办公网敏感主机安全管理制度

文件编号：TM-ISMS-002

发布版本号：2.0

发布日期：2011/12/14

密级：内部公开

文档信息表

文档名称	办公网敏感主机安全管理制度		
文档编号	TM-ISMS-002	保密级别	内部公开
制作人	wuxinglin	制作日期	2011-8-2
复审人	aceway	复审日期	2011-12-14
扩散范围	全体员工		
扩散批准人	xml		

文档修订信息			
日期	版本	变更人	变更内容
2011-12-2	2.0	wuxinglin	增加处罚条款；删除表 1.1 中的范围。

■ 版权声明

■ 保密级别

根据文档重要程度不同，可将文档分为以下四级：

- ◆ 完全公开：任何人可以随意传阅文档；
- ◆ 内部公开：仅限上海淘米网络科技有限公司、上海圣然信息科技有限公司全体员工传阅文档；
- ◆ 限制分发：仅限文档内指定的直接或间接相关人员传阅文档；
- ◆ 商业机密：仅限文档内指定的直接相关人员传阅文档。

目 录

第一章 概述

1.1 总则

为进一步加强公司办公网敏感主机的安全管理（敏感主机概念参见 1.3 ），确保敏感主机信息安全，建立健全信息安全体系，特制定本管理制度。

本管理制度明确了办公网敏感主机在安全管理方面的基本要求，通过对办公网敏感主机进行安全管理，可以有效规避信息安全风险，从而最大限度的确保敏感主机的信息安全。

1.2 目的

1、 明确办公网敏感主机在安全管理方面的基本要求；
2、 规避信息安全风险，最大限度的确保敏感主机的信息安全。

1.3 名词解释

◆ **敏感主机**

所谓敏感主机，指办公网中存在的，用于保存重要数据或提供重要服务的主机，包括：**敏感岗位个人办公主机**和**敏感服务器**。

注意：各部门总监可根据部门情况自行增报敏感主机。

◆ **敏感岗位个人办公主机**

所谓敏感岗位个人办公主机，指一旦出现中毒、黑客入侵等信息安全事件时，影响范围大，后果严重的主机，一般为敏感岗位工作人员使用的办公主机（敏感岗位如财务部、人力资源部、IT 支持组、内审内控组等）。

办公网敏感岗位工作人员详见表 1.1 ：

表 1.1 办公网敏感岗位工作人员明细表

部门	范围	备注
财务部	所有成员	掌握财务重要数据
人力资源部	薪资福利组成员	掌握人力资源重要数据
信息安全部	内审内控组成员	掌握大量权限、敏感数据信息

◆ **敏感服务器**

所谓敏感服务器，指办公网中使用的，用于提供基础办公服务或保存重要数据的服务器，包括：域控服务器、共享服务器、邮件服务器等。

敏感服务器的维护人员通常指管理工程部 IT 支持组、系统维护组，特殊情况除外（如

研发部敏感业务测试服务器由研发部自行维护）。

办公网敏感主机范围详见表 1.2 ：

表 1.2 办公网敏感主机范围

大类	小类	部门	范围	备注
敏感主机	敏感岗位个人办公主机	财务部	所有主机	包含财务重要数据
		人力资源部	薪资福利组专用主机	包含人力资源重要数据
		信息安全部	内审内控组专用主机	可访问的目标广、权限大
	敏感服务器	财务部	财务数据服务器	包含财务重要数据
		人力资源部	人力资源数据库服务器	包含人力资源重要数据
		管理工程部	域控服务器	正常办公基础服务器
			DNS 服务器	正常办公基础服务器
			邮件服务器	正常办公基础服务器
			RTX 服务器	正常办公基础服务器
			网关服务器	正常办公基础服务器
			文件共享服务器	包含敏感文件、数据
			SVN 服务器	包含游戏源代码
			BBS 服务器	包含域帐号等相关数据
		运营开发部	二组/三组开发服务器	包含重要敏感项目源代码
			一组测试服务器	包含重要敏感项目源代码
			一组开发服务器	包含重要敏感项目源代码
		信息安全部	安全平台	包含敏感监控数据
			服务器跳转系统	包含敏感数据
			VPNLOG	包含敏感数据
		质量管理部	项目管理系统服务器	包含游戏相关文档数据

办公网敏感主机 IP、负责人详见《TM-ISMS-002-办公网敏感主机明细表》。

1.4 适用范围

本管理制度建立在《上海淘米网络科技有限公司信息安全管理制度》基础上，针对敏感主机制订了更严格的安全管理要求，因此敏感岗位工作人员和敏感服务器维护人员首先应遵守《上海淘米网络科技有限公司信息安全管理制度》，其次应遵守本管理制度的规定。

若本管理制度内容与《上海淘米网络科技有限公司信息安全管理制度》发生冲突，则敏感岗位工作人员和敏感服务器维护人员应当优先遵守更严格的规定（即两个制度中针对冲突内容的规定，以较严格的为执行依据）。

本管理制度自发布之日起生效。

1.5 处罚条例

1.5.1 重大影响定义

符合以下情形之一的视为产生重大影响：

1、 一旦发生将导致公司网络被木马、病毒、黑客攻击，或导致公司机密信息泄露；

2、 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；

3、 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；

4、 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。

1.5.2 处罚措施

违反本管理制度的行为将会视情节严重程度进行处罚，具体处罚办法如下：

◆ 处罚对象

对于违反本管理制度的行为，除当事人将受到处罚外，当事人的直属上级和所在部门主管将承担管理责任。

◆ 处罚级别

根据情节的严重程度，处罚可分为四个级别，分别为：警告、记小过、记大过、开除；对于情节特别严重且触犯刑法的，公司保留追究法律责任的权利。

◆ 处罚方法

对于违反本管理制度的，在其当次绩效总分中扣除相应的分数，具体扣分如下：

警　告：扣除 0.1 分；

记小过：扣除 0.4 分；

记大过：扣除 0.8 分。

以上处罚均由人力资源部进行登记并公告，绩效考核成绩整理完成时由人力资源部统一扣除处罚分数（处罚扣分将被累计）。

第二章　基本安全管理制度

敏感岗位工作人员、敏感服务器维护人员应当遵守以下安全管理要求：

2.1　物理安全

第一条　禁止携带公司以外的人员进入敏感岗位办公场所及办公网机房，特殊情况需要临时进入的，必须经过部门总监审批，并有专人全程陪同及进行有效登记；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第二条　禁止携带、接入公司以外的主机到敏感主机所在办公场所，特殊情况需要临时携带、接入的，必须经过部门总监审批，并进行有效登记；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第三条　禁止拍摄敏感主机相关的数据影像；

处罚方法：

违反此规定未造成信息泄漏的，给予警告处分；造成信息泄漏但未造成重大影响的，给予记小过处分；造成信息泄漏且造成重大影响的，给予记大过处分。

第四条　禁止在办公桌面放置包含敏感数据的纸质文件（有独立办公室的除外，但下班后办公室必须上锁），敏感岗位工作人员和敏感服务器维护人员下班后抽屉必须上锁；

处罚方法：

违反此规定未造成信息泄漏的，给予警告处分；造成信息泄漏但未造成重大影响的，给予记小过处分；造成信息泄漏且造成重大影响的，给予记大过处分。

第五条　禁止将包含敏感数据的纸质文件直接丢弃或遗留在打印机上，不再使用的纸质文件必须进行粉碎（如使用碎纸机）；

处罚方法：

违反此规定未造成信息泄漏的，给予警告处分；造成信息泄漏但未造成重大影响的，给予记小过处分；造成信息泄漏且造成重大影响的，给予记大过处分。

第六条　任何一台敏感主机必须有明确的负责人。

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

2.2 系统安全

第七条 禁止将敏感主机交由他人使用，或让他人登录；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。）

第八条 禁止在敏感主机上使用移动存储设备（如 U 盘、移动硬盘等），对于特殊原因需要临时使用的，必须由部门总监审批，并进行有效登记；

处罚方法：

违反此规定未造成信息泄漏的，给予警告处分；造成信息泄漏但未造成重大影响的，给予记小过处分；造成信息泄漏且造成重大影响的，给予记大过处分。

第九条 敏感主机必须安装防病毒软件，并且设置为定时自动更新病毒库；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第十条 禁止擅自安装、更换操作系统，或擅自更改敏感主机的系统权限（如添加用户、退出域等）；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第十一条 禁止将敏感主机的口令设置为弱口令；禁止整个部门、整批服务器共用一个口令；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第十二条 禁止将敏感主机相关口令告诉他人；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第十三条 禁止开启敏感主机的口令自动记忆功能；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第十四条 敏感主机必须开启系统日志审计功能；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第十五条 敏感主机必须开启屏幕保护功能，且恢复时使用密码保护；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第十六条 敏感岗位工作人员和敏感服务器维护人员离开正在使用的敏感主机时，必须立即进行锁屏；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第十七条 当敏感主机出现异常时（如中毒、丢失文件、发现有非正常改动痕迹等），应及时记录异常并上报；

第十八条 敏感岗位工作人员和敏感服务器维护人员出现内部调动时，管理工程部必须收回其不再使用的系统、网络访问权限；信息安全部必须收回其不再使用的应用系统访问权限；内部调动人员的直接上级必须更换调动人员对应的敏感帐户密码；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第十九条 敏感岗位工作人员和敏感服务器维护人员离职后，管理工程部必须收回其对应的系统、网络访问权限，信息安全部必须收回其对应的应用系统访问权限，其交接出的工作中使用的敏感帐户必须更换密码。

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

2.3 网络安全

第二十条 禁止在敏感主机上从事与工作无关的互联网访问行为，对于有内外网两台主机的工作人员（内网主机用于办公，外网主机用于上网），禁止使用内网主机访问互联网（已授权访问的特定网站除外）；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第二十一条 禁止在网络上明文传输敏感主机相关口令，口令必须加密后再进行传输（如将口令写在文本文件中，再用压缩工具加密压缩后进行传输）；

处罚方法：

违反此规定未造成安全问题的，给予警告处分；造成安全问题但未造成重大影响的，给予记小过处分；造成安全问题且造成重大影响的，给予记大过处分。

第二十二条 敏感主机上的共享文件夹禁止设置为所有人完全控制。

处罚方法：

违反此规定未造成信息泄露的，给予警告处分；造成信息泄露但未造成重大影响的，给予记小过处分；造成信息泄露且造成重大影响的，给予记大过处分。

2.4 数据安全

第二十三条 禁止将敏感主机上与工作有关的数据外发、外带到工作以外的环境；

处罚方法：

违反此规定未造成信息泄露的，给予警告处分；造成信息泄露但未造成重大影响的，给予记小过处分；造成信息泄露且造成重大影响的，给予记大过处分；造成信息泄露且造成重大影响，同时触犯国家法律的，给予开除处分，公司保留移交司法机关处理的权利。

第二十四条 敏感主机废弃或下线不再使用时，敏感岗位工作人员必须删除工作相关数据（销毁数据建议使用专用的销毁工具）；

处罚方法：

违反此规定未造成信息泄露的，给予警告处分；造成信息泄露但未造成重大影响的，给予记小过处分；造成信息泄露且造成重大影响的，给予记大过处分。

第二十五条 敏感主机下线后若需要另做它用，IT 支持组必须重装系统且对全盘进行格式化后方可交付使用。

处罚方法：

违反此规定未造成信息泄露的，给予警告处分；造成信息泄露但未造成重大影响的，给予记小过处分；造成信息泄露且造成重大影响的，给予记大过处分。

第三章 敏感岗位安全管理制度

敏感岗位工作人员除应遵守“基本安全管理制度”外，还应遵守以下安全管理要求：

3.1 物理安全

第二十六条 禁止擅自更换个人办公主机的硬件设备，或擅自更换办公场所，如有需要必须由 IT 支持组统一进行更换；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

3.2 系统安全

第二十七条 禁止在个人办公主机上安装与工作无关的软件（包括各种绿色版本），对于工作中需要的软件，需向部门总监汇报，总监授权后方可安装；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第二十八条 在初次登录敏感岗位个人办公主机时，必须修改初始口令；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第二十九条 敏感岗位个人办公主机安全配置应符合《办公网敏感主机安全配置规范》的要求。

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

3.3 网络安全

第三十条 在条件允许的情况下，管理工程部应当将敏感岗位个人办公主机与上网主机进行隔离；

第三十一条 在条件允许的情况下，管理工程部应当将敏感岗位办公网络与其它岗位办公网络进行隔离，禁止直接互通；

第三十二条 在条件允许的情况下，管理工程部应当限制其它主机访问敏感岗位个人办公主机的权限（遵循权限最小化原则）。

3.4 数据安全

第三十三条 禁止将工作数据发送、展示给其他无关人员；

处罚方法：

违反此规定未造成信息泄露的，给予警告处分；造成信息泄露但未造成重大影响的，给予记小过处分；造成信息泄露且造成重大影响的，给予记大过处分；造成信息泄露且造成重大影响，同时触犯国家法律的，给予开除处分，公司保留移交司法机关处理的权利。

第三十四条 敏感岗位工作人员本地保存的重要数据应当进行加密（如财务部 WORD、EXCEL 文档应当设置密码），在条件允许的情况下建议使用 Truecrypt 加密盘。

第四章　敏感服务器安全管理制度

敏感服务器维护人员除应遵守“基本安全管理”制度外，还应遵守以下安全管理要求：

4.1　物理安全

第三十五条 敏感服务器必须统一放置在办公网机房，禁止随意放置服务器；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第三十六条 必须对办公网机房采取防断电、防灰尘、进门刷卡等安保措施；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第三十七条 敏感服务器上必须张贴明显的标识以方便识别，标识上应写明服务器编号、用途、IP 地址等；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第三十八条 敏感服务器使用的网线两端必须进行对应标识，禁止乱拉网线；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第三十九条 敏感服务器对应的配件必须妥善保管，禁止随意丢弃配件（如光盘、说明书等）。

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

4.2　系统安全

第四十条　禁止使用敏感服务器从事任何商业行为或与工作无关的行为；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分；造成重大影响，同时触犯国家法律的，给予开除处分，公司保留移交司法机关处理的权利。

第四十一条 对敏感服务器所做的任何变更（包括开机、关机），必须通知敏感服务器负责

人及管理工程部总监，且必须对变更内容进行有效登记；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记大过处分。

第四十二条 敏感服务器必须根据《办公网敏感主机安全配置规范》进行安全加固，新采购的敏感服务器在上线前必须经过部门总监审批。

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

4.3 网络安全

第四十三条 在条件允许的情况下，管理工程部应当将敏感服务器网络与其它办公网络隔离，敏感服务器应当部署在 DMZ 区，禁止从敏感服务器访问办公网；

第四十四条 在条件允许的情况下，管理工程部应当限制办公网主机访问敏感服务器的权限（遵循权限最小化原则）；

第四十五条 敏感服务器维护人员远程登录到敏感服务器且不再继续使用时，必须注销当前登录；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

第四十六条 敏感服务器必须开启登录超时机制。

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记小过处分。

4.4 数据安全

第四十七条 除文件服务器外，禁止在敏感服务器上保存与业务无关的文件；

处罚方法：

违反此规定未造成重大影响的，给予警告处分；造成重大影响的，给予记大过处分。

第四十八条 禁止将真实环境数据拷贝到敏感业务测试服务器上；

处罚方法：

违反此规定未造成信息泄露的，给予警告处分；造成信息泄露但未造成重大影响的，给予记小过处分；造成信息泄露且造成重大影响的，给予记大过处分；造成信息泄露且造成重大影响，同时触犯国家法律的，给予开除处分，公司保留移交司法机关处理的权利。

第四十九条 在条件允许的情况下，敏感服务器维护人员应当对敏感服务器的数据进行定期备份，对于特别重要的敏感服务器（如财务数据库服务器），建议使用双机备份。

处罚方法：

违反此规定未造成信息泄露的，给予警告处分；造成信息泄露但未造成重大影响的，给予记小过处分；造成信息泄露且造成重大影响的，给予记大过处分。