# 服务器安全操作指引

（信息与设备管理处　2029 年 9 月发布）

## 一、服务器信息安全防护十原则：

1.设置复杂的服务器密码（10 位以上含大小字母、数字、特殊字符），并至少每半年更改一次（比如:pzSBC@)@$sbn，即培正设备处 2024 上半年，等等，复杂但好记）。

2.必须安装正版杀毒软件，并定期升级和更新（至少一周查杀一次）。

3.修改超级管理员的登录账号（比如:sbcsvr_admin）。

4.开启系统自带的防火墙，除应用必须开放的端口外，其余端口一概禁用。

5.服务器上不要安装盗版软件。

6.不要在一台服务器上部署多个应用(比如既做文件存储，又做 WEB 应用发布)，有必须的、有条件的信息系统应考虑上云（同步作好安全措施和快照），不要本地化部署。

7.修改服务器默认的远程桌面 3389 端口号（具体方法可咨询设备处）；加强第三方服务商的管控，不得直接远程服务器作业，不要在服务器上进行测试工作。

8.做好数据的定期备份，除本地备份外，还须定时脱机备份。

9.所有部署在服务器（或云服务器）上的信息系统，务必及时向设备处报备；系统上线前，应对该系统和部署的服务器进行一次安全测评，对外提供系统服务的，还应实施网络安全等级保护。

10.加强对部门内各计算机终端的安全管理和人员教育，安装杀毒软件，并作好网络安全宣贯（历史表明，大多数安全事件是由终端计算机的不安全行为导致的）。

## 二、安全防护要点

### （一）计算机用户与弱口令问题

在计算机安全领域，口令（密码）是进入系统的第一道钥匙，如果钥匙太简单，就很容易被木马或黑客入侵，导致系统中毒，从而出现各种安全问题。

【防护要点】

1. 禁用系统自带的 guest 用户和其他非必要用户；

2. 修改超级用户的用户名（不用 administrator 或 admin，可改为:sbcsvr_admin）

3. **设置强度较高的用户密码**（10 个字符以上，含大小写字母、数字、特殊字符），**切忌设置空密码或弱口令**（比如:pzSBC@)@$sbn）。

**【特别注意】**部门公用电脑或服务器可能有 24 小时开机的需要，更容易成为黑客的目标而被木马病毒侵入，因此一定要设置强密码（至少每半年更换一次密码），并由专人管理，定时更新系统，定时杀毒，定时进行数据的脱机备份或在线异地备份。

### （二）病毒防治

计算机病毒是目前计算机安全最大的威胁，能造成计算机运行缓慢、频繁重启或死机、程序无法启动、数据文件丢失或被盗、文件被勒索病毒加密、网络堵塞等各种危害。

病毒的分类主要有：引导区、文件、宏、脚本、蠕虫、木马病毒、勒索病毒等。

病毒的传播载体包括：网络电子文件、移动介质（如光盘、U 盘、移动硬盘等）。

病毒的传播途径有：可执行文件(exe/bat 等)、Office 文档（宏病毒）、电子邮件、非法网站、即时通信工具、网络共享等。

【防护要点】

以**预防**为主：每台服务器都必须**安装正版杀毒软件**，并设置**每天定时更新、每周定期进行全盘扫描**。

## （三）系统安全漏洞补丁更新

操作系统非常庞杂，难免存在许多程序漏洞，如果被病毒等恶意软件利用，容易导致计算机系统中毒，产生诸多安全风险与问题，需要更新“系统补丁”封堵漏洞。

【防护要点】

1.正版 Windows 系统可以通过设置,**开启自动更新,并至少每周安装一次更新补丁**。

2.通过杀毒软件、安全卫士自带的修复系统漏洞功能进行更新修复。

3.开启系统自带的防火墙和 Windows Defender 防护程序。

## （四）硬盘安全与数据备份

计算机中存储数据的部件主要为机械硬盘 HDD 或固态硬盘 SSD，HDD 使用寿命约为**五年**，SSD 寿命更短，当计算机开始出现如下异常时，应**及时备份数据并更换新硬盘**：(1)硬盘工作时经常出现怪异的不规则响声；(2)系统频繁死机、崩溃，文件出现乱码等；(3)对文件或文件夹进行操作时，速度非常缓慢；(4)服务器有硬盘故障报警灯提示。

【防护要点】

1.**服务器硬盘应做 RAID 阵列**，有故障提示及时更换，硬盘至少 5 年更新一次。

2.**要重视数据的脱机备份**，除本地备份外，建议服务器每周脱机备份一次。

3.不要在一台服务器上既做文件存储，又做 WEB 应用发布，一旦中毒将损失惨重。

4.建议部门配备 NAS 服务器或文档管理系统，对重要的数据文件进行归档和保存。

## （五）安全策略与安全操作

操作系统中，默认会开启众多策略以及远程桌面、文件共享等服务，实际上很多都是非必要的，这些开放的策略、服务，因为管理不严格会让服务器面临更多的风险。同时，一些不安全的操作习惯，是导致系统中毒的主要原因。

【防护要点】

1.参照二级等保要求，开启或关闭相应的管理策略，比如密码强度策略等。

2.修改服务器默认的远程桌面 3389 端口号，非必要远程的可关闭此端口。

3.开启防火墙，默认关闭服务器上所有端口，必要端口设置开放策略放行。

4.关闭文件共享、打印、IIS、RPC 等无用、无关服务，开启日志管理（保留 60 天）。

5.系统上线前应向设备处报备，并组织对系统和服务器进行一次安全测评。

6.对外提供服务的信息系统，申请开放端口前，应制定网络安全等级保护计划。

7.加强第三方服务商管控，不要直接远程服务器作业或在服务器上开展测试工作。

## （六）日常使用习惯

1.离开服务器时，要按 WIN 徽标键+L 键锁定电脑屏幕，防止被他人非法利用。

2.非必要情况，不得直接在服务器上作业，可使用一台客户机作为跳板机。

3.**非工作时间，重大节假日前，应关闭服务器**。

4.从其他地方拷贝文件到服务器前，一定要**用杀毒软件对优盘等介质进行扫描。**

5.服务器上不得安装盗版软件,不要轻易下载不明站点的软件或程序,如驱动人生、免费软件、破解软件、盗版软件、绿色软件等，**很多下载链接都是钓鱼网站，非专业人士一般很难分辨**。驱动、软件等应尽量从官方网站提供的链接下载；软件应先在客户机上进行试安装后，再上服务器安装，切忌在服务器上直接下载后安装。