中国矿业大学网络信息安全管理办法

第一章　总　则

第一条　为加强学校对网络信息安全工作的组织管理，提高网络信息安全防护能力和水平，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等国家法律法规，按照《党委（党组）网络安全工作责任制实施办法》《教育部关于加强教育行业网络与信息安全工作的指导意见》《教育部关于进一步加强直属高校直属单位信息技术安全工作的通知》等相关文件要求，结合我校网络安全工作实际情况，特制定本办法。

第二条　本办法所称网络信息安全，是指由学校建设、运行、维护或管理的校园网络、信息系统的安全。

本办法适用于使用校园网络及使用学校信息系统的任何用户，本办法所指学校各单位包括各学院、部、处、室、直附属单位以及独立运行的科研平台等。

第三条　按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全网络信息安全责任体系，学校各单位、全体师生员工应依照本办法要求及相关标准规范履行网络信息安全的义务和责任。

第二章　组织机构与职责

第四条　学校网络安全和信息化领导小组主管全校网络信息安全工作，学校主要负责人是学校网络信息安全的第一责任

人，分管信息化工作的校领导协助主要负责人履行学校网络信息安全责任。

第五条 信息化建设与管理处是学校网络信息安全归口管理、技术支撑单位，负责统筹学校网络信息安全工作。具体职责包括:

（一）制定网络信息安全总体规划，并组织实施;

（二）拟定网络信息安全管理规章制度，组织开展网络安全等级保护工作;

（三）负责学校网络信息安全防护系统的建设、运行维护、技术指导和服务支持;

（四）负责网络信息安全应急处置，协调与政府网络信息安全管理部门的关系;

（五）组织网络信息安全宣传和教育培训工作;

（六）负责网络信息安全监督检查工作;

（七）学校网络信息安全的其他工作。

第六条 学校各单位主要负责人为本单位网络信息安全第一责任人，负责本单位网络信息安全工作。

各单位应设一名网络信息安全管理员，负责本单位网络信息安全保护措施的落实，参加学校组织的网络信息安全培训，对上网人员进行网络信息安全教育和培训，与信息化建设与管理处协同配合，共同做好本单位网络及信息系统安全运行、管理和维护工作。

第三章　校园网络安全

第七条　校园网络是指连接学校各单位信息系统及信息终端的计算机网络，包括校园有线网络、无线网络和各种虚拟专网。

第八条　校园网络与互联网及其他公共信息网络实行逻辑隔离，由信息化建设与管理处统一出口、统一管理和统一防护。未经批准，学校各单位在校园内不得擅自通过其他渠道接入互联网及其他公共信息网络。

第九条　校园网络设施是学校重要的通讯基础资源，其使用和管理受国家相关法律和学校有关规定的保护，学校各单位和个人未经允许不得擅自改造、迁移、拆除和对设备进行操作。各单位(个人）须对部署在本单位（个人）办公区(宿舍）内的网络设施的物理安全负责，物业管理部门对部署在辖区公共区域内的网络设施的物理安全负责。因违反有关规定而造成网络设施损坏的，相关部门应责令其恢复原状、赔偿损失，并追究有关人员的责任。对恶意破坏校园网设施的行为，交由执法部门依法处理。各单位自行部署的防火墙、交换机等网络设备，应向信息化建设与管理处报备后，方可接入校园网络。

第十条　信息化建设与管理处应采取访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等措施加强校园网络边界防护。

第十一条　师生员工接入校园网络，实行实名认证制度；学校非涉密信息系统接入校园网络，实行接入审批和备案登记

制度。涉密信息系统不得接入校园网络。

单位和个人不得窃取或盗用他人的用户名、口令、IP 地址和 MAC 地址等。严禁利用校园网络进行挖矿等违法违规活动。

第十二条 接入校园网络的机房、电子阅览室等原则上不对社会开放，上网人员必须持有校园“一卡通”或凭身份证、学生证、工作证等有效证件登记后，方可上网。机房必须安装管理软件，自动记录上网人员身份和上下网时间、机号、IP 地址等，网络使用记录保存时间不得少于 6 个月。

第十三条 校园网络接入单位负责提供本单位所需的网络设备间和电源保障，负责其安防和消防安全管理。

第四章 信息系统及其数据安全

第十四条 信息化建设与管理处负责学校核心信息系统的备份与恢复管理，制订备份与恢复计划，根据业务实际需要对重要数据和信息系统进行备份，定期测试备份与恢复计划，并确保备份数据和备用资源的有效性。

第十五条 学校各单位和个人应依托校园网络开展信息系统建设。涉及学校基础数据、师生员工个人信息或敏感信息的信息系统，原则上不得部署在校外。需要在校外部署信息系统的单位和个人，应到信息化建设与管理处进行备案（备案表见附件一），并承担该信息系统的网络信息安全责任。

第十六条 学校各单位和个人不得私自建设联网的信息系统。根据教学和科研实际工作需求，确实需要建立信息系统的，建设方案须经信息化建设与管理处进行信息系统技术评估，满

足网络信息安全要求后方可启动建设。

各单位新建、改建、扩建的信息系统上线前，应由信息化建设与管理处进行安全检测，通过后方可上线运行。信息系统必须具有日志记录功能，历史记录保存时间不得低于 6 个月。

第十七条 信息化建设与管理处负责对学校各单位服务器和信息系统进行必要的安全检查和评测，对达不到安全要求的，关闭对外服务，整改合格后系统方可上线运行。

第五章 互联网网站安全

第十八条 学校各单位开办互联网网站，应使用学校互联网域名和互联网 IP 地址，并遵守相关规章制度。

第十九条 信息化建设与管理处统一建设学校网站集群平台并负责纳入该平台网站的技术安全。未纳入学校网站集群平台的网站，其技术安全由网站开办单位负责。

第二十条 学校各单位开办互联网网站应优先选择学校网站集群平台，有特殊需求的可独立建站，投入运行前，应按照本办法第十六条相关规定，通过安全检测后方可上线。

第二十一条 互联网网站运行维护单位应建立网站值守制度，制订应急处置流程，组织专人对网站进行监测，发现网站运行异常及时处置。

第二十二条 互联网网站的内容安全由网站开办单位负责。互联网网站开办单位应建立完善的网站信息发布与审核制度，确定负责内容编辑、内容审核、内容发布的人员名单，明确审核与发布程序，保存相关操作记录。

第二十三条 原则上，学校各单位不得提供电子公告服务。确有需要，经批准备案后方能提供电子公告服务。提供电子公告服务的互联网网站开办单位承担电子公告服务内容管理的主体责任，并按国家有关规定落实专项安全管理和技术措施。

第六章 电子邮件安全

第二十四条 学校为各单位和师生员工提供电子邮箱服务，信息化建设与管理处负责学校电子邮箱的安全管理。学校各单位和师生员工使用学校电子邮箱应遵守学校电子邮箱管理等相关规章制度。

第二十五条 信息化建设与管理处应采取必要的技术和管理措施，加强电子邮箱系统安全防护，减少垃圾邮件、病毒邮件侵袭。

第二十六条 全校师生员工须对使用其电子邮箱账号开展的所有活动负责，应妥善保管本人使用的电子邮箱账号和密码，确保密码具有一定强度并定期更换。师生员工如发现他人未经许可使用其电子邮箱，应立即通知信息化建设与管理处处理。

第七章 终端计算机安全

第二十七条 终端计算机是指由学校师生员工使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括显示屏、台式电脑、笔记本电脑及其他移动终端。

第二十八条 终端计算机使用人按照“谁使用，谁负责”的原则，对其终端负有保管和安全使用的责任。信息化建设与管理处对终端计算机的安全管理提供技术支持和指导。

第二十九条 终端计算机设备上安装、运行的软件应为正版软件。在终端上使用盗版软件带来的安全和法律责任由终端使用人承担。

第三十条 终端计算机应当设置系统登录账号和密码，登录密码应具有一定强度并定期更改。

第三十一条 终端计算机使用人应做好数据日常管理和保护，定期进行数据备份。非涉密计算机不得存储和处理涉密信息。

第三十二条 终端使用人应做好终端计算机的安全防范，如发现终端计算机出现可能由病毒或攻击导致的异常系统行为或其他安全问题，应立即断网后进行处置。

第三十三条 机房、电子阅览室等公共区域内终端计算机的安全管理工作由终端计算机所属单位负责，应定期定时对终端计算机进行杀毒及还原重置。

第八章 存储介质安全

第三十四条 存储介质是指存储数据的载体，主要包括硬盘、存储阵列、磁带库等不可移动存储介质，以及移动硬盘、U盘等可移动存储介质。

第三十五条 原则上，大容量存储介质应托管在学校数据中心，统一运行、维护和管理。信息化建设与管理处应采取必要技术措施防范数据泄露风险，确保存储数据安全。

第三十六条 非涉密移动存储介质不得用于存储涉密信息，不得在涉密计算机上使用。

第三十七条 移动存储介质在接入终端计算机和信息系统前，应当查杀病毒、木马等恶意代码。

第三十八条 介质使用人应注意移动存储介质的内容管理，对送出维修或销毁的介质应事先清除敏感信息。

第九章 人员安全管理

第三十九条 学校各单位应明确岗位及人员的网络信息安全责任。关键岗位的信息系统使用和管理人员应签订网络信息安全与保密协议，明确网络信息安全与保密要求和责任。

第四十条 学校各单位应加强人员离岗、离职管理，严格规范人员离岗、离职过程，及时终止相关人员的所有访问权限，收回学校提供的软硬件设备，并签署安全保密承诺书。

第四十一条 学校各单位应定期对网络信息安全岗位的人员进行安全知识和技能的考核，并对考核结果进行记录和保存。

第四十二条 学校各单位应建立外部人员访问机房等重要区域的审批制度，外部人员须经审批后方可进入，并安排工作人员现场陪同，对访问活动进行记录和保存。

第四十三条 外包服务商是指以签订合同方式提供网络和信息系统技术开发、运维、安全检查、等保测评、应急处置等服务的机构。学校各外包服务需求单位与外包服务商签订服务合同时，应将学校统一制定的网络信息安全与保密承诺书作为合同附件（见附件二），明确外包服务商的网络信息安全与保密责任，要求外包服务商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息和各类电子数据，不得占有服务

过程中产生的任何信息资产，不得以服务为由强制要求委托方购买、使用指定产品。

第四十四条 外包服务商派出的服务人员（以下简称外包人员）访问信息系统需经信息系统所属单位审批后，由该单位信息系统管理人员为其开设账户、分配权限、并登记备案，服务结束后应及时清除其所有的访问权限。禁止在未授权的情况下通过远程方式接入信息系统。外包人员离岗时，学校各单位应及时完成外包人员的账号撤销、技术资料移交等工作。

第十章 网络信息安全应急管理

第四十五条 信息化建设与管理处负责学校网络信息安全应急工作的统筹处置，制定学校网络信息安全事件报告与处置流程，以及安全应急工作的技术支撑和保障。

第四十六条 信息化建设与管理处定期组织网络信息安全应急演练，评估并适时组织网络信息安全应急预案修订。学校各单位应组织开展网络信息安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第四十七条 信息化建设与管理处负责组建学校信息安全应急队伍，完善 24 小时应急值守制度，提高信息安全事件的预防、预警和应对能力，预防和减轻信息安全事件造成的损失和危害。

第四十八条 学校各单位应按照学校网络信息安全事件报告与处置流程，做好事发紧急报告与处置、事中情况报告与处

置和事后整改报告与处置工作。做到安全事件早发现、早报告、早控制、早解决。

第四十九条 学校各单位及师生员工均有义务及时向信息化建设与管理处报告网络信息安全事件，不得在未授权情况下对外公布或利用所发现的安全漏洞或安全问题。

第十一章 网络信息安全教育培训

第五十条 信息化建设与管理处负责组织学校网络信息安全宣传和教育培训工作，建立健全相关制度。

第五十一条 信息化建设与管理处定期组织开展针对师生员工的网络信息安全教育，提高师生员工的安全和防范意识。

第五十二条 信息化建设与管理处定期开展针对网络信息安全管理人员和技术人员的专业技能培训，提高网络信息安全工作能力和水平。

第十二章 网络信息安全检查监督

第五十三条 学校各单位定期对本单位信息系统的安全状况、安全保护制度及措施的落实情况进行自查，并配合有关部门的网络信息安全检查、信息内容检查、保密检查与审批等工作。

第五十四条 信息化建设与管理处对学校各单位的网络信息安全工作落实情况进行检查，对发现的问题下达限期整改通知书，责成相关单位制订整改方案并落实到位。

第五十五条 信息化建设与管理处对年度安全检查情况进行全面总结，按照要求完成检查报告并报网络安全和信息化领导小组。

第十三章　网络信息安全责任追究

第五十六条　学校建立网络信息安全责任追究和倒查机制。

第五十七条　有关单位在收到网络信息安全限期整改通知书后，整改不力的，学校给予通报批评；玩忽职守、失职渎职造成严重后果的，依纪依法追究相关人员的责任。

第五十八条　学校各单位应按照网络信息安全事件报告与处置流程及时、如实报告和妥善处置网络信息安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关单位责任人进行约谈或通报。

第五十九条　师生员工违反本办法规定的，责令改正，并通报批评；拒不改正或者导致危害网络信息安全等严重后果的，根据学校有关规定给予以处分。触犯法律的，移交司法机关处理。

第十四章　附　则

第六十条　涉及国家秘密的信息系统，执行国家保密工作的相关规定和标准，由校党委保密委员会办公室监督指导。

第六十一条　本办法未尽事宜按照国家有关法律法规和规范性文件规定处理。

第六十二条　本办法由信息化建设与管理处负责解释，自发布之日起施行。原《中国矿业大学网络信息安全管理办法（试行）》（中矿大〔2017〕24号）同时废止。

附件：1.信息系统校外部署备案表

2.网络信息安全与保密承诺书

3.管理办法中事项办理流程

附件 1

信息系统校外部署备案表

<table>
<tr><td colspan="5">信息系统校外部署备案表</td></tr>
<tr><td>信息系统名称</td><td colspan="2"></td><td>备案时间</td><td></td></tr>
<tr><td>信息系统管理单位</td><td colspan="4"></td></tr>
<tr><td rowspan="2">信息系统负责人</td><td>姓名</td><td></td><td>职务</td><td></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮箱</td><td></td></tr>
<tr><td rowspan="2">信息系统联系人</td><td>姓名</td><td></td><td>职务</td><td></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮箱</td><td></td></tr>
<tr><td rowspan="4">信息系统情况描述</td><td>业务类型</td><td colspan="3">☐网站类 ☐办公类 ☐教学类 ☐科研类
☐其他，请说明:</td></tr>
<tr><td>服务对象</td><td colspan="3">☐校内人员 ☐社会公众</td></tr>
<tr><td>业务描述</td><td colspan="3"></td></tr>
<tr><td>存储数据描述</td><td colspan="3">1. 学生基本信息: ☐姓名 ☐学号 ☐身份证号
☐手机号 ☐其他，请说明:
2. 教职工基本信息: ☐姓名 ☐工号 ☐身份证号
☐手机号 ☐其他，请说明:
3. 其他个人信息数据:
4. 其他业务数据:</td></tr>
</table>

附件 2

网络信息安全与保密承诺书

网络信息安全与保密承诺书

我方_ **公司名称（必填）** _-按中国矿业大学委托履行_**项目名称（必填）**合同工作，有必要获得学校有关的信息，以便我方了解和使用。鉴于在合作的过程中，学校提供给我方或我方自行接触到的信息，我方不能向任何第三方进行任何披露，因此我方特向学校做出如下陈述与承诺，并保证受本承诺书的约束。

第一条：定义

本承诺书中，有关术语含义如下:

- “信息”指任何以口头、书面、图表或电子形式存在的

（a）任何涉及学校过去、现在或将来的商业计划。规章制度、操作规程、处理手段、财务信息;

（b）任何学校的技术措施、技术方案、软件应用及开发，硬件设备的品种、质量、数量、品牌等;

（c）任何学校的技术秘密或专有知识、文件 、报告、数据、客户软件、流程图、数据库、发明、知识、技术需求及贸易秘密;

（d）任何其他的以有形方式或无形方式存在的信息。

无论上述信息是否享有知识产权。

- “保密信息”指学校明确表示我方应当保守秘密的任何“信息”，该明确表示可以通过:

（1） 书面（含电子文档）的形式;

（2） 口头的形式;

该明确表示可以发生在我方接受或接触到的该信息的当时，也可以发生于在此之后的任何时间。

第二条：我方保密的义务

1. 我方对于从学校处收到的保密信息，在未经学校事先书面允可的情况下，不以任何方式提供给任何第三方。

2. 我方对于从学校处得到的保密信息，应当通过建立内部保密制度、培训员工等方式和措施确保保密信息的安全，并且如果我方内部已有保密制度的，应将从学校处得到的保密信息视同我方自己企业内部的保密信息一样进行安全管理。

3. 我方严格保证:

(1)所收到的信息只能用于我方为学校提供项目需要的产品及实施服务的目的，而不得用于任何其他目的;

(2)所收到的信息在本企业内部能得到谨慎的使用，只能透露给本企业或本企业所属之分支机构、子公司内部参与我方与学校合作项目建设的雇员，并且该雇员在知晓保密信息之前已经充分了解了本承诺书的内容。如该雇员在离开我方后泄露本承诺书所规定的保密信息，则仍由我方承担本承诺书项下的违约责任。

(3)对于所收到的信息，除为合作项目之目的在本企业内部进行适当的复制外，不进行任何复制和传播。

4. 在未经学校事先书面允许的情况下，我方不为开发同类产品之目的使用学校取得的经验、材料、产品以及其他学校所有的信息，不将上述经验、材料、产品和信息作为案例、模型或其他任何形式的材料，在任何场合演示和推广。

5. 除非学校同意，否则我方不向第三方披露我方与学校的任何会谈、会议、协商或共同工作的内容。

第三条：非保密信息

下述信息不视为保密信息：

- ✓ 非由于我方违反本承诺书的原因进入公共领域的信息；
- ✓ 我方在收到信息前已经合法掌握的信息；
- ✓ 我方在收到信息前已经通过正当途径获得的信息；

第四条：保密责任的例外

在下述两情况下，如发生保密信息的泄露，应免除我方相应的责任；

1. 我方被国家法律要求披露有关保密信息；
2. 由于我方不可预见、不可避免、不可控制的原因，即不可抗力的原因，导致了保密信息的泄露。

如因上述两情况造成保密信息的泄露，我方将立即书面告知学校，并采取一切措施减少学校的损失。

第五条：对本承诺书的保证

未经学校书面同意，本承诺书不以任何方式进行修改、终止或解除。本承诺书项下的权利义务不得转让。

第六条：本承诺书的效力范围

1. 本承诺书的效力仅限于保密责任。在任何情况下，我方向学校提交本承诺书都不表示或意味着学校有责任与我方建立任何形式的商业合作关系。同时，学校与我方交换信息的行为不应被视为是双方之间建立合作关系的合同，或者被视为学校的签订合同或协议的承诺。

2. 学校提供信息的行为不被视为是以任何方式授予技术许可，或是转让著作权、商标权、专利权或技术秘密的行为。我方取得信息并不表明取得了信息的任何知识产权；对学校所提供的任何信息的知识产权和财产权利，全部归学校所有。

第七条：产生于泄密的责任

任何保密信息的泄露或任何其它违反本承诺书的行为给学校造成损失，我方应承担相应的赔偿责任及其它所有可能涉及的民事（包括侵权）的、行政的和刑事的法律责任。

第八条：司法管辖和法律适用

如我方与学校因本承诺发生民事纠纷，应通过友好协商解决。协商不成，可起诉于中华人民共和国有管辖权的人民法院，由法院适用中国法律加以判决。

第九条 承诺书的有效期

本承诺书自合同签订之日起生效，将一直保持有效。

第十条 个人保密责任

因发生该业务，我方相关业务人员前往学校执行业务，将同样签署保密承诺书，以明确执行保密责任。

承诺方： **（公司名称）**

授权签字人： **（签字）**

（公司盖章）

地址：

日期： 年 月 日

附件 3:

管理办法中事项办理流程

序号	流程名称	流程入口
1	信息系统技术评估	特别说明：信息系统技术评估已与“采购与招标管理系统”对接，招采系统的项目不需要再次进行技术评估。【融合门户】-【一网通办】-【“一网通办”服务中心】-搜索“信息系统技术评估”；
2	信息系统验收评估	特别说明：信息系统验收可与单位组织的线下项目验收同步进行，亦可申请线上验收。【融合门户】-【一网通办】-【“一网通办”服务中心】-搜索“信息系统验收评估”。