保密工作知识

一、保密工作基本常识

（一）核心定义

1.国家秘密：关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围人员知悉的事项。

2.密级划分（三级）

绝密：最重要的国家秘密，泄露会使国家安全和利益遭受特别严重损害；

机密：重要的国家秘密，泄露会使国家安全和利益遭受严重损害；

秘密：一般的国家秘密，泄露会使国家安全和利益遭受损害。

3.保密工作方针：积极防范、突出重点、依法管理、既确保国家秘密安全，又便利信息资源合理利用。

（二）保密责任

实行谁主管、谁负责，谁在岗、谁负责责任制，全员都是保密责任人。

单位主要负责人为本单位保密工作第一责任人。

二、涉密载体管理（文件、资料、U盘、硬盘等）

1.涉密文件

涉密文件专人签收、登记、传阅，不得擅自复印、摘抄、转发、带出办公区域；

传阅限时办结，严禁横传、私存，阅后及时归档清退；

作废涉密纸质文件必须统一销毁，不得随意丢弃、售卖、当作废纸处理。

2.存储介质（U盘、移动硬盘、光盘）

严格区分涉密载体、非涉密载体，涉密 U 盘严禁接入互联网、非涉密电脑；

涉密介质专人保管、编号登记，不得转借、赠送、丢弃；

禁止使用普通U盘交叉混用涉密与非涉密数据。

三、计算机及网络保密（高频风险点）

1.物理隔离铁规

涉密计算机、涉密网络必须与互联网、外网、办公WiFi实行物理隔离，严禁一机两用、内外网交叉混用。

2.涉密电脑严禁连接无线网卡、蓝牙、摄像头、音箱等无线设备。

3.不在非涉密电脑、外网、云盘、微信、QQ、邮箱存储、编辑、传输任何涉密信息、内部敏感工作信息。

4.办公电脑设置开机密码、屏幕保护密码，离开工位及时锁屏。

5.严禁外来人员随意使用单位办公电脑、翻阅电脑文件。

四、日常办公行为保密规范

（一）会议保密

1.涉密会议明确参会范围，严禁无关人员入场、旁听；

2.会议涉密内容不记录、不录音、不拍照、不外传；

3.会议材料统一发放、会后统一收回，不得私自带走。

（二）口头与通讯保密

1.不在公共场所、家属区、社交场合谈论涉密及内部敏感事项；

2.不在微信、抖音、短视频、朋友圈、微信群、电话中谈及涉密内容、未公开工作部署、内部数据；

3.不使用普通传真、微信传发涉密文件、敏感材料。

（三）接待与外来人员管理

1.外来访客、施工人员、校外人员不得随意进入涉密场所、机要室、档案室；

2.陪同外来人员全程跟进，严禁其私自翻阅文件、操作设备、拍照录像。

五、人员管理与离岗离职保密

1.新入职人员必须开展岗前保密教育，签订保密承诺书。

2.调离、辞职、退休、临时离岗人员：

清退全部涉密文件、载体、证件、钥匙；

办理保密交接手续；

离岗后仍需履行脱密期保密义务，不得泄露原单位涉密及内部信息。

六、泄密应急处置

1.发现泄密隐患、疑似泄密事件，第一时间上报本单位

保密工作负责人，不得隐瞒、拖延。

2.立即采取补救措施，切断传播渠道，控制知情范围。

3.配合保密管理部门开展核查、整改。

七、高校重点提醒

1.内部工作方案、考核数据、人事信息、招生信息、纪检线索、舆情研判、未公开会议纪要等，均按内部敏感信息管控，参照保密要求管理。

2.公文、请示、报告、专项材料在正式发文公示前，不得提前对外泄露。

3.档案室、机要室、文印室实行专人管理、关门上锁，下班前检查门窗、文件、设备。

保密行为“十不准”

一、不准泄露党和国家机关机密。

二、不准在无保密保障的场所阅办、存放秘密文件、资料，要切实做好日常保管的同时，重点加强节假日及下班期间的管理。

三、不准擅自或指使他人复制、摘抄、销毁或私自留存带有密级或涉及密级内容的文件、资料。确因工作需要复印件应按同等密级文件管理。

四、不准在非保密笔记本或未采取保密措施的电子信息设备中记录、传输和储存党和国家机关秘密事项。

五、不准携带秘密文件、资料进入公共场所或进行社交活动；特殊情况确需要携带时，须经主管领导批准，并由本人或指定专人严格保管。

六、不准用无保密措施的通信设施和普通邮政传递党和国家机关秘密，不准在连接互联网的电脑上保存涉密文件。

七、不准与亲友和无关人员谈论党和国家机关秘密，管好身边工作人员和配偶、子女。

八、不准在私人通信及公开发表的文章、著作、讲演中涉及党和国家机关秘密，不得随意将涉及密级内容或可能造成一定影响的文件、报告等有关材料进行拍照、发朋友圈或进行网络公开。

九、不准在接受记者采访中涉及党和国家机关秘密；确因工作需要涉及或提供党和国家机关秘密的，应事先报经主要领导批准。

十、不准在考察等活动中携带涉及党和国家机关秘密的文件、资料或物品，确因工作需要携带的，须按有关规定办理审批手续，并采取严格的保密措施。

手机及移动终端设备使用“十严禁”

一、严禁在手机及移动终端通信中涉及国家秘密事项。

二、严禁在手机及移动终端设备上存储、处理、传输涉密信息。

三、严禁将手机及移动终端设备连接涉密计算机、涉密网络及涉密存储设备。

四、严禁在手机及移动终端设备上存储核心涉密人员工作单位、职务等敏感信息。

五、严禁在涉密公务活动中开启和使用手机及移动终端设备的位置服务功能。

六、严禁在申请号码、注册手机邮箱或开通其他功能时填写禁止公开的涉密单位名称和地址等信息。

七、严禁使用未经国家电信管理部门进网许可的手机和境外机构、人员赠送的移动终端设备。

八、严禁在涉密场所使用手机及移动终端设备进行录音、录像、拍照、视频通话和连接互联网等。

九、严禁在机密级以上会议或公务活动中带入手机及移动终端设备，应设置禁用标志；特殊情况需要携带时，须经主要领导批准，并登记备案。

十、严禁在机关保密要害部门、涉密会议或活动场所使用手机等移动终端设备，应设置禁用标志；必要时，应安装和使用手机信号干扰设备。

保密提醒 20 条

1.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。

2.不得在涉密计算机与非涉密计算机之间交叉使用优盘等移动存储介质

隐患分析：优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境外情报机构控制的特定主机上，造成泄密。

防范对策：涉密优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。

3.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，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。

4.不得违规设置涉密计算机的口令

隐患分析：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。

防范防策：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。

5.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。

6.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。

7.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。

8.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。

9.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。

10.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。

11.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。

12.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。

13.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。

14.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。

15.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。

16.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。

17.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。

18.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，或被植入“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。

19.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。

20.不得使用普通传真机、电话机和手机传输或谈论涉密信息

隐患分析：使用普通传真机、电话机和手机传输或谈论涉密信息，就是通过公共信息网络传输涉密信息，可能被他人截获或窃听。

防范对策：使用符合保密要求的通信方式传输涉密信息，不在普通传真机、电话机和手机通信中涉及国家秘密。

警惕工作中常见泄密行为 共筑保密防线

在数字化、信息化快速发展的今天，泄密风险点不断增多，从 AI 工具违规使用到图文识别软件使用疏漏，从社交软件随意传文件到涉密人员管理松懈，泄密风险进一步加剧。本文梳理了工作中常见失泄密案例，供以案警醒，举一反三，务必绷紧保密之弦，筑牢安全防线！

1.图文识别软件识别涉密材料：某次重大活动服务保障期间，某单位副职领导王某在落实上级机关下发的机密级安保工作方案时，要求第三方服务人员李某，把该方案通过技术手段转化为方便编辑的 word 格式文档。李某不会操作，便请同为第三方服务人员的同事袁某帮忙。袁某用手机拍摄该方案后，用图文识别小程序进行转化，相关涉密信息上传云端，造成泄密。事后，王某被给予行政警告处分，李某、袁某被解除劳动合同。

2.使用 AI 工具处理涉密材料：某涉密单位工作人员冯某在起草一份涉密材料时，苦于没有头绪，便将部分敏感内容替换成字母代码，同时将相关涉密背景材料输入 AI 写作工具辅助生成文稿，导致涉密信息暴露在数据库中。事件发生后，冯某受到严肃处理。

3.内部网络平台传输涉密文件：2023 年 1 月，某县委公职人员李某拟修改完善 2 份涉密文件征求意见稿并了解领导

小组成员单位情况。因其外出工作，李某要求办公室主任海某将该涉密材料通过单位内部 OA 系统传送给他。海某提醒李某涉密材料不能如此传递，但李某认为短暂传递一次，事后立即撤销应该不会出问题。随后，海某迫于压力将该涉密材料通过单位内部 OA 系统传递给李某，造成泄密。事件发生后，县纪委监委给予李某党内警告处分，县委某部给予海某批评教育处理。

4.非涉密计算机处理涉密文件：某高校申报某涉密科研项目，陶某使用互联网计算机填写涉密项目审查表，并将审查表拷贝至汤某个人优盘。之后，汤某将优盘中存储的涉密任务书、审查表拷贝至个人互联网计算机中，合并成一个文档，使用电脑版微信转发给莫某修改。随后，汤某又将该文档转发至项目组微信群，造成泄密。事件发生后汤某、莫某被给予纪律处分，陶某以及其他负有监管责任、领导责任的人员均受到相应处理。

5.涉密文件撤回≠泄密行为消除：2024 年，某市某单位发生了一起微信泄密事件。该单位办公室工作人员王某某，在未经允许的情况下，擅自使用手机微信将 1 份涉密文件拍照并发送至单位的微信工作群中。同为群成员的办公室负责人陶某某发现后，立即通过电话通知王某某撤回消息，王某某随即将所有照片撤回。最终，王某某因违规操作被给予警告处分，陶某某则接受了提醒谈话。同时，该单位相关领导

也受到了诫勉处理并接受提醒谈话。

从技术层面来讲，“撤回”根本无法彻底清除涉密内容。微信、QQ 后台为加速查看，通常会自动下载文件，即使“撤回”，文件可能已永久性地存储在对方设备的缓存中，仍能通过文件管理工具查找到。

保密提醒

规范涉密载体使用：涉密电脑不得连接互联网，不得安装非授权软件，定期进行安全检测；严禁将涉密电脑中的文件拷贝至非涉密设备，非涉密电脑严禁存储、处理、传输涉密信息。

规范网络传输：严禁涉密信息通过互联网传输，确保涉密不上网、上网不涉密，微信、QQ 等社交软件、内部办公平台（如 OA）等不得传输涉密文件。涉密信息需通过符合安全管理要求方式进行传递。

规范办公软件使用：不得使用图文识别软件处理涉密文件；严禁使用任何开源 AI 工具存储、处理涉密信息，不得将涉密文件、数据提交至此类工具进行分析或生成内容。