上海淘米网络科技有限公司
信息安全管理制度

文件编号：TM-ISMS-001

发布版本号：2.0

发布日期：2011/6/9

密级：内部

编写	审核	批准	版本号	发布日期
Lisawang/王丹	aceway/艾维	总办	1.0	2011/3/9
Lisawang/王丹	aceway/艾维	总办	2.0	2011/6/9

目录

1. 引言

1.1 目的

为了提高员工信息安全防范意识和操作技能，保障公司信息安全，依据公司信息安全管理制度的要求，制定本制度。全体员工须遵守本制度，共同维护和保障公司信息安全，确保公司各项业务正常开展。

本制度遵循“信息安全，人人有责”、“谁使用，谁负责”的原则。公司全体员工人人行动起来，积极学习信息安全知识，提高防范意识和操作技能，自觉遵守信息安全制度，共同保障公司信息系统的安全运行。

1.2 适用范围

所有上海淘米网络科技有限公司和上海圣然信息科技有限公司的正式、非正式员工。从合作伙伴、合资方或是签约方得到授权访问许可的非淘米网络科技有限公司、非圣然信息科技有限公司的员工。

1.3 处罚方式

（1） 视情节严重程度，处罚级别分为：警告，记过，开除。

（2） 按照处罚级别，在当次绩效总分中扣除相应的分数，处罚累计.

- 警告 ：扣除 0.1 分。
- 记小过：扣除 0.4 分。
- 记大过：扣除 0.8 分。

（3） 所有处罚都会由人事部门进行登记，绩效考核成绩整理时统一扣除处罚分数。

1.4 责任、权利和义务

（1）除非在公司承认的文件中特别说明，信息安全部门对此规范的执行和维护工作负责。系统管理员可通过文件或其它方式委托（授权）他人代操作，但相应的责任仍为委托（授权）

者所负责。

（2）适用本制度的所有人有义务遵循本条列。

1.5 法律责任

故意违反本制度，给公司造成重大损失的，将依法追究其法律责任。

1.6 重大影响定义

本定义根据安全事件等级的划分为依据。安全事件等级的划分以事件的发生后产生的影响为依据。

（1）一旦发生将直接影响公司的正常运转、直接影响公司的品牌声誉、直接影响公司在市场上的竞争力、直接影响公司的收入等事件。

（2）一旦发生将影响或暂时中断公司的在线业务、影响公司对外形象，在半个工作日内得不到解决的事件。

（3）一旦发生将对后继工作造成不便或安全隐患，一个半工作日内得不到解决的事件。

2. 口令使用

安全优质的用户口令是保障信息安全的第一步。员工应为个人使用电脑设置好开机、屏幕保护口令，为各类帐户设置好登录口令，口令设置遵循以下基本原则：

2.1 安全等级

不同安全等级、不同应用用途的用户应设置不同口令。例如：业务用户和非业务用户、公司内部用户和普通上网用户等应分别设置不同口令。

2.2 密码长度

密码长度必须满足公司规定要求，密码的长度必须为 7 个以上，并满足公司密码复杂度要求。

2.3 密码复杂度

密码应该是小写字母+数字+符号、大写字母+数字+符号、大写字母+小写字母+数字等组合。

2.4 修改密码

（1）当怀疑他人的密码可能泄密时，立即修改密码。

（2）在第一次登陆时，改变或要求改变事先分配的、默认的、临时的密码。

2.5 密码保密

（1）使用人对账号的安全性负责，安装非 windows 机器的同事对自己的机器安全性负责。

（2）未经部门总监允许不得将个人账户密码泄露给他人、不得打听或猜测他人账户密码。

（3）避免将密码记录在他人可能容易获取的地方，新用户在第一次登录时应修改其临时设置的密码。

（4）设置缺省密码的新用户，用户生效后及时登录并修改密码，公司内部员工禁止盗用非本人账户和密码。

2.6 补充说明

以上条列适用于所有上海淘米网络科技有限公司和上海圣然信息科技有限公司的机器，包括测试机器，并作为补充条列与公司其它密码要求条列并行。

2.7 处罚条例

2.7.1 未经上级允许，将个人密码泄露给他人，视情节不等，给予警告或记过处分。

（1）未经上级允许，将个人密码故意泄露给他人，他人使用此账户操作，本人和他人均给予警告处分。

（3）未经上级允许，将个人密码故意泄露给他人，造成公司信息泄露，未产生重大影响，本人和他人均给予记小过处分。

（4）未经上级允许，将个人密码故意泄露给他人，造成公司资源泄露，产生重大影响，

本人和他人均给予记大过处分。

2.7.2 新用户第一次登录忘记修改密码或设置弱密码出现账户被盗用情况，视情节不等，给予警告或记过处分。

（1）新用户第一次登录忘记修改密码或设置弱密码,出现账户被盗用情况，未造成重大影响，给予警告处分。

（2）新用户第一次登录忘记修改密码或设置弱密码,出现账户被盗用情况，造成重大影响，给予记小过处分。

2.7.3 个人办公电脑因管理不善重装系统、安装虚拟机、使用盗版软件等，造成公司资源泄露，视情节不等，给予警告、记过或开除处分。

（1）个人办公电脑因管理不善重装系统、安装虚拟机、使用盗版软件等，造成公司资源泄露，导致公司非机密资源泄露，未造成重大影响，给予警告处分。

（2）个人办公电脑因管理不善重装系统、安装虚拟机、使用盗版软件等，造成公司资源泄露，导致公司非机密资源泄露，造成重大影响，给予记小过处分。

（3）个人办公电脑因管理不善重装系统、安装虚拟机、使用盗版软件等，造成公司资源泄露，导致公司机密资源泄露，给予记大过处分。

（4）个人办公电脑因管理不善重装系统、安装虚拟机、使用盗版软件等，造成公司资源泄露，恶意泄露公司重要资源，给予开除处分。

2.7.4 公司内部员工禁止盗用非本人账户和密码，视情节不等，给予记过或开除处分。

（1）公司内部员工盗用非本人账户和密码，未导致公司机密资源泄漏，未造成重大影响，给予记大过处分。

（2）公司内部员工盗用非本人账户和密码，导致公司机密资源泄漏，造成重大影响，给予开除处分或提交司法机关处置。

3. 病毒防范

计算机病毒及木马等恶意程序能导致系统破坏、数据泄露、网络中断等严重安全事件发生，是信息系统的最大安全威胁之一。员工应配合做好个人办公机及个人业务终端等的病毒防范工作。

3.1 安装杀毒软件，防火墙

（1） 员工应检查确认个人所用电脑（测试用机）已安装公司制定防病毒软件。如未安装应及时联系管理员安装。

（2） 员工必须确认杀毒软件及其病毒库正常更新。

（3） 在使用 U 盘、光盘、软盘等移动介质前，一定要先进行病毒检查；员工不得制造、传播计算机病毒。

3.2 处罚条例

3.2.1 员工制造、传播计算机病毒，造成重大影响者，视情节不等，给予警告、记过或开除处分。

（1）员工传播计算机病毒，未造成重大影响，给予警告处分。

（2）员工制造计算机病毒，未造成重大影响，给予记小过处分。

（3）员工制造计算机病毒，导致公司数据泄漏，给予记大过处分。

（4）员工恶意制造计算机病毒，导致公司数据泄漏，并造成重大影响，给予开除处分或提交司法机关处置。

4. 互联网

互联网是一个开放的网络环境，上网时可能受到恶意网站或者黑客的攻击，导致系统感染病毒、系统被破坏、数据泄露等安全事件发生。

4.1 遵守国家法律法规

员工上网过程中应遵守国家法律法规，不得利用公司网络制作、复制、查阅、传播违反国家法律法规的有害信息。员工不得在未经公司授权的情况下在互联网上发布公司信息。员工不得利用公司上网资源上传、下载与工作无关的文件。

4.2 账户管理

应当避免在网吧等公用上网电脑登录公司内部系统，严禁未经授权通过远程控制方式从互联网或其他外部网络远程操作公司电脑，如工作中有此类需要则必须得到主管及相关部门批准，并做好记录。

4.3 处罚条例

4.3.1 利用公司网络制作、复制、查阅、传播违反国家法律法规的有害信息，给予记过处分。

（1）利用公司网络制作、复制、传播违反国家法律法规的有害信息，未造成重大影响者，给予记小过处分。

（2）利用公司网络制作、复制、传播违反国家法律法规的有害信息，造成重大影响者，给予记大过处分。

4.3.2 在未经公司授权的情况下在互联网上发布公司信息，视情节不等，给予警告或记过处分。

（1）在未经公司授权的情况下在互联网上发布公司信息，未泄露机密数据信息，未造成重大影响，给予警告处分。

（2）在未经公司授权的情况下在互联网上发布公司信息，泄露机密数据信息，未造成重大影响，给予记小过处分。

（3）在未经公司授权的情况下在互联网上发布公司信息，泄漏机密数据信息，造成重大影响，给予记大过处分。

4.3.3 未经上级领导批准，通过远程控制方式从互联网或其他外部网络远程操作公司电脑，视情节不等，给予警告或记过处分.

（1）未经上级领导批准，通过远程控制方式从互联网或其他外部网络远程操作公司电脑，拷贝公司资源，未造成重大影响，给予警告处分。

（2）未经上级领导批准，通过远程控制方式从互联网或其他外部网络远程操作公司电脑，泄露公司数据，未造成重大影响，给予记小过处分。

（3）未经上级领导批准，通过远程控制方式从互联网或其他外部网络远程操作公司电脑，窃取公司资源，造成重大影响，给予记大过处分。

5. 电子邮件

员工在使用电子邮件时应自觉做好相应防范工作，严禁通过电子邮件传播病毒、泄露公司机密信息等。

5.1 防范垃圾邮件

公司内部邮箱，禁止在互联网上公开（例如：网上调查表填写、网站用户注册、BBS论坛等，人事招聘、对外业务等特殊情况除外），且不要通过公司邮箱回复可疑邮件、垃圾邮件、不明来源邮件。

5.2 防范电子邮件传播病毒

在收发电子邮件前，应确认防病毒软件实时监控功能已开启；对每次收到的电子邮件，使用前均检查病毒；在收到来自公司内部员工发来的含有病毒的邮件，除自己进行杀毒外，还应及时通知对方杀毒；不打开可疑邮件、垃圾邮件、不明来源邮件等提供的附件或网址，对这类邮件直接删除。

5.3 防范数据泄露

收发公司业务相关的邮件时，必须使用公司内部邮箱，并尽量要求对方使用对方公司内部邮箱。发送敏感数据时，应采用加密邮件方式发送。不要在免费邮箱上保存敏感数据。

5.4 处罚条例

5.4.1　未经部门总监正式同意，私自在互联网上公开公司内部邮箱地址（例如：网上调查表填写、网站用户注册、BBS论坛等，人事招聘、对外业务等特殊情况除外），造成不良影响，视情节不等，给予警告或记过处分。

5.4.2　未经部门总监正式同意，私自使用公司外部邮箱收发敏感数据，造成不良影响，视情节不等，给予警告或记过处分。

5.4.3　传播含有病毒的邮件，造成不良影响，视情节不等，给予警告或记过处分。

6. 网络使用

6.1 个人网络使用

（1）未经网络管理员允许，员工不得私自更改个人所用电脑的网络参数，包括 mac 地址，ip 地址绑定等信息。

（2）未经允许不得启用任何其它网络协议远程拨入公司主机等设备。

6.2 公司网络使用

(1)非网络管理员在未明确授权时不得修改公司网络设备及其配置。

(2)员工不得私自更改到公司网络设备的连接，严禁私自让外来人员电脑接入公司网络。

(3)员工与工作相关的笔记本电脑、PDA 设备通过无线方式接入公司网络时，须经网络管理员和部门主管批准同意。

(4)严禁利用公司网络资源从事和工作无关的网络活动。

6.3 VPN 网络使用

(1) 已经获得授权使用 VPN 帐户远程操作公司电脑、网络的员工，有义务做好相应保密工作，不得将拨入号码、用户密码等信息泄露给他人。

(2) 在适用 VPN 登录公司网络时，确保操作环境的安全性，避免泄露 VPN 信息。

(3) 同事之间不得公用公司 VPN 账户。

6.4 处罚条例

6.4.1 未经网络管理员允许，员工私自更改个人所用电脑的网络参数，造成重大影响，给予警告处分。

6.4.2 已经获得授权使用 VPN 帐户远程操作公司电脑、网络的员工将账户信息泄露给他人，视情节不等，给予警告、记过或者开除处分。

（1）已经获得授权使用 VPN 帐户远程操作公司电脑、网络的员工将账户信息泄露给他人，未导致公司数据泄漏，未造成重大影响，给予警告处分。

（2）已经获得授权使用 VPN 帐户远程操作公司电脑、网络的员工将账户信息泄露给他人，导致公司数据泄漏，未造成重大影响，给予记小过处分。

（3）已经获得授权使用 VPN 帐户远程操作公司电脑、网络的员工将账户信息泄露给他人，导致公司重要数据泄漏，造成重大影响，给予开除处分。

6.4.3　未经部门总监正式同意，私自更改公司网络设备及其配置，造成重大影响，给予记大过处分。

6.4.4　未经部门总监正式同意，私自带外来人员使用公司电脑或者私自让外来人员电脑接入公司网络，视情节不等，给予警告或记过处分。

（1）未经部门总监正式同意，私自带外来人员使用公司电脑或者私自让外来人员电脑接入公司网络，导致公司信息泄露，未造成重大影响，给予警告处分。

（2）未经部门总监正式同意，私自带外来人员使用公司电脑或者私自让外来人员电脑接入公司网络，导致公司重要信息泄露，造成重大影响，给予记小过处分。

7. 数据和文件安全

公司业务数据、客户数据、重要文件、技术文档等均属于公司信息资产，员工应注意保护，防止数据泄露，不得利用网络、计算机收集泄漏公司机密信息。

7.1 个人电脑上的数据

公司个人电脑上的敏感数据使用者有义务做好保密工作，对于不再需要的数据要求执行不可恢复式的删除。移动电脑上如保存有公司敏感信息时，应对数据采取加密存放措施。严禁私自拷贝业务数据、客户数据等带离工作场所，如因工作需要时，须经过部门负责人审批同意。严禁个人私自重装操作系统、还原操作系统（必须经部门主管同意，由管理工程部 IT 支持组同事操作）。

7.2 共享存储上的文件数据

针对共享存储系统上的文件数据，个人不允许随意拷贝并删除数据，如有特殊需求，须经过管理员和部门主管同意审批。对于存放到服务器上临时文件夹下的数据，个人在使用完后应及时进行清除。

7.3 SVN 数据

不允许通过任何途径将 SVN 上的项目源代码带出公司，如因工作有特殊需求，必须经过公司审批授权。对于从 SVN 上迁出的数据，迁出者应做好相应保密工作，不得随意传播，对于不再使用的数据应及时删除。

7.4 公司系统资产

公司笔记本个人丢失，个人有责任，相关领导有连带责任。接触到 IDC 的用户数据、OA 数据的运维、开发同事要严格对数据保密。开通统计平台、客服平台和人事等相关 OA 系统的权限，审批人需要对申请权限人负责。

机要岗位人员要对公司机要信息保密，任何项目运营等业务产生数据的获取、发布、须经严格审批，任何擅自获取，泄露机密业务数据信息的人员，将追究责任。机要岗位人员不得带领任何无关人员进入保管机要信息的场所。机要岗位员工必须自觉接受公司各项安全管理监督，积极配置信息安全审计工作。

7.5 其他配置管理工具软件上数据

适用 SVN 数据条列。

7.6 处罚条例

7.6.1 未经部门总监正式批准，私自拷贝业务数据、客户数据等并带离工作场所，视情节不等，给予警告、记过或开除处分。

（1）未经部门总监正式同意，私自拷贝业务数据、客户数据等带离工作场所，未导致公

司数据泄漏，给予警告处分。

（2）未经部门总监正式同意，私自拷贝业务数据、客户数据等带离工作场所，导致公司数据泄漏，未造成重大影响，给予记小过处分。

（3）未经部门总监正式同意，私自拷贝业务数据、客户数据等带离工作场所，导致公司数据泄漏，造成重大影响，给予记大过处分。

（4）窃取、买卖公司业务数据，导致公司数据泄漏，造成重大影响，给予开除处分。

7.6.2 未经部门总监正式同意，私自拷贝共享存储系统上的文件数据并随意删除数据，视情节不等，给予警告或记过处分。

（1）未经部门主管正式同意，私自拷贝共享存储系统上的文件数据并随意删除数据，未造成重大影响，给予警告处分。

（2）未经部门主管正式同意，私自拷贝共享存储系统上的文件数据并随意删除数据，造成重大影响，给予记小过处分。

7.6.3 未经部门总监正式同意，私自将 SVN 上的项目源代码带出公司并随意传播，视情节不等，给予记过或者开除处分。

（1）未经部门总监正式同意，私自将 SVN 上的项目源代码带出公司，未导致公司资源泄露，未造成重大影响，给予记小过处分。

（2）未经部门总监正式同意，私自将 SVN 上的项目源代码带出公司，导致公司资源泄露，造成重大影响，给予开除处分或提交司法机关处置。

7.6.4 丢失公司笔记本，视情节不等，给予记过处分。

（1）丢失公司笔记本，未造成重大影响，给予记小过处分。

（2）丢失公司笔记本，造成重大影响，给予记大过处分。

7.6.5 接触到 IDC 的用户数据、OA 数据等重要数据的人员，泄露公司数据，视情节不等，给予记过或开除处分。

（1）接触到 IDC 的用户数据、OA 数据等重要数据的人员，泄露公司数据，未造成重大影响，给予记小过处分。

（2）接触到 IDC 的用户数据、OA 数据等重要数据的人员，泄露公司数据，造成重大影响，给予开除处分。

7.6.6 审批人随意给不符合要求的人员授予公司系统的权限，视情节不等，给予警告或记过处分。

（1）审批人随意给不符合要求的人员授予公司系统的访问权限，未泄露公司机密，未造成重大影响，给予警告处分。

（2）审批人随意给不符合权限要求的人员授予公司系统的访问权限，泄漏公司机密数据，给予记小过处分。

7.6.7 机要岗位人员（包括安全管理人员，系统管理员，DBA 人员，财务人员，人事人员，后台开发人员）违反公司安全管理制度，擅自获取，泄露机密业务数据信息，视情节不等，给予记过或开除处分。

（1）机要岗位人员故意违反公司安全管理制度，擅自获取，泄露机密业务数据信息，未造成重大影响，给予记大过处分.

（2）机要岗位人员故意违反公司安全管理制度，擅自获取，泄露机密业务数据信息，造成重大影响，给予开除处分.

7.6.8 由于本职工作失职导致公司信息泄露，涉及的相关人员均给予警告或记过处分。

（1）由于本职工作失职导致公司非机密信息泄露，给予警告处分。

（2）由于本职工作失职导致公司机密信息泄露，未造成重大影响，给予记小过处分。

（3）由于本职工作失职导致公司机密信息泄露，造成重大影响，给予记大过处分。

7.6.9 未经部门总监正式同意，个人私自重装操作系统、还原操作系统，视情节不等，给予警告、记过处分。

（1）未经部门总监正式同意，个人私自重装操作系统、还原操作系统，给予警告处分。

（2）未经部门总监正式同意，个人私自重装操作系统、还原操作系统，造成数据丢失，给予记小过处分。

（3）未经部门总监正式同意，个人私自重装操作系统、还原操作系统，造成重要数据永久性丢失，给予记大过处分。

7.6.10 未经部门总监正式同意，个人私自收集、获取内部机密数据信息，视情节不等，给予警告、记过或开除处分。

（1）未经部门总监正式同意，个人私自收集、获取与本人工作无关的内部机密数据信息，给予警告处分。

（2）未经部门总监正式同意，个人私自收集、获取与本人工作无关的内部机密数据信息，造成信息泄密，给予记小过处分。

（3）未经部门总监正式同意，个人私自收集、获取与本人工作无关的内部机密数据信息，造

成重要信息泄密，产生重大影响，视情节不等给予记大过或开除处分。

8. 系统使用

8.1 员工禁止使用

员工不得私自开启计算机机箱，不得私自装配并使用可读写光驱、磁带机、磁光盘机和 USB 硬盘等外置存储设备；未经部门主管及相关部门同意员工不得将公司配备的个人工作用笔记本电脑借给他人使用；员工不得私自在公司服务器系统中设立和工作无关的网站、论坛、游戏等站点。员工不得私自登录未授权操作系统，查看、收集和本工作无关的敏感数据；

8.2 终端使用

业务终端上严禁安装与业务无关的软件。个人办公电脑均应设置自动锁屏状态。员工离开座位时应设置电脑为退出状态或锁屏状态。禁止个人办公电脑长期不关机，如因工作需要则需通过部门主管审批并报相关部门登记备案。

登录相关应用系统，在使用完毕后应及时退出。无人值守的终端，操作人员离开时应主动设置为锁屏状态或其他防护措施。

8.3 处罚条例

8.3.1　未经部门总监正式同意，私自开启计算机机箱，私自装配并使用可读写光驱、磁带机、磁光盘机和 USB 硬盘等外置存储设备，造成公司资源泄露，视情节不等，给予警告、记过处分。

（1）私自开启计算机机箱，私自装配并使用可读写光驱、磁带机、磁光盘机和 USB 硬盘等外置存储设备，导致公司资源泄露，未产生重大影响，给予警告处分。

（2）私自开启计算机机箱，私自装配并使用可读写光驱、磁带机、磁光盘机和 USB 硬盘等外置存储设备，导致公司资源泄露，造成重大影响，给予记大过处分。

8.3.2　将公司配备的个人工作用笔记本电脑借给他人使用，导致公司资源泄露，造成重大影响，给予警告处分。

8.3.3　未经部门总监正式同意，私自在公司服务器系统中设立和工作无关的网站、论坛、游戏等站点，视情节不等，给予记过或开除处分。

（1）未经部门总监正式同意，私自在公司服务器系统中设立和工作无关的网站、论坛、游戏等站点，泄露公司信息，给予记大过处分。

（2）未经部门总监正式同意，私自在公司服务器系统中设立和工作无关的网站、论坛、游戏等站点，泄露公司信息，造成重大影响，给予开除处分。

8.3.4　员工离开座位时没有设置电脑为退出状态或锁屏状态，给予警告处分。

8.3.5　无人值守的终端，操作人员离开没有设置锁屏或其他防护措施，视情节不等，给予警告或记过处分。

（1）无人值守的终端，操作人员离开没有设置锁屏或其他防护措施，泄漏公司信息，未造成重大影响，给予警告处分。

（2）无人值守的终端，操作人员离开没有设置锁屏或其他防护措施，导致重要信息泄漏，造成重大影响，给予记小过处分。