公司网络安全管理制度优秀7篇（公司网络安全管理制度优秀7篇内容）

作者：有故事的人 来源：范文网 www.wtabcd.cn/fanwen/

本文原地址：https://www.wtabcd.cn/fanwen/meiwen/a91880977ee9eefbc9fd98fe99912039.html

在不断进步的时代，需要使用制度的场合越来越多，制度是指在特定社会范围内统一的、调节人与人之间社会关系的一系列习惯、道德、法律(包括宪法和各种具体法规)、戒律、规章(包括政府制定的条例)等的总和它由社会认可的非正式约束、国家规定的正式约束和实施机制三个部分构成。拟起制度来就毫无头绪？t7t8美文号为您精心收集了7篇《公司网络安全管理制度》，希望能够满足亲的需求。

公司网络安全管理制度 篇一

一、目的：

合理利用工厂网络资源，更好服务于大家，同时杜绝违规上网现象，特订立本办法。

二、适用范围：

适用于工厂所有电脑使用者。

三、内容：

（一）总则

1.工厂建立网络信息设施、综合信息管理的网络支撑环境，实现各部门电脑互联、支持信息资源共享，并通过Internet与互联网联接，提供互联网信息服务办公。

2.电脑部负责工厂网络规划，承担网络建设、管理和维护工作，并对各联网部门提供技术支持和培训，是工厂网络管理之主责部门。

（二）上网要求

1.上网用户必须遵守《计算机信息网络国际联网安全保护管理办法》，严格执行安全保密制度，对所提供的信息负责。不得利用工厂网络从事危害工厂安全、泄露工厂秘密等违规活动，不得制作、查阅、复制和传播有碍社会治安和有伤风化的信息。

2.上网用户必须遵守《国家计算机信息系统安全保护条例》，不在工厂网络上进行任何干扰网络用户、破坏网络服务和破坏网络设备的活动。这些活动主要包括（但并不局限于）在网络上发布不真实的信息、散布计算机病毒、使用网络进入未经授权使用的计算机、以不真实身份使用网络资源等。

3.上网用户必须接受并配合工厂相关部门依法进行的监督检查，有义务向管理部门报告网上违法犯罪行为和有害信息。

4.遵守《国家计算机信息网络国际联网管理暂行规定》和国家有关法律、法规。不允许利用网络传播小道消息或进行人身攻击。

5.上网时，禁止浏览色情、反动及与工作无关的网页。浏览信息时，不要随意下载网页信息，特别是不要随意打开不明来历的邮件及附件，避免网上病毒入侵。

（三）网络开通

1.电脑部将根据工作需要及职级开通网络，有特殊要求需由公司主管领导批准后开通。

2.网络使用人填写《上网申请表》提出目前遇到的困难和所需功能要求，按表中内容经电脑部及部门主管、经理签批后，同时经行政部加签意见，报电脑部办理开通手续。

（四）网络管理

1.上网时，禁止浏览与工作无关的内容；禁止浏览色情、反动及与工作无关的网页。浏览信息时，不要随便下载网页的信息，特别是不要随便打开不明来历的邮件及附件，以免网上病毒入侵。禁止进行与工作无关的各种网上活动。

2.邮件与网络系统都属于工厂资产，工厂有权监视工厂内部电子邮件与网络行为。

3.为避免员工沉迷于网络、占用网络带宽、影响其它人正常使用网络工作、以及电脑感染病毒、网络无法正常运行，工厂利用网络管理系统进行网络自动控制，对各种网络应用进行控制和记录，包括实时记录局域网内电脑所有对外收发的邮件、浏览的网页以及上传下载的文件，监视和管理网内用户的聊天行为，限制、阻断网内用户访问指定网络资源或网络协议等等。

（五）违规处理

网络用户必须接受工厂网络主管部门的监督检查，对违规的用户，将视其情节轻重分别对其进行警告、处罚、记过、辞退等处理，情节严重者将追究其法律责任。

1.避免浪费电力、保护电脑设施及安全考虑，各人员白天下班时，应自行把显示器关闭，晚上不加班者或加班完毕后，电脑主机及显示器需统一关闭，违者给予记缺点处理。若因工作需要不能关机的应在电脑上贴标识或小标签说明“电脑在处理工作运行中”，避免他人不知情帮你关闭。

2.不允许电脑荧屏上设置色彩斑斓之“明星图片、宠物图片及其它照片”，只可用Windows原有的荧屏图片。违者记缺点一次。

3.接收到不明或病毒邮件，须按电脑部提示及时删除，不得点击运行造成感染病毒。

4.严禁使用网络下载与工作无关的内容，因工作需要下载资料，应安排合理时间下载(如下班或晚上加班时间)。违者处改善金100元/次。

5.工作时间内，上网浏览与工作无关的内容或出现异常上网记录（如：上班时间有QQ聊天记录、论坛聊天记录等），处改善金50元/次。若因个人事务需要使用网络资源，如接收邮件或搜寻数据，在与本规定没有抵触的情况下，可在用餐后的工余时间使用。

6.严禁盗用他人IP地址及帐户，窃取他人电脑资料；严禁利用“黑客软件”、“木马程序”等攻击他人计算机，窃取他人网络资源。违者视情节给予记大过或开除处分。

7.利用工厂网络传播病毒，危害工厂网络安全；制作、下载、复制、查阅、发布、传播或以其它方式使用反动、淫秽色情等有害信息的，给予记大过或开除处分，情节严重的追究其法律责任。

8.利用网络泄露工厂机密的，将根据《员工保密协议》相关条款追究法律责任。

四、附则

（一）本办法由行政部负责解释。

（二）本办法自二0xx年十一月十日起执行。

公司网络安全管理制度 篇二

计算机网络为集团局域网提供网络基础平台服务和互联网接入服务，由信息部负责计算机连网和网络管理工作。为保证集团局域网能够安全可靠地运行，充分发挥信息服务方面的重要作用，更好地为集团员工提供服务。现制定并发布《网络及网络安全管理制度》。

第一条：所有网络设备（包括光纤、路由器、交换机、集线器等）均归信息部所管辖，其安装、维护等操作由信息部工作人员进行。其他任何人不得破坏或擅自维修。

第二条：所有集团内计算机网络部分的扩展必须经过信息部实施或批准实施，未经许可任何部门不得私自连接交换机、集线器等网络设备，不得私自接入网络。信息部有权拆除用户私自接入的网络线路并进行处罚措施。

第三条：各部门的联网工作必须事先报经信息部，由信息部做网络实施方案。

第四条：集团局域网的网络配置由信息部统一规划管理，其他任何人不得私自更改网络配置。

第五条：接入集团局域网的客户端计算机的网络配置由信息部部署的DHCP服务器统一管理分配，包括：用户计算机的IP地址、网关、DNS和WINS服务器地址等信息。未经许可，任何人不得使用静态网络配置。

第六条：任何接入集团局域网的客户端计算机不得安装配置DHCP服务。一经发现，将给予通报并交有关部门严肃处理。

第七条：网络安全：严格执行国家《网络安全管理制度》。对在集团局域网上从事任何有悖网络法规活动者，将视其情节轻重交有关部门或公安机关处理。

第八条：集团员工具有信息保密的义务。任何人不得利用计算机网络泄漏公司机密、技术资料和其它保密资料。

第九条：任何人不得在局域网络和互联网上发布有损集团形象和职工声誉的信息。

第十条：任何人不得扫描、攻击集团计算机网络。

第十一条：任何人不得扫描、攻击他人计算机，不得盗用、窃取他人资料、信息等。第十二条：为了避免或减少计算机病毒对系统、数据造成的影响，接入集团局域网的所有用户必须遵循以下规定：

1、任何单位和个人不得制作计算机病毒；不得故意传播计算机病毒，危害计算机信息系统安全；不得向他人提供含有计算机病毒的文件、软件、媒体。

2、采取有效的计算机病毒安全技术防治措施。建议客户端计算机安装使用信息部部署发布的瑞星杀毒软件和360安全卫士对病毒和木马进行查杀。

3、定期或及时更新用更新后的新版本的杀病毒软件检测、清除计算机中的病毒。第十三条：集团的互联网连接只允许员工为了工作、学习和工余的休闲使用，使用时必须遵守有关的国家、企业的法律和规程，严禁传播淫秽、反动等违犯国家法律和中国道德与风俗的内容。集团有权撤消违法犯纪者互联网的使用。使用者必须严格遵循以下内容：

1、从中国境内向外传输技术性资料时必须符合中国有关法规。

2、遵守所有使用互联网的网络协议、规定和程序。

3、不能利用邮件服务作连锁邮件、垃圾邮件或分发给任何未经允许接收信件的人。

4、任何人不得在网上制作、查阅和传播宣扬反动、淫秽、封建迷信等违犯国家法律和中国道德与风俗的内容。

5、不得传输任何非法的、骚扰性的、中伤他人的、辱骂性的、恐吓性的、伤害性的等信息资料。

6、不得传输任何教唆他人构成犯罪行为的资料，不能传输助长国内不利条件和涉国家安全的资料。

7、不能传输任何不符合当地法规、国家法律和国际法律的资料。

第十四条：集团门户网即将改版成功，为了发挥好网站的形象宣传作用，各部室要及时向信息部提供有关资料，以便充实网站内容，加大宣传影响。由信息部统一整理、编辑上传及内容更新。

第十五条：各部门人员每日上班及时打开计算机，进入集团办公系统、浏览相关文件信息、学习

有关文件资料。如有自己业务相关的工作信息，要及时处理，处理结果及时回馈有关责任人员。

第十六条：充分利用办公系统的'优势信息处理平台，浏览的相关情况由办公系统后台数据库自动生成详细记录，以便领导检查相关登陆信息提供记录参考。

第十七条：各部门人员必须及时做好各种数据资料的录入、修改、备份和数据保密工作，保证数据资料的完整准确和安全性。

第十八条：严禁外来人员对计算机数据和文件进行拷贝或抄写以免泄漏集团机密，对集团办公系统或其它集团内部平台帐号不得相互知晓，每个人必须保证自己帐号的唯一登陆性负责，否则由此产生的数据安全问题由其本人负全部责任。

公司网络安全管理制度 篇三

计算机网络为集团局域网提供网络基础平台服务和互联网接入服务，由网络维护中心负责计算机连网和网络管理工作。为保证集团局域网能够安全可靠地运行，充分发挥信息服务方面的重要作用，更好地为集团员工提供服务，现制定并发布《集团网络安全管理制度》。

第一条所有网络设备（包括路由器、交换机、集线器、光纤、网线等）均归网络维护中心所管辖，其安装、维护等操作由网络维护中心工作人员进行，其他任何人不得破坏或擅自维修。

第二条所有集团内计算机网络部分的扩展必须经过网络维护中心实施或批准实施，未经许可任何部门不得私自连接交换机、集线器等网络设备，不得私自接入网络。网络维护中心有权拆除用户私自接入的网络线路并报告上级领导。

第三条各分公司、处（室）的联网工作必须事先报经网络维护中心，由网络维护中心做网络实施方案。

第四条集团局域网的网络配置由网络维护中心统一规划管理，其他任何人不得私自更改网络配置。

第五条接入集团局域网的客户端计算机的网络配置由网络维护中心部署的服务器统一管理分配，包括：用户计算机的IP地址、网关、DNS和WINS服务器地址等信息。未经许可，任何人不得更改网络配置。

第六条网络安全：严格执行国家《网络安全管理制度》。对在集团局域网上从事任何有悖网络法规活动者，将视其情节轻重交有关部门或公安机关处理。

第七条集团员工具有信息保密的义务。任何人不得利用计算机网络泄漏公司机密、技术资料和其它保密资料。

第八条：严禁外来人员对计算机数据和文件进行拷贝或抄写以免泄漏集团机密，对集团办公系统或其它集团内部平台帐号不得相互知晓，每个人必须保证自己帐号的唯一登陆性，否则由此产生的数据安全问题由其本人负全部责任。

第九条：各部门人员必须及时做好各种数据资料的录入、修改、备份和数据保密工作，保证数据

资料的完整准确和安全性。

第十条任何人不得在局域网络和互联网上发布有损集团公司形象和职工声誉的信息。

第十一条任何人不得扫描、攻击集团计算机网络和他人计算机。不得盗用、窃取他人资料、信息等。

第十二条为了避免或减少计算机病毒对系统、数据造成的影响，接入集团局域网的所有用户必须遵循以下规定：

1、任何部门和个人不得制作计算机病毒；不得故意传播计算机病毒，危害计算机信息系统安全；不得向他人提供含有计算机病毒的文件、软件、媒体。

2、采取有效的计算机病毒安全技术防治措施。建议客户端计算机安装使用网络维护中心部署发布的相关杀毒软件和360安全卫士对病毒和木马进行查杀。

3、定期或及时用更新后的新版杀病毒软件检测、清除计算机中的病毒。

第十三条：集团的互联网连接只允许员工为了工作、学习和工余的休闲使用，使用时必须遵守有关的国家、企业的法律和规程，严禁传播淫秽、反动等违犯国家法律和中国道德与风俗的内容。一经发现集团网络维护中心有权撤消违纪者互联网的使用权。使用者必须严格遵循以下内容：

1、从中国境内向外传输技术性资料时必须符合中国有关法规。

2、遵守所有使用互联网的网络协议、规定和程序。

3、不能利用邮件服务作连锁邮件、垃圾邮件或分发给任何未经允许接收信件的人。

4、任何人不得在网上制作、查阅和传播宣扬反动、淫秽、封建迷信等违犯国家法律和中国道德与风俗的内容。

5、不得传输任何非法的、骚扰性的、中伤他人的、辱骂性的、恐吓性的、伤害性的信息资料。

6、不得传输任何教唆他人构成犯罪行为的资料，不能传输助长国内不利条件和涉及国家安全的资料。

7、不能传输任何不符合当地法规、国家法律和国际法律的资料。

第十四条：为了发挥好网站的形象宣传作用，各分公司、处（室）要及时向网络维护中心提供有关资料，以便充实网站内容，加大宣传影响。由网络维护中心统一整理、编辑上传及内容更新。

第十五条：各分公司、处（室）人员在下班离开前必须关闭计算机和电源插座，避免浪费电能和发生消防隐患，违纪者通报批评并进行相应的处罚。有加班需要的工作人员必须提前通知网络维护中心。

公司网络安全管理制度 篇四

1、总经办作为公司网络的规划、设计、建设和管理部门，对公司网络运行情况进行监管和控制，并有权对公司网络上的信息进行检查和备案，任何引入与发出的邮件，进行备份审查。

2、查处在网络上从事与工作无关的事项，违反者将受到处罚。同时也不允许任何与工作无关的信息出现在网络上，否则要追查责任。

3、统一规划建设并负责管理维护公司网络结构，任何部门和个人不得私自更改网络结构，总经办如需安装集线器等必须事先总经办取得联系。个人电脑及实验环境设备等所用ip地址必须按所在地点总经办指定的方式设置，不可擅自改动，擅自改动者将受到处分。

4、随时监督网络的运行情况，严禁任何人以任何手段，蓄意破坏公司网络的正常运行，或窃取公司网上的保护信息。

5、总经办统一规则公司网上服务，如：dns、dhcp、wins等，任何部门和个人不得在网上传送超大文件。

6、对公司应高度重视保护的技术秘密和商业秘密，及要上网的各类保密信息必须保证进行严密的授权控制。

7、对各种工作用文件服务器的申请，需经总经办审核登记，交由系统管理员进行协助处理。

8、对公司信息进行整理，做好公司信息数据库，实现全公司的资源共享及总经办各项工作的网络检索功能，及时对数据库内容进行更新。

9、能熟练掌握常用的办公系统及办公软件，全力做好办公服务工作。

10、做好公司的网站建设，及时更新网站新闻，不断总结经验，全力做好公司的对外宣传工作。

11、定期对网络管理情况检查，发现任何可疑情况及时调查处理，对于违法乱纪行为，要及时上报公司领导。

12、全力完成领导交办的其他任务。

公司网络安全管理制度 篇五

一、信息网络安全管理制度

1、局域网由市公司信息中心统一管理。

2、计算机用户加入局域网，必须由系统管理员安排接入网络，分配计算机名、IP地址、帐号和使用权限，并记录归档。

3、入网用户必须对所分配的帐号和密码负责，严格按要求做好密码或口令的保密和更换工作，不得泄密。登录时必须使用自己的帐号。口令长度不得小于6位，必须是字母数字混合。

4、任何人不得未经批准擅自接入或更改计算机名、地址、帐号和使用权限。业务系统岗位变动

时，应及时重新设置该岗帐号和工作口令。

5、凡需联接互联网的用户，必需填写《计算机入网申请表》，经单位分管领导或部门负责人同意后，由信息中心安排和监控、检查，已接入互联网的用户应妥善保管其计算机所分配帐号和密码，并对其安全负责。不得利用互联网做任何与其工作无关的事情，若因此造成病毒感染，其本人应付全部责任。

6、入网计算机必须有防病毒和安全保密措施，确因工作需要与外单位通过各种存储媒体及网络通讯等方式进行数据交换，必须进行病毒检查。因违反规定造成电子数据失密或病毒感染，由违反人承担相应责任，同时应追究其所在部门负责人的领导责任。

7、所有办公电脑都应安装全省统一指定的趋势防病毒系统，并定期升级病毒码及杀毒引擎，按时查杀病毒。未经信息中心同意，不得以任何理由删除或换用其他杀毒软件（防火墙），发现病毒应及时向信息中心汇报，由系统管理员统一清除病毒。

8、入网用户不得从事下列危害公司网络安全的活动：

（1）未经允许，对公司网络及其功能进行删除、修改或增加；

（2）未经允许，对公司网络中存储、处理或传输的数据和应用程序进行删除、修改或增加；

（3）使用的系统软件和应用软件、关键数据、重要技术文档未经主管领导批准，不得擅自拷贝提供给外单位或个人，如因非法拷贝而引起的问题，由拷贝人承担全部责任。

9、入网用户必须遵守国家的有关法律法规和公司的有关规定，如有违反，信息中心将停止其入网使用权，并追究其相应的责任。

10、用户必须做好防火、防潮、防雷、防盗、防尘和防泄密等防范措施，重要文件和资料须做好备份。

二、计算机使用管理制度

1、使用计算机必须经过培训学习后才能上岗。开启、关闭计算机应按照正确步骤进行，严禁直接人为的非法关机。主机和键盘旁不要放置水杯等盛满液体的容器。

2、不得私自拆装计算机和安装来历不明的软件。计算机发生故障不能工作时，不得擅自维修，应及时向系统管理员报告，由系统管理员或专业技术人员负责维护。

3、严禁私自带外设接入互联网。严禁将计算机中存储的软件和其它信息文档擅自拷贝给他人使用。也不得擅自修改、移动或删除计算机文件和系统设置。

4、不准使用来历不明的光盘、软盘。工作软盘、光盘应妥善保管，不得乱放乱用。

5、计算机系统中要求设置密码的地方都应设置个人密码并妥善保存，不可透露给无关人员。由于不设置个人密码或密码保密不力而发生问题的，由本人负全责。

6、计算机一般要求专人专用。多人共用的计算机，要求设置各自的登录用户名及密码，不可越权使用。办公计算机不得用于业务以外的用途，与本工作无关的人员不得使用计算机。

7、对计算机保存的重要资料必须经常做好异机备份，以防系统崩溃而丢失。

8、所有办公电脑都应安装全省统一的趋势防病毒系统，并定期升级病毒码及杀毒引擎，未经信息中心同意，不得以任何理由删除系统内的防病毒软件，以保证电脑及网络安全。

9、计算机操作人员应采取措施做好电脑防尘、防盗、防潮、防触电、防鼠咬等工作。

三、计算机病毒防范制度

1、信息网络管理员负责计算机病毒防范工作，并及时升级病毒库和杀毒引擎，定期进行病毒检测。

2、电脑操作员在工作中发现计算机有被病毒感染的迹象或因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故时，应及时向系统管理员报告，并保护现场。

3、所有办公电脑都必须安装全省统一的趋势防病毒软件，任何人不得以任何理由关闭或删除系统内的病毒防火墙，以免电脑系统感染病毒，影响网络安全和日常工作。

4、载入办公网络电脑的软件系统安装前应进行病毒检测，禁止运行未经病毒检测的软件。

5、禁止在办公电脑上安装游戏软件以及使用QQ等即时通讯软件。

6、经远程通信传送的程序或数据，必须经过检测确认无病毒后方可使用。

7、任何部门和个人不得制作和传播计算机病毒，不得发布虚假的计算机病毒疫情。

8、各部门及电脑操作员在计算机病毒防治工作中应当履行下列职责：

（1）不得故意输入计算机病毒；

（2）不得向他人提供含有计算机病毒的文件、软件、媒体；

（3）对在互联网上接收到来历不明的电子邮件，不要打开其附件，防止受到计算机病毒的攻击；

（4）从互联网上直接下载的软件和浏览器插件要有可靠来源，因其可能有破坏性程序，必须对此严加防范；

（5）及时检测、清除计算机信息系统中的病毒，无法清除的，应当迅速采取隔离、控制措施，保护现场和相关数据，并及时向系统管理员报告。

四、计算机软件管理制度

1、核心业务软件使用全省统一软件，各单位、各部门不得自行设计、开发、购买。办公类计算机软件由信息中心统一配置或采购，数量较大的软件项目采购应采取招标或议标方式，并经公司决策层批准。

2、购置的计算机软件由信息中心登记，填写《计算机软件档案卡》，每个软件一卡；并且必须采购正版软件，不得购买盗版软件。

3、购置的软件技术资料应归档保管。

4、需要安装业务系统和OA系统的，须经主管领导批准同意，其它软件安装须经信息中心同意。软件的安装与删除由系统管理员操作。

5、软件一经安装使用，未经领导批准或信息中心同意，任何人不得将其卸载、删除。

6、软件不得随意借入非信息部门人员使用，不得借入非本公司人员使用。

7、加强对计算机软件使用权限的管理。因业务需要开通使用权限，需经部门负责人同意，由系统管理员设置相应权限。

五、计算机设备管理制度

计算机设备管理是指计算机主机设备、网络通信设备和外围设备的采购、领用、维修和报废等的管理。计算机设备管理由信息中心负责。

（一）设备采购

1、各单位、各部门因业务需要配制计算机设备，应先填写《计算机设备需求申请表》，经领导批准后，由信息中心汇同有关部门按规定统一采购。

2、在购置设备前应首先考虑调移、升级现有计算机设备，现有设备无法满足需求的情况下再组织采购。

3、计算机设备选型必须综合考虑可靠性、耐用性、适用性和经济性，尽可能选用重点知名品牌和性价比高的产品。

4、采购计算机配件单一品种超过一千元以上的应报请主管领导批准。一次采购设备单一品种价值超过一万元以上的，必须比质比价，按办公用品集中采购的有关规定执行。

5、对新购置的设备，由系统管理员安装、测试、验收合格后交由使用部门使用，并通知有关部门做好财产登记。

（二）设备领用

1、计算机设备使用须履行领用手续，由使用人填写《计算机设备使用登记表》，由系统管理员建立设备管理档案。

2、对闲置不用的计算机设备，使用部门应将设备退回信息中心统一保管或调移其它部门使用，并办理财产转移手续。

3、计算机设备的配件领用、更换由信息中心系统管理员统一配置。

（三）设备维修

1、非系统管理员或专业维修人员不得擅自维修计算机及其他设备。

2、系统管理员在接到设备故障报告后，一般应在一个工作日内完成修复，需延长维修时间的应向使用部门说明原因。

3、系统管理员不能维修时，应及时与供应商或产品维修中心联系，派专业技术人员维修。

4、设备维护应做好记录，并建立管理档案。

（四）设备报废

1、对性能不稳定、陈旧换代、寿命终结或难于满足业务需求的设备，如无法通过升级、维修使其胜任工作，应作设备报废处理。

2、报废设备由使用部门提出申请，填写《设备报废申请表》，由系统管理员提出鉴定意见和有关部门审查后，报领导审批。

3、设备报废应做好登记并通知有关部门核销。

六、信息系统维护管理制度

1、本制度所指系统包括：各业务应用系统、计算机操作系统、数据库系统、通讯系统、邮件系统等信息系统。

2、系统管理员每月至少一次定期对各信息系统进行检查是否正常运行，并填写《系统维护登记表》。

3、要定期核实各系统功能是否达到公司业务需求，如有不符，应报告上级领导并做好需求方案。

4、对各信息系统进行升级的时候，须谨慎、严格地执行升级步骤。升级前应该分析系统升级维护的风险，进行严格的测试，并选择在非业务操作时间进行系统升级维护工作。

公司网络安全管理制度 篇六

1. 目的

1.1 为了加强计算机网络、软件管理，保证网络系统安全，保证软件设计和计算的安全，保障系统、数据库安全运行特制定本制度。

1.2 本制度适用于对公司网络系统的运行维护和管理。

2. 范围

2.1 计算机网络系统由计算机硬件设备、软件及路由器、交换机组成。

2.2 软件包括：操作系统、应用软件、及有关的专业应用软件等。

2.3 个人办公的网络系统配置包括客户机在网络上的名称，IP地址分配Internet的配置等。

2.4 系统软件是指：操作系统（如 WINDOWS xP等）软件。

2.5 平台软件是指：办公用软件（如OFFICE 2019）、邮箱软件等平台软件。

3. 职责

3.1 信息部为计算机系统、网络安全运行的归口部门，负责计算机网络系统的日常维护和管理；负责计算机网络的安全运行及计算机系统防病毒管理；

4. 管理

4.1服务器维护

4.1.1 对于系统和网络出现的异常现象，系统管理员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，并如实将异常现象进行记录。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、预防措施等内容记录。

4.1.2 每月3日前对相关服务器数据、重要部位电脑的数据进行备份。

4.1.3 维护Internet 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。

4.1.4 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。

4.2 客户机维护

4.2.1 按照人事部下达的新员工（或外借人员）姓名、分配单位、人员编号为新的计算机用户分配计算机名、IP地址等。

4.2.1.1帐号申请：新员工（或外借人员）需使用计算机帐号，先向部门经理提出申请经批准后，由系统管理员负责分配计算机和IP等。

4.2.2 如有移动用户需访问局域网，由用户提出申请，部门经理审核、信息部经理审批后，系统管理员负责提供服务。

4.2.3 根据用户需要为其配置 Internet接入权限，一般员工只有接入局域网权限，如有工作需要接入Internet，由部门经理审核后、子公司与中心的负责人审核后，由管理总监审批后，由网络管

理员提供服务。

4.2.4 网络用户不得随意移动信息点接线。因房屋调整确需移动或增加信息点时，应由计算机管理人员统一调整，并及时修改“ 网络结构图 ”。

4.2.5 对于网络用户传播、复制、制造计算机病毒或采用技术而致使计算机网络瘫痪造成重大损失的情况，将给予严肃处理。

4.2.6计算机日常维护由使用者负责，电脑整洁、干净、不得有污垢、灰尘现象。爱护计算机和网络设备，如人为因素发生设置非正常损坏，除对当事人进行处罚外，另由当事人按照损坏程序进行赔偿。

4.2.7使用者的重要文件，禁止放在系统盘（C盘）及我的桌面和文档，以免系统瘫痪后丢失数据。

4.3 软件维护

4.3.1公司计算机，必须由系统管理员统一安装操作系统、OFFICE等软件，用户可以在系统管理员的授权下，自行安装系统和专业软件。

4.3.2严禁擅自在计算机中安装非工作软件和程序，严禁擅自删除计算机中的系统文件，由此可能导致数据丢失或计算机操作系统破坏，以致计算机瘫痪而影响工作；如确实工作需要安装或删除软件和程序应当向网络系统管理人提出申请，同管理人员统一安装或删除。

4.3.3用户如有中毒、操作系统缓慢、死机等问题时，向系统管理人员提出口头请求，接到请求的系统管理人员应及时提供维护服务，并查明出现故障的原因，如因看电影、下载与工作无关的东西所造成的，根据情节按下列规定进行处罚。

4.4 计算机病毒防治

4.4.1 计算机上必须安装防病毒软件，防病毒软件由用户定期更新。

4.4.1 使用U盘前，必须对U盘进行病毒扫描确认无毒后方能使用。

4.4.3 计算机对于外来软件的安装、图纸和文件的使用，在使用前要进行病毒扫描。

4.4.4 送外维修和将要联入公司局域网的计算机必须经过病毒检测后，方可联入网络。

4.4.5 为了防止病毒侵蚀，员工不得从internet网下载游戏及与工作无关的软件，不得在微机上安装、运行游戏软件。

4.5 IP地址和用户密码管理

4.5.1 局域网IP地址由系统管理员负责管理，用户不得擅自更改客户端的IP地址及计算机名。

4.5.2如有必要，计算机用户可自行设置用户名和登录密码。

4.6 对外接口管理（Internet服务器， OA服务器）

4.6.1用户应避免利用 OA传送较大容量的附件 （10M以上的 ）、图纸和图片，最大控制在10M以内，定期清理，保证 OA的正常运行。

4.6.2 上网用户 必须遵守《国家计算机信息系统安全保护条例》，在公司网络上进行任何干扰网络用户、破坏网络服务和破坏网络设备的活动。严禁通过互联网传入或传出内容不宜的信息（如政治上敏感的或反动、淫秽、封建迷信等违犯国家法律和中国道德与风俗的内容），也不传播收到的此类信息。不得浏览、传播违法和不健康的内容，违反规定的用户将被终止上网权利。

5. 处罚

5.1上网行为处罚

5.1.1对上网用户在上班时间下载电影、软件等与工作无关的，或者在线音乐、在线视频等，严重占用网络宽带，导致网络堵塞，一经发现，罚款100元；

5.1.2员工访问了不明网站，病毒、蠕虫、木马、恶意代码及间谍软件等通过网页、Email、聊天工具、下载软件等方式，侵入到内网的各个角落，严重影响公司网络的正常运行，一经发现罚款100元。

5.1.3上班时间浏览与工作无关网页、炒股、购物、游戏等一经发现罚款50元。

5.1.4使用BT、电驴、迅雷、网际快车、超级旋风等P2P下载软件和PPlive、UUsee、PPstream、迅雷看看等P2P视频软件。使得局域网网络资源被消耗殆尽，导致企业正常的网络应用无法进行，严重干扰了公司的经营活动的一经发现罚款500元。

5.1.5 未经许可私自修改电脑IP地址，导致局域网出现IP地址冲突，电脑掉线现象，严重影响了局域网的稳定和畅通。一经发现罚款100元。

5.1.6 未经许可私自移动公司在各点分布的网络设备及布线，乱拉线等，一经发现罚款100元。

5.1.7部门共用的电脑，查不到责任人时，由部门责任人承担。

5.2. 系统软件破坏处罚

5.2.1 公司电脑系统以及应用平台等经系统管理员装好后一个月内，由于上网、中病毒、自己装卸软件等人为因素导致电脑瘫痪、办公软件、平台无法正常运行的对电脑负责人罚款50元。

5.3 保密

5.3.1刻意或无意泄漏经营数据的或市场经营决策的，一经查实，罚款500-1000元，后果严重者移交法律机构进行处理；

5.3.1严格保密本公司的数据和文件，严禁外来人员对计算机数据和文件拷贝或抄写。也不得私自通过互联网发送本公司涉密的数据和文件。如工作需要，必须经过领导同意方可以进行操作。

6、此制度由信息部起草，规范化讨论通过；

7、此制度于20xx年xx月xx日试行，于20xx年xx月xx日正式执行；

企业网络安全管理制度 篇七

1、 组织工作人员认真学习《计算机信息网络国际互联网安全保护管理办法》，提高工作人员的维护网络安全的警惕性和自觉性。

2、 负责对本网络用户进行安全教育和培训，使用户自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。

3、 加强对单位的信息发布和BBS公告系统的信息发布的审核管理工作，杜绝违犯《计算机信息网络国际互联网安全保护管理办法》的内容出现。

4、 一旦发现从事下列危害计算机信息网络安全的活动的：

（一）未经允许进入计算机信息网络或者使用计算机信息网络资源；

（二）未经允许对计算机信息网络功能进行删除、修改或者增加；

（三）未经允许对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）从事其他危害计算机信息网络安全的活动。做好记录并立即向当地公安机关报告。

5、 在信息发布的审核过程中，如发现有以下行为的：

（一）煽动抗拒、破坏宪法和法律、行政法规实施

（二）煽动颠覆国家政权，推翻社会主义制度

（三）煽动分裂国家、破坏国家统一

（四）煽动民族仇恨、民族歧视、破坏民族团结

（五）捏造或者歪曲事实、散布谣言，扰乱社会秩序

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪

（七）公然侮辱他人或者捏造事实诽谤他人

（八）损害国家机关信誉

（九）其他违反宪法和法律、行政法规将一律不予以发布，并保留有关原始记录，在二十四小时内向当地公安机关报告。

6、 接受并配合公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

读书破万卷下笔如有神，以上就是t7t8美文号为大家带来的7篇《公司网络安全管理制度》，希望可以对您的写作有一定的参考作用。