武汉市国土资源和规划局江岸分局

网络安全保密

资料汇编

二〇一六年

目　　录

岸土资规字[2016]27号

关于调整局保密工作领导小组的通知

局直各科室：

为贯彻落实上级有关计算机、信息安全保密工作文件精神，切实搞好安全保密工作，结合我局实际情况，经局党组研究决定，重新调整局安全保密工作领导小组。人员组成如下：

组长：叶忠元

副组长：邓宝航、皮文胜、林萱、刘尚勇

成员：张涛、刘佩玲、张文倩、张兵、潘虹
向宝成、童燕平

领导小组下设办公室，由张涛同志兼任办公室主任，专门负责安全保密日常工作。

武汉市国土资源和规划局江岸分局
二0一六年十月二十六日

主题词：机构调整　　保密工作领导小组　　通知

发：局党组成员局直各科室

武汉市国土资源和规划局江岸分局办公室2016年10月26日印发

关于加强涉密网络和移动存储介质管理的八项规定

一、严禁在外网上处理、存储、传输涉及国家秘密信息和内产敏感信息。“上网不涉密，涉密不上网”。禁止涉密网络用户采用各种途径拨号连接互联网或其他公共信息网。禁止涉密网络数据库连接互联网或其他公共网络。所有涉密计算机都要设置开机密码。

二、严禁涉密移动存储介质在内外网上交叉使用。涉密网络与国际互联网或其他公共网络等外网必须实行“物理隔离”。外网U盘和移动硬盘不能在内网上使用，内网U盘要统一安装移动存储介质管理系统，内网使用的U盘要统一编号、统一配发，逐一造册登记。凡工作人员调动、离职、退休前，必须将所保管、使用的涉密移动存储介质退给原工作单位，按有关规定处理。

三、严格涉及国家秘密的计算机信息系统建设的审批。涉密信息系统的建设单位应根据国保发[2005]5号文件要求，选择具有资质的企事业单位承担系统的开发、设计和建设。新建的涉密信息系统网络安全保密方案在建设前，须经保密行政管理部门评估、审批通过后方可实施。涉密信息系统建设完成后，必须经保密行政管理部门检测、审批后，方可投入使用。未经审批前，不得存储、处理和传输国家秘密信息。

四、严格执行上网信息保密审查审批制度。已建立对外公开政务网络和在互联网上发布信息的机关、单位，要严格按照“谁公开、准负责”的原则，对登载到互联网上的信息要严格保密审查。

五、严禁在社会上的打印店打印文件、资料。所有党政机关和有涉密资料的单位，一律不得到社会上的打印店和其他外单位、外人的计算机上打印文件、资料。发现此类问题，严格按照有关法律、法规查处。

六、严禁将涉密文件、资料，涉密计算机、移动存储介质等，作为废品卖给任何单位、个人和废品收购站等。发现此类问题，严格按照有关法律、法规查处。

七、严格执行涉密计算机定点维修制度。所有党政机关的涉密计算机一律到有保密资质的培训的计算机定点单位进行维修，不得到其他任何单位维修，违规者要按照有关法律法规查处。

八、严格执行中央关于涉密载体（包括涉密计算机、笔记本电脑、移动硬盘、U盘等）实行统一销毁的规定。全局各股、所、队、中心、国土资源所、驻政务大厅国土窗口要严格执行涉密载体销毁管理制度，销毁泄密载体要经本机关单位主管领导审核批准，履行清点登记手续，统一送当地保密行政管理部门的涉密载体销毁中心进行销毁。

网络安全保密管理制度

一、为保证我局内部计算机国土资源系统网络信息安全，防止计算机网络失密泄密事件发生，特制定本制度。

二、为防止病毒造成严重后果，对外来移动存储介质、软件要严格管理，原则上不允许外来移动存储介质、软件在内网计算机上使用。确因工作需要使用的，事先必须进行防（杀）毒处理，证实无病毒感染后，方可使用。

三、接入国土资源系统网络的计算机严禁将计算机设定为网络共享，严禁将机内文件设定为网络共享文件。

四、为防止黑客攻击和网络病毒的侵袭，接入网络的计算机一律统一安装360天擎网络版杀毒软件，并要定时对杀毒软件进行升级。

五、如考核酝酿及其他重大事项保密期间，将有关涉密材料保存到非上网计算机上，签订保密协议方可使用。

六、禁止将涉密办公计算机擅自联接国际互联网。

七、局中心机房禁止无关人员随意出入，坚持每日查看网络机房设备安全和运行情况，并填写好机房设备运行情况登记表。

计算机上网安全保密管理规定

一、未经批准涉密计算机一律不许上互联网,如有特殊需求，必须事先提出申请报局保密工作领导小组批准后方可实施，并安装物理隔离卡和单独的链接互联网的硬盘，在相关工作完成后撤掉网络。

二、国际互联网必须与涉密计算机系统实行物理隔离。

三、在与互联网相连的信息设备上不得存储、处理和传输任何涉密和工作资料信息。

四、加强对上网人员的保密意识教育，提高上网人员保密观念，增强防范意识，自觉执行保密规定。

计算机维修维护管理规定

一、涉密计算机系统进行维护检修时，须保证所存储的涉密信息不被泄露，对涉密信息应采取涉密信息转存、删除、异地转移存储媒体等安全保密措施。无法采取上述措施时，涉密股室负责人必须在维修现场，对维修人员、维修对象、维修内容、维修前后状况进行监督并做详细记录。

二、设备的故障现象、故障原因、扩充情况记录在设备的维修档案记录本上。

三、凡需外送修理的涉密设备，必须经局保密领导小组批准，报请市、区保密部门同意后，并将涉密信息进行不可恢复性删除处理后方可实施。

四、高密级设备调换到低密级单位使用，要进行降密处理，并做好相应的设备转移和降密记录。

五、指定专人负责各涉密股室计算机软件的安装和设备的维护维修工作，严禁使用者私自安装计算机软件和擅自拆卸计算机设备。

六、涉密计算机的报废交局保密领导小组监督专人负责送至市、区保密部门指定的地点销毁。

用户密码安全保密管理规定

一、用户密码管理的范围是指所有涉密计算机所使用的密码。

二、机密级涉密计算机的密码管理由专人负责，秘密级涉密计算机的密码管理由使用人负责。

三、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）秘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）机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7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。

四、密码的保存

（1）秘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；若工作需要必须转告，应请示主管领导认可。

（2）机密级计算机设置的用户密码须登记造册，并将密码本存放于保密柜内，由部门负责人管理。

涉密电子文件保密管理规定

一、涉密电子文件是指在计算机系统中生成、存储、处理的机密、秘密和内部的文件、图纸、程序、数据、声像资料等。

二、电子文件的密级按其所属项目的最高密级界定，其生成者应按密级界定要求标定其密级，并将文件存储在相应的目录下。

三、各用户需在本人的计算机系统中创建“机密级文件”、“秘密级文件”、“内部文件”三个目录，将系统中的电子文件分别存储在相应的目录中。

四、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。

五、电子文件必须定期、完整、真实、准确地存储到不可更改的介质上，并集中保存，然后从计算机上彻底删除。

六、各涉密股室自用信息资料要定期做好备份，备份介质必须标明备份日期、备份内容以及相应密级，严格控制知悉此备份的人数，做好登记后进保密柜保存。

七、对备份电子文件进行规范的登记管理。备份可采用光盘刻录的形式。

八、涉密文件和资料的备份应严加控制。未经许可严禁私自复制、转储和借阅。对存储涉密信息的磁介质应当根据

有关规定确定密级及保密期限，并视同纸制文件，分密级管理，严格借阅、使用、保管及销毁制度。

九、涉密电子文件进出内网要签订保密协议。

十、备份文件和资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施，并进行异地备份。

涉密计算机系统病毒防治管理规定

一、涉密计算机必须安装经过国家安全保密部门许可的查、杀病毒软件。

二、每周升级和查、杀计算机病毒软件的病毒样本。确保病毒样本始终处于最新版本。

三、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。

四、每周对涉密计算机病毒进行一次查杀检查。

五、涉密计算机应限制信息入口，如软盘、光盘、U盘、移动介质等的使用。

六、对必须使用的外来移动存储介质（磁盘、光盘，U盘、移动存储介质等），必须先进行计算机病毒的查、杀处理，登记后才可使用。

七、对于因未经许可而擅自使用外来介质导致严重后果的，要严格按照相关法律追究相关人员的责任。

数字复印机多功能一体机保密管理规定

一、用于专门处理涉密信息的数字复印机、多功能一体机按所接入设备的最高定密等级定密。

二、严禁将用于处理国家秘密信息的具有打印、复印、传真等多功能的一体机与普通电话线连接。

三、严禁维修人员擅自读取和拷贝数字复印机、多功能一体机等涉密设备存储的国家秘密信息。涉密电子设备出现故障送外维修前，必须将涉密存储部件拆除并妥善保管；涉密存储部件出现故障，如不能保证安全保密，必须按照涉密载体销毁要求予以销毁；如需恢复其存储信息，必须由市、区保密工作部门指定的具有数据恢复资质的单位进行。

上网发布信息保密规定

一、上网信息的保密管理坚持“谁发布谁负责”的原则。凡向国际联网的站点提供或发布信息，必须经过保密审查批准，报领导审批。提供信息的单位应当按照一定的工作程序，健全信息保密审批制度。

二、凡以提供网上信息服务为目的而采集的信息，除在其它新闻媒体上已公开发表的，组织者在上网发布前，应当征得提供信息单位的同意。凡对网上信息进行扩充或更新，应当认真执行信息保密审核制度。

三、涉密人员在其它场所上国际互联网时，要提高保密意识，不得在聊天室、电子公告系统、网络新闻上发布、谈论和传播国家秘密信息。

四、使用电子函件进行网上信息交流，应当遵守国家保密规定，不得利用电子函件传递、转发或抄送国家秘密信息。

涉密计算机及移动存储介质保密管理细则

一、涉密计算机及移动存储介质的定义

1、涉密计算机是指存储、处理、传输涉及国家秘密信息的计算机（含笔记本电脑）。

2、涉密移动存储介质是指以文字、数据、符号、图形、图像、声音等方式记载国家秘密信息的存储介质载体，包括计算机硬盘、软盘、优盘、光盘、磁带、存储卡及其它具有存储功能的各类介质。

二、涉密计算机及移动存储介质的管理原则

3、涉密计算机及移动存储介质的管理坚持“谁主管、谁负责；积极防范，突出重点，明确责任，依法管理、确保安全”的原则。

4、涉密计算机及移动存储介质的保密管理要建立制度、明确职责、分级负责、责任到人。

三、涉密计算机及移动存储介质的确定

5、凡拟用于处理国家秘密信息的计算机及移动存储介质，必须经我局保密工作领导小组审核批准确定，并报同级保密工作部门备案。严禁在未确定的涉密计算机及移动存储介质中存储、处理和传递国家秘密信息。

6、涉密移动存储介质要由我局保密工作领导小组统一购置、统一标识、统一备案、授权使用、集中管理；确定后的涉密计算机及移动存储介质，要统一进行密级标识、建档管理并报同级保密工作部门备案。

7、依据《国家秘密及其密级具体范围的规定》，对确定

在涉密计算机及移动存储介质中存储的涉密信息进行规范定密，并按照涉密信息的最高密级，对涉密计算机及移动存储介质进行涉密级别定级。按照绝密、机密、秘密三个级别对涉密计算机及移动存储介质实行分级管理和采取相应的保密技术防范措施。

四、涉密计算机及移动存储介质的使用

9、涉密计算机及移动存储介质严禁随意更换操作人员和使用人。

10、涉密计算机和移动存储介质在使用时要有口令和身份识别认证。口令安全，秘密级不少于8位，更换周期不长于1个月；机密级不少于10位，更换周期不长于1周；绝密级应使用生理特征（指纹、虹膜等）、智能卡等与口令相结合的方式进行保护。

11、涉密计算机待机5分钟以上，应采取保密防范措施，恢复使用时应有身份识别机制。

12、涉密计算机及移动存储介质不使用时，应关机或存入安全可靠的保密防范设备中。

13、严禁将涉密计算机及移动存储介质带入与工作无关的场合。确因工作需要带出办公场所的，秘密级的需经使用部门主要负责人批准，机密级以上的需经单位主管领导批准，报单位保密委员会（领导组）备案并采取严格的保密措施。

14、涉密计算机及移动存储介质严禁安装、存储和运行与工作无关的软件和信息；严禁擅自更改与涉密性质相关的监控软件、系统软件、硬件连接方式和有关设置。

15、涉密计算机及移动存储介质严禁连接国际互联网和非涉密网，不得具有红外、蓝牙及无线联网功能，严禁使用无线网卡、键盘、鼠标及其它能够与互联网连接的外围设备。

16、严禁在涉密计算机上使用非涉密移动存储介质或在非密机上使用涉密移动存储介质；高密级涉密信息严禁在低密级涉密计算机及移动存储介质中存储、传输和处理。

17、涉密移动存储介质拷贝、复制涉密信息要履行严格审批手续。拷贝、复制秘密、机密级信息，须制发机关允许后经我局保密工作领导小组批准；拷贝、复制绝密级信息，须经信息产生单位批准。

18、处理秘密级或机密级信息的计算机，要采用低泄射的信息设备，或安装经国家保密部门批准使用的电磁信号干扰器。处理绝密级信息的涉密计算机，应当采用符合相应密级标准的低泄射设备，或在防电磁泄漏发射的屏蔽机柜及电磁屏蔽室内使用。

19、与涉密计算机联接的输出载体，也要按照同等密级及有关涉密载体的保密管理规定进行管理，严格保密安全防范，防止显示、打印输出结果被非授权查看和获取。

20、涉密计算机配置使用的安全保密防范设备（产品），必须使用国家保密局等相关主管部门认证许可或经保密、安全等主管部门授权的测评机构检测合格的国产设备（产品），在无相应国产设备时，可使用经国家保密、安全等主管部门检测、批准的国外设备。

21、涉密计算机配置的安全保密技术产品不得对外公开招标采购。

五、涉密计算机及移动存储介质的维护维修及报废

22、涉密计算机及移动存储介质和相关设备的维护应当

在现场进行，并指定专人全程监控，确需到外维修的，应到市、区国家保密部门指定的涉密计算机定点维修单位进行维修。

23、涉密计算机及移动存储介质和相关设备存储数据的恢复，须经我局保密工作领导小组批准后，到市、区保密工作部门审批指定的具有相关资质的单位进行。

24、涉密计算机及移动存储介质和相关设备在变更用途时，须到市、区保密部门进行技术处理后方可变更用途，并要进行登记备案注销涉密计算机编号。

25、涉密计算机及移动存储介质和相关设备报废时，要上交市、区保密部门进行技术处理或销毁，确认计算机内不包含任何形式的国家秘密信息并登记备案、注销涉密计算机及移动存储介质编号。

26、涉密计算机及移动存储介质使用人员因调动、调离或退休等原因离开工作岗位，所在部门应当即时变更涉密计算机系统访问授权，收回其使用的与涉密计算机及移动存储介质和相关物品，并将变更的使用人员情况报同级保密工作部门备案。

六、其它

27、集中处理工作秘密的单台计算机，参照秘密级涉密计算机信息系统基本防护要求进行防护和管理。

28、对违反保密法律法规或本细则，故意或过失泄露国家秘密的，依据《中华人民共和国保守国家秘密法》及相关法律法规依法追究有关人员的法律责任。

29、本细则由武汉市国土资源和规划局江岸分局保密工作领导小组负责解释。

30、本细则自下发之日起施行。

非涉密计算机保密和非涉密移动存储介质管理制度

根据《中华人民共和国政府信息公开条例》、《中华人民共和国保密法》的相关规定，为了加强和规范非涉密计算机和非涉密移动储存介质保密管理工作，确保国家秘密信息的安全，杜绝内部信息外泄，结合我局工作实际，制定本制度。

一、非涉密计算机操作人员必须遵守国家有关法律，任何人不得利用计算机从事违法活动。

二、非涉密计算机操作人员未经上级领导批准，不得对外提供内部信息、资料以及用户名、口令等内容。

三、非涉密网络设备必须安装防病毒工具，并具有漏洞扫描和入侵防护功能，以进行实时监控，定期检测。

四、连接互联网的非涉密计算机操作人员对计算机系统要经常检查，防止漏洞，禁止通过互联网传递涉密文件和工作相关的资料信息。

五、非涉密的U盘、光盘等移动存储介质要由相关责任人编号建档，严格保管。除需存档和必须保留的副本外，非涉密不连接互联网和业务内网的工作计算机系统内产生的文档一律删除，在处理过程中产生的样品等必须立即销毁。

六、具有互联网访问权限的计算机访问互联网及其它网络时，严禁浏览、下载、传播、发布违法信息；严禁接收来历不明的电子邮件；严禁处理涉密信息资料；严禁处理与工作相关的信息资料。

七、对重要数据要定期备份，定期复制副本以防止因存储工具损坏造成数据丢失。备份工具可采用光盘的方式，并妥善保管。

八、非涉密计算机操作人员调离时应将有关材料、档案、软件移交给其它工作人员，调离后对需要保密的内容要严格保密。接替人员应对系统重新进行调整，重新设置用户名、密码。

九、对于违反本规定，发生泄密事件的，将视情节轻重追究相关法律责任。

十、非涉密移动储存介质是指不用来存储、传递、国家秘密信息的移动储存介质。它包括移动硬盘、软盘、U盘、光盘、磁带及各种存储卡。

十、非涉密移动储存介质禁止以任何形式传输国家秘密和工作秘密的信息。

十一、非涉密移动储存介质信息发布、传输的保密管理工作坚持“谁上网谁负责”和“上网信息不涉密、涉密不上网”的原则，向网站提供或发布信息必须经过局保密工作领导小组审查并严格登记。

十二、非涉密移动储存介质的保密工作实行股室、部门负责制，局保密工作领导小组确定专职管理人员具体负责这项工作。

十三、本制度由武汉市国土资源和规划局江岸分局保密工作领导小组负责解释。

十四、本制度自印发之日起执行。