文档密级：C

恶意代码防范管理规范

一、 总则

1. 目的

本文档为加强对恶意代码的预防和治理，保护公司信息系统安全，根据公安部《计算机病毒防治管理办法》以及有关计算机病毒防治的规定，制定本制度。

2. 适用范围

本文档适用于大象集团苏南总部。

3. 职责

由安全局负责恶意代码防治的日常管理工作，负责计算机病毒的监控、处理、汇总、通报、上报等工作，负责计算机杀毒软件的安装、升级、运行、监控和维护等工作。信息安全工程师需定期分析防病毒软件检测到的全网病毒情况，并进行分析记录，必要时可上报信息部总经理，并在全公司范围内通报。

二、 管理细则

1. 恶意代码系统的规划与部署

（1） 每台接入终端、服务器，必须安装统一的网络版杀毒软件客户端软件，主系统将自动启动计算机恶意代码特征码升级和本机恶意代码查杀功能，查杀结果将会自动上传至防恶意代码系统控制台。

（2） 安装杀毒软件的计算机、服务器，不得自行卸载或安装第二套防杀恶意代码软件，以免造成杀毒功能失效或系统不稳定情况。

（3） 任何人员不得擅自停用杀毒软件。

2. 恶意代码防范的日常管理

（1） 信息系统所使用的软件必须是正式版本，不得使用测试版和盗版软件。

（2） 定期进行培训，提高所有用户的 防病毒及恶意代码意识和安全技能。

（3） 在读取移动存储设备、介子（磁盘、光盘、移动硬盘和U盘等）上的数据以及网络上接收文件或邮件之前，先进行病毒及恶意代码检查。

（4） 由信息安全局对网络和主机进行病毒及恶意代码检测并保存检测记录；

（5） 定期检查信息系统内恶意代码库的升级情况，对主机防病毒及恶意代码产品、网关和邮件防病毒及恶意代码网关上截获的危险恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

（6） 终端用户要及时进行补丁升级，避免因操作系统漏洞而造成的病毒及恶意代码入侵，并做好本机重要数据的备份。

（7） 连接互联网的终端用户需提高警惕,不下载和运行来历不明的程序,对于不明来历的邮件附件也不要随意打开。下载的软件、信息和数据要先查毒后使用。

（8） 各部门负责本部门所辖设备的安全管理，移动介质、移动设备接入网络要进行严格控制，如因上述原因发生病毒及恶意代码感染事件，由本部门承担责任；

（9） 各部门负责本部门所辖网络的接入管理，禁止任何人私自扩展、加装计算机网络和私自跳接计算机连网的信息点，并严禁在网上侦听，如因上述原因发生信息安全事件，由本部门承担责任。

（10） 对各个部门安装的办公软件都应从该软件官方地址获取，受限制的软件需获取授权后才可使用。不得使用破解、修改后的非官方软件版本。有不确定其安全性的软件。

（11） 服务器区域因业务需要使用外来移动介质（设备）的，必须由使用人递交介质使用申请，获负责人批准，并将介质接入杀毒专用计算机（与系统物理隔离）进行恶意代码检测，确认无毒后，方可接入网络内使用。

（12） 各部门要严格遵守本管理办法，不断加强恶意代码的防治工作，一旦发现违反本管理办法，对使用者及该部门根据情节严重作出相应处罚。

3. 恶意代码的查杀与处理

（1） 一旦发生病毒及恶意代码入侵事件，应第一时间进行物理隔绝，并通知信息安全局处理。

（2） 一旦部门局域网或服务器区域内计算机发生感染恶意代码疫情，为避免计算机疫情扩散，应第一时间封堵该部门局域网与业务网之间的物理链路，待采取进一步措施查杀灭病毒及恶意代码，在疫情警报解除后，再恢复网络间物理链路的连接。

（3） 对于新恶性病毒大规模爆发，信息安全局应立即升级病毒库，并做好安全防范措施和安全检查工作，另外紧急通知全公司各部门立即进行病毒库更新升级，同时立即进行病毒扫描，并对病毒情况汇报信息技术部领导。

三、 附则

1. 对违反上述安全管理条例的员工，依据《信息安全惩戒规范》进行处理。
2. 本制度由公司信息安全局负责解释和修订。
3. 本制度自发布之日起开始执行。

四、 附件

1. 《病毒分析记录表》