材料科学数据共享工程技术标准

材料数据安全管理规范

（试行稿）

（本稿完成日期：2010 年 07 月）

2010-07 发布

材料科学数据共享标准规范课题组

目 录

材料数据安全管理规范

1 范围

本标准规定了材料科学数据共享网在建设、运行、维护等数据在安全管理方面的要求。

本标准适用于材料科学数据共享中心(网)以及参加材料科学数据中心（网）的各个单位子系统或资源节点的数据安全的管理。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注明日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，凡是不注日期的引用文件，其最新版本适用于本标准。

国家科学数据共享工程技术标准《国家科学数据中心建设技术规范》

国家保密局发布《计算机信息系统国际联网保密管理规定》

《中华人民共和国计算机信息系统安全保护条例》

GB/T13745-1992　　学科分类代码

GB/T7156-1987　　文献保密等级代码

BMZZ1-2000　　涉及国家秘密的计算机信息系统保密技术要求

GB50174-93　　电子计算机机房设计规范

SDS/T　2313— 2004　　科学数据中心（网）运行管理

3 术语

科学数据资源 Scientific data resources

特指以公益性和基础性为研究应用价值的数据资源，包括观测、监测、调查、试验、实验以及研究等科学技术研究活动过程中产生的原始性数据，以及按照不同科技活动需求进行系统加工整理的各类数据。

主体数据库 Core database

依据国际标准、国家标准或行业标准分类体系构建的二级学科及其分支学科的科学数据集，并基于计算机系统运行的数据库。

元数据 Metadata

关于数据的数据。

科学数据共享服务 Scientific data shared services

为提供科学数据共享所提供的技术服务，包括：目录服务、导航服务、数据信息发布、数据检索、数据产品加工、数据以数据产品分发等。

数据服务基础平台 Infrastructure for data services

用于实现科学数据共享服务功能的信息基础设施，主要包括 Internet 服务、数据库服务等。

B/S

浏览器/服务器（Browser/Server）结构。

数据管理 data management

利用数据库、数据仓库、元数据和网络等技术，建立分布式、集中式或集中加分布式数据管理系统，开展数据接收、组织存储、运行维护、更新、共享交换等工作，实现对数据资源的有效组织和应用。

数据安全 data security

适用于数据的计算机软硬件存储、备份和授权保护策略，以防止不合法的使用或访问所造成的数据更改、破坏、损毁或泄密。

突发事件　emergency

突然发生的、未曾预防的、需要立即处理的紧急事件、灾害事故等

4 材料科学数据共享网

材料科学数据共享网是将多个数据库聚合到一个较大的节点，再将各个子节点相互连接成材料共享网络，向外提供服务。

4.1 系统的层次

材料科学数据共享网的逻辑结构可以分为三层。

物理层

共享中心和各分节点的运行环境，保证节点可以在网络环境下运行，配置高性能大容量的服务器支撑数据资源的存储和访问。

数据资源层

数据资源是共享网的核心部分，是共享网所要共享的内容。它包括共享中心的主体数据库和各分节点的数据库。

应用服务层

提供用户和共享网进行交互功能，根据用户请求，共享网处理数据资源层的数据资源并将处理结果提供给用户。

4.2 数据的共享服务

数据的保密分级

根据《GB/T7156-1987 文献保密等级代码》，将数据划分为 6 个保密级别，分别为公开数据、国家内部数据、部门内部数据、秘密数据、机密数据、绝密数据。

（1）公开数据：指数据可以向国外提供，可以进行国际交换。也就是可以提供国际范围共享的数

据，该类数据主要包括那些国家间、地区间及国际机构相互交流、使用的数据。

（2）国家内部数据：指数据可以在国内提供和交换。

（3）部门内部数据：指数据可以在系统或系统某部门进行内部发行和交换。

（4）保密数据：指数据内容涉及国家一般秘密的数据。

（5）机密数据：指数据内容涉及国家重要秘密的数据。

（6）绝密数据：指数据内容涉及国家核心机密的数据。

数据共享和保密

材料共享网的目的是保证不同保密级别的数据在不同的范围内得到安全的数据共享服务。例如部门内部数据是在部门内部共享的，在部门以外应该是绝对保密的不可见的。材料科学数据共享网主要的还是公开数据，国家内部数据以及部门内部数据的数据共享服务。从数据的角度，分为两种数据，一种是数据本身，一种是描述数据的数据。在材料共享网内，描述数据的数据应该都属于公开数据，而数据则有密级之分。

5 数据的安全管理

现代信息系统的安全管理既是一个复杂的技术问题，也是一项要求严格的管理规范。信息系统是一种内容繁多、结构复杂、环境多变的人机系统，要想有效地保护信息系统的安全，必须从信息安全技术、组织机构与人事管理、信息安全法制建设等方面采取综合治理措施。

5.1 技术管理

1．硬件环境安全管理

机房环境管理：为保证机房内所有设备的安全、稳定、无故障运行，监控机房的环境、监测并定期检查电源、通风、接地等所有机房设施的工作状态，发现

并报告问题和提出变更建议，应考虑机房内通风、温度、湿度、灰尘、灯光等的配置；考虑设备放置与冷却效率和制冷单元热点的关系；以及可能因功能扩大引起的冷却效率问题，设备之间的干扰等问题。

电源管理：将电源有效分配到系统中不同的设备组件，保持各设备的电源供给稳定。应考虑电源设备参数对设备的影响，如过压、过流、浪涌、短路、杂波干扰等。

服务器设备管理：计算机信息系统设备的日常运行和管理、可靠性评价，须定期监测设备的使用情况，不定期进行效能优化处理。考虑不同的设备的散热、电磁干扰、电压电流等因素的相互影响。系统中的关键部分满足冗余配置。

网络设备管理：网络设备是数据传输的通道，交换机、路由器等网络设备需要具备一定的网络安全管理功能，如 IP 控制、ARP 防护等，重要节点和重要数据的网络设备应带有防火墙功能。

布线系统管理和维护：监控、诊断、分析设备间、弱电井等区域配线设备、线缆、信息插座等设施，及网络通信线路的工作状态和可能的故障状态，发现并报告问题，提出维护建议，保证系统运行的高可靠性和维护的高效率。

监控系统管理和维护：监控、诊断、分析门禁系统、各类监控设备等的运行状态、参数变化、提示信息等，发现并报告问题，及时变更、维护，保证监控系统的可靠性。机房电源环境要做到防火、防水、防雷、安全用电和烟雾探测报警。

应急管理：主要应对突发事件。电源方面，应配备大型 UPS 电源，保证应急期间服务器等设备的的不间断供电。服务器设备方面，应具有备份系统，备份服务器的数据应尽量与主服务器上的尽量保持一致。在应急时自动启动。环境方面，配备应急照明设备，配备安装机房监控系统作为保障。对配电系统、环境系统、消防系统、保安系统、网络系统进行监测、监视、报警。

日常检修管理：对于机房环境和各种设备应有专人负责定期检修，及时排除隐患。

原则上硬件安全配置上应满足《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》第三级物理安全的技术要求。

2．软件安全管理

操作系统

操作系统属于底层支撑系统，是共享网运行的软件环境的基础，要求由专门的管理人员来维护，安装稳定高的的操作系统，进行必要的操作系统的安全配置，定期对系统进行升级、修补系统漏洞，监测和优化操作系统与数据库系统及其他应用软件的工作效能。操作系统的用户帐号和使用人数应有严格控制，设置系统控制参数和系统运行监视，同时用户的操作必须有详细的日志记录，定期备份日志。严禁非业务用软件的运行和拷贝。

数据库

材料共享网的各节点应尽量采用成熟的大型数据库管理系统，数据库的管理采用分布式结构管理，并严格遵循国际开放标准和规范。对数据库用户的的权限进行严格限制，要求配备专门的数据库管理人员，定期对数据库进行必要的监测和优化，提高检索速度，完善备份恢复策略，同时详细记录操作日志。

网站

共享中心以及各个子节点的站点向用户提供服务，要求配置有相应的维护人员，各站点要求留有站点的负责方的联系方式，网站服务出现异常时，维护人员应能及时排除故障，恢复网站的正常运行。各网站在网络的数据安全方面应采用数据加密、数字签名、数字证书及内容防篡改等技术，防止敏感数据被非法访问、修改和破坏，保证数据的完整性。

其它应用软件

应用软件是数据共享系统的支撑平台，涉及种类很多，包括 Web Service、数据处理等，也涉及到多个厂商的技术支持。对于这些软件的维护和管理须分门别类来进行，建立相应的维护流程，保证应用软件的可靠、高效运行。采用适当的加密防护措施、数据备份措施、防病毒措施及防火墙技术，并定期升级更新相关软件，确保所使用网络安全防护软件为最新版本。

在软件配置上，非涉密系统网络基础设施建设应符合《GB/T 20270-2006 信息安全技术 网络基础安全技术要求》；涉及国家机密、部门敏感信息的局域网的

安全标准不得低于《GB 17859-1999 计算机信息系统安全保护等级划分准则》中规定的第二级－系统审计保护级。

5.2 组织管理

以数据安全为重点，统一规划，建立信息安全认证体系、运行环境的安全保障系统和功能完备的容灾备份系统，确保数据中心的物理安全、网络安全、系统安全和数据安全。所有汇交的数据资料应严格按照有关数据资料管理规定进行分类存档管理；应设立信息安全管理工作的职能部门，配备专职安全管理员，负责数据中心数据安全工作，并与关键岗位人员签署岗位安全协议和保密协议；

5.3 法制管理

根据国家保密有关法律法规，组织完成数据安全定级工作，明确制度、分清职责、分级管理、逐级落实；在数据资源终止阶段，对于数据转移、暂存和清除、设备迁移或废弃、存储介质的清除或销毁等活动须按照《GB/T XXXXX-XXXX 信息安全技术 信息系统安全等级保护实施指南》的要求执行，如果是涉密数据，应该按照国家相关部门的规定进行转移、暂存和清除；涉密数据资料的存储、传输、共享、使用应指定专人负责，并严格按照国家有关保密的法律、法规执行。

6 附录

附录 A

材料科学数据共享网数据安全管理规定

第一条　为了加强对材料科学数据共享网计算机信息系统数据的安全管理，确保网络数据信息的安全，根据《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》等有关规定，结合材料科学数据共享网实际，制定本规定。

第二条　加强对材料科学数据共享网计算机信息系统数据安全保护工作的目的是：确保材料科学数据共享网计算机信息系统正常运行，维护数据信息应用工作的正常开展，预防、打击利用或针对材料科学数据共享网计算机信息系统数据进行违法犯罪活动的行为，提高材料科学数据共享网计算机信息系统数据整体安全水平，净化网络信息环境。

第三条　本规定中所指计算机信息系统数据是指各常规工作中所建立和存储在电子设备和计算机内的业务、材料科学数据、人员管理等电子数据。

第四条　材料科学数据共享网系统内计算机信息系统数据安全保护工作应按照“谁主管、谁负责，预防为主、综合治理，制度防范与技术防范相结合”的原则，逐级建立数据安全管理领导问责制和岗位责任制，加强制度建设，逐步实现数据安全管理的科学化、规范化。

第五条　材料科学数据共享网计算机信息系统内部数据实行安全等级保护，计算机信息系统数据的建设和存储应符合相应的安全等级标准，使用的安全产品必须具有《计算机信息系统安全专用产品销售许可证》，其等级应与计算机信息系统数据确定的安全等级相适应。

第六条　材料科学数据共享网数据安全管理小组负责组织工作人员的计算机安全教育培训，设立有关计算机安全课程，学习计算机安全管理法律、法规，提高全体工作人员的法律意识。

第七条　建立计算机信息系统安全登记备案制度。参加共享网的单位的计算机信息系统上线使用前，要向数据安全管理小组申请安全检查验收与系统备案登记，确定系统安全等级，指定数据安全责任人。

第八条　计算机信息系统必须使用正版软件，并及时进行系统升级或更新补丁；计算机信息系统必须装有防毒杀毒软件，并定期进行病毒检验；与互联网相联的计算机信息系统要有防止非法入侵措施。

第九条　计算机信息系统必须有全面、规范、严格的用户管理策略或办法。重要的计算机信息系统必须有双人互备做为系统管理员，系统管理员必须对计算机信息系统的各种服务器加设口令，严禁采用系统默认超级管理员用户命或口令；由系统管理员对用户实行集中管理，对用户按职能分组管理，设定用户访问

权限，严禁跨岗位越权操作；严防非法用户或非授权用户对非授权服务、数据及文件的访问、使用和修改等。对计算机信息系统的用户身份、主机身份、事件类型等应进行安全审计，并留存审计日志，审计日志应进行妥善保存。

第十条　计算机信息系统的主要硬件设备、软件、数据等要有完整可靠的备份机制和手段，并具有在要求时间内恢复系统功能以及重要数据的能力。对重要计算机信息系统及设备要有应急处理预案，数据安全管理小组要对应急预案备案登记，并每年定期举行数据安全应急演习。

第十一条　计算机信息系统与数据库主机必须建立在正规机房，机房要在场地面积、用电环境、使用环境、消防防雷等方面符合国家有关规定。

第十二条　IT 部门人员进入机房必须经领导许可，其他人员进入机房必须经 IT 部门领导许可，并有有关人员陪同。值班人员必须如实记录来访人员名单、进出机房时间、来访内容等。非 IT 部门工作人员原则上不得进入中心对系统进行操作。如遇特殊情况必须操作时，经 IT 部门负责人批准同意后有关人员监督下进行。对操作内容进行记录，由操作人和监督人签字后备查。

第十三条　机房内不准随意丢弃储蓄介质和有关业务保密数据资料，对废弃储蓄介质和业务保密资料要及时销毁（碎纸），不得作为普通垃圾处理。严禁机房内的设备、储蓄介质、资料、工具等私自出借或带出。

第十四条　计算机信息系统主机或存储设备发生故障时，要尽量现场维修，系统管理员要在现场监督；确需要送出维修时，注意防止数据外泄。

第十五条　各类计算机信息系统的安装、升级、调试和维护由系统管理员负责。未经系统管理员许可，不得随意在计算机信息系统的客户机上安装新软件。

第十六条　对重要或涉密数据的存储和传输应进行加密处理。对重要或涉密数据的存储介质，应采取必要的安全保护措施，并建立相应的登记管理制度。对保密信息不得遗失、泄露。未经同意，涉密计算机不得使用U盘、移动硬盘、刻录机等相关设备。

第十七条　对废弃的涉密数据要严格按照保密要求进行清零覆盖处理。

第十八条　接入互联网的计算机应具备必要的防黑客攻击、防病毒以及过滤

有害信息等安全技术措施。对计算机、服务器账户均设置密码，各种账户和密码严格保密。根据信息的安全规定和权限，确定使用人员的存取、使用权限。通过网络传送的程序或信息，必须经过安全检测，方可使用。各类操作人员必须具有病毒防范意识，做好计算机病毒的预防、检测、清除工作，及时升级防病毒系统，定期进行病毒的查杀，发现病毒要及时处理，并做好记录。防止各类针对网络的攻击，保证数据安全。

第十九条　提供电子邮件服务的计算机应具备有害信息和垃圾邮件过滤功能，相应技术参数应符合国家相关标准。

第二十条　在国际互联网上提供ＷＷＷ、ＦＴＰ、ＩＤＣ、邮件、交互式栏目、ＳＰ等服务的，应当报当地公安机关公共信息网络安全监察部门备案。

第二十一条　任何单位和个人不得利用国际互联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。第五章　数据维护及备份管理

第二十二条　建立计算机信息系统管理员制度。重要的计算机信息应用系统要实行系统管理员双人互备。系统管理员承担系统的运行维护和数据的安全管理工作。

第二十三条　各计算机信息应用系统本着“谁应用谁负责”的原则，由系统管理应用单位制定数据安全管理方案，配备专职系统管理员，并将数据安全管理方案、数据备份策略、管理流程和人员组织情况向厅数据安全管理小组登记备案。

第二十四条　系统管理员要严格遵守数据备份策略，及时做好数据的备份工作。严格数据库管理员口令管理，要定期更换数据库管理员口令。在系统升级或数据有较大变动情况时必须备份并长期异地保存；系统数据每天应作数据库的增量备份，每周应作数据库的完全备份；各类统计报表、各类外部电子信息数据应每月备份；重要数据读入系统后应及时备份。

第二十五条　数据备份采用在线存储与脱机介质两种形式进行双备份。一方面要将数据备份到非本机的存储设备上；另一方面备份到脱机介质上，脱机备份要实行本地与异地双存储。数据备份后要认真填写数据管理日志。

第二十六条　重要数据必须定期、完整、真实、准确地备份到不可更改的介质上，并要求做到集中和异地双备份保存。对长期保存的数据光盘等备份介质，应每年进行一次以上检查，以防止存储介质损坏造成损失。

第二十七条　备份数据资料保管地点应有防火、防潮、防尘、防磁、防盗等安全设施。废弃的数据信息存储介质要严格按照保密要求进行粉碎处理。

第二十八条　系统出现故障和遭到破坏时，由系统管理员负责完成数据恢复工作，系统管理员必须保证备份数据能够及时、准确、完整地恢复。确因特殊原因不能恢复的，应及时向分管领导汇报，妥善处理。数据恢复后要认真填写数据管理日志。

第二十九条　对数据的各项操作实行日志管理，严格监控操作过程，对发现的数据安全问题，要及时处理和上报。

第三十条　未经批准，系统管理员不得直接对后台数据库进行数据更改操作，确需后台操作的，必须上报分管领导批准，并事先对数据库进行备份后进行，同时，详细记录操作过程及数据更改情况存档备查。

第三十一条　计算机管理人员调离时，必须按规定移交全部技术资料和有关数据，设有口令密钥的要及时进行更换。涉及重要业务的人员调离时，应确认对业务不会造成危害后方可调离。

第三十二条　操作人员必须遵守有关计算机管理的安全保密法律法规，各类应用系统的使用必须实行用户身份验证，对自己的帐号负责。操作人员应注意自己用户名和口令的保密，并定期或不定期修改口令。如出现他人借用或盗用本人帐号引起不良后果的，要按规定追究有关责任人的责任。

第三十三条　发生重大计算机事故，应当立即报告计算机信息系统数据安全工作领导小组和专职部门。

第三十四条　发现计算机违法、犯罪案件，须立即向公安机关公共信息网络安全监察部门报案。第七章　档案管理

第三十五条　本规定自下发之日起执行。