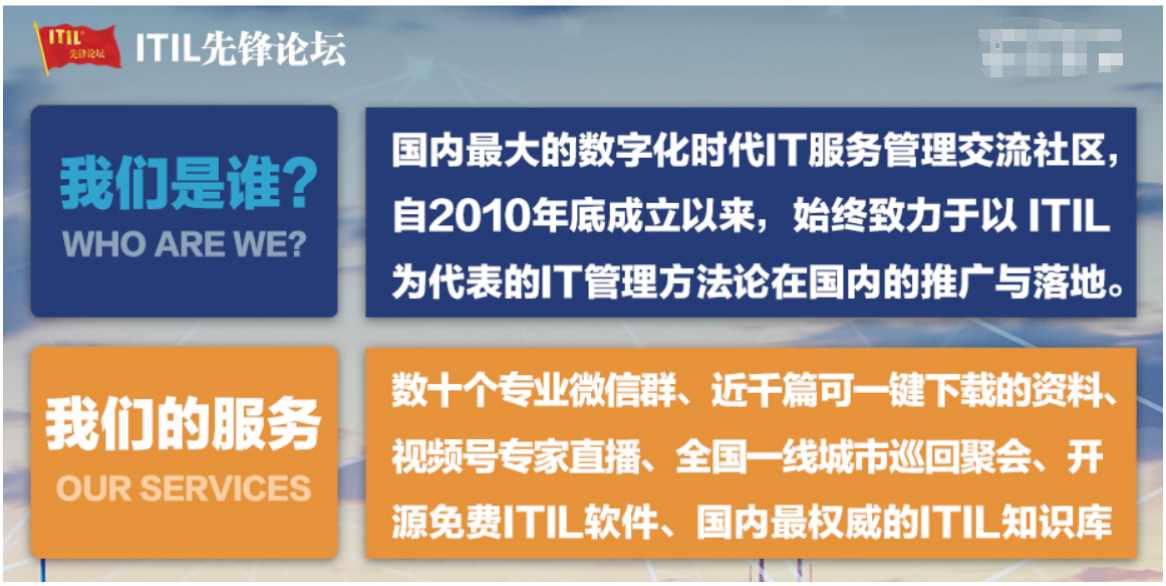
# XXXXXX 有限公司

# IT 管理制度

版本号：1.0



为了规范集团（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申请，IT 部确定具体配置，书面申请经总经理、财务副总批准后由 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。申请经财务副总经理批准后，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。未经责任部门经理批准，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，必须经使用部门提出申请，由公司最高主管（如公司总经理）或部门主管同意后，由 IT 部门工程师检查系统安全性后并统一安装公司防 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。

备注：在硬件条件允许的情况下，IT 将逐步在各分公司实施 802.1X 安全认证，采用技术手段防止外来设备未经允许的接入情况发生。同时要求各分公司新购网络设备符合 802.1X 的标准。在各厂实施 802.1x 条件未成熟的情况下，可先使用电脑 MAC 地址与 IP 绑定的办法，防止外来电脑随意接入。

## 二、计算机软件管理

1、软件的使用：各部门及人员所使用的软件，由各部门会同 IT 部共同确定，由 IT 部进行登记。

2、公司需用的软件，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。

3、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，经总经理批准后，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。

4、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。

5、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。

6、工作时间（包括加班时间）公司员工不得使用工作用机玩游戏，听音乐观看电影。

7、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。

8、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。

9、使用外网邮件：员工在打开外网邮件时必须激活防火墙或“XX 邮件监控”程序（视具体杀毒软件而定）。

10、软件安装和使用过程中病毒的预防：员工不得在工作机上安装来历不明的软件；安装软件前，应对该安装盘进行杀毒。安装软件时应打开防火墙，防止病毒入侵。

11、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一律由该员工负责。

12、IT 部负责对公司所有电脑软件使用情况的督查和监控。

**三、公司局域网管理：**

1、部门新进员工在服务器文件目录下个人专用目录的创建，应由员工所在部门经理签字或主管副总到 IT 部签写局域网员工权限变更登记表，并签字生效，IT 部凭单设定用户名、密码，创建目录及分配访问权限。

2、由于员工工作的调动等情况需更改目录访问权限者，应由员工所在部门经理签字或主管副总到 IT 部签写局域网员工权限变更登记表，并签字生效（特殊情况须总经理审批签字），IT 部凭单重置用户密码、目录及访问权限。

3、对于离职人员目录访问权限的删除及相关数据的备份，应由员工所在部门经理

签字或主管副总到 IT 部签写局域网员工权限变更登记表，并签字生效，IT 部凭单删除目录访问权限并对相关数据进行备份。

4、每位使用公司文件服务器的员工，其对应个人专用目录下均有如下目录： “部门”、“领导”、“公有”。目录的操作权限分别如下：

**公有：** a、 本人有完全控制的读写权限

b、 公司其他人员均仅有读取权限

**部门：** a、 本人有完全控制的读写权限

b、所在部门内所有其他人员均仅有读取权限

c、 所在部门以外所有人员均无任何访问权限

**领导：** a、 本人有完全控制的读写权限

b、 仅公司领导有读取权限

c、 除以上人员外公司其他人员均无任何访问权限

**说明：**

b、 如部门内部员工间进行数据交换，可在本人专用目录下的“部门”中进行；

b、 如部门以外员工间进行数据交换，可在本人专用目录下的“公有”中进行；

c、 数据交换执行完毕请务必及时清理。

5、各部门使用人员，必须将本地计算机和文件服务器相关目录中的工作数据定 期进行备份，以防止因硬、软故障造成数据资料损失，备份由 IT 部执行，备份资料统一存入公司资料室。

6、为推进公司无纸化办公、提高工作效率、降低办公成本。IT 部使用 NOTES 软件，设置内部局域网邮箱，并为每人设置内部电子邮件地址，各部门使用人必须定时进行查看、回复、整理，所有邮件数量不得超过 10 条。

7、禁止将与工作无关的图片、音频、视频等文件存放于工作所用电脑或公司文件服务器，绝对禁止将含有淫秽、色情、暴力的文字、图片、音频、视频等文件存放于工作所用电脑或公司文件服务器。如违反上述规定，公司将追究责任并严肃处理，因此导致的电脑故障或损坏，则由本人承担一切责任。

**四、Internet（互联网）使用管理：**

1、公司注册域名为：

公司邮箱域名为：

凡有访问 Internet 的权限的用户电脑，IE 默认主页地址必须设为两者之一，公司员工有责任熟记公司域名及邮箱域名。

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 B T 等可给公司网络造成严重带宽压力的软件进行下载，一经发现，IT 部即刻查封 IP，截止时间以总经理批示可重新接入公司网络为准，其间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、工作时间（包括加班时间）公司员工不得使用任何网络聊天工具，包括 QICQ、ICQ、MSN、网易泡泡等，不得进入聊天室聊天。

7、公司员工上网时必须激活病毒防火墙，不得随意下载文件、信件，防止病毒侵入公司内部网络，如违反该规定，一切后果由本人承担。

8、各部门上报的因工作需要的上网名单，经公司领导批准后，由 IT 部统一调配公司员工上网权限。对于私自盗用他人上网权限的用户，按有关规定处理。

9、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查看、回复、整理。

10、公司员工不得私自更改本机 IP、DNS、网关地址。对于因私自更改造成的一切后果由本人承担。

11、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。

12、无上网权限的员工因工作需要，可以申请访问 INTERNET，经部门经理批准后，由 IT 部分配其上网权限，公司有权对用户的上网行为作记录，IT 将保留最近 2 个月的上网日志，以供相关部门主管查询。

## 五、信息安全管理：

### A、目的

制定信息安全制度的目的是：确保 XX 公司的网络系统运行在一种合理的安全状态

下，同时不影响公司员工使用网络。

具体目标包括：保障数据安全和系统安全。

**1、数据安全**

1.1 防止未经授权修改数据；

1.2 防止未经发觉的遗漏或重复数据；

1.3 防止未经授权泄露数据；

1.4 确保数据发送者的身份正确无误；

1.5 确保数据接收者的身份正确无误；

1.6 数据的发送者、接收者以及数据的交换仅对发送者与接收者是可见的；

1.7 在取得明确的可访问系统的授权后，才能与该系统通信。

**2、系统安全**

2.1 防止未经授权或越权使用系统；

2.2 控制网络流量，防止过量的访问使系统资源过载导致的系统崩溃。内部网络流量超负荷，保障外网服务(Internet)、内网邮件服务（Notes）的安全。

## B、适用范围

信息安全制度适用于：

1、任何与 XX 公司网络设备相连的 IP 网络，所有连接到上述网络上的设备；

2、任何 XX 公司所属数据传输经过的网络，所有上述网络上传输的数据；

3、对数据进行管理的人员，如果要将新的设备增加到 XX 公司的网络中，适用于该项目的负责人；

4、所有连接到 XX 网络中的设备，以及 XX 公司职员在该网络中使用的任何设备；

## C、责任

在信息安全制度的涉及范围内，每个部门的信息安全由部门负责人或由其指定专人来负责。

D、内容

**1、内部人员的攻击，包括有意和无意两种。主要表现为：**

1.1 保密观念不强，或不懂遵守保密守则，随便泄漏机密；打印复制机密文　件；随便打印出系统保密字或向无关人员泄露有关机密信息；

1.2 由于业务不熟练、操作失误，导致文件丢失或者误发，或因未遵守操作规则而造成泄密；

1.3 因规章制度不健全造成人为泄露事故，如对机密文件管理不善，各种文件存放混乱，违章操作等造成不良后果；

1.4 素质差，缺乏责任心，没有良好的工作态度，明知故犯，或有意破坏网络系统和设备；

1.5 利用窃取系统的磁盘、磁带或纸带等记录载体或利用被废弃的打印文件、复写纸来窃取系统用户信息；

1.6 通过非法窃取他人的用户名和口令来进入他人的计算机，拷贝文件或进行破坏；

1.7 使用带有病毒的外来介质，带毒的磁盘、存储设备；

1.8 浏览具有恶意代码的互联网网页。

**2、外部人员的攻击或非法访问**

2.1 外来设备企图联入本企业的局域网；

2.2 通过物理连接试图窃取管理员身份、或窃取重要文件；

2.3 通过发送病毒邮件、蠕虫攻击；

2.4 外部人员非法在本企业局域网中安装、使用木马、嗅探器等程序。

**3、技术故障所带来的威胁。通常指突发事故**

3.1 由于硬件原因造成系统的故障；

3.2 人为删除系统重要文件：BOOT.INI、NTDETECT.COM、NTLDR.SYS、IO.SYS、MSDOS.SYS、C:\WINNT 或 C:\WINDOWS 目录及其中的文件等；

3.3 新软件、硬件的不当安装引起系统无法正常使用；

3.4 内部人员擅自使用其他软件或更改网络配置(如 IP 地址)导致服务器不能正常工作；

3.5 由于不可抗拒的因素导致硬件损坏。

**4、数据的意外丢失**

4.1 由于硬件的损坏导致数据丢失；

4.2 由于系统的不稳定导致数据丢失；

4.3 电力系统故障造成的数据丢失；

## E、解决方案

**1、软件资源的安全和管理方案**

主要规范软盘、光盘、移动存储设备使用、网络下载、使用外网邮件、软件安装和使用过程中病毒的预防及使用控制。

**2、数据资源的安全和管理方案**

数据存储的安全管理

2.1 存放有业务数据或程序的磁盘、磁带或光盘，应视同文字记录妥善保管。必须注意防磁、防潮、防火、防盗，必须垂直放置；

2.2 对硬盘上的数据，要根据安全分级建立有效的权限，并严格管理，对于内部访问级和机密级的数据要进行严格的 NTFS 权限设置和必要的加密，以确保硬盘数据的安全；

2.3 存放有业务数据或程序的磁盘、磁带或光盘，管理必须落实到人，并分类建立登记薄，记录编号、名称、用途、规格、制作日期、有效期、使用者、批准者等；

2.4 对存放有重要数据的磁盘、磁带、光盘，至少要备份两份并分两处妥善保管；

2.5 日常工作数据不存放于引导分区及操作系统所在的磁盘分区(如：我的文档、桌面、C 盘)；

2.6 打印有业务数据的打印纸，要视同档案进行管理；

2.7 凡超过数据保存期磁盘、磁带、光盘，必须经过特殊的数据清除处理，否则不能视同空白磁盘、磁带、光盘；

2.8 凡不能正常记录数据的磁盘、磁带、光盘，须经测试确认后由 IT 部进行毁，并做好登记；

2.9 对需要长期保存的有效数据，应在磁盘、磁带、光盘的质量保证期内进行转储，转储时应确保内容正确。

数据的使用管理

2.10 数据必须严格保密，未经上级主管部门同意，一律不准对外提供任何数据和程序；

2.11 数据按规定进行拷贝以外，任何人不得以任何借口和形式进行拷贝。

**F、密码安全和管理方案**

1、培养良好的安全操作习惯，在指定的计算机或终端上操作，不要把密码写在记事本或电脑上，有事离开计算机时应将其锁定；

2、防止电脑缓存、Cookies 记录重要密码，特别是办公室的电脑里；

3、做到口令专管专用，定期更改并在失密后立即报告；

4、人员调离时，应采取相应的安全管理措施。例如：人员调离的同时马上移交工作、更换口令、取消帐号。

**六、网络机房管理：**

**A、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、非工作人员进入机房，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)，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。

**B、计算机病毒防范制度**

1、网络管理人员应有较强的病毒防范意识，定期进行病毒检测(特别是邮件服务器)，发现病毒立即处理并通知管理部门或专职人员。

2、采用国家许可的正版防病毒软件并及时更新软件版本。

3、未经上级管理人员许可，当班人员不得在服务器上安装新软件，若确为需要安装，安装前应进行病毒例行检测。

4、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。

**C、数据保密及数据备份制度**

1、各部门根据数据的保密规定和用途，确定使用人员的存取权限、存取方式。

2、禁止泄露、外借和转移专业数据信息。

3、公司统一封闭电脑 USB 端口、需使用移动存储设备传递数据的，经主管副总批准后，统一到 IT 部办理。

4、每天当班人员制作数据的备份并异地存放，确保系统一旦发生故障时能够快速恢复，备份数据不得更改。

5、业务数据必须定期、完整、真实、准确地转储到不可更改的介质上，并要求集中和异地保存，保存期限至少 2 年。

6、备份的数据由公司资料室负责保管，由管理人员按规定同备份部门进行交接。

7、备份数据资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。

**本制度自公布之日起执行，对违反制度的部门和人员，由公司酌情给予罚款及除名处理。本制度由 IT 部负责解释和修改。**

XXX 有限公司

IT 部

2010 年 06 月 08 日