**国防科技安全保密六条规定**

1. 禁止私自在机关、单位登陆互联网；
2. 禁止在家用计算机处理涉密信息；
3. 禁止涉密网与互联网连接或在连接互联网计算机处理涉密信息；
4. 禁止私自留存涉密计算机、涉密移动存储介质或涉密文件资料；
5. 禁止在涉密计算机与非涉密计算机之间交叉使用移动存储介质；
6. 禁止擅自对外披露单位涉密信息和内部信息。

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。
 涉密计算机及其网络一旦直接或间接接入互联网及其他公共信息网络，就有可能被植入“木马”窃密程序，因而遭到窃密。因此，涉密计算机及网络与互联网及其他公共信息网络必须实行物理隔离，不可互联，即与互联网及其他公共信息网络之间不可建立任何信息传输通道。

保密技术防范常识二
 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。
 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。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木马植入者控制的特定主机上，造成泄密。因此，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。

保密技术防范常识三
 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。
 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。因此，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中，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。

保密技术防范常识四
 不得违规设置涉密计算机的口令。
 涉密计算机的口令如果设置不符合保密规定，很容易被破解。口令一旦被破解，破解者就可以冒充合法用户进入涉密计算机窃取信息。因此，涉密计算机应严格按照保密规定设置口令：处理秘密级信息的口令长度不少于8位，更换周期不超过1个月；处理机密级信息的应采用IC卡或USB Key与口令相结合的方式，且口令长度不少于4位；如仅使用口令方式，则长度不少于10位，更换周期不超过1个星期；设置口令时，要采用多种字符和数字混合编制；处理绝密级信息的应采用生理特征（如指纹、虹膜）等强身份鉴别方式。