# 2024年医保信息安全管理制度(五篇)

来源：网络 作者：蓝色心情 更新时间：2024-07-27

*范文为教学中作为模范的文章，也常常用来指写作的模板。常常用于文秘写作的参考，也可以作为演讲材料编写前的参考。范文怎么写才能发挥它最大的作用呢？以下是小编为大家收集的优秀范文，欢迎大家分享阅读。医保信息安全管理制度篇一第一条 总则 通过加强公...*

范文为教学中作为模范的文章，也常常用来指写作的模板。常常用于文秘写作的参考，也可以作为演讲材料编写前的参考。范文怎么写才能发挥它最大的作用呢？以下是小编为大家收集的优秀范文，欢迎大家分享阅读。

**医保信息安全管理制度篇一**

第一条 总则 通过加强公司计算机系统、办公网络、服务器系统的管理。保证网络系统安全运行，保证公司机密文件的安全，保障服务器、数据库的安全运行。加强计算机办公人员的安全意识和团队合作精神，把各部门相关工作做好。

第二条 范围

1、计算机网络系统由计算机硬件设备、软件及客户机的网络系统配置组成。

2、软件包括：服务器操作系统、数据库及应用软件、有关专业的网络应用软件等。

3、客户机的网络系统配置包括客户机在网络上的名称，ip地址分配，用户登陆名称、用户密码、及internet的配置等。

4、系统软件是指：操作系统(如windows xp、windows 20xx等)软件。

5、平台软件是指：防伪防窜货系统、办公用软件(如office 20xx)等平台软件。

6、专业软件是指：设计工作中使用的绘图软件(如photoshop等)。

第三条 职责

1、信息网络部门为网络安全运行的管理部门，负责公司计算机网络系统、计算机系统、数据库系统的日常维护和管理。

2、负责系统软件的调研、采购、安装、升级、保管工作。

3、网络管理人员负责计算机网络系统、办公自动化系统、平台系统的安全运行;服务器安全运行和数据备份;internet对外接口安全以及计算机系统防病毒管理;各种软件的用户密码及权限管理协助各部门进行数据备份和数据归档。

4、网络管理人员执行公司保密制度，严守公司商业机密。

5、员工执行计算机安全管理制度，遵守公司保密制度。

6、系统管理员的密码必须由网络管理部门相关人员掌握。

第三条 管理办法

i、公司电脑使用管理制度

1、从事计算机网络信息活动时，必须遵守《计算机信息网络国际联网安全保护管理办法》的规定，应遵守国家法律、法规，加强信息安全教育。

2、电脑由公司统一配置并定位，任何部门和个人不得允许私自挪用调换、外借和移动电脑。

3、电脑硬件及其配件添置应列出清单报行政部，在征得公司领导同意后，由网络信息管理员负责进行添置。

4、电脑操作应按规定的程序进行。

(1)电脑的开、关机应按按正常程序操作，因非法操作而使电脑不能正常使用的，修理费用由该部门负责;

(2)电脑软件的安装与删除应在公司管理员的许可下进行，任何部门和个人不允许擅自增添或删除电脑硬盘内的数据程序;

(3)电脑操作员应在每周及时进行杀毒软件的升级, 每月打好系统补丁;

(4)不允许随意使用外来u盘，确需使用的，应先进行病毒监测;

(5)禁止工作时间内在电脑上做与工作无关的事，如玩游戏、听音乐等。

5、任何人不得利用网络制作、复制、查阅和传播宣传封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪的内容

6、电脑发生故障应尽快通知it管理员及时解决，不允许私自打开电脑主机箱操作。

7、电脑操作员要爱护电脑并注意保持电脑清洁卫生，并在正确关机并完全关掉电源后，方可下班离开。

8、因操作人员疏忽或操作失误给工作带来影响但经努力可以挽回的，对其批评教育;因操作人员故意违反上述规定并使工作或财产蒙受损失的，要追究当事人责任，并给予经济处罚。

9、为文件资料安全起见，勿将重要文件保存在系统活动分区内如：c盘、我的文档、桌面等;请将本人的重要文件存放在硬盘其它非活动分区(如：d、e、f)。(保存前用杀毒软件检察无病毒警告后才可)。并定期清理本人相关文件目录，及时把一些过期的、无用的文件删除，以免占用硬盘空间。

10、所有电脑必须设置登陆密码，一般不要使用默认的administrator作为登陆用户名，密码必须自身保管，严禁告诉他人，计算机名与登陆名不能一致,一般不要使用含有和个人、单位相关信息的名称。

11、其他管理办法请参看《it终端用户安全手册》

ii、网络系统维护

1、系统管理员每周定时对托管的网络服务器进行巡视，并对公司局域网内部服务器进行检查，如：财务服务器。

2、对于系统和网络出现的异常现象网络管理部门应及时组织相关人员进行分析，制定处理方案，采取积极措施。针对当时没有解决的问题或重要的问题应将问题描述、分析原因、处理方案、处理结果、及时制定出解决方案。

3、定时对服务器数据进行备份。

4、维护服务器，监控外来访问和对外访问情况，如有安全问题，及时处理。

5、制定服务器的防病毒措施，及时下载最新的防病毒疫苗，防止服务器受病毒的侵害。

iii、用户帐号申请/注销

1、新员工(或外借人员)需使用计算机向部门主管提出申请经批准由网络部门负责分配计算机、和登入公司网络的用户名及密码。如需使用财务软件需向财务主管申请，由网络管理部门人员负责软件客户端的安装调试。

2、员工离职应将本人所使用的计算机名、ip地址、用户名、登录密码、平台软件信息以书面形式记录，经网络管理人员将该记录登记备案。网络管理人员对离职人员计算机中的公司资料信息备份，方可对该离职人员保存在公司服务器中所有的资料删除。

iv、数据备份管理

服务器数据备份，应对数据库进行自动实时备份，并每周应至少做一次手工备份，并在备份服务器中进行逻辑备份的验证工作，经过验证的逻辑备份存放在不同的物理设备中。个人电脑的备份统一由各部门自行负责，可申请移动硬盘、信息光盘等储存介质进行安全备份。

第四条 计算机/电脑维修

1、计算机出现重大故障，须填写《计算机维修单》，并交it管理员进行维修。

2、it管理员对《计算机维修单》存档，便于查询各电脑使用情况。

3、须外出维修，须报分管领导审批。须采购配件，按采购管理流程执行。

第五条 公司信息系统管理(暂定)

1、新中大财务系统服务器(以下简称：服务器)，放置地点暂放为财务室办公室内，财务室现有办公室已达到视频监控、防盗、温度控制等条件。待条件成熟时重新搭建独立机房，便以安全管理。

2、对于服务器数据(包括财务软件系统)由管理员每月定期异地备份一次，并设置服务器自动每周备份二次数据库;异地备份数据由财务部安排存放在异地。

3、系统后台数据只能由服务器系统管理员进行维护，若需外援时，必须在管理员的陪同下进行操作，其他终端用户不得设置权限进入数据管理后台。

4、终端用户的开通及变更需以书面形式提交给相关部门领导签字确认，其中包括用户的权限变更、账号密码变更、终端软件更新。

5、当遇到服务器需要变更时，管理员应该做好详细的变更记录。如：程序变更、紧急变更、配置/ 参数变更、基础架构变更、数据库修改等。

6、定于每月25号对公司服务器账号进行核查及管理。

7、相关记录表格如下：

a、信息中心机房巡查记录表

b、信息中心用户账号登记表

c、数据库备份记录表

d、外来人员工作记录

e、终端用户系统变更申请

第六条 违规操作赔偿标准

1、违规操作者：没有造成经济损失的，当事人和责任人赔偿工作时间误工费50-100元。

2、违规操作者：造成经济损失的，除造价赔偿外，另外当事人与责任人赔偿误工费100元。

第六条 附则

1、本制度由信息管理部门负责解释，自公布之日起实施。

2、本制度有不妥之处在运行中修改并公布。

**医保信息安全管理制度篇二**

一、信息系统安全包括：软件安全和硬件网络安全两部分。

二、网络信息办公室人员必须采取有效的方法和技术，防止信息系统数据的丢失、破坏和失密;硬件破坏及失效等灾难性故障。

三、对系统用户的访问模块、访问权限由使用单位负责人提出，交信息化领导小组核准后，由网络信息办公室人员给予配置并存档，以后变更必须报批后才能更改，网络信息办公室做好变更日志存档。

四、系统管理人员应熟悉并严格监督数据库使用权限、用户密码使用情况，定期更换用户口令或密码。网络管理员、系统管理员、操作员调离岗位后一小时内由网络信息办公室负责人监督检查更换新的密码;厂方调试人员调试维护完成后一小时内，由系统管理员关闭或修改其所用帐号和密码。

五、网络信息办公室人员要主动对网络系统实行监控、查询，及时对故障进行有效隔离、排除和恢复工作，以防灾难性网络风暴发生。

六、网络系统所有设备的配置、安装、调试必须由网络信息办公室人负责，其他人员不得随意拆卸和移动。

七、上网操作人员必须严格遵守计算机及其他相关设备的操作规程，禁止其他人员进行与系统操作无关的工作。

八、严禁自行安装软件，特别是游戏软件，禁止在工作用电脑上打游戏。

九、所有进入网络的软盘、光盘、u 盘等其他存贮介质，必须经过网络信息办公室负责人同意并查毒，未经查毒的存贮介质绝对禁止上网使用，对造成“病毒”蔓延的有关人员，将对照《计算机信息系统处罚条例》进行相应的经济和行政处罚。

十、在医院还没有有效解决网络安全(未安装防火墙、高端杀毒软件、入侵检测系统和堡垒主机)的情况下，内外网独立运行，所有终端内外网不能混接，严禁外网用户通过u 盘等存贮介质拷贝文件到内网终端。

十一、内网用户所有文件传递，不得利用软盘、光盘和u 盘等存贮介质进行拷贝。

十二、保持计算机硬件网络设备清洁卫生，做好防尘、防水、防静电、防磁、防辐射、防鼠等安全工作。

十三、网络信息办公室人员有权监督和制止一切违反安全管理的行为。

一、对网络故障的判断

当网络系统终端发现计算机访问数据库速度迟缓、不能进入相应程序、不能保存数据、不能访问网络、应用程序非连续性工作时，要立即向网络信息办公室汇报，网络信息办公室工作人员对科室提出的上述问题必须重视，经核实后给予科室反馈信息。网络信息办公室负责人应召集有关人员及时进行讨论，如果故障原因明确，可以立刻恢复工作的，应立即恢复工作;如故障原因不明确、情况严重不能在短期内排除的，应立即报告医务部和院领导，在网络不能运转的情况下由机关协调全院工作以保障医疗工作的正常运转。网络故障分为三类：

一类故障：服务器不能工作;光纤损坏;主服务器数据丢失;备份盘损坏;服务器工作不稳定;局部网络不通;数据被人删改;重点终端故障;规律性的整体、局部软、硬件故障。

二类故障：单一终端软、硬件故障;单一患者信息丢失;偶然性的数据处理错误;某些科室违反工作流程要求。

三类故障：各终端由于不熟练或使用不当造成的错误。针对上述故障分类等级，处理方案如下：

一类故障———由网络信息办公室主任上报医务部和院领导，由医务部组织协调恢复工作。

二类故障———由技术工程师上报网络信息办公室主任，由网络信息办公室集中解决。

三类故障———由技术工程师单独解决，并详细登记情况。

二、网络整体故障的首要工作

(一)当网络信息办公室一旦确定为网络整体故障，首先是立刻报告医务部。医务部应立即按上报程序向院领导汇报。网络信息办公室需马上组织恢复工作，并充分考虑到特殊情况如节假日、病员量大、人员外出及医院的重大活动对故障恢复带来的时间影响。

(二)当发现网络整体故障时，根据故障恢复时间的程度将转入手工工作的时限明确如下：

1、10分钟内不能恢复———门诊挂号、住院登记、药房转入手工操作;门诊收费、住院核算、西药房工作转入老系统操作。

2、6小时内不能恢复———原则上将医师工作站、护士工作站、药房、急诊检查、入院、手术室、医技检查转入手工操作(具体实行时间及步骤由医务部、护理部通知)。

3、24小时以上不能恢复———将出院核算转入手工。

三、具体协调工作

(一)所有手工工作的统一时间须由医务部或网络信息办公室通知，相关单位严格按照通知时间协调工作，在未接到新的指示前不准私自操作计算机。

(二)门诊挂号工作协调

1、门诊挂号协调工作由门诊部护士长负责协调请示，如手工挂号的转入、转出时间等;

2、当网络系统中断时，改为手工挂号;

3、网络恢复后，及时将中断期间的患者信息输入到计算机;

4、在以后的工作中如发现某位患者的信息系统内没有记载，应详细询问患者以前是否是在网络故障时就诊过。

(三)门诊收费系统工作协调

1、由收款处科主任负责总体协调，并与网络信息办公室保持联系，及时反馈沟通最新消息;

2、当网络系统运行中断超过10分钟时，应通知收款处转入手工收款工作;

3、门诊收款负责同志应建立手工发票使用登记本，对发票使用情况做详细登记;

4、当系统恢复正常时，由收款处负责同志负责对网络运行稳定性进行监测，如不稳定，及时向网络信息办公室反映情况。

5、在接到使用计算机的指令并重新启动运行后，门诊收款负责人应组织收款员逐步转入到机器操作。

(四)住院费用核算系统工作协调

1、由住院处科主任总体负责协调工作;

2、当系统停止运行超过2天时，对普通出院患者，推迟出院结算时间;对急出院的患者应根据病历和临床科室护士工作站记录，进行手工核算出院。

3、在网络停止运行期间，出院患者急需结算时，应由该科护士工作站追查是否还有正在进行的检查，向结算室提供详细费用情况后，方可送交核算。

(五)临床工作系统协调

1、临床科工作由医务部、护理部共同协调;

2、网络故障期间临床科室详细记录患者的所有费用执行情况;

3、科室详细填写每个患者的药品请领单(包括姓名、id 号、费别、药品名称及用量)，一式两份，一份用于科室补录医嘱，另一份送西药房;

4、出院带药由经管医师负责掌握经费情况，如出现费用超支情况由该医师负责;

5、根据医务部通知恢复运行时间，按要求补录医嘱。

6、如患者急需出院，应向核算室提供详细费用情况，对正在进行的检查应予以说明。

(六)医技检查工作协调

1、在网络停运期间应详细留取、整理检查申请单底联;

2、网络恢复后根据检查单底联登记，通过手工记价补录患者费用;

3、对出院快或有出院倾向的患者各科在申请单上注明，检查科室应及时通知科室或出院处沟通费用情况。

(七)药房工作协调

1、中心摆药应严格按照网络信息办公室规定的时间及要求进行计算机操作;

2、网络故障时，根据临床科提供的药品请领单发药;

3、网络恢复时对临床科室补录的摆药医嘱进行发药补充确认，同时与发药时药品请领单内容详细核对，如发现内容不符，必须详细追查;

4、网络恢复后对出院带药处方及时进行录入;

5、数据补录工作结束后应查看系统内库存与实际库存相符情况。

各信息点接到重新运行通知时，需重新启动计算机，整体网络故障的工程恢复工作，由网络信息办公室严格按照服务器数据管理要求进行恢复工作。

四、网络修复后的数据处理

(一)由各科组织核校患者费用情况;

(二)药房校查库存;

(三)临床科室补录患者医嘱。

各科室要严格各项操作并及时反馈执行中的有关情况。

**医保信息安全管理制度篇三**

第一条 根据xx集团公司下达的集科[]83号文件《xx集团公司多媒体广域网络系统管理办法及信息技术规范的通知》的要求。制定网络安全管理制度，适合在大同发电有限公司内的管理信息网络中使用。

第二条 安全管理制度须从以下几个方面进行规范：物理层、网络层、平台安全，物理层包括环境安全和设备安全、网络层安全包含网络边界安全、平台安全包括系统层安全和应用层安全。

第三条 大同发电公司网络机房是网络系统的核心，除网络信息处管理人员外，其他人不经允许不得入内，网络信息处的管理人员不准在主机房内会客或带无关人员进入。未经许可，不得动用机房内设施

第四条 机房工作人员进入机房必须遵守相关工作制度和条例，不得从事与本职工作无关的事宜，每天下班前须检查设备电源情况，在确保安全的情况下，方可离开。

第五条 为防止磁化记录的破坏，机房内不准使用磁化杯、收音机等产生磁场的物体。

第六条 机房工作人员要严格按照设备操作规程进行操作，保证设备处于良好的运行状态。

第七条 机房温度要保持温度在18±5摄氏度，相对湿度在50%±5%。

第八条 做好机房和设备的卫生清扫工作，定期对设备进行除尘，保证机房和设备卫生、整洁。

第九条 机房设备必须符合防雷、防静电规定的措施，每年进行一次全面检查处理，计算机及辅助设备的电源须是接地的电源。

第十条 工作人员必须遵守劳动纪律，坚守岗位，认真履行机房值班制度，做好防火、防水、防盗等工作。

第十一条 机房电源不可以随意断开，对重要设备必须提供双套电源。并配备ups净化电源供电。公司办公楼如长时间停电须通知信息主管部门，制定相应的技术措施，并指明电源恢复时间。

第十二条 网络系统的主设备是连续运行的，网络信息处每天必须安排专职值班人员。

第十三条 负责监视、检查网络系统运行设备及其附属设备(如电源、空调等)的工作状况，发现问题及时向网络信息处领导报告，遇有紧急情况，须立即采取措施进行妥善处理。

第十四条 负责填写系统运行日志、操作日志，并将当日发生的重大事件填写在相关的记录本上。负责对必要的数据进行备份操作。

第十五条 负责保持机房的卫生及对温度、湿度的调整，负责监视并制止违章操作及无关人员的操作。

第十六条 不准带电拔插计算机及各种设备的信号连线。不准带电拔插计算机及各种设备。不准随意移动各种网络设备，确需移动的要经网络信息处领导同意。

第十七条 在维护与检修计算机及设备时，打开机箱外壳前须先关闭电源并释放掉自身所带静电(可摸一下暖气管或接地线)。

第十八条 公司网络与信息系统中，在网络边界和对外出口处必须配置网络防火墙。

第十九条 未实施网络安全管理措施的计算机设备禁止与internet相连。

第二十条 任何接入网络区域中的网络安全设备，必须使用经过国家有关安全部门认证的网络安全产品。

第二十一条 在计算机联入企业信息网络之后，禁止一其他任何方式(如拨号上网、isdn、adsl等)与internet相连。

第二十二条 对于公司企业内部网路应当根据应用功能不同的要求，必须进行网络分段管理，以防止通过局域网“包广播”方式恶意收集网络的信息。

第二十三条 禁止下载互联网上任何未经确认其安全性的软件，严禁使用盗版软件及游戏软件。

第二十四条 密码管理：密码的编码必须采用尽可能长并不易猜测的字符串，不能通过电子邮件等明文方式传送传输，密码必须定期更新。

第二十五条 登陆策略：仅给经过授权的用户暴露账号，不得设置多人共用的账号，连续登陆三次失败，须暂时禁止此账号并通知该账号用户。

第二十六条 普通系统用户：未经相关部门许可，禁止与其他人员共享账号和密码;禁止运行网络监听工具或其他黑客工具;禁止查阅别人的文件。

第二十七条 系统管理员：不得随意在系统中增加账号，随意修改权限，未经管理部门的许可，严禁委托他人行使管理员权利。

第二十八条 外来软盘或光盘须在没联网的单机上检查病毒，确认无毒后方可上网使用。私自使用造成病毒侵害要追究当事人责任。

第二十九条 网络系统的所有软件均不准私自拷贝出来赠送其它单位或个人，违者将严肃处理。

第三十条 实行专人负责检测病毒，定期进行检查，配备相应的实时病毒检测工具。

第三十一 条 严禁随意使用软盘和u盘等存储介质，如工作需要，须经过病毒检测方可使用。

第三十二条 严禁以任何途径和媒体传播计算机病毒，对于传播和感染计算机病毒者，视情节轻重，给予适当的处分。制造病毒或修改病毒程序制成者，要给予严肃处理。

第三十三条 发现病毒，应及时对感染病毒的设备进行隔离，情况严重时报相关部门并及时妥善处理。

第三十四条 实时进行防病毒监控，做好防病毒软件和病毒代码的智能升级。

第三十五条 应当注意保护网络数据信息的安全，对于存储在数据库中的关键数据，以及关键的应用系统应作数据备份，数据备份应当满足《电力大同发电公司数据备份管理制度》的要求。

第三十六条 本办法从公布之日起实施。 本办法由总经部网络信息处负责解释

**医保信息安全管理制度篇四**

1、医院计算机操作人员必须按照计算机正确的使用方法操作计算机系统。严禁暴力使用计算机或蓄意破坏计算机软硬件。

2、未经许可，不得擅自拆装计算机硬件系统，若须拆装，则通知信息科技术人员进行。

3、计算机的软件安装和卸载工作必须由信息科技术人员进行。

4、计算机的使用必须由其合法授权者使用，未经授权不得使用。

5、医院计算机仅限于医院内部工作使用，原则上不许接入互联网。因工作需要接入互联网的，需书面向医务科提出申请，经签字批准后交信息科负责接入。接入互联网的计算机必须安装正版的反病毒软件。并保证反病毒软件实时升级。

6、医院任何科室如发现或怀疑有计算机病毒侵入，应立即断开网络，同时通知信息科技术人员负责处理。信息科应采取措施清除，并向主管院领导报告备案。

7、医院计算机内不得安装游戏、即时通讯等与工作无关的软件，尽量不在院内计算机上使用来历不明的移动存储工具。

1、不得在医院网络中制作、复制、查阅和传播国家法律、法规所禁止的信息。

2、不得在医院网络中进行国家相关法律法规所禁止的活动。

3、未经允许，不得擅自修改计算机中与网络有关的设置。

4、未经允许，不得私自添加、删除与医院网络有关的软件。

5、未经允许，不得进入医院网络或者使用医院网络资源。

6、未经允许，不得对医院网络功能进行删除、修改或者增加。

7、未经允许，不得对医院网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加。

8、不得故意制作、传播计算机病毒等破坏性程序。

9、不得进行其他危害医院网络安全及正常运行的活动。

二、 网络硬件的管理网络硬件包括服务器、路由器、交换机、通信线路、不间断供电设备、机柜、配线架、信息点模块等提供网络服务的设施及设备。

1、各职能部门、各科室应妥善保管安置在本部门的网络设备、设施及通信。

2、不得破坏网络设备、设施及通信线路。由于事故原因造成的网络连接中断的，应根据其情节轻重予以处罚或赔偿。

3、未经允许，不得中断网络设备及设施的供电线路。因生产原因必须停电的，应提前通知网络管理人员。

4、不得擅自挪动、转移、增加、安装、拆卸网络设施及设备。特殊情况应提前通知网络管理人员，在得到允许后方可实施。

1、计算机及外设所配软件及驱动程序交网络管理人员保管，以便统一维护和管理。

2、管理系统软件由网络管理人员按使用范围进行安装，其他任何人不得安装、复制、传播此类软件。

3、网络资源及网络信息的使用权限由网络管理人员按医院的有关规定予以分配，任何人不得擅自超越权限使用网络资源及网络信息。

4、网络的使用人员应妥善保管各自的密码及身份认证文件，不得将密码及身份认证文件交与他人使用。

5、任何人不得将含有医院信息的计算机或各种存储介质交与无关人员。更不得利用医院数据信息获取不正当利益。

**医保信息安全管理制度篇五**

近年来， 随着计算机技术和信息技术的飞速发展，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。如何规范日趋复杂的信息安全保障体系建设，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：企业的信息及其安全隐患。

在我公司，我部门对信息安全做出整体规划：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，并针对信息安全提出解决方案。涉及到企业安全的信息包括以下方面：

a. 技术图纸。主要存在于技术部、项目部、质管部。

.b. 商务信息。主要存在于采购部、客服部。

c. 财务信息。主要存在于财务部。

d 服务器信息。主要存在于信管部。

e 密码信息。存在于各部门所有员工。

针对以上涉及到安全的信息，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，轻则丢失工作文件，重则泄露机密信息。

②不法分子等黑客风险。计算机网络的飞速发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发觉，尤其是技术部、项目部和财务部电脑若被黑客植入后门，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分布式拒绝服务攻击都由此而来，它会导致受攻击方服务器资源耗尽，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。若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，危害到企业的生存发展。

② 文件的打印风险。若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 文件的传真风险。若员工将纸质重要资料或技术图纸传真出去，以及将其他单位传真给公司的技术文 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。若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。若有动机不良的员工，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。若用户的开机密码、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;若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，甚至会被窃取整个服务器数据。

⑦ 机房设备风险。主要包括服务器、ups电源、网络交换机、电话交换机、光端机等。这些风险来自防 盗、防雷、防火、防水。若这些自然灾害发生，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安全。有些员工缺乏安全意识，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，若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安全保密，公司所有人员必须严格遵守企业信息安全管理总则，以安全总则为基础，各部门具体细则为安全管理行为标准，从各个层面杜绝信息安全隐患。

二、总则：从整个公司层出发，针对这些信息隐患制订安全防范措施。

1.计算机设备安全管理。

1) 公司所有人员应保持清洁、安全、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安全的物品。

2) 严格遵守计算机设备使用、开机、关机等安全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丢失的，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，原则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.部门资料安全管理。

1) 外接存储设备安全管理。

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。若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。为确保硬盘的安全，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，若信管部进行电脑硬件故障排查时，拆除封条标签后，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，若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，若需要为用户处理电脑故障时，信管部在打开锁柜处理完电脑故障时，一定要锁好主机柜，确保主机内硬盘的安全。

2) 文件传真安全管理。

所有人员对外发送传真，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传真文件，一经发现，所有后果将由个人承担。在对内传真文件时，应即刻通知传真接收人接收并取走传真件，在传真结束时，应马上取走传真原件。若因传真时没有取走传真件，导致传真件丢失，造成本部门信息外泄，则由本人承担一切后果。

3) 文件打印安全管理。

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。若在上班时间，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，若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，若因打印后，文件丢失，造成信息资料外泄，则由本人承担相关责任。

4) 文件的存储安全管理。

所有部门人员应每周清理计算机中的文件，清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。若因个人原因未执行备份，造成数据资料丢失时，将由本人承担相关后果。若员工离职，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，若没有执行此安全过程，离职员工损失的文件资料由该部门承担。

5) 办公区域的安全管理。

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。若因资料没有存放好，被他人取走，

造成的后果将由本人承担。

3.帐号密码安全管理。

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部分：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，若更改密码后，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丢失等问题，信管部不承担责任。

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安全性的复杂密码，严禁用户将密码设置为如123456等傻瓜式密码，若密码设置过于简单，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，若产生此情况，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。若因以上原因造成的信息安全后果将由本人承担。

3)采用用户身份认证系统：目前我公司登陆服务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服务器登陆密码，从而可能会被动机不良的员工登陆到服务器，破坏服务器数据;在企业外，容易遭到黑客字典扫描破解密码，从而攻击各应用服务器，破坏或盗取商业数据等。因此，我部门在未来的发展规划中，要将用户身份认证当作安全的一个重大隐患，想办法解决这个问题。

这里，我们可以采取动态口令牌或usb key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，保证服务器的登陆基于网内的行为、网外的行为都是安全的。

4..杀毒软件安全管理。

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.各类软件安全管理。

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.邮件安全管理。

所有因公对外联系的电子邮件一律通过公司邮箱或 或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安全防范意识，具体应做到：

日常工作信息安全：

1)员工应对在自己公司电脑内公司机密信息的安全负责，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，若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。

假期时间办公室的安全： 确保工作电脑的安全，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。

确保数据的安全：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：如果你发现在安全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。

常规注意事项

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.否则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，若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、申请人等项目，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。

三、细则：从各部门级出发，针对这些信息隐患制订安全防范措施。

1.采购部的安全处理措施如下：

1)采购招标的安全管理。

由采购部门编写招标计划，经部门负责人签字后，上报总经理审批，总经理根据生产过程的物料需求及原有的物料采购价格决定是否需要寻找新的货源，若审批同意后，采购部才可以开展招标工作。采购部门制定招标邀请书，邀请众多有法人资格、供货条件的单位参与我公司的招标活动。在发标书的过程中。采购部应遵守下列原则：①招标的公开性：对于采购的招标信息应该公开;评标的标准和程序应该公开;中标的结果应该公开。②招标的公平与公正：对待各方投标者一视同仁，不得对任何投标方带有主观意见。③招标的保密性：采购部人员严禁以任何形式向投标方透露招标的意向。评标完成后提交评标报告给总经理，最后由总经理中标、授标。

2)采购价格及供应商的信息安全保密。

采购信息的保密要求采购部所有人员不得以任何形式向其他部门或外部人员透露物料采购的价格，严禁向他人透露各种物料的供货来源。采购部门人员要随时检查个人办公区域的文件资料是否存放好，防止因打印的采购价格表和供应商联络单没有存放好，导致采购信息资料外泄。要求部门人员要严格保管好工作纸质文件，同时一定要在电脑中设置带密码的屏幕保护确保价格信息与供应商资料的电子信息安全。

2.客服部有如下工作存在安全隐患：

1)及时向甲方传递发货信息与到货信息。

2)甲方基地发货及库存统计：记录甲方发往各风场的数据，盘点甲方各基地库存数;

3)总经办工作安排。

以上存在的安全隐患及处理措施如下：

a)发货、到货、现场库存信息安全。

客服部人员在统计往风场发货及现场库存的时候，可能会因为客服部盘点疏忽，最终统计的库存结果不准确。这会造成公司的发货信息与现场到货数量不一致，从而得迅速查找整个发货到货流程的出错环节;甚至会因为库存统计的不准确，延迟发货到货时间，导致现场库不能及时向风场发货，从而影响客户的业务。客服部现场人员必须每日在oa中编写日记，以便部门领导能随时掌握此现场人员的工作动态，现场人员要认真盘点到货数量及现场库存信息，在现场与甲方进行每月、每季、每年度的数据核对，确保到货数量与

发货数量一致，并随时向部门负责人汇报。

b)总经办的日程安排管理。

在实际的工作中，总经理因工作繁忙暂时不在公司，一些待办理的工作无法通过审核。客服部负责人要了解总经办的行程，并确保行程不被泄露，保证总经理的其他事务不会受到打扰，在总经理方便时，提醒总经理处理一些比较紧急的待办文件;若总经理不在公司，以先短信后电话的形式给总经理汇报待办理的文件类型，在总经理办理完成后，及时将文件下发给相应部门。

3.项目部的安全处理措施如下：

1)图纸的安全管理。

项目部的图纸只允许在部门内部传阅。在进行项目生产时，工艺员申请借阅项目图纸，经签字确认后，档案专员将图纸副本发放给工艺员，工艺员负责监督技术人员和操作人员严格按照图纸进行生产，确保生产过程符合iso9000体系要求。生产完成后，工艺员将图纸返还给档案专员，图纸副本重新归档。在借阅过程中，严禁借用人将图纸传阅给其他人员，一经发现，必将严肃处理。

2)工艺技术文件的安全管理。

项目生产的工艺技术文件由计划员归档保存，在组织生产人员进行操作培训时，指导操作人员学习质量文件和相关工艺规程，培训过程中，确保工艺技术文件只在培训过程中流转，培训完成后，收回所有的技术文件，禁止任何人以任何理由将文件带出公司。禁止任何人复印、传真此类文件。

3)人员的安全管理。

项目部保管着生产技术文件和图纸，公司的人员流动很容易造成技术的泄露。鉴于此，部门应严格控制工艺技术文件及图纸的传阅。文件将由专员保管。禁止部门人员在未经允许的情况下传真或复印此类文件;在部门员工调动或离职前，由部门档案专员收回该员工所有工作文件。若档案专员调动或离职，由部门经理亲自收回该岗位所有的工作资料，并清点所有书面文件和电子文件是否存在缺省或丢失的情况，最大程度避免人员的流动造成技术资料的外泄。

4.仓储部存在的安全隐患及处理措施如下：

a)物料库存安全。

物料采购入库后，仓储部做好物资的保管工作，如实登记仓库实物账，经常清查、盘点库存物资，确保系统帐、查存卡、实物一致;做好物资采购、存储、生产领用各环节平衡衔接工作，做到物料的先进先出，当保管物料的库存量不足时，及时通知采购部，由采购部制定新的计划进行物料采购，再入库存，确保生产有序进行。

b)物料信息安全。

仓储部所有人员不得向任何人以任何形式透露各种物料的供货数量、供货来源。仓储部负责人应严格规范

部门人员的安全防范意识，并严格存放好入库单和领料单等纸质单据，确保不会因为单据的存放不善而泄露物料供货信息。

c)仓库整体安全。

做好物资的存储工作，按品种、规格、体积、重量等特征决定存放的方式与位置，仓库物品堆放整齐、平稳，合理利用储物空间，减少地面负荷，便于盘存和领取，并有效做到先进先出;做好仓库的安全、防火、防盗、防爆、卫生工作，确保仓库和物资的安全;对危险品需进行单独存放与隔离、管制。

5.技术研发部的安全处理措施如下：

1)图纸的归档

a) 外来书面图纸：公司指定收件人收到后整理并编制归档，确认完整无误后，交由综合部档案管理员。图纸蓝图邮寄到北京，复印件登记，入库经总经理批示发放至相应部门。

b) 电子版图纸：外来电子版图纸，由公司指定专人负责接收。打印一份，并同时将电子文件交档案管理员登记入库，经总经理批示发放至相应部门;若外来电子版图纸已由对方传至我方项目人员处，项目人员应将图纸资料整理后报综合部存档，由综合部统一打印及按公司规定下发至相应的职能部门，若出现图纸变更时，综合部应及时替换旧版电子图，并回收已发放的旧版图纸。

c) 内部设计电子版图纸：在工程完工后一周内，技术人员应将最后定稿图纸交由综合部，由其在三天内加密统一刻录光盘。一式两份，公司领导及综合部档案管理员各保管一份。

2)外来工艺文件、技术规格书

技术人员在收到文件后1个工作日内整理无误，交综合部档案管理员登记、入库经总经理批示后方能发放。

3)内部拟定的工艺文件、技术规范文件

a) 公司自行编写的生产工艺文件，经总经理审批签署后交综合部档案管理员入库存档。

b) 移交文件时，移交人应备有档案实体和目录，经档案管理员对照验收无误后方能办理移交登记手续。

c) 档案管理专员应仔细检查文件材料是否完整、齐全、签署是否齐全、凡不符合规定要求者，有权拒绝接收，并限期改正补交。

d) 移交时，移交和 接收文件方均应建立书面移交记录。

4)技术图书、期刊、标准的管理

公司购入的技术图书、期刊和标准，均属公司固定资产，应由综合部加盖行政专用章后登记、入库、领用、借用、查阅应办理审批、发入登记手续。损坏、丢失应由责任人负责全价赔偿或购买新书。

5)技术，项目往来传真件

综合部收到技术文件后，下发到相应部门，相关责任人签收签字。同时保留复印件，按项目不同分类，待项目结束后，各负责人将其保存的传真复印件整理装订后归档。

6)技术，项目往来电子邮件

由公司指定接收人以及综合部邮箱管理员定期下载整理。每月将电子邮件交综合部统一刻制成光盘存档。

7)本行业其他公司宣传画册、样本、产品信息等文件，由综合部按《样本资料明细表》登记保管，使用人可查询使用，不得私自留存。

8)技术文件的复印

归档的技术文件确因工作原因需要复印时，须由使用人到综合部填写《资料复印申请表》经总经理批准后，综合部指定人员复印后发放至使用人。

9)技术文件的借阅

a)借阅手续：各部门有关工作人员因工作需要借阅归档技术文件，应办理调阅手续，经部门负责人签字，交公司领导批准后方可办理借阅手续。

b)借阅记录：档案管理员应有清楚、准确的借阅记录，包括借阅人、借阅资料名称、借阅时间、归还时间、签字等。

c)借阅时间：一般最长不超过8个工作时，超过8个小时需在办理调档申请时特别说明。如员工因工作原因经批准需要带出资料时，则其返回后一个工作日内归还。

d)归还要求：借阅的资料交还时，必须由经办人当面点交清楚，如发现遗失或损坏，应立即报告领导，同时应追究使用人的责任。

公司所有技术文件均应先由综合部专人登记入库后，经总经理批示后分发至相应部门负责人处，由其向部门员工下发。各部门负责人应做好本部门技术资料的保密工作，若保管技术资料人员离职时应向综合部交回相关的技术资料。综合部下发技术文件时，须由签收人签字确认。

6.质管部的安全处理措施如下：

1)工艺文件的安全管理。

部门档案专员保管本部门的工艺文件。此文件用于检验新工艺生产过程中各环节是否存在质量不合格的情况，若要进行生产过程检验，在部门负责人授权下，部门档案专员将工艺文件副本传阅给质量管理工程师及部门其他管理人员，质量工程师或其他管理人员根据工艺文件的标准，对生产现场各道工序施工工艺、方法、操作规程进行检查监督，提出生产过程中的不合项，对不合格项进行跟踪验证。生产过程检验完毕后，质量工程师将工艺文件副本返还给部门档案专员，最后由档案专员进行文件归档。工艺文件仅允许部门内部管理人员传阅，不得借阅给其他任何部门及工人。若部门管理人员借阅工艺文件后，造成的文件丢失，则借阅者承担相关责任。

2)验收图纸的安全管理。

验收图纸用于检验生产完工后的产品是否合格，由部门档案专员保管。质量工程师借阅验收图纸后，以此为标准对完工产品进行鉴定，若合格，则调入成品库;若不合格，则对不合格项进行跟踪验证，直到产品合格为止。验收图纸借阅分为以下几种情况：①内部管理人员借阅。验收图纸只允许本部门内管理人员的互相传阅，借阅人在档案专员处登记，确定归还时间后，档案专员对其分发验收图纸副本，借阅完后，及时归还给档案专员，禁止传阅给部门非管理人员。②技术研发部人员借阅。只有技术研发部人员才能借阅本部门验收图纸。在借阅时，要遵守借阅流程，在技术研发部经理签字后，上报总经理审批，总经理审核通过后，质管部方可将验收图纸副本借阅给相关人员，并要求在8个小时内归还图纸。图纸借阅过程中，严禁将图纸传阅给其他人员，或私自将图纸进行复印或扫描，一经发现，必将严肃处理。③验收图纸不得传阅给其他部门人员，也不得传阅给本部门非管理人员。一经发现，追究档案专员相关责任。

7.财务部的安全处理措施如下：

1)财务部为公司重要数据信息部门，除本部门在内工作外，其他无关人员不得入内。

2)财务人员去银行取现金、支票等，应两人以上同行，禁止途中办理任何与此项工作无关事宜。

3)妥善存放支票，支票与有效密码及专用印鉴要分别存放。

4)出纳人员不得私配保险柜钥匙，不得将保险柜密码外传，过节或放假时，要与综合部配合，对保险柜加贴封条。 若因密码钥匙保管不善，导致现金及其他财产损失，将由本人承担一切损失。

5)会计人员应妥善保管好各类凭证及发票，不得在凭证发票随意摆放在办公桌的情况下离开办公区域。凭证发票录入核对完毕，应立即整理存放到财务凭证专柜中，同时确保上锁，并妥善保管好钥匙，若因以上原因造成财务数据丢失，将由本人承担一切后果。

6)财务人员应保管好电子银行或其他一切与财务有关的加密锁，在使用时，使用人不得离开电脑，确保所做的一切操作均出自本人之手。若使用完毕，一定要将加密锁存放于财务专柜中妥善保管。

7)财务部门因为数据的重要性，因此对安全的要求很高。在使用电脑时，要求财务部门人员一定要每天升级杀毒软件，若电脑出现异常，应联系信管部查明原因，是否能安全操作。

8)财务部是企业工资的发放部门，掌管着企业全体人员的工资详情。由于工资向来是公司的敏感信息，因此，财务的工作要求财务所有人员应严格遵守职业素养，严禁财务部人员以任何形式向任何人透露工资或奖金信息。

8.综合部的安全处理措施如下：

1)技术类文件、图纸和图书的安全管理。

综合部指定收件人收到外来书面图纸后整理并编制归档，确认完整无误后，交由档案管理员。图纸蓝图邮寄到北京，将复印件登记，再经总经理批示后发放至相应部门。综合部指定收件人接收到外来电子版图纸，打印一份，并同时将电子文件交档案管理员登记入库，经总经理批示发放至相应部门，若图纸出现变更时，综合部应及时替换旧版电子图，并回收已发放的旧版图纸。公司购入的技术图书、期刊和标准，均属公司固定资产，应由综合部加盖行政专用章后登记、入库、领用、借用、查阅应办理审批、发入登记手续。损坏、丢失应由责任人负责全价赔偿或购买新书。

2)涉外合同的安全管理。

综合部统一管理各部门的涉外合同。各部门将已盖章的合同原件提交给综合部后，由综合部将其分类归档到指定的档案盒中，并将档案盒编号题名存放于指定的档案柜中，将档案柜锁好。由指定的档案管理员保管钥匙。各部门需要借阅已归档的合同资料，需要向综合部提出申请，经综合部负责人审批通过后，档案管理员方可开启档案盒调出文件发放给相关部门;原则上不允许各部门向综合部借阅其他部门的合同资料，若确因工作原因需要借阅，则应提交总经理审批，综合部在看到总经理的签字后方可指派档案管理员借出资料，并规定借阅时间不得超过8个小时，由借阅人签字，在借阅过程中造成的合同资料丢失，将由借阅人承担相关后果。严禁档案管理员在未经许可的情况下私自开启任何类型的档案盒;严禁档案管理员将档案柜钥匙借给任何人，若因此造成的合同信息泄露、合同丢失将由档案管理员承担一切责任。

3)工资编制的安全管理。

综合部统一核算管理人员和工人工资。工资针对于所有部门都是保密的，综合部在核算员工工资的时候，应该谨慎处理，如在电子表的发送之前，可以设置相应的密码，防止不小心发送到其他人电脑上，在打印工资表的时候，应单独设置非监控直接打印，并立即去打印机取走打印表。工资的核算应严格以考勤、绩效为依据核算，不得擅自更改原始依据。工资核算完成后，上报公司领导审批。 严禁工资核算人向他人透露公司工资及奖金信息，严禁在任何场合与他人讨论工资话题，一经发现，将追究其相关责任。

9.信管部的安全处理措施如下：

1)计算机网络设备安全管理。

公司所有计算机及网络设备统一归信息管理部管理。本制度所涉及产品的界定：

a) 计算机是指为公司内部员工使用的pc机(包括cpu、硬盘、内存、机箱、显示器、网卡、键盘和鼠标。主机板和显示卡由本公司提供，如非特殊需要不配备光驱和软驱。)

b)网络设备是指公司内部使用的服务器、网络交换机、路由器、集线器、以及网络接入设备等。

c)计算机其他配件是指公司备用的光驱、软驱等。

d) 附带软件包括计算机驱动盘、系统安装盘、程序安装盘等。

e) 包括计算机及耗材的采购计划、故障维修等项工作。

在员工电脑各组件老化或损坏，严重影响工作效率时，信管部可申请以旧换新或报废处理。若需要报废，则填写报废申请单经部门负责人确认后上报总经理审批，审批通过后才能作报废处理，信管部不得擅自处理破旧的电脑或电子设备。

2)公司所有输入输出设备统一归信息管理部管理。

输入输出设备包括扫描仪，传真机，打印机。使用者在使用此相关设备遇到问题可寻信息管理部帮助。在使用设备过程中遇到故障要及时向信息管理部反映，以便信息管理部及时查找原因，解决故障。

3)公司视频会议设备和视频监控设备统一由信息管理部管理。

a)视频会议设备包括视频会议服务器、视频会议终端、sony摄像头、会议话筒、电视、投影仪以及键盘、接收器、遥控器和线材部分。信息管理部负责以上设备的维护管理工作包括视频会议的搭建。

b)视频监控设备包括监控服务器、监控系统以及各路视频采集器。信息管理部负责各路视频的监控以及备份和维护工作。

4)信息化系统erp、oa帐户安全管理

系统管理帐号的设置与管理

a)erp、oa系统管理帐号必须经过总经理授权取得。

b)erp系统管理员负责erp系统帐套环境生成、维护，负责一般操作帐号的生成和维护，负责故障恢复等管理及维护;oa系统管理员负责oa系统自定义表单的生成、流程的建设和优化。

c)erp、oa系统管理员对业务系统进行数据整理、故障恢复等操作，必须有相关部门的签字和领导的审批授权。

d)erp、oa操作用户需要增加或修改权限需要填写erp/oa用户权限申请表，并经过本部门负责人签字后交由总经理审核，通过后，再由信息管理部作权限相关处理。

e)系统管理员不得使用他人帐号进行业务操作。

f)系统管理员调离岗位或离职，信息管理部负责人应及时注销其帐号并生成新的系统管理员帐号。 一般操作帐号的设置与管理

a)一般操作帐号由系统管理员根据各类应用系统操作要求生成，应按每用户一帐号对应设置。

b)操作员调离岗位，系统管理员应及时注销其帐号并在新员工入职时根据需要生成新的操作员帐号。

5)密码安全管理

a)终端计算机密码安全管理：系统管理员及时登记公司所有用户电脑密码，制成《用户电脑密码登记》文件。在用户人员变动或电脑更换时，系统管理员及时登记相应的新密码。

b)应用服务器密码安全管理：包括erp服务器、oa服务器、域服务器、邮箱服务器。信息管理部为确保服务器置于外网相对安全，针对每个服务器创建一个复杂的、不同的密码，并每年更换一次新密码。制成《服务器密码登记》文件，并提交给部门负责人。

c)防火墙/路由器密码安全管理: 防火墙和路由器的密码和服务器管理方法一样，设置成不同的、复杂的密码，并每年更换一次，将密码登记到《网络设备密码登记文件》中，并提交给部门负责人。

d)erp/oa系统密码安全管理: erp/oa系统密码分为管理员密码和操作用户密码。系统管理员登录密码由erp/oa管理员掌管，为保证系统安全需要定期更改时，及时上报部门负责人。操作用户密码由erp/oa管理员在创建帐户时初始生成，信息管理部发放帐号密码后，由用户本人修改密码，并自行保管好自己的密码，如特殊原因忘记密码时，由erp/oa管理员帮其初始化密码。

信管部应将所有的服务器和网络设备设置不同的密码，所有的密码仅限于信管部内部人员掌握，不得向其他部门人员透露，在特殊情况下，需要供应商做远程调试时，方可透漏相关设备密码，在调试结束后，应尽快更改密码。并通知部门内其他人员。由于服务器及网络设备均置于公网上，容易受到不法分子攻击，因此，需要定期更改密码，且密码复杂性尽可能设置高。

6)数据备份安全管理

定期备份erp服务器、oa服务器、邮箱服务器。具体备份方法如下：

a)erp服务器备份：每天早上自动备份e3帐套和5000帐套。

b)oa服务器备份：每天早上9：00备份oa数据库，并于每周五早上9：00备份oa系统文件夹。

c)邮箱服务器备份：每周五早上9：00在邮箱控制台执行备份操作，并于每月28日备份邮箱目录文件夹。备份完成后，将备份文件转存到其他电脑上或移动硬盘上做异地归档，以防本地硬盘发生故障时能随时做灾难恢复。

数据清理前必须对数据进行备份，在确认备份正确后方可进行清理操作。历次清理前的备份数据要根据备份策略进行定期保存或永久保存，并确保可以随时使用。数据清理的实施应避开企业网络应用高峰，避免对各部门工作造成影响。数据的清理包括：

a)erp系统中错误单据的清理、错误初始资料的清理、人员变动记录的清理。

b)oa系统中错误流程的清理、错误审批单的清理、人员变动记录的清理。

c)邮箱系统中垃圾邮件的清理、人员变动记录的清理。

d)用户电脑中系统垃圾文件的清理、ie缓存的清理。

7)信息资料安全管理

a)加密系统管理;目前我公司使用的是天盾文档加密系统，对常用办公软件office、pdf、autocad文件加密，公司内部的此类文件被带出公司后，显示在其他的电脑上均为乱码，保证了各个部门在未授权的情况无法将公司的文件资料泄露出去。然而，我公司因为之前的需求，加密软件使用的是单机版与网络版混合使用的，网络版可以根据策略的下发，实现文件在企业网的加密、反截图、禁usb等功能，但脱离局域网后，电脑无法打开文件，若有出差人员在外地使用电脑，就无法使用网络版;而单机版就解决了出差人员电脑加密的问题，可以正常打开公司的文件，但这里存在一个安全风险，若出差人员的电脑被盗，将会造成企业信息资料的外泄。针对以上情况，我们需要寻找一种更加适合的加密软件，确保使用一种版本就能够融合单机与网络的优势。我们需要这种加密软件实现如下功能：能够通过控制台在公司网内加密指定类型的文件，同时可以设置不同的加密权限对应于不同的用户组;能够根据需要设置文件能否在脱离公司网的情况下使用以及使用的时间限制等;能够加密原加密软件不支持的文件类型;能够荧荧于所有的windows平台上;能够禁用usb存储设备，不禁用usb外设;能禁止用户屏幕截图;能审计打印等。

b)大蓝监控软件管理：监控软件在很大程度上起到威慑作用，监控软件能够记录所有用户在个人电脑上的一举一动，通过实时屏幕监控、屏幕录象、插入存储设备报警、网页及程序过滤等功能及时抓出威胁企业信息安全的元凶。

c)打印控制软件管理：打印控制软件应用后，员工的打印需要在管理员审核通过后方能打印，若管理员审核到某员工的打印内容涉及本公司信息安全，拒绝员工的打印。在审核通过、打印完成后，管理员可随时调出以前的打印记录，保证了及时信息安全责任追究。

d)设备送外维修，须经设备管理部门负责人批准。送修前，需将设备存储介质内应用软件和数据备份后删除，并进行登记。对修复的设备，设备维修人员应对设备进行验收、病毒检测和登记。

e)信息管理部和综合部对报废设备中存有的程序、数据资料进行备份后清除，并妥善处理废弃无用的资料和介质，防止泄密。

f)信息管理部负责计算机病毒的防治工作，建立本单位的计算机病毒防治管理制度，经常进行计算机病毒检查，发现病毒及时清除。

g)用户计算机未经信息管理部允许不准安装其它软件、不准使用来历不明的载体(包括软盘、光盘、移动硬盘等)。

8)机房安全管理

①非信息管理部人员不得进入机房，信管部人员要确保机房大门时刻处于关闭状态。若因为工作需要进入机房时，完成相关操作后，一定要关好机房大门，并保管好机房钥匙。

②保持机房整齐清洁，各种机器设备按维护计划定期进行保养，保持清洁光亮。

③确保机房防水，定期检查机房天花板、四壁有无漏水现象，保证机房内的服务器和其他电器设备的安全。

a)发生机房漏水时，信管部应立即通知综合部联系大厦物业，同时，信管部第一时间保护好服务器及其他设备，避免设备浸水后损坏。

b)若为墙体或窗户渗漏水，应急领导小组应立即采取有效措施确保机房安全，同时安排通知综合部协助及时清除积水，维修墙体或窗户，消除渗漏水隐患。

④确保机房防火，定期检查机房内灭火器状态完好无损。

a)完善机房环境，确保机房具备二氧化碳灭火器;禁止携带易燃易爆物品进入机房。

b)一旦发生火灾，迅速切断机房电源，避免灾情的扩散，并迅速拨打物业管理和119火警电话。

c)等待消防车到来期间,应组织物业保安或工作人员在保证安全的前提下灭火,应急领导小组应在第一时间内集中所有二氧化碳灭火器,抓住时机,尽可能的把火扑灭。

d)配合消防部门调查事故原因，对造成的损失和起火原因做好记录，以便进行灾后总结。

⑤确保机房防雷，遇到暴风雨恶劣天气，应作防范性处理。

a)遇雷暴天气，信管部在下班后应及时关闭所有服务器，切断电源，暂停内部计算机网络工作。

b)雷暴天气结束后，信管部应及时开通服务器，恢复内部计算机网络工作，对设备和数据进行检查。出现故障的，事发部门应将故障情况及时报告应急领导小组。

c)因雷击造成损失的，信管部应会同综合部进行核实、报损，并在调查工作结束后一日内书面报告领导。 应急领导小组每日查看、清点设备并锁好机房大门。

⑥确保在停电后，业务应用的安全管理。

信管部在接到停电通知时，应设置便签提醒自己具体要停电的时间，若停电时间在上班时间，则提前发出通知给北京和常州所有人员，避免在停电时出现文件损坏或资料丢失;若停电时间发生在下班时间，则在下班时通知所有人关闭电源，同时信管部及时关闭服务器，以免停电损坏主机电源。 停电结束后，打开各应用服务器，并谨记要打开视频监控服务器，恢复闭路监控系统正常工作。 ⑦确保机房防盗，针对此环节，作相关防范处理。

a)信息管理部每日查看、清点设备并锁好机房大门。

b)信息管理部每日检查录像监控服务器状态，确保监控画面正常，并检查每日录像正常性、完整性。

c)发生设备被盗或人为损害设备情况时，使用者或管理者应立即报告信息管理部，同时保护好现场。

d)信管部接报后，即刻调出监控录像，搜查可疑行迹，若无法解决，可联系公安部门处理。

提高行业信息化管理水平，信息安全是关键。而信息安全构建必须管理、技术两者双管齐下：

1)加强管理，综合防范。 安全体系是一个整体的、系统的工程，不是简单的“技术积木”。它是技术、管理的有机结合体。管理者必须以预防为主、综合管理、人员防范和技术防范相结合，逐级建立多层次的安全防护体系，综全防范实现分级阻止违规行为，实现一体化的安全系统。

2)完善制度，强化培训。完善的信息安全管理制度是行业信息系统安全运行的基础保证。为系统资源规定明确使用的权限，对员工按其职责划定必要的最小授权范围，明确安全责任。确保安全措施落实、有效，加强员工的信息安全教育和培训，强化安全意识和法治观念。提高员工的职业道德和信息化应用水平。

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找