

计算机病毒防范策略

文件编号：VT-WI-I-0011

版 次 ： A/0

文件类型：

编制日期： 2023 年 2 月 15 日

生效日期： 2023 年 2 月 22 日

编制： 蔡嘉荣

审核： 何健伟

批准： 冯永辉

 广东威铝铝业股份有限公司 Guangdong Victor Aluminum Co., Ltd.		文件编号	VT-WI-I-0011
		版 次	A/0
		编制日期	20230215
		生效日期	20230222
主 题	计算机病毒防范策略	页 码	2 / 4

1.目的

为了规范日常的病毒防控工作，指导信息系统病毒防范处理操作过程。

2.适用范围

该策略适用于使用公司信息资源的所有人员。

3.术语

所谓信息系统病毒，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、木马及恶意移动代码等。

4.职责

4.1 信息管理部

负责对公司内办公终端和业务支撑系统生产终端的防病毒系统采取集中管理和监控，负责病毒定义码、扫描引擎、产品修正等日常升级维护工作，对防病毒体系的日常运作的监督责任；

4.2 网络运维课

负责病毒控制的技术指导工作，并执行各项防病毒工作的安全检查工作，对于违反信息安全相关规定的人员将进行通报。

5.病毒防范策略

5.1 对于访问外部互联网的网络设备，出口防火墙配置有防病毒安全策略，同时在服务器和客户端上安装杀病毒软件（深信服 EDR）。

5.2 车间各操作终端及办公区终端由网络运维课安装杀毒软件客户端；防病毒系统定期更新服务器上病毒库，客户端自动链接服务器进行更新升级确保病毒库的及时更新；对于可以登录外网并安装杀毒软件的用户每天会自动上服务器进行病毒库的更新；

5.3 网络运维课按《防病毒系统日常维护管理制度检查表》每周在服务器检查各终端运行情况。

5.4 不安装杀毒软件的 WINDOWS 系统不得接入外部互联网、可移动设备，如接入外部网络则必须安装杀毒软件。

5.5 网络运维课负责设置企业版防病毒 EDR 服务器，每日通过互联网自动进行病毒库的更新升级。

5.6 公司计算机接受防病毒 EDR 服务器的管理，在每次开机时自动从防病毒服务器上下载最新病毒库。

5.7 特殊情况，如某种新恶性病毒大规模爆发，应立即升级病毒库，并紧急通知所有部门人员立即进

 广东威铝铝业股份有限公司 Guangdong Victor Aluminum Co., Ltd.		文件编号	VT-WI-I-0011
		版 次	A/0
		编制日期	20230215
		生效日期	20230222
主 题	计算机病毒防范策略	页 码	3 / 4

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管理部。

5.8 公司内部员工在使用部门以外的任何外置设备前都应对其进行病毒扫描，对发现病毒的电子媒体应禁用，应及时通知网络运维课，并按 5.15《病毒处理流程》执行。

5.9 所有员工，应在计算机启动后检查是否已启动防病毒客户端。如未启动，应在进行其它操作前启动防病毒客户端。

5.10 所有员工，在使用电子邮件或下载软件时应启动病毒实时监测系统的实时防护，以便对电子邮件进行病毒检查。

5.11 网络管理员需加强对特洛伊木马的探测与防治。通过以下措施予以控制：

- a) 安装反病毒软件；
- b) 使用正版软件；
- c) 对软件更改进行控制。

5.12 对重要系统的防范恶意软件的特殊要求

- a) 网络运维课应与防火墙供应商保持联系，确保功能及时升级并实施严密的安全策略，确保网络的安全。
- b) 对于涉及机密等重要系统严格实施网络隔离政策，严禁采取其它措施与互联网连接。
- c) 信息管理部应按照《数据备份与恢复管理规定》的要求进行重要数据和软件的备份。
- d) 如果发生病毒或其它种类的恶意软件攻击的事故，应由网络运维课确认事故原因后，对被破坏数据或软件进行恢复。

5.13 员工如受到各种恶意软件攻击或感觉计算机使用异常，应及时通知网络运维课，并按《应急处理管理程序》执行。

5.14 网络运维课专员对发现的病毒或遭受攻击的计算机按 5.15《病毒处理流程》进行操作。

5.15 病毒处理流程

- a) 病毒可以由防病毒系统或网络监控设备等方式发现，一经发现，需要及时通过日志定位受感染的机器地址和发起攻击的地址。立即进行网络隔离，缩小病毒在网络中的扩散范围。
- b) 网络运维课专员与安全厂商取得联系获取技术支持，下载专杀工具、病毒所利用的漏洞补丁程序等。应该按照厂商提供的修复方式对系统中发生病毒受损的设备等进行杀毒处理测试，尽快确定该病毒发作的处理操作方案。

 广东威铝铝业股份有限公司 Guangdong Victor Aluminum Co., Ltd.		文件编号	VT-WI-I-0011
		版 次	A/0
		编制日期	20230215
		生效日期	20230222
主 题	计算机病毒防范策略	页 码	4 / 4

- c) 通过机器当前的症状和病毒软件的日志发现病毒感染的类型、名称。利用安全厂商提供的专杀工具对系统进行扫描修复，并下载安装病毒所利用的漏洞补丁程序。如果需要，还应该按照厂商提供的修复方式对系统受损的文件、注册表等进行手工修复。同时，还应该将病毒定义码升级到最新，对系统做全盘扫描。
- d) 经过上述操作后，如果系统可以正常运行，则可以接回网络。必要时，需要备份用户数据，重新安装系统。然后再安装防病毒软件，更新到最新的定义码，做全盘扫描。确认系统正常运行后，再接回网络恢复工作。

6. 附录

6.1 防病毒系统日常维护管理制度检查表

防病毒系统日常维护管理制度检查表

任务编号	检查点	检查内容	取数方法	检查周期
1	病毒代码	防病毒软件病毒代码是否定期及时更新	通过服务器检查	1 周
2	病毒检查	是否定期检查病毒感染状况	通过服务器检查	1 周
3	病毒清除	病毒清除状况，清除和未清除数量及状态	通过服务器检查	1 周

6.2 病毒处理流程

