关于加强公司网络安全管理的通知（精选4篇）

篇1：关于加强公司网络安全管理的通知

公司各部门及各所属公司、基地关联产业公司：

长期以来，外网网络环境复杂，木马及各类恶意软件横行，严重威胁网络平台的安全和健康运行，用户误入悖社会公德陷阱、机密材料被篡改窃取、网上财务损失等事件层出不穷。随着总公司、各公司信息化和办公自动化进程的推进，计算机及网络的安全管理成为公司安全管理工作的重要内容。为确保公司计算机系统及网络系统的安全运行，现将有关事项通知如下：

一、计算机及网络管理

总公司、下属公司计算机系统及网络系统（含计算机财务系统）须指定责任人统一管理，并严格甄选服务商对计算机及网络进行维护维修，未经责任人安全确认，不得随意装卸系统软件。

二、计算机及网络的使用

1、计算机使用人对内存资料负有保管和保密责任，必须严格按照相关规定审批转存；

2、禁止任何人利用公司计算机和网络进行以下操作：

1）浏览不健康网站、非法网站及国家明令禁止的网页；

2）下载电影、游戏软件或与工作无关的其他资料；

3）上班时间通过QQ、MSN等聊天工具接收未知具有安全隐患的文件、发送有关任何涉及公司机密的内容及文件；

4）不得在各种网站、论坛、微博发布或上传不健康言论内容以及任何涉及有关企业机密的帖子。

三、病毒防护和维护保养

1、公司所有计算机必须安装杀毒软件和防火墙，一旦发现病毒及木马程序须及时查杀；

2、移动磁盘等设备在使用前，必须确保无病毒，若发现病毒应及时查杀或通知公司指定的专业技术人员进行处理。

四、公司随时对计算机及网络使用情况进行检查，发现以下情形将追究当事人责任，给予处罚（原则上50元/次/人,情节严重者,可加重处罚）：

1、计算机感染病毒不及时报告和处理者；

2、因私自安装和使用软件给公司造成各种损失者；

3、擅自使用他人计算机或外设造成不良影响和后果者；

4、违反本通知规定或其他危害计算机及网络系统事件；

5、使用公司计算机不当，导致公司重要机密外泄者；

本通知自公布之日起施行。

2021年2月20日

篇2：关于加强公司网络安全管理的通知

尊敬的各位员工：

为了进一步加强和保障我们的网络安全，确保公司信息和数据的安全性和稳定性，我们制定了一系列的网络安全措施和准则。特此通知各位员工，务必严格遵守以下网络安全要求：

1.保护账号安全和密码保密性：

-每位员工应定期更改密码，并确保密码的复杂性。

-不得将个人账号和密码外泄给他人，也不可共享账号和密码。

-注意在公共场所和他人面前输入密码时的隐私保护。

2.防范网络钓鱼和恶意软件：

-定期更新安全软件和操作系统，及时修补安全漏洞。

3.保护公司机密信息和数据：

-不得将公司机密信息外泄给不相关的人员。

-使用公司提供的安全传输通道进行信息传输。

-即使在公司内部，也要遵守信息的内部传递制度和权限控制。

4.妥善管理办公设备和存储设备：

-禁止将公司办公设备和存储设备外借或私自带离公司。

-定期备份重要数据，并保证存储设备安全可靠。

5.敏感信息保护和数据处理：

-在处理敏感信息时要严格遵守相关法律法规，确保信息的安全和隐私。

-对于不再需要的数据和文件，要进行彻底的销毁或安全存储。

我们相信，只有全体员工共同努力，才能真正实现网络安全的目标。请大家认真遵守上述要求，并不断提升自身网络安全意识和知识。如有任何问题或遇到网络安全风险，请及时向IT部门报告。

感谢各位员工的支持和合作！

此致，

XXX公司网络安全办公室

日期：XXXX年XX月XX日

篇3：关于加强公司网络安全管理的通知

为了进一步加强网络安全工作，确保广大群众的网络安全意识和防护能力提升，现将有关网络安全新闻宣传工作的最新通知如下：

1.提升宣传力度：各级媒体和宣传机构要加强对网络安全问题的宣传，通过多种方式、多种形式，向公众普及网络安全知识，提高公众的网络安全意识。

2.创新宣传方式：针对不同人群的需求和特点，要创新宣传方式，采用图文并茂、生动形象的方式宣传网络安全知识，提高宣传的有效性和影响力。

3.强化合作机制：各级政府部门、网络安全企事业单位和媒体机构要加强信息共享和合作，建立健全网络安全宣传工作的协作机制，形成合力，共同推进网络安全宣传工作。

4.加强网络安全教育：要加大网络安全教育力度，推动网络安全知识进校园、进企业、进家庭，提高广大人民群众的网络安全素养。

5.提高舆论引导能力：要加强网络安全舆论引导，积极引导公众形成正确的网络安全价值观和行为习惯，营造健康、和谐、安全的网络环境。

请广大媒体和宣传机构按照上述要求，积极组织开展网络安全新闻宣传工作，共同维护社会的网络安全稳定。

谢谢大家的支持与配合。

网络安全办公室

日期：XXXX年XX月XX日

篇4：关于加强公司网络安全管理的通知

各单位、项目部、机关各部门：

根据集团《关于加强集团网络安全工作的通知》要求，为维护网络办公环境、保障信息安全、防范病毒攻击、阻断病毒传播，切实做好网络安全工作，现将有关事项通知如下：

一、提高思想认识

当前网络安全形势严峻，网络攻击和信息安全风险交错叠加，各单位要高度重视网络安全工作，进一步增强“四个意识”，坚持底线思维，提高警惕，加强防范。要进一步梳理本单位及所属项目网络资产，排查隐患，堵塞漏洞，坚决清理僵尸网络。

二、落实查杀工作

1，各单位、项目部组织对所有在用办公电脑进行病毒、网络威胁进行防护查杀，下载并安装官方火绒安全软件，将病毒库升级到最新，全面查杀木马、后门类等病毒。

下载地址：s://.huorong/person5.html

2，各单位汇总统计计算机使用者姓名、所属单位（项目）、计算机网络IP（公网+局域网）、计算机MAC地址、查杀木马等病毒情况的截图（如无也需要截查杀后的截图），其中截图保存到WORD文档中并注明人员信息，汇总后，于3月17日18时前将电子版报送至公司信息管理部。

三、注意事项

1，安装火绒安全软件时，如电脑安装了其它杀毒软件，可能会提醒阻止或允许，请选择允许。

2，查到宏病毒时，如不能自动杀毒，出现隔离、信任选择时，要暂时选择信任，并将文件内容复制到新创建的文件中，防止内容丢失。

3，MAC地址可在控制面板（win10为设置）网络网络和共享中心本地连接或无线网连接详细信息的物理地址上查询，如下图：

四、网络安全工作要求

各单位在工作中应督促网络办公人员做到以下几点：

1、收到电子邮件后，应先与发件人联系，确认后再打开，不要打开来历不明的电子邮件和附件，不要轻易下载和运行未知网页上的软件，以防感染木马和病毒。

2、定期修改、使用高强度的邮箱密码，防止密码被恶意破解。经常在邮箱管理设置中检查是否存在邮件被转发、代收和异常登录的情况，如有此类情况应立刻更改密码并做相应处理。

3、及时升级计算机、手机安全防护软件和木马病毒库，并定期进行全面木马查杀。

4、严禁通过计算机、手机及电子邮箱存储、传输敏感或涉密文件和内容。

5、下载并安装最新的系统补丁包，及时做好重要数据的备份。

6、使用U盘等设备连接电脑时，注意扫描U盘是否存在病毒，并及时清除。

如有疑问请联系信息管理部******，联系方式：152**********。

******有限公司

2023年6月17日