集团保密工作专题培训内容整理

(2017 年 8 月 21 日)

能投集团保密工作专题培训于 8 月 18 日在集团综合集控楼举办。旨在加强集团的保密管理工作，提高全体员工的保密意识和工作能力。本次专题培训主要涉及内容有：目前严峻的保密形势，保密相关法律法规，以及违反保密规定需承担的责任点等。因培训过程不允许录音，不发放课件材料，现将日常工作中的保密要求整理如下：

一、收文

（一）收文

接收涉密文件和其他涉密载体时应检查送达的密件是否发给本单位的，不是发给本单位的，不能接收，并当即退给投递人员。

检查信封等密封是否完好无损，确认未被拆开，才能接收。若发现问题，应立即将情况报告单位领导和发文单位。检查签收单上的登记与涉密实物是否相符，若果不符，不能接收，同时要及时报告发文单位。

各项情况检查核对无误后，还要认真清点文件数量、检查顺序号，再履行签收等手续。

（二）登记

涉密文件应在专用登记本上予以登记，详细登记收文日期，收文编号，文件编号，发文字号，文件标题，密级，文件份数等信息。

涉密文件的标题、发文字号与文件正文一样，都属于国

家秘密，在文件解密前不得在单位内部文件、简报资料、内部刊物、内部网站上引用。

应将党委、政府文件和密码电报实行分类登记，以便管理。

不能在非涉密计算机上进行收文登记。

（三）阅办

涉密文件必须使用专用文件夹传送，文件夹要有明显的标识区分开一般文件夹，并在文件夹内附上涉密文件阅文注意事项。

及时将文件送达或者电话通知需要知悉的相关部门来领取文件，并要严格履行登记、签收手续。

送阅涉密文件应当面送交，立等收回，严禁随意放置其办公桌上或者交换箱内。传阅领导或者工作人员确实因工作需要保留的，也应在阅读（使用）完毕后及时交还或者通知机要管理人员收回，不可直接转入下一环节。涉密文件传递应采用“轮辐式”传递方式，严禁文件横传。

（四）复制和汇编

机密级、秘密级涉密载体复制，应当经过机关、单位负责任批准，不得改变密级、保密期限和知悉范围;

必须履行登记手续，复制件应当加盖复制机关、单位的复印戳记，并视同于原件管理，使用完毕后需退回原机关、单位;

未经原定密机关、单位或者上级机关批准，不得复制和摘抄绝密级涉密载体。

汇编、摘抄国家秘密文件、资料，应当经原制发机关、单位批准；经批准汇编的涉密文件、资料的密级、保密期限和知悉范围，应与原件一 致;

汇编本应当按所汇编涉密文件、资料的最高密级和最长保密期限作出密级标志和进行保密管理;

摘录、引用国家秘密内容的笔记本和其他形式的涉密载体，要做出原件一致的保密管理。

（五）清退销毁与归档

清退：按照省保密局要求，下一年度必须将上一年度印发的中央和省委涉密文件清退回保密局，并严格履行清退手续。所需清退的文件主要包括文件字号为：中发、中办发、中办通报、云发、云办发、云厅字、 滇情通报等涉密文件。政府部门和省委其他部门的涉密文件一般不要求清退。

销毁：需要销毁的文件一律交由机要保密部门，任何人不得擅自处理。对本部门旧报纸的出售，部门负责人要亲自把关，除有公开刊号的出版物（含报纸、杂志）外，所有红头文件、内部刊物、资料、简报、信息等一切纸质文件均不准出售。

立卷归档：应对涉密文件的密级和保密期限进行重新鉴定，卷内有多份涉密文件时，应对档案卷宗按最高密级和最长保密期限作出密级标志。

文件保存：保存涉密文件的场所应符合相关硬件要求，必须安装“三铁一器”，即防盗门、防盗网、保险柜和报警器。

二、发文

文件的起草全过程必须在涉密计算机上进行。严禁将涉密计算机和非涉密移动存储介质连接。如需将数据资料传输给涉密计算机，只能用刻录光盘的形式传输。

（一）送签

文件的会签及签发：发文稿纸和文件初稿必须由连接涉密计算机的涉密打印机打印。

涉密文件在分发前的会稿、核稿、审阅、签发、编号、校对等各个环节必须由拟稿人员或者涉密文件管理人员专人传递。随时掌握文件的去向。

（二）分发传递

分发的涉密文件，必须要求收文人签字。每个单位和部门需指定专人收文。

传递涉密文件，必须通过机要交通或者机要通信部门，不得通过普通邮政、快递等无保密措施的渠道传递；指派专人传递时，要选择安全的交通工具和交通路线，并采取安全保密措施；向驻外机构传递时，应通
过外交信使传递。

个人档案必须通过机要交通进行传递。

通过机要信件邮寄或者通过机要局密传邮寄时应当包装密封，并在信封上标明密级、编号和收文单位全称等;

遇到急件，需要发密码电报时，应按照机关单位所在地党委机要局的格式要求提前拟好文件，并送至当地党委机要局发送。

（三）汇编归档

与收文的汇编归档要求相同，都要按所汇编和归档文件的最高密级进行标示，并按保密规定进行管理。

三、计算机及其网络管理

各单位必须配齐涉密计算机、打印机、复印机、扫描仪和涉密移动存储介质。涉密设备严禁连接互联网，并对设备作出涉密标示，对涉密计算机设置密码口令，以防其他人员误操作。

在选购涉密产品时原则上选购国产设备。如需选购进口设备，要选购经国家有关主管部门检测认可和批准的产品。不要选购带无线网卡和具有无线功能的产品。如果已经购买并准备用于处理涉密信息的，使用前必须拆除具有无线功能的硬件模块。

严禁使用的包括无线键盘、无线鼠标、无线网卡等。

严禁在连接互联网的计算机上处理涉密信息。

严禁用 qq、微信和邮箱等传递涉密信息，其中也包括公司的工作秘密。

严禁移动存储介质在涉密计算机和非涉密计算机上交叉使用。

处理涉密信息的办公自动化设备出现故障时，必须送到保密工作部门指定的单位维修，严禁送到社会上的维修点维修。若在保修期内，在送往销售单位保修时，必须将存储涉密信息的硒鼓、硬盘等电磁介质拆卸下来，并派专人到现场监督修理，确保涉密信息安全。

需要淘汰、报废的办公自动化设备，要进行清点、登记 。经单位主管领导批准，送交保密工作部门指定的涉密载体销毁单位销毁，禁止将其转送、捐赠他人，更不能当做废品出售或随意扔弃。

各单位要对本单位的网络设备，特别是互联网边缘设备和网络安全设备要进行检查，提高安全策略，优化配置，加强网络异常监控。对计算机终端网络接入情况、软件安装情况和数据存储情况要进行检查和清理。进一步完善网络安全保障系统，重点考虑增加漏洞扫描、系统检测、入侵防御等安全设备的投入使用。确保公司工作秘密的安全。

四、信息公开

在单位门户网站登载信息应严格遵守信息公开保密审查制度，对拟在门户网站上登载的信息要进行严格的保密审查，确保涉密信息不上网、上网信息不涉密。

严禁泄露拟制中不宜公开的法规、规章草案和政策文稿。

严禁泄露不宜公开的会议材料、领导讲话材料。

严禁泄露不宜公开的规划、计划和总结，以及财务预算、决算；拟议中的机构设置、工作分工、人事调整和职务任免、奖惩事项。

严禁泄露不宜公开的领导办公电话等涉及工作秘密事项。

五、注意在涉外活动中的保密管理工作，无论是在国内还是国外。各类相关保密知识详细信息、及法律规定请查阅省保密局官方网站。http://www.ynbm.yn.gov.cn/