安全保密技术防范常识

一、不得将涉密计算机及网络接入互联网及其他公共信息网络

隐患分析：涉密计算机及网络直接或间接接入互联网及其他公共信息网络，可能被境外情报机构植入“木马”窃密程序进行窃密。

防范对策：涉密计算机及网络直接与互联网及其他公共信息网络必须实行物理隔离，即与互联网及其他公共信息网络之间没有任何信息传输通道。

二、不得在涉密计算机与非涉密计算机之间交叉使用 U 盘等移动存储介质

隐患分析：U 盘等移动存储介质在非涉密计算机上使用时，有可能被植入“木马”窃密程序进行窃密。当这个移动存储介质又在涉密计算机上使用时，“木马”窃密程序会自动复制到涉密计算机中，并将涉密计算机中的涉密信息打包存储到移动存储介质上。当移动存储介质再次接入到连接互联网的计算机上时，涉密信息就会被自动发往境外情报机构控制的特定主机上，造成泄密。

防范对策：涉密 U 盘等移动存储介质不得在非涉密计算机上使用；非涉密移动存储介质以及手机、数码相机、MP3、MP4 等具有存储功能的电子产品不得在涉密计算机上使用。

三、不得在未采取防护措施的情况下将互联网及其他公共信息网络上的数据复制到涉密计算机及网络

隐患分析：在未采取防护措施的情况下，从互联网及其他公共信息网络下载数据复制到涉密计算机及网络时，可能

同时将计算机病毒，特别是“木马”窃密程序复制到涉密计算机及网络中，存在严重泄密隐患。

防范对策：确需将互联网及其他公共信息网络上的数据复制到涉密计算机及网络时，应采取必要的防护措施，如使用一次性光盘刻录下载，设置中间机，或者使用经国家保密行政管理部门批准的信息单向导入设备。

四、不得擅自在涉密计算机上安装软件或复制他人文件

隐患分析：在涉密计算机上擅自安装软件，尤其是安装从互联网下载的软件，可能同时将计算机病毒，特别是“木马”窃密程序安装到涉密计算机中，带来泄密隐患。随意复制他人文件，也有同样的风险。

防范对策：涉密计算机安装软件或复制他人文件资料须经批准，并进行必要的病毒查杀，特别是对“木马”窃密程序的查杀。

五、不得将无线外围设备用于涉密计算机

隐患分析：涉密计算机使用无线鼠标、无线键盘等无线外围设备，涉密信息会随无线信号在空中传递，极易被他人截获，造成泄密。

防范对策：涉密计算机应使用有线连接的外围设备。

六、不得将涉密计算机及移动存储介质通过普通邮寄渠道寄运或违规交由他人使用、保管

隐患分析：将涉密计算机及移动存储介质通过普通邮寄渠道寄运或违规交由他人使用、保管，会使涉密载体失去有效的保密防护，存在泄密隐患。

防范对策：认真执行涉密载体使用保密管理规定，不得将涉密载体通过普通邮寄渠道寄运或违规交由他人使用、保管。

七、不得擅自携带涉密笔记本电脑及移动存储介质外出

隐患分析：携带涉密笔记本电脑及移动存储介质外出，容易丢失或被窃，存在严重泄密隐患。

防范对策：在一般情况下，不允许携带涉密笔记本电脑及移动存储介质外出。确需携带外出的，要严格履行审批手续，采取有效管理措施，确保涉密笔记本电脑及移动存储介质始终处于严密监控之下。同时采取强身份认证、涉密信息加密等保密技术防护措施。

八、不得擅自将处理涉密信息的计算机及移动存储介质、传真机、复印机等办公自动化设备交由外部人员维修

隐患分析：处理涉密信息的计算机及移动存储介质、传真机、复印机等办公自动化设备，是重要的涉密载体，擅自交由外部人员维修，可能会使存储的涉密信息失控。

防范对策：处理涉密信息的计算机及移动存储介质、传真机、复印机等办公自动化设备应当在单位内部进行维修，现场有专门人员监督；确需外送维修的，应当拆除信息存储部件或进行专业销密。

九、不得将未经专业销密的涉密计算机等办公自动化设备出售、赠送、丢弃

隐患分析：涉密计算机等办公自动化设备中的涉密信息被简单删除或格式化处理后，仍可以通过技术手段恢复。因此，未经专业销密就擅自处理，存在严重泄密隐患。

防范对策：1.在将涉密计算机等办公自动化设备出售、赠送、丢弃之前，应使用符合国家保密标准的设备对涉密信息或内部敏感信息进行清除，确保不被还原。2.将准备淘汰的涉密计算机等办公自动化设备送交保密行政管理部门授权的销毁机构或指定的承销单位销毁。

十、不得将处理涉密信息的多功能一体机与普通电话线路连接

隐患分析：多功能一体机具有传真、扫描、打印、复印和信息存储等功能。处理涉密信息的多功能一体机与普通电话线路连接，可能将涉密信息传输到公共通信网络上，或被境外情报机构通过普通电话线路远程控制，窃取机内存储的信息，造成泄密。

防范对策：处理涉密信息的多功能一体机，必须与普通电话线路断开。

十一、不得在涉密场所中连接互联网的计算机上配备和安装视频、音频输入设备

隐患分析：涉密场所中连接互联网的计算机如果配备和安装视频、音频输入设备，境外情报机构就可能通过互联网远程控制这台计算机，启动视频、音频输入设备对涉密场所进行窃照、窃听，造成泄密。

防范对策：涉密场所中连接互联网的计算机不得配备和安装视频、音频输入设备。

十二、不得将手机带入重要涉密场所

隐患分析：手机具有网络定位功能，带入重要涉密场所，易暴露涉密目标。手机在重要涉密场所处于通话状态时，会同时将周围的语音信息传输出去。被安装了窃听软件的手

机，即使关机或待机，也可在无振铃、无屏幕显示的情况下转为通话状态，成为一部窃听器。

防范对策：进入重要涉密场所之前，应将手机放入手机屏蔽柜内。也可使用保密会议手机干扰器对涉密场所进行手机信号屏蔽。

十三、不得在连接互联网及其他公共信息网络的计算机上存储、处理涉密信息

隐患分析：在连接互联网及其他公共信息网络的计算机上存储、处理涉密信息，相当于把涉密信息放到了无安全保护的公共场所，为他人特别是境外情报机构获取涉密信息提供了可乘之机。

防范对策：不在与互联网及其他公共信息网络连接的计算机上存储、处理涉密信息。

十四、不得在非涉密办公网络上存储、处理涉密信息

隐患分析：非涉密办公网络缺乏安全保密防护措施，如果存储、处理涉密信息，泄密风险很大。

防范对策：不在非涉密办公网络上存储、处理涉密信息。

十五、不得在政府门户网站上登载涉密信息

隐患分析：政府门户网站是建立在互联网上的信息发布平台，在政府门户网站上登载涉密信息，相当于将涉密信息发布在互联网上。

防范对策：严格遵守信息公开保密审查制度，对拟在政府门户网站上登载的信息进行严格的保密审查，确保涉密信息不上网。

十六、不得使用具有无线互联功能的计算机处理涉密信息

隐患分析：具有无线互联功能的计算机，在开机状态可自动与无线网络连接，可能被他人远程控制。即使关闭联网程序，也可以使用技术手段，通过无线网络将其激活，窃取信息。同时，无线上网传输信号暴露在空中，可被任何具有接收能力的设备截获。

防范对策：处理涉密信息的计算机，必须拆除机内无线网卡等无线互联设备，切断无线联网渠道；无法拆除的，不得用于处理涉密信息。

十七、不得使用个人计算机及移动存储介质存储、处理涉密信息

隐患分析：个人计算机及移动存储介质无法按国家保密规定进行管理，且往往连接互联网，可能感染计算机病毒，或被植人“木马”窃密程序，用来存储、处理涉密信息，泄密风险很大。

防范对策：不用个人计算机及移动存储介质存储、处理涉密信息，也不要把个人计算机及移动存储介质带入重要涉密场所。

十八、不得将未经保密技术检测的办公自动化设备用于保密要害部门、部位

隐患分析：办公自动化设备特别是进口设备，有可能被安装窃密装置，存在泄密隐患。

防范对策：用于处理涉密信息的办公自动化设备应当随机采购，并进行安全保密技术检测。