

涉密数据及载体安全保密管理制度

产品名称	涉密数据及载体安全保密管理制度
公司名称	贯标集团
价格	.00/件
规格参数	
公司地址	南京市仙林大道10号三宝科技园1号楼B座6层
联系电话	4009992068 13382035157

产品详情

涉密数据及载体安全保密管理制度

第一条 为规范地理信息成果的管理，保障涉密数据的安全和完整，根据《中华人民共和国测绘法》（2002年8月29日中华人民共和国主席令第75号）、《中华人民共和国测绘成果管理条例》（2006年5月国务院第136次常务会议通过，2006年9月1日施行）、《基础测绘成果资料提供使用管理暂行办法》（国测法字[2006]13号），制定本制度。

第二条 各部门应遵循管理程序，坚持分工负责的制度，保证涉密数据及载体管理各环节落实到相应部门和责任人。

第三条 建立健全保密管理领导责任制，成立安全保密领导小组，加强对保密工作的组织领导，切实履行保密职责和义务；依据接触、使用、保管涉密地理信息成果数据（以下简称涉密数据）的人员情况，区分核心、重要和一般涉密人员，实行分类管理，进行岗前涉密资格审查，取得上岗资格，签署保密责任书，加强日常管理和监督。

第四条 各部门应当严格执行涉密数据日常管理与维护制度，并由部门主管人员指定专人负责实施，落实责任制并纳入科室年度考核。

第五条 各部门涉密数据管理人员，负责对所管理数据的整理、归档、维护，严禁参与与所管理数据使用相关的业务活动，严禁擅自在许可权限范围外对数据进行操作，一切违规行为将按照国家有关规定严肃处理；使用用于承载及处理涉密数据成果计算机的人员，须严格遵守《计算机信息系统保密管理暂行规定》（国保发[1998]1号）、《计算机信息系统国际联网保密管理规定》（2000年1月国家保密局发布）等计算机信息系统保密管理的有关规定，杜绝外传、丢失、泄密事件的发生。

第六条 涉密仪器、设备须有相应密级标识；处理、传输、存储涉密成果数据的计算机软件和硬件系统必须采取安全保密防护措施，设置登录密码和屏幕保护密码，系统管理员密码长度不得少于十个字符，普通用户密码长度不得少于8个字符；系统管理员密码最长使用时间不能超过两周，普通用户的密码最长使用时间不能超过四周。当密码使用期满时，应更换新的密码。

第七条 安装加密防、杀毒软件，涉密计算机及信息系统应采取物理隔离措施，不得与互联网、外部网络相联，不得使用无线网卡等无线联网装置；与涉密计算机相连的打印机、传真机等设备按涉密计算机同等密级进行管理。

第八条 设置中间机完成内部办公网络、国际互联网及涉密数据的迁移，对中间机的使用实行专管制度；登录中间机的双重密码须两人负责，负责人不得相互或对外泄密码信息，并定期修改各自密码；对中间机的操作，应有专人按照有关规定的相关流程负责进行杀毒处理、内容查验、数据迁移并实行备案登记制度，严格记录迁移资料的内容、数据量、迁移原因、迁移时间及申请迁移人并签字，人员离机，应及时锁屏。

第九条 保密要害部门和保密要害场所出入口应设立门禁、电子监控和警报系统，合理设置访问授权权限，对人员进出情况进行严格登记和记录。

第十条 各部门应定期对服务器中的数据进行备份、清理，以避免因各种原因一次性丢失大量数据。存放备份数据的介质，必须具有明确的密级标识。存放临时性数据的介质必须为保密专用设备，涉密介质必须经过主管领导审批才能带离机房或办公地点。

第十一条 服务器内任何数据、设备、介质，在调拨、转让、废弃或销毁时必须上报主管领导审批后方可执行，以保证数据安全。

第十二条 各部门管理人员应尽可能的改善网络系统的安全策略设置，尽量减少安全漏洞，关闭不使用的服务项，对不同级别的网络用户设置相应的资源访问权限。局域网的安全配置应达到《计算机信息系统安全保护登记划分准则》（GB 17859—1999）中规定的第二级系统审计保护。

第十三条 局域网中的信息网络系统自运行开始，必须做好备份与恢复等应急措施，一旦系统出现问题能够及时恢复正常，各部门管理员负责数据的备份与恢复的技术规划、实施和操作，并做好详细的记录。

第十四条

各部门管理人员要定期对操作系统和数据库管理系统进行系统运行记录和数据库运行记录，以备检查。

第十五条 对移动存储介质进行统一管理，设立各密级专用载体介质，非涉密介质禁止进入涉密计算机及相关设备；被分配使用涉密计算机的工作人员应保管好计算机使用权限，无权限工作人员及外来人员不得使用涉密计算机。

第十六条 涉密计算机及外设要移出涉密计算机信息系统，使用部门须向安全保密领导小组领导提出申请，批准后使用部门对其涉密介质进行脱密处理并更换后方可移出。脱密处理应使用国家保密局许可使

用的信息清除工具。

第十七条 涉密计算机及外设在使用过程中发生变动，使用部门须向安全保密领导小组提出申请，批准后同样须实施安全保密控制措施方可使用。

第十八条 涉密移动存储介质要按照“统一购置、统一标识，严格登记、集中管理”原则，严格控制发放和使用范围。

第十九条 安全保密领导小组负责涉密移动存储介质的统一购置、统一标识，介质管理人员负责建立台账。使用部门及个人在本单位内部使用移动存储介质，需向介质管理员提出申请，填写《涉密移动存储介质领用登记表》；领取用于日常分发服务的涉密移动存储介质，填写《领取介质登记表》。使用部门须指定专人负责涉密移动存储介质的领取、使用和管理。

第二十条 除日常提供和应急保障工作外，各部门内部和部门之间通过内部网络进行数据交换，禁止使用移动存储介质进行数据交换。

第二十一条 涉密移动存储介质须有明确的密级标识，并按照相应密级进行数据存储。涉密移动存储介质不得私自改变密级使用；不得私自拆卸涉密计算机内置的存储介质作为移动存储介质使用。

第二十二条 涉密移动存储介质应在使用部门所属涉密计算机上使用，禁止在非涉密计算机上使用，不得私自在其他部门或外单位使用。

第二十三条 安全保密领导小组负责对涉密移动介质进行监控软件注册、登记管理。未进行监控软件注册登记的涉密移动硬盘、U盘不能接入涉密计算机；确因工作需要，其他涉密测绘单位的移动介质接入单位涉密计算机时，按照单位同类设备进行安全保密管理。

第二十四条 单位内部使用的涉密移动存储介质确因工作需要带出办公场所的，须经主管领导批准，同时对带出介质的密级、编号、复制内容履行严格的登记制度。

第二十五条 工作人员严禁将尚未履行统一登记和使用手续的移动存储介质存储涉密信息。

第二十六条 涉密移动存储介质的保存管理应采取与相应密级的文件、地图等资料相同的安全措施，严防被盗及丢失。

第二十七条 单位配发给各部门的计算机及外设日常由使用人员保管，人员离职前必须将所保管使用的设备、涉密移动存储介质全部移交部门。

第二十八条 计算机、外设及存储介质的维修、报废、销毁应由使用部门提出申请，固定资产管理部门、安全保密领导小组及使用部门联合履行清点和登记造册手续，报河北省地理信息局备案后到河北省

保密局指定部门进行维修、销毁，任何部门或个人不得擅自销毁。

第二十九条 违反本规定情节较轻者，由安全保密领导小组给予批评教育；情节较重造成失泄密隐患的，按有关规定处理。