太极集团有限公司文件

TAIJI GROUP LIMITED COMPANY

太极集团〔2012〕685 号　　签发人：杨靖

关于印发《太极集团有限公司涉密载体管理（试行）办法》的通知

各厂、司：

为了加强公司商业机密的保密工作，提高涉密信息保护，杜绝和减少涉密载体使用中泄漏涉密信息为公司造成损失，特制定《太极集团有限公司涉密载体管理（试行）办法》，现印发给你们，请认真遵照执行。

特此通知！

附件：太极集团有限公司涉密载体管理（试行）办法

二〇一二年五月十七日

主题词：信息　管理　通知

太极集团有限公司办公室　　2012 年 5 月 28 日印发

拟稿：燕勇　　校核：燕勇

附件

太极集团有限公司涉密载体管理（试行）办法

第一章　　总　则

第一条 为了提高涉密信息保护，杜绝和减少涉密载体使用中泄漏涉密信息为公司造成损失，特制定本办法。

第二条 涉密载体是指存储处理涉密信息的计算机、移动硬盘、光盘、优盘、录音带、录像带、存储卡等存储介质。

第三条 涉密信息分类及定义

涉密信息分绝密和机密二类:

一、绝密级即内容泄露后将对公司利益造成重大危害的最终文档，未明确标注期限的，按二十年期限实行保密，到期自动解密。主要有以下几类:

1.公司总体发展规划及规划中对各项工作的指导计划;

2.涉及公司年度中长期发展规划实施具体指示性的最终文档;

3.涉及公司运作流程、产品销售政策、广告促销方案、科研成果及专利申请、成果转让、产品成本、产品配方、资金运作、票据防伪、原料仓储、市场情报、经营数据等内容的最终文档;

4.其他经领导审核认定为绝密级的。

二、机密级即内容泄露后将对公司利益造成较大危害的最终文档，未明确标注期限的，按十年期限实行保密，到期自动解密。主要有以下几类:

1.企业各项管理活动的经济责任制考核办法、规章制度;

2.涉及公司技术改造、项目论证、事故分析、产品试制等内容的最终文档;

3.涉及未公开披露的会计、生产、经营等数据的;

4.其他经领导审核认定为机密级的。

第二章　涉密载体管理范围和职责

第四条 涉密载体管理的目的是杜绝载体在使用过程中的主动或被动泄密。

第五条 涉密载体管理的对象为本单位的涉密载体及涉密载体的持有人(含在职、借调、聘用等)。

第六条 涉密载体由各单位指定专门部门统一购置、统一标识、严格管理。

第七条 涉密载体管理要坚持“预防为主、积极防范”和“谁使用、谁负责”的原则。

第八条 涉密载体管理部门主要职责

一、严格执行集团公司涉密载体管理相关制度和规定，结合本单位情况，制定实施细则。

二、负责本单位涉密载体的采购、验收、入库、调配、维修、档案和业务台账等的管理工作。

三、负责本单位涉密载体使用人员上岗前的保密培训，定期进行保密教育和涉密载体使用检查。

第三章　涉密载体申请、配置、验收、入库、领用管理

第九条 涉密载体申请、配置、验收、入库、领用、报损、档案管理参照《太极集团信息设备管理制度（试行）》（太极集团[2008]575号）通知执行。

一、涉密载体申请增加密级审核。

二、涉密载体验收增加由涉密载体管理部门按密级分类进行编码和贴标。

三、涉密载体入库、领用和报损必须附明细包括: 编号、密级、使用部门、使用人、使用地点、型号、启用日期、硬盘号、序列号。

四、涉密载体需按密级进行设置后领用，需签订《涉密载体操作员责任书》见附件1。

第四章　涉密载体使用、借用、外出、调配管理

第十条 涉密计算机（包括笔记本电脑）管理

一、 用户密码安全保密管理

1.用户密码管理的范围是指所有涉密载体所使用的密码。

2.用户密码使用规定

（1）密码必须由数字、字符和特殊字符组成;

（2）机密级计算机设置的密码长度不能少于8个字符，密码更换周期不得多于30天;

（3）绝密级计算机设置的密码长度不得少于10个字符，密码更换周期不得超过15天;

（4）涉密计算机需要分别设置BIOS、操作系统开机登录和屏幕保护三个密码。

3.密码的保存和管理

（1）机密级计算机设置的用户密码由使用人自行保存，严禁将自用密码转告他人；因工作需要必须转告，应报部门及以上领导书面批准。

（2）绝密级计算机设置的用户密码须登记造册，由部门负责人管理。

（3）任何人不得以任何手段窃取他人的密码，也不得以他人的帐号、IP地址等试图登录。

二、涉密计算机必须安装防木马病毒程序，定期进行杀毒和升级，每次接入移动介质时必须进行杀毒检查。绝对禁止涉密计算机在线升级防病毒软件病毒库，同时对离线升级包的来源进行登记。

三、涉密计算机原则上不能上互联网，因特殊需求需上网的，必须事先提出申请报分管领导批准后，经涉密载体管理部门负责人同意方可实施，并安装物理隔离卡，在相关工作完成后撤掉网络。

四、涉密计算机应限制信息入口，如光盘、优盘、移动硬盘等

的使用。

五、防止涉密笔记本电脑失控或丢失后被破译，必须采取开机状态身份鉴别；对于经常携带外出的涉密笔记本电脑要采取保密措施。

六、严禁使用或配备红外、蓝牙等无线通信模块或无线鼠标、无线键盘，通过 USB、1394 等接口使用手机连接涉密计算机的。

第十一条 涉密载体接入局域网络的计算机和机内文件严禁设定为网络共享，在局域网中应进行保密处理。

第十二条 各操作员需在本人的涉密载体中创建绝密级文件、机密级文件二个目录，将文件分别存储在相应的目录中。电子文件要有密级标识，电子文件的密级标识不能与文件的正文分离，一般标注于正文前面。涉密文档在保存中必须根据密级运用简单易操作的文件和文件夹加密产品等进行加密保存。

第十三条 涉密载体只能在涉密计算机内使用，须按密级标识使用。高密级信息不得存储到低密级载体内，低密级信息可以存储到高密级载体中。密级变动要申请，填写《涉密载体变更申请表》见附件 2，由涉密载体管理部门审核变更。

第十四条 严禁通过电子邮件、QQ 等即时通讯软件、网络硬盘、云平台等网络载体传输涉密信息。

第十五条 涉密载体借用管理

涉密载体不得擅自借用，由于工作需要借用要经公司领导批准，涉密载体管理部门登记、备案，并对涉密信息进行处理。

一、绝密级涉密载体必须由需求部门负责人申请，总经理批准；

二、机密级涉密载体必须经需求部门负责人和秘密事项生成部门负责人和分管领导同时批准。

第十六条 所有涉密载体均不得擅自带离公司或向外界提供；特殊需要时，均必须经分管领导或总经理批准，对于携带外出的涉

密载体要采取保密措施。

第十七条 离岗或内部调动时，应通知涉密载体管理部门参与清点并收回或移交管理；更换涉密载体必须进行信息清除；存档和使用过的涉密载体，在没有交清前，不得办理离岗或调动手续。

第五章 涉密载体的维修和报损

第十八条 需指定专人负责各涉密载体维修维护工作，严禁操作员私自安装计算机软件。

第十九条 对发生故障的涉密载体，维修应保证信息不被泄露，对涉密信息应采取转存、删除、异地转移存储媒体等安全保密措施，由使用人员全程跟踪维修。

第二十条 凡需外送修理的涉密载体，必须经涉密载体管理部门分管领导批准，并将涉密信息进行不可恢复性删除处理后方可实施。如确需进行数据恢复的，必须到由国家保密工作部门指定的具有保密资质的单位进行。

第二十一条 涉密载体的报损，应经本单位领导审核批准，并履行清点、登记手续后由涉密载体管理部门统一组织，到指定的销毁点销毁，严禁自行销毁或作为废品处理，现场处置人员必须是二人以上，做好处置记录，填写《涉密载体报损处置表》（详见附件3）。

第六章 涉密载体账务管理

第二十二条 涉密载体管理部门需对各类涉密载体建立业务台账和报损台账。

一、业务台账：主要是记录涉密载体自采购至报损的全过程，包括涉密载体的基本情况、设备编码、入库、移库（含领用、交接）、出库（含报损、处置）、变更（含维修费用、升级）、设备状态、对应的财务编码等情况，该账薄为涉密载体管理的主要台账，由涉密载体管理员凭相关单据作为登记依据。

二、报损台账：主要是记录涉密载体报损全过程，包括报损审批、实物处置、残值回收、账务处理等信息，该账簿由涉密载体管理员建账和管理。

第二十三条 各种账簿和凭单应妥善保管，不得随意涂改。

第七章 涉密载体管理处罚

第二十四条 涉密载体管理部门将不定期检查涉密载体是否采取加密措施等使用情况；每年组织对涉密载体保密管理工作情况进行检查。

第二十五条 各涉密载体使用和管理人员必须自觉遵守本办法，提高保密安全防范意识，防止泄密事件的发生。凡发生泄密事件的，对于过失泄密将按照国家和公司有关法规追究当事人责任；对故意泄露公司秘密的，根据情节轻重及损害公司利益的程度将加重惩罚。

第二十六条 任何单位和个人发现涉密载体泄密后，都应第一时间采取补救措施并按有关规定向有关部门和上级报告，由相关保密管理部门进入处置程序；出现秘密泄密、公司负面信息影响重大的第一时间按集团公司重大事件报告制度的通知要求执行。

第八章 附 则

第二十七条 本办法由信息处负责解释、补充、执行。

附件：1、涉密载体操作员责任书

2、涉密载体变更申请表

3、涉密载体报损处置表

附件 1

涉密载体操作员责任书

涉密载体操作员须熟悉涉密载体的基本操作和公司信息保密管理的有关规定，明确自身的工作职责，严格执行相关管理规定，同时按以下规定执行:

1、非涉密计算机和非涉密移动存储介质不得存储涉密信息。

2、禁止涉密载体光盘、移动硬盘、优盘等在上互联网的计算机上使用。

3、禁止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设备。

4、禁止在没有防护措施的情况下将公共信息网络上的数据拷贝到涉密计算机系统。

5、禁止使用具有无线互联功能的设备处理涉密信息。

6、电子密件及其存放目录应采用技术手段加密。离开办公位时，在办公用机上打开的电子密件应予关闭，暂时离开要锁定计算机。

7、涉密载体的保存要符合保密要求。绝密级的要指定专人统一保管；机密级的，由使用人员保管，涉密文档必须进行加密管理。

8、保证通过上岗培训才能对相关载体进行操作。

凡违反以上规定，罚款 50—200 元。

操作员签字:　　部门第一负责人签字:　　涉密载体管理负责人签字:

签字日期　　签字日期　　签字日期

附件 2

涉密载体变更申请表

时间

申请部门		联系方式	
原操作员		现操作员	
变更申请原因			
部门负责人意见			
部门分管领导意见			
涉密载体管理部门负责人意见			
涉密载体管理部门分管领导意见			
经办人		回复方式及时间	

太极集团信息处制

附件 3

涉密载体报损处置表

时间

序号	载体名称	载体编号	序列号	购进时间	资产所属	现使用部门	操作员	品牌及规格型号	报损原因

处置小结:

分管领导　　部门负责人　　经办人

太极集团信息处制