,公司将对其责任人进行罚款处理，每次金额 50 元～500 元。

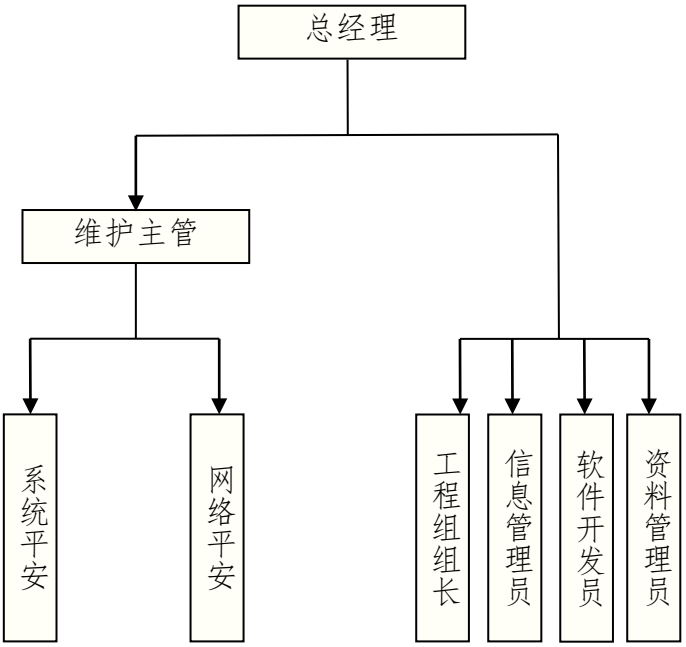
2〕个人未经公司领导允许不得擅自将公司保密的商务资料、技术文件输出，假设需输出必须履行审批手续。申请人填写申请单，写明输出资料内容、份数、路径、用途、申请日期、申请人等工程，经部门领导和公司领导共同签字审批后，交由专人上机操作。

3〕未经系统管理员许可，不得从因特网上下载任何软件安装，系统管理员将不定期检查，发现有违反本条规定的，将给予 50 元～500 元的罚款。

4〕严禁在工作时间利用计算机网络从事与本职工作无关的活动，发现有违反本条规定的，将给予 50 元～200 元的罚款。

技术部组织架构及岗位职责

为实现公司信息化目标，标准公司信息化建设，建立和完善公司信息化管理体系，明确管理职责，保障公司信息系统平安、高效、稳定运行，为公司提供准确、有效的财务、生产、技术及其它相关信息，为公司高层科学决策提供依据，从而进一步增强企业的核心竞争力**组织架构**



三、公司信息部部门及岗位职责

1. 信息部部门职责

(1) 负责公司信息化建设的总体规划及网络体系结构的设计，负责公司信息化系统选型工作，并负责编制公司信息化总体规划与选型报告，并报公司领导审批。

(2) 负责公司信息化系统的推进与执行，负责公司信息化工程实施工作的日常管理，并协调解决工程实施过程中碰到的问题。

(1) 负责组织调研公司各部门信息化需求并汇总，负责组织公司财务、生产、技术、办公自动化系统软件的开发，使公司信息化系统形成一个无缝连接的整体。负责公司各种汇总报表、查询软件、分析软件的二次开发，为领导决策和各业务经营环节提供及时、准确的决策信息。

(2) 负责公司所有信息化工程的持续改进与日常维护，负责公司计算机网络及信息管理系统的平安管理、技术支持和维护工作，在保证公司的计算机网络平安运行的前提下，树立效劳意识，为公司领导、各业务职能部门提供最优质效劳。

(3) 负责公司人员计算机应用方面的培训，提高公司计算机应用的整体水平和办公效率。

(4) 负责公司计算机及相关设备的采购及维修方案编制。

2.岗位职责

1.总经理

〔1〕负责主持信息部的全面日常工作，负责制定本部门的管理制度及组织建设，并监督本部人员全面完成部门职责范围内的各项工作任务；负责本部门员工的工作检查、考核及评价。

〔2〕贯彻落实本部岗位责任制和工作标准，密切各部门工作关系，加强与集 团各部门的协作配合，做好衔接协调工作；

〔3〕负责公司信息化系统总体构架，构建公司信息化实施组织，结合业务流程、工程管理，实施公司集成信息化系统。

〔4〕负责控制信息化工程预算。负责控制本部门信息化预算，降低费用本钱。

〔5〕负责公司信息化工程关键控制点的监督、控制和风险评价；

〔5〕负责组织公司的信息平安工作，持续加强公司的信息平安管理。

〔6〕组织对公司计算机及周边设备、网络设备和办公自动化设备的维护、添置、验收以及发放登记归档；

〔7〕负责组织对计算机网络及信息系统的维护，保证网络及信息系统的正常运行。

〔8〕负责主持信息化新系统、新工程的开发，并对信息工程系统开发全过程负责。

〔9〕负责组织公司信息化工程的持续改进与日常维护。

〔10〕完成领导指派的其它工作；

2. 维护主管

〔1〕负责 IT 维护方面的日常管理工作。负责安排及监督系统管理员及系统维护员的工作。

〔2〕负责主持计算机及网络系统的设计及改进工作。

〔3〕负责主持对计算机网络及硬件系统的维护，保证网络及硬件系统的正常运行。

〔4〕负责检测并实施适当措施保障网络及硬件系统应用平安。

〔5〕负责对公司计算机及周边设备、网络设备和办公自动化设备的维护、添置、验收以及发放登记归档；

〔6〕负责公司上外网权限控制

〔7〕主管指派的其它工作；

3. 工程组组长

〔1〕 进行工程可行性论证；

〔2〕 按照方案执行工程的实施；

〔3〕 协调工程组内的工作；

〔4〕 主管指派的其它工作；

4. 信息管理员

〔1〕 依据新信息系统工程的开发方案展开开发工作；

〔2〕 负责公司有关信息系统的持续改进与日常维护，负责公司信息系统的平安管理、技术支持和维护工作，树立效劳意识，为公司领导、各业务职能部门提供最优质效劳。

〔3〕 负责公司的信息系统平安工作，持续加强公司的信息平安管理。

〔4〕 主管指派的其它工作；

5. 软件开发员

〔1〕负责新系统、新程序的技术调研工作；

〔2〕依据公司自主开发软件工程的方案进行软件开发设计，并进行推广。

〔3〕负责调研公司各部门信息化需求并汇总，负责公司外购软件〔财务、生产、技术、办公自动化系统软件、人事管理系统〕的二次开发，负责公司各种汇总报表、查询软件、分析软件的二次开发，为领导决策和各业务经营环节提供及时、准确的决策信息。

〔4〕主管指派的其它工作；

6. 信息平安

〔1〕负责主持计算机及网络系统的设计及改进工作。

〔2〕负责检测并实施适当措施保障网络及硬件系统应用平安。

〔3〕负责维持运行于网络平台上的各种效劳稳定运行。

〔4〕主管指派的其它工作；

7. 网络平安

〔1〕负责排除计算机及网络系统〔包括软件〕的故障。

〔2〕维修或更换损坏的计算机及网络设备或部件；

〔3〕协助维护计算机网络的稳定运行与平安；

〔4〕主管指派的其它工作；

XXXXXXXXXX计算机网络信息平安保密制度

为保证我公司计算机网络信息平安，防止计算机网络失密泄密事件发生，特制定本制度。

一、为防止病毒造成严重后果，对外来存储介质〔硬盘、光盘、软盘、移动硬盘或U盘〕、软件要严格管理，严格禁止外来存储介质、软件在单位涉密计算机上使用。

二、为防止黑客攻击和网络病毒的侵袭，接入网络的计算机一律安装杀毒软件，并要定时对杀毒软件进行升级。

三、各部门在各项重大事项保密期间，将有关涉密材料保存到不联网的计算机上。

四、我公司所有办公计算机的联网均通过公司进行，各部门禁止将计算机擅自接入其他互联网运营商。

五、保密级别在秘密以下的材料可通过网络传递和报送，严禁保密级别在秘密以上的材料通过网络传递和报送。

XXXXXXXXXX用户密码平安保密管理规定

一、用户密码管理的范围是指办公室内所有涉密计算机所使用的密码。

二、机密级涉密计算机的密码管理由涉密部门负责人负责，秘密级涉密计算机的密码管理由使用人负责。

三、用户密码使用规定

〔1〕密码必须由数字、字符和特殊字符组成；

〔2〕秘密级计算机设置的密码长度不能少于8个字符，密码更换周期不得多于30天；

〔3〕机密级计算机设置的密码长度不得少于10个字符，密码更换周期不得超过7天；

〔4〕涉密计算机需要分别设置BIOS、操作系统开机登录和屏幕保护三个密码。

四、密码的保存

〔1〕秘密级计算机设置的用户密码由使用人自行保存，严禁将自用密码转告他人；假设工作需要必须转告，应请示主管领导认可。

〔2〕机密级计算机设置的用户密码须登记造册，并将密码本存放于保密柜内，由部门主任管理。

XXXXXXXXXX电子文件保密管理规定

一、涉密电子文件是指在计算机系统中生成、存储、处理的机密、秘密和内部的文件、图纸、程序、数据、声像资料等。

二、电子文件的密级按其所属工程的最高密级界定，其生成者应按密级界定要求标定其密级，并将文件存储在相应的目录下。

三、各用户需在本人的计算机系统中创立“机密级文件”、“秘密级文件”、“内部文件”三个目录，将系统中的电子文件分别存储在相应的目录中。

四、电子文件要有密级标识，电子文件的密级标识不能与文件的正文别离，一般标注于正文前面。

五、电子文件必须定期、完整、真实、准确地存储到不可更改的介质上，并集中保存，然后从计算机上彻底删除。

六、各涉密部门自用信息资料要定期做好备份，备份介质必须标明备份日期、备份内容以及相应密级，严格控制知悉此备份的人数，做好登记后进保密柜保存。

七、各部门要对备份电子文件进行标准的登记管理。备份可采用磁盘、光盘、移动硬盘、U盘等存储介质。

八、涉密文件和资料的备份应严加控制。未经许可严禁私自复制、转储和借阅。对存储涉密信息的磁介质应当根据有关规定确定密级及保密期限，并视同纸制文件，分密级管理，严格借阅、使用、保管及销毁制度。

九、备份文件和资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施，并进行异地备份。

XXXXXXXXXX计算机系统病毒防治管理规定

一、涉密计算机必须安装经过国家平安保密部门许可的查、杀病毒软件。

二、每周升级和查、杀计算机病毒软件的病毒样本，确保病毒样本始终处于最新版本。

三、绝对禁止涉密计算机在线升级防病毒软件病毒库，同时对离线升级包的来源进行登记。

四、涉密计算机应限制信息入口，如软盘、光盘、U 盘、移动硬盘等的使用。

五、对必须使用的外来介质〔磁盘、光盘，U 盘、移动硬盘等〕，必须先进行计算机病毒的查、杀处理，然后才可使用。

六、对于因未经许可而擅自使用外来介质导致严重后果的，要严格追究相关人员的责任。

数字复印机多功能一体机保密管理规定

一、用于专门处理涉密信息的数字复印机、多功能一体机按所接入设备的最高定密等级定密。

二、严禁将用于处理国家秘密信息的具有打印、复印、　　等多功能的一体机与普通　　线连接。

三、严禁维修人员擅自读取和拷贝数字复印机、多功能一体机等涉密设备存储的国家秘密信息。涉密电子设备出现故障送外维修前，必须将涉密存储部件撤除并妥善保管；涉密存储部件出现故障，如不能保证平安保密，必须按照涉密载体销毁要求予以销毁；如需恢复其存储信息，必须由保密工作部门指定的具有数据恢复资质的单位进行。

XXXXXXXXXX计算机保密管理制度

为进一步加强我公司涉密计算机信息保密管理工作，杜绝泄密隐患，确保国家秘密的平安，维护公司稳定与平安，根据《中华人民共和国保守国家秘密法》，结合我公司实际，制定本制度。

第一条　公司保密委员会负责全校涉密计算机保密管理工作的指导、协调和监督工作。保密技术防范和管理工作由公司网络中心负责。

第二条　凡涉及国家秘密、公司各单位内部不宜公开的办公事项严禁进入公司和国际互联网，与国际互联网相连的计算机系统严禁处理、存储、传输国家秘密和单位内部不宜公开办公事项。

第三条　但凡涉密计算机不得直接或间接接入公司公共网和国际互联网，必须进行物理隔离。禁止任何单位和个人将网络平安隔离与交换器用于涉密计算机和网络之间。

第四条　凡经公司保密委员会审查登记备案的涉密计算机，必须指定专人负责管理，实行专机专用，凡涉密计算机一机多人共用的必须采取保密技术措施，加强保密工作，严格按规定标准操作。

第五条　各单位对上网信息要建立健全严格的保密审查制度。公司主页由公司领导负责保密审查，各单位上网信息由单位主要领导负责保密审查，坚持“谁上网，谁负责”的原那么，未经保密审查的信息不得入网。

第六条　凡违反保密规定，利用涉密计算机、公司、国际互联网从事危害国家平安和利益，泄露国家秘密和公司业务工作秘密的活动，一经查出，将追究单位主要领导和当事人的责任。

第七条　涉密的计算机信息在打印输出时，打印出的文件应当按照相应密级文件管理，打印过程中产生的残、次、废页应当及时销毁。

第八条　凡涉及国家秘密信息的计算机设备的维修，应保证储存的国家秘密信息不被泄露。到保密工作部门指定的维修点进行维修，并派技术人员在现场负责监督。

第九条 各单位报废涉密计算机，必须经校保密委员会派专人将涉密内容作技术处理〔消除〕，公司保密委员会备案后，方能作出处理。否那么，作违规论处，将追究单位主管领导和当事人的责任。

第十条　各单位增加涉密计算机，必须先到公司保密委员会备案后使用。

第十一条　　本制度由公司保密委员会办公室负责解释。

第十二条　　本制度自下发之日起执行。

XXXXXXXXXX移动存储介质管理制度

为加强我公司移动存储介质管理，确保国家秘密的平安，根据《中华人民共和国保守国家秘密法》，结合我公司实际，制定本制度。

第一条　校保密委员会办公室负有建立健全使用复制、转送、携带、移交、保管、销毁等制度以及对单位所执行本制度的监督、检查职责。保密工作领导小组界定涉密与非涉密移动存储介质〔包括硬盘、移动硬盘、软盘、U盘、光盘、磁带及各种存储卡〕，并由保密委员会办公室登记造册。

第二条　各单位必须指定专人负责涉密移动存储介质的日常管理工作。涉密移动存储介质必须妥善保存。日常使用由使用人员保管，暂停使用的交由指定的专人保管。

第三条　涉密移动存储介质严禁在互联网外网上使用。确因工作需要携带涉密移动存储介质外出，须报分管领导批准，履行相关手续和采取严格的保密措施。严禁将涉密移动存储介质借给外单位使用。

第四条　涉密移动存储介质需要送外部维修时，必须到国家保密工作部门指定的具有保密资质的单位进行维修，并将废旧的存储介质收回。涉密移动存储介质在报废前，应进行信息去除处理。

第五条　涉密移动存储介质的销毁，经分管领导批准后，到自治区国家保密局指定的销毁点销毁或送交自治区国家保密局统一销毁，不得擅自销毁。禁止将涉密移动存储介质作为废品出售。

第六条　工作人员不按规定管理和使用涉密移动存储介质造成泄密事件的，将依法依规追究责任，构成犯罪的将移送司法机关处理。

第七条　本制度由校保密委员会办公室负责解释。

第八条　本制度从下发之日起执行。

XXXXXXXXXX计算机维修、更换及报废保密管理规定

第一条 涉密计算机进行维护检修时，须保证所存储的涉密信息不被泄露，对涉密信息应采取涉密信息转存、删除、异地转移存储媒体等平安保密措施。无法采取上述措施时，平安保密人员和涉密单位计算机系统维护人员必须在维修现场，对维修人员、维修对象、维修内容、维修前后状况进行监督并做详细记录。

第二条 凡需外送修理的涉密设备及涉密介质，必须经校保密委员会和分管领导批准，并将涉密信息进行不可恢复性删除处理前方可实施。

第三条 网络管理中心负责对涉密计算机软件的安装和设备的维护维修工作，严禁使用者私自安装涉密计算机软件和擅自拆卸计算机设备。

第四条 涉密计算机报废由保密领导小组专人负责，交由自治区国家保密局定点销毁。

第五条 本制度由校保密委员会办公室负责解释。

第六条 本制度从下发之日起执行。

XXXXXXXXXX 互联网发布信息保密管理制度

为加强互联网发布信息的保密管理，确保国家秘密平安，根据《中华人民共和国保守国家秘密法》、国家保密局《计算机信息系统保密管理暂行规定》、《计算机信息系统国际联网保密管理规定》等有关要求，结合我公司实际，制定本制度。

第一条 在互联网上发布的信息是指经公司主要领导或分管领导审核批准，提供应国际互联网站或其他公众信息网站，向社会公开、让公众了解和使用的信息。

第二条 互联网发布信息保密管理坚持“谁发布谁负责”的原那么。凡向国际互联网站提供或者发布信息，必须经公司主要领导或分管领导审查批准，并应该按照一定的工作程序，完善和落实信息登记、审批责任制。

第三条 除新闻媒体已公开发表的信息外，各部门及院〔系〕提供的上网信息应确保不涉及国家秘密。

第四条 单位内部工作秘密、内部资料等，虽不属于国家秘密，但应作为内部事项进行管理，未经公司主要领导或分管领导批准不得擅自发布。

第五条 禁止网上发布信息的根本范围：

〔一〕标有密级的国家秘密。

〔二〕未经相关部门批准的，涉及国家平安、社会政治稳定等敏感信息。

〔三〕未经制文单位批准，标注有“内部文件〔资料〕”和“注意保存”〔保管、保密〕等警示字样的信息。

〔四〕公司认定为不宜公开的内部办公事项。

第六条 保密工作分管领导应履行的职责：

〔一〕定期对网络管理人员进行保密法规、保密纪律、保密常识教育，增强信息保密观念和防范意识，自觉遵守并执行有关保密规定。

〔二〕建立健全上网信息保密管理制度，落实各项平安保密防范措施。

〔三〕发现国家秘密网上发布的，立即采取补救措施，并及时向有关部门报告。

〔四〕定期或不定期向自治区国家保密局通报网上发布信息保密管理情况。

第七条 校保密委员会办公室主任应履行的职责：

〔一〕指导、监督各部门网上发布信息的保密管理工作。

〔二〕协助参与涉及几个部门拟发布信息的保密审查。

〔三〕向自治区国家保密局报告网上发布信息保密审查中的重要情况。

〔四〕负责对网上发布信息进行经常性保密监督检查，发现问题，立即采取补救措施，查明原因，并及时向自治区国家保密局报告。

〔五〕协助有关部门对违反规定造成网上泄密的事件依法进行查处。

第八条 提供信息发布的部门应履行的职责：

〔一〕对拟发布信息是否涉及国家秘密进行审查。

〔二〕对已发布信息进行定期保密检查，发现涉密信息的，立即采取补救措施，查清泄密渠道和原因，并及时向公司分管领导或保密委员会报告。

〔三〕接受上级机关和自治区国家保密局的监督检查。

第九条 违反本制度，对网上发布信息保密审查把关不严，导致严重后果或平安隐患的，按照规定严肃查处。

第十条　本制度由校保密委员会办公室负责解释。

第十一条　本制度从下发之日起执行。

XXXXXXXXXX 计算机
信息发布、传递保密管理制度

为了加强和标准公司非涉密计算机信息系统信息发布、传递的保密管理工作，确保国家秘密和公司工作秘密的平安，根据《计算机信息系统国际联网保密管理规定》〔国保发[1999]10 号〕等国家相关法规有关要求，结合公司实际，制定本制度。

第一条 本制度所称非涉密计算机信息系统是指公司内部直接或间接接入国际互联网的计算机网络和单机。信息发布是指在各类网站、网页、网上论坛等信息发布平台上公开发布信息的行为；信息传递是指通过电子邮件、即时通信等方式传送信息的行为。

第二条 公司非涉密计算机信息系统禁止以任何形式发布、传递国家秘密和工作秘密信息。

第三条 公司非涉密计算机信息系统信息发布、传递的保密管理工作遵循

“业务谁主管，保密谁负责”的根本原那么，确保所发布、传递的信息均经过保密审查、审批，绝对不涉及国家秘密和工作秘密。

第四条 公司对非涉密计算机信息系统信息发布、传递实行保密审查、审批制度。

一、发布、传递一般性的信息由非涉密计算机信息系统使用管理单位自行进行保密审查。

二、发布、传递公司党、政文件或其它可能涉及国家秘密和公司工作秘密的信息，须送党委办公室、校长办公室及相关领导进行保密审查。

三、发布、传递的信息中可能涉及国家秘密、工作秘密而相关业务主管部门又无法明确界定的，须送公司保密委员会进行保密审查，并报公司主管领导审批。

第五条 非涉密计算机信息系统发布、传递信息保密审查、审批程序：在学生社团或学生个人制作的网站上发布的信息，由学生部〔处〕、团委审核；各单位〔部门〕在本单位〔部门〕网站上发布的信息或在公司主页上发布的信息由该单位〔部门〕负责信息发布的领导审核。审核合格后，签字盖章，留档备案，再进行信息发布。

一、利用非涉密计算机信息系统发布、传递信息时，承办人、拟稿人须填写发布申请表，由所在单位负责人审查；

二、根据发布、传递信息的性质选择送公司相应业务主管部门审查、无法明确界定的送保密处审查，并报公司主管领导、保密委员会审批；

三、将审查、审批后的发布申请表及所要发布、传递的信息内容，一同送交发布、传递承办单位或人员；

四、信息发布、传递承办单位或人员确认所要发布、传递的信息经保密审查、审批合格后，方可在非涉密计算机信息系统上公开发布、传递信息。

第六条 公司公司信息发布、传递的保密审查、审批方法：

一、公司主页信息发布的保密审查、审批。

公司党委办公室、校长办公室及网络中心明确专人负责信息的采集和发布，并对一般性的信息进行保密审查；

公司党、政文件、涉及公司平安稳定的信息以及其它可能涉及国家秘密、工作秘密的信息，经保密审查、审批，确认无密后，方可公开发布。

二、公司下设的部门网站〔包括各院〔系〕、部、处、中心的自办网站以及主页等〕信息发布的保密审查、审批。

各主管单位要明确专人负责信息的采集和发布。发布本单位业务、专业内的信息，由本单位主管领导、负责人进行保密审查，审查情况要有文字记载。发布本单位业务、专业以外的信息，按照本规定第四、五条执行。

三、公司各级各类论坛、聊天室等交互式网站信息发布的保密审查、审批。

主办单位要明确专人负责监管，并在论坛、聊天室等明显位置注明保密要求。论坛、聊天室等网络管理员要对所发布的信息进行实时审查、监控，对敏感信息要及时采取有效的控制措施，确保所发布的信息不涉及国家秘密、工作秘密。

四、公司内或通过公司向外传递信息的保密审查、审批。

公司各单位利用公司传递本单位业务、专业内的信息，由本单位主管领导、负责人进行保密审查，审查情况要有文字记载。传递本单位业务、专业以外的信息，按照本制度第四、五条执行。

第七条 对违反本制度，未进行保密审查、审批，擅自在公司

及国际互联网上发布、传递，造成或可能造成泄密问题的，依据有关规定给予处分。情节严重，构成重大泄密事件的，送司法机关追究责任。

第八条 本制度由公司保密委员会办公室负责解释。

第九条 本制度自发布之日起施行。

XXXXXXXXXX公司管理方法

第一章 总那么

第一条 为加强XXXXXXXXXX公司网络的运行和使用管理，确保网络平安、可靠、稳定地运行,促进我公司网络工作的健康、持续开展，根据《中华人民共和国计算机信息系统平安保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中华人民共和国计算机信息网络国际联网平安保护管理方法》、《中国教育和科研计算机网管理方法〔试行〕》和国家有关规定，特制定本管理方法。

第二条 公司是为全校教学、科研和行政管理建立的计算机信息网络，其目的是利用先进实用的计算机技术和网络通信技术，实现校内计算机互联、计算机局域网互联，并通过中国教育和科研计算机网〔CERNET〕与国际互联网络〔INTERNET〕互联，实现信息的快捷沟通和资源共享。其效劳对象主要是全校各单位及部门的办公、教学用户、学生、教职工个人用户。

第三条 但凡使用公司络资源的单位和个人用户必须按本管理方法执行。

第二章 组织与管理机构

第四条 公司成立信息化工作领导小组，负责审定公司建设规划、网络运行经费预算及讨论、决定公司管理中的其它重要问题。

第五条 计算机网络管理中心〔以下简称网管中心〕是公司公司管理的职能部门，负责公司的根底建设、技术管理、日常运行管理和网络开展工作。其主要职责是：

1、执行公司审定通过的网络建设和管理的方案和方案。

2、负责统一协调公司的主页建设工作，制定加强公司信息化和公司站建设的方案、措施。

3、负责相应的网络平安和信息平安工作。

4、负责保存网络运行有关记录并接受上一级网络和国家平安机关的监督和检查。

5、指导和监督子网建设并使其接入主干网运行，负责二级接入单位和用户的监管、技术咨询等工作。

6、负责拟订《公司运行收费管理方法》。

第六条 公司的建设、管理由公司统一规划、统一领导，实行分级管理、分层负责制。网管中心对公司网络资源〔包括硬件资源和软件信息资源〕进行管理，各院、系、部、处等部门应指定一人为计算机网络信息管理员,负责对自己内部的资源进行管理。

第七条 各接入单位的自建局域网络，由各单位自行负责建设、运行和管理，并接受网管中心的监管。

第三章 主干网与接入子网

第八条 网管中心负责主干网的运行管理、设备管理和开展规划，保证主干网的畅通。

第九条 需要建设子网的单位应向网管中心提交申请和子网规划，由网管中心审批。未经批准，任何单位和个人不得私自扩充子网和与校外单位连网。否那么，网管中心有权加以制止并拒绝其参加公司络

第十条 子网接入单位职责：

1、在网管中心的统一规划和指导下，负责按有关要求和规定对子网进行建设、运行和管理。

2、指导计算机系统管理员和用户对各自负责的网络系统、计算机系统和上网资源进行管理。

3、负责和承当下一级接入单位和用户的管理和技术咨询工作。

4、负责本级网络相应的网络平安和信息平安工作。

5、负责保存本级网络运行的有关记录并接受上一级网络的监督和检查。

第四章 IP 地址管理及用户入网申请

第十一条 全公司网络用户使用公司均需进行实名认证并使用真实 IP。IP 地址由网管中心负责统一管理和分配。入网单位和个人应严格使用由网管中心及本单位网络管理员分配的 IP 地址，不得使用 NAT(地址转换)，严禁盗用他人 IP 地址或私自乱设 IP 地址。网管中心有权切断经过 NAT 转换的子网及其它乱设的 IP 地址入网，并对盗用他人 IP 地址者予以处分，以保证公司络的正常运行。

第十二条 计算机无论以何种方式接入公司，均须办理入网手续。未办理入网手续，任何单位和个人不得私自将计算机接入公司。

第十三条 用户入网须按以下程序办理入网手续

单位集体用户〔如公共机房〕入网，应向网管中心提出申请，由网管中心审核通过并签署《公司入网平安协议》，方可入网运行。

各系部办公用户、家属院及单身教工用户、学生宿舍用户入网，均需填写公司络用户上网申请表，由网管中心审核并办理相关手续后，方可入网运行。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/995022232104011310