受控副本章	
发放编号	003
有效版本	A 版 0 次
实施日期	2010-05-01
使用部门	管理者代表

恶意软件控制程序

1 范围

为防止各类恶意软件造成破坏，确保公司的软件和信息的保密性、完整性与可用性。

适用于公司各部门对恶意软件的控制管理工作。

2 职责

2.1 网管负责全公司恶意软件的管理控制工作，负责全公司防病毒软件的安装及病毒库的更新管理，为各部门信息处理设施的防范恶意软件提供技术性支持。

2.2 各个部门具体负责其部门信息处理设施的病毒清杀及其它预防措施的实施。

3 程序文件

所谓恶意软件，是指编制或者在计算机程序中插入的破坏计算机功能、毁坏数据、窃取数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码，主要是指各类计算机病毒。

3.1 防范措施

主要是安装防火墙、安装杀病毒软件。具体方法如下：

a) 网络管理员在所有工作站上安装防病毒软件，并周期性对病毒库进行升级。使用 PC 的员工，开启实时防护功能，操作系统自带防火墙要求开启。网络管理员负责定期检查并填写到[杀毒软件及系统补丁升级检查表]中；

b) 如某种新恶性病毒大规模爆发，网络管理员应紧急通知全公司员工对所使用 PC 或笔记本立即进行病毒库更新升级，同时立即进行病毒扫描，并将病毒情况汇报；

c) 员工发现防病毒软件报警后，应立即拔掉本机网线，确保及时与网络隔离，并将情况及时上报给网络管理员，网络管理员应马上对中毒机器进行查杀或操作系统恢复，确保病毒彻底去除后，才能将计算机接入公司网络；

d) 员工在使用任何电子媒体前都应对其进行病毒扫描，对发现病毒的电子媒体应禁用，待病毒清除后方可使用，对于不能清除的病毒，应及时报告给网管处理；

e) 客户来访时，如有接入公司网络的需要，首先要求对准备接入网络的设备（笔记本等）进行检查，如果发现该设备没有安装防病毒软件或杀毒软件没有及时升级，应拒绝接入公司网络的要求。待安装最新防病毒软件后方可允许；

f) 网管应不定期安排对公司员工进行有关防病毒及其他后门程序等恶意软件预防工作的培训。

3.2 预防恶意软件的通用要求

安全意识和适当的系统权限是保护不受恶意软件攻击的基础。所有员工应养成良好的防范恶意软件意识并遵守一下规定：

a) 按照本程序规定的要求使用防病毒软件；

b) 禁止使用来历不明的软件；

c) 删除来历不明的电子邮件，并及时从垃圾箱中清空；

d) 使用 U 盘时必须进行病毒扫描。

3.3 重要系统防范恶意软件的特殊要求

a) 网络管理员应关注防火墙、入侵检测系统供应商的产品动态，确保功能及时升级并对其实施严密的安全策略，以保证公司网络的安全。

b) 对于涉及公司机密等重要系统严格实施网络隔离政策，严禁与互联网连接。

3.4 备份

员工应按照信息备份的要求（见《重要信息备份管理程序》）进行重要数据和软件的备份。

3.5 恢复

如果发生信息处理设施受到病毒或其他种类的恶意软件攻击的事故，应由网管确认事故原因后，对被破坏数据或软件进行恢复。

3.6 外购软件安装

对安装的外购软件必须由网管检测其安全性，经确认后方可安装使用。

3.7 下载软件

对于下载软件及下载软件安装，应当在下载后检查是否含有恶意代码，对公司网络环境是否有破坏等，如果不能判定，可请网管员下载检查后给员工安装。

4 相关文件和记录

《重要信息备份管理程序》

[杀毒软件及系统补丁升级检查表]　　保存部门：行政公关部　　保存期限：1 年

附加说明：

本标准由湖南丰汇银佳科技有限公司提出。

本标准由湖南丰汇银佳科技有限公司行政公关部起草。

起草：郑安武　　审核：杨彬　　批准：刘熙　　日期：2010-04-28