

## IT 管理制度

为了规范公司 IT 各项工作，提高 IT 系统的可靠性，提高 IT 系统与设备的总体服务水平，并使得相关工作具有持续改善性及相互协作性，特制定统一的 IT 规范及标准，包括建立统一的硬件设备管理规范，统一的 IT 网络、软件安全标准，统一的系统管理维护流程以及信息安全管理的目的与责任等。根据公司质量管理体系，以及计算机应用的需要，由 IT 部制定本管理制度，并负责本管理制度的具体执行。

### 一、计算机硬件管理

1. 公司的所有计算机及外围设备是公司的固定资产，根据实际工作需要配备给各部门人员使用，各部门使用人员必须加以爱护、保持整洁，并保证良好的使用环境。若用户使用的设备发生人为损坏、设备遗失等，需要按具体规章制度执行赔偿。
2. 由 IT 部对公司所有计算机设备进行统一编号，建立计算机硬件明细台帐，并定期对硬件进行维护、检查各部门使用情况。
3. 设备添置、更换、升级：由各部门根据实际工作需要提出申请，IT 部确定具体配置，书面申请经部门经理批准后由 IT 部进行采购（按公司实际采购流程执行）。
4. 硬件故障：各部门使用人员发现硬件故障时，应及时向 IT 部说明情况，由 IT 部进行确定并及时处理，各部门人员不得擅自拆装更换硬件设备。
5. 部门如需领取耗材，需到 IT 部（行政部）填写耗材申请单。申请单须清晰注明耗材申请原因。批准后由 IT 部（行政部）进行发放。
6. 计算机的使用人即为该设备的责任人，使用部门为责任部门。任何人不得使用其他部门或他人计算机。
7. 原则上非公司电脑设备不得接入公司网络，公司员工的个人私有电脑(非公司资产)如有特殊原因，必须提出申请，经部门主管及经理同意后，由 IT 部检查系统安全性后并安装防毒软件和补丁升级等系统安全程序方可加入公司网络。
8. IT 部负责对公司所有电脑硬件使用情况的督查和监控。

### 二、计算机软件管理

软件的使用：各部门及人员所使用的软件，由 IT 部进行安装。不得删除系统中的重要文件，如 BOOT.INI、NTDETECT.COM、NTLDR.SYS、IO.SYS、MSDOS.SYS、C:\WINNT 或 C:\WINDOWS 目录及其中的文件等。

1. 公司需用的软件（软件加密设备），由 IT 部统一购买、保管，并登记造册。各部门的专用软件，由部门经理安排使用，IT 部保管备案。
2. 软件的安装、删除和升级：由各部门根据工作需要，提出书面需求申请，经批准后，由 IT 部进行安装、删除和升级。未经 IT 部批准，各部门和人员不得自行进行上述操作。
3. 软件故障：各部门使用人员发现软件故障时，应及时向 IT 部说明情况，由 IT 部进行确定并及时处理，各部门人员不得擅自处理。
4. 员工不得私自在工作机上安装与工作无关的程序，mp3、影音文件播放程序、聊天工具、游戏等。
5. 工作时间（包括加班时间）公司员工不得使用工作机玩游戏，听音乐观看电影。
6. 移动存储设备使用管理：为了防止公司资料非法外流以及病毒入侵公司内部网络，严格限制员工使用外来软盘、光盘、移动硬盘等移动存储设备。
7. 网络下载管理：为了防止病毒侵入公司内部网络，保障网络资源的合理使用，不得随意下载文件、信件。
8. 软件的版本管理和控制：为了防止公司内的软件版本混乱和文件格式不兼容，由 IT 部控制公司内工作用软件的版本升级。做到统一版本、统一升级。由于员工个人升级软件版本造成的文件格式不兼容问题由该员工负责。
9. IT 部负责对公司所有电脑软件使用情况的督查和监控。

### 三、Internet（互联网）管理

1. 公司注册域名为：[http://www.\\*\\*\\*\\*\\*.com](http://www.*****.com)  
公司邮箱域名为：[https://mail.\\*\\*\\*\\*\\*.com](https://mail.*****.com)
2. 任何时间公司员工不得使用公司的电脑浏览淫秽、色情、暴力、违反国家安全的网站。
3. 工作时间（包括加班时间）公司员工不得浏览与工作无关的网站，不得下载与工作无关的文件，包括 mp3、Flash、影音文件、游戏等。
4. 公司员工不得使用 BT 等可给公司网络造成严重带宽压力的软件进行下载，经发现，造成的不能正常访问公司局域网及互联网等故障及损失，由本人承担一切责任。
5. 工作时间（包括加班时间）公司员工不得通过网络玩在线游戏，听音乐观看电影。
6. 公司为工作需要员工统一分配 Email 地址，各使用人员必须定时进行检查、回复、整理。
7. 公司员工不得私自更改本机 IP、DNS、网关地址。
8. 公司员工不得使用他人电脑上网，不得将外人带入公司使用公司电脑和通过公司内网上网。

### 四、网络机房管理：

1. 要有安全防范意识。早进入、晚离开时要检查设备情况；离开时察看灯、门、窗、锁是否关闭好。
2. 路由器、交换机和服务器以及通信设备是网络的关键设备，不得自行配置或更换，更不能挪作它用。
3. 工作人员进入机房，要事先征得同意；未经许可一律不准触碰开关和设备。
4. 机房工作人员要掌握防火技能，定期检查消防设施是否正常。出现异常情况应立即报警，切断电源，用灭火设备扑救。
5. 计算机房要保持清洁、卫生，并由专人负责管理和维护（包括温度、湿度、电力系统、网络设备等等），无关人员未经管理人员批准严禁进入机房。
6. 严禁易燃易爆和强磁物品及其它与机房工作无关的物品进入机房。不能明火作业。机房一律禁止吸烟，凡不听劝告者，一律逐出机房。
7. 建立机房登记制度，对本地局域网络、广域网的运行，建立档案。未发生故障或故障隐患时当班人员不可对中继、网线及各种设备进行任何调试，对所发生的故障、处理过程和结果等做好详细登记。
8. 网管人员应做好网络安全工作，服务器的各种帐号严格保密。监控网络上的数据流，从中检测出攻击的行为并给予响应和处理。

9. 做好操作系统的补丁修正工作。
10. 网管人员统一管理计算机及其相关设备，完整保存计算机及其相关设备的驱动程序、保修卡及重要随机文件。
11. 计算机及其相关设备的报废需经过管理部门或专职人员鉴定，确认不符合使用要求后方可申请报废。
12. 制定数据管理制度。对数据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、丢失及破坏。当班人员应在数据库的系统认证、系统授权、系统完整性、补丁和修正程序方面实时修改。