**北京汇聚融达网络科技有限公司**

**—防病毒安全管理制度**

**文件编码：HJRD-5-07**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 防病毒安全管理制度 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-5-07 | | **牵头部门** | 技术部 | |
| **分发范围** | 制度管控员工 | | | | |
| **版本修订** | | | | | |
| **生效日期** | **版本号** | **版本说明** | **制作** | **复审** | **批准** |
| 上半年 | V1.0 | 第一版 | 刘少会/刘陵镇 | CTO | CEO |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：文档基本信息记录本文档提交时的当前有效的基本控制信息，当前版本文档注有效期将在新版本文档生效时自动结束。文档版本小于1.0 时，表示该版本文档为草案，仅可作为参照资料之目的。

**第一条 【控制措施】**网络与信息中心指定安全管理员负责计算机病毒防范，负责防毒软件的升级、维护，病毒信息获取与提前防护，以及对病毒事件的处理。

（一）每台计算机必须安装公司指定的防病毒软件。如遇到特殊情况，必须在网络与信息中心备案。

（二）必须遵守软件使用许可，禁止使用未授权的软件。

（三）各部门统一安装部署防病毒程序，公司员工应自觉进行防病毒软件的升级和定期扫描检测，不允许自行删除、停用防病毒程序，或终止升级病毒库等。

（四）公司员工在将移动存储设备连接到北京汇聚融达网络科技有限公司电脑，或将笔记本接入公司内网时，必须事先进行病毒检测，不允许将病毒引入公司内部信息系统，违者将追究相关责任。

（五）公司员工不允许利用办公电脑设备访问与工作无关的网页，下载与工作无关的文件，使用与工作无关的网络聊天程序等，因违反本规定造成电脑设备中毒的，将追究相关责任。

（六）公司员工在发现自身电脑设备感染病毒之后，应立即拔出网线，断开与网络的连接，并及时联系安全管理员进行检查修复。

（七）对于从外部获得的数据（光盘、磁盘、U盘等媒体，以及电子邮件等）必须经过病毒检查，才能在公司内部使用。

（八）对防病毒服务器，应定期检查病毒服务器的病毒定义代码版本，如有必要，手工下载最新病毒定义代码并导入病毒服务器，确保防病毒服务器的病毒定义代码保持最新。当接收到病毒预警信息时，应及时检查防病毒服务器的病毒定义代码版本并更新。

（九）安全管理员负责对系统所出现的病毒作记录，并察其原因。

（十）各部门应及时报告病毒攻击事件，系统管理员负责协助对受病毒破坏的计算机系统进行恢复。

（十一）系统管理员应定期检查服务器的病毒历史记录，对发现的病毒进行检查和查杀，并及时向安全管理员报告。

（十二）windows操作平台服务器，原则上不允许使用文件共享形式进行文件传送。

（十三）对非windows操作平台的服务器，系统管理员应定期对服务器进行检查，如发现可疑文件应进行隔离，并及时向安全管理员报告。

（十四）安全管理员负责将本月的病毒防范工作，在每月“系统月度运行报告”的“网络信息安全”部分中上报。

**第二条【操作程序】**

（一）升级病毒库

内容：升级杀毒软件的病毒库。

标准：病毒库为最新版本。

操作：启用杀毒软件的自动升级病毒库功能，并设定自动升级的时间，可设置自动更新病毒库的时间为每天、每周或每月，原则上至少每三天升级一次病毒库，安全管理员负责填写《病毒库升级记录表》；保证防病毒服务器能连接到杀毒软件厂商的升级网站，进行病毒库更新；安装了网络版杀毒软件的客户端接受防病毒服务器的统一管理，及时从防病毒服务器下载最新病毒库进行更新。

关键点：在线升级应选择速度最快的网站进行更新，填写《病毒库升级记录表》。

特情处理：如果软件不能自动升级，到杀毒软件厂商的网站手工下载升级包并手工升级病毒库。

（二）扫描查杀病毒

内容：扫描、查杀硬盘中文件。

标准：扫描范围包括所有的硬盘空间，查杀扫描出来的所有病毒文件。

操作：使用杀毒软件扫描所有的硬盘分区，以发现硬盘中可能存在的病毒或异常情况；对外来的软盘、光盘和其它介质、电子邮件和从互联网下载的文件做病毒检查；定期或不定期地进行磁盘文件备份工作，重要的数据应当定期备份，备份前先要进行查病毒工作，建议主机每个季度做一次硬盘全面病毒扫描、查杀工作；对新购置的计算机软件在使用前也要进行病毒检测。

关键点：注意扫描出来的新病毒。

（三）记录杀毒日志

内容：记录杀毒日志。

标准：包括时间，染毒文件名，病毒名。

操作：将杀毒日志记录从信息处理设施中导出来，并作保存。如不能从计算机中导出杀毒日志记录，则安全管理员手工填写《杀毒日志记录表》。

关键点：日志记录要写得准确、详细。

（四） 病毒事件响应

内容：定期检查北京汇聚融达网络科技有限公司所有计算机是否有新病毒出现，并响应出现的病毒或异常事件。

标准：及时有效处理病毒或异常事件。

操作：网络与信息中心定期组织对所有计算机进行扫描；公司的系统管理员及其他人员在发现不可清除的病毒和异常情况时，及时报告给防病毒专职人员—安全管理员。安全管理员对用户报告的病毒事件进行响应，并记录病毒检测和处理的情况，手工填写《杀毒日志记录表》，该文档可作为北京汇聚融达网络科技有限公司的病毒防治知识库，为以后问题的处理提供帮助。病毒异常情况包括：

1、系统运行速度比平时明显变慢。

2、有打印、显示异常现象。

3、文件夹下有不明的文件自动生成。

4、磁盘空间自动产生坏簇或磁盘空间无故减少。

5、系统文件无故丢失。

7、系统异常死机的次数增加。

关键点：注意调查新病毒的来源，记录要写得准确、详细。

（五）预防通知

内容：通知北京汇聚融达网络科技有限公司所有人员注意新病毒的防护。

标准：所有人员知道详细的新病毒情况。

操作：安全管理员定期收集、整理、分析新病毒信息，描述新病毒的名称、特征和危害，并向公司全体员工发出防范该病毒的通告。

关键点：及时地通知到公司的各个部门。