中国地质大学
CHINA UNIVERSITY OF GEOSCIENCES
武汉 · WUHAN

内部资料
注意保密

数字化转型推进会暨网信领导小组扩大会议

学习资料

2023年11月

目　录

二、其他相关资料

一、国家相关政策文件

中华人民共和国数据安全法

第一章 总 则

第一条 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政

策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成

的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或

者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

第三十四条 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者

吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自 2021 年 9 月 1 日起施行。

中华人民共和国密码法

第一章 总 则

第一条 为了规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，制定本法。

第二条 本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

第三条 密码工作坚持总体国家安全观，遵循统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的原则。

第四条 坚持中国共产党对密码工作的领导。中央密码工作领导机构对全国密码工作实行统一领导，制定国家密码工作重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设。

第五条 国家密码管理部门负责管理全国的密码工作。县级以上地方各级密码管理部门负责管理本行政区域的密码工作。

国家机关和涉及密码工作的单位在其职责范围内负责本机关、本单位或者本系统的密码工作。

第六条 国家对密码实行分类管理。

密码分为核心密码、普通密码和商用密码。

第七条 核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。

核心密码、普通密码属于国家秘密。密码管理部门依照本法和有关法律、行政法规、国家有关规定对核心密码、普通密码实行严格统一管理。

第八条 商用密码用于保护不属于国家秘密的信息。

公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

第九条 国家鼓励和支持密码科学技术研究和应用，依法保护密码领域的知识产权，促进密码科学技术进步和创新。

国家加强密码人才培养和队伍建设，对在密码工作中作出突出贡献的组织和个人，按照国家有关规定给予表彰和奖励。

第十条 国家采取多种形式加强密码安全教育，将密码安全教育纳入国民教育体系和公务员教育培训体系，增强公民、法人和其他组织的密码安全意识。

第十一条 县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级财政预算。

第十二条 任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统。

任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

第二章 核心密码、普通密码

第十三条 国家加强核心密码、普通密码的科学规划、管理和使用，加强制度建设，完善管理措施，增强密码安全保障能力。

第十四条 在有线、无线通信中传递的国家秘密信息，以及存储、处理国家秘密信息的信息系统，应当依照法律、行政法规和国家有关规定使用核心密码、普通密码进行加密保护、安全认证。

第十五条 从事核心密码、普通密码科研、生产、服务、检测、装备、使用和销毁等工作的机构（以下统称密码工作机构）应当按照法律、行政法规、国家有关规定以及核心密码、普通密码标准的要求，建立健全安全管理制度，采取严格的保密措施和保密责任制，确保核心密码、普通密码的安全。

第十六条 密码管理部门依法对密码工作机构的核心密码、普通密码工作进行指导、监督和检查，密码工作机构应当配合。

第十七条 密码管理部门根据工作需要会同有关部门建立核心密码、普通密码的安全监测预警、安全风险评估、信息通报、重大事项会商和应急处置等协作机制，确保核心密码、普通密码安全管理的协同联动和有序高效。

密码工作机构发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患的，应当立即采取应对措施，并及时向保密行政管理部门、密码管理部门报告，由保密行政管理部门、密码管理部门会同有关部门组织开展调查、处置，并指导有关密码工作机构及时消除安全隐患。

第十八条 国家加强密码工作机构建设，保障其履行工作职责。

国家建立适应核心密码、普通密码工作需要的人员录用、选调、保密、考核、培训、待遇、奖惩、交流、退出等管理制度。

第十九条 密码管理部门因工作需要，按照国家有关规定，可以提请公安、交通运输、海关等部门对核心密码、普通密码有关物品和人员提供免检等便利，有关部门应当予以协助。

第二十条 密码管理部门和密码工作机构应当建立健全严格的监督和安全审查制度，对其工作人员遵守法律和纪律等情况进行监督，并依法采取必要措施，定期或者不定期组织开展安全审查。

第三章 商用密码

第二十一条 国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。

各级人民政府及其有关部门应当遵循非歧视原则，依法平等对待包括外商投资企业在内的商用密码科研、生产、销售、服务、进出口等单位（以下统称商用密码从业单位）。国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。

商用密码的科研、生产、销售、服务和进出口，不得损害国家安全、社会公共利益或者他人合法权益。

第二十二条 国家建立和完善商用密码标准体系。

国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准。

国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

第二十三条 国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用。

国家鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。

第二十四条 商用密码从业单位开展商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求。

国家鼓励商 用密码从业单位采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。

第二十五条 国家推进商用密码检测认证体系建设，制定商用密码检测认证技术规范、规则，鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。

商用密码检测、认证机构应当依法取得相关资质，并依照法律、行政法规的规定和商用密码检测认证技术规范、规则开展商用密码检测认证。

商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务。

第二十六条 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。

商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

第二十八条 国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。商用密码进口许可清单和出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布。

大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

第二十九条 国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理。

第三十条 商用密码领域的行业协会等组织依照法律、行政法规及其章程的规定，为商用密码从业单位提供信息、技术、培训等服务，引导和督促商用密码从业单位依法开展商用密码活动，加强行业自律，推动行业诚信建设，促进行业健康发展。

第三十一条 密码管理部门和有关部门建立日常监管和随机抽查相结合的商用密码事中事后监管制度，建立统一的商用密码监督管理信息平台，推进事中事后监管与社会信用体系相衔接，强化商用密码从业单位自律和社会监督。

密码管理部门和有关部门及其工作人员不得要求商用密码从业单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息，并对其在履行职责中知悉的商业秘密和个人隐私严格保密，不得泄露或者非法向他人提供。

第四章 法律责任

第三十二条 违反本法第十二条规定，窃取他人加密保护的信息，非法侵入他人的密码保障系统，或者利用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动的，由有关部门依照《中华人

民共和国网络安全法》和其他有关法律、行政法规的规定追究法律责任。

第三十三条 违反本法第十四条规定，未按照要求使用核心密码、普通密码的，由密码管理部门责令改正或者停止违法行为，给予警告；情节严重的，由密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

第三十四条 违反本法规定，发生核心密码、普通密码泄密案件的，由保密行政管理部门、密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

违反本法第十七条第二款规定，发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患，未立即采取应对措施，或者未及时报告的，由保密行政管理部门、密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

第三十五条 商用密码检测、认证机构违反本法第二十五条第二款、第三款规定开展商用密码检测认证的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得三十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足三十万元的，可以并处十万元以上三十万元以下罚款；情节严重的，依法吊销相关资质。

第三十六条 违反本法第二十六条规定，销售或者提供未经检测认证或者检测认证不合格的商用密码产品，或者提供未经认证或者认证

不合格的商用密码服务的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足十万元的，可以并处三万元以上十万元以下罚款。

第三十七条 关键信息基础设施的运营者违反本法第二十七条第一款规定，未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者违反本法第二十七条第二款规定，使用未经安全审查或者安全审查未通过的产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第三十八条 违反本法第二十八条实施进口许可、出口管制的规定，进出口商用密码的，由国务院商务主管部门或者海关依法予以处罚。

第三十九条 违反本法第二十九条规定，未经认定从事电子政务电子认证服务的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得三十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足三十万元的，可以并处十万元以上三十万元以下罚款。

第四十条 密码管理部门和有关部门、单位的工作人员在密码工作中滥用职权、玩忽职守、徇私舞弊，或者泄露、非法向他人提供在履行职责中知悉的商业秘密和个人隐私的，依法给予处分。

第四十一条 违反本法规定，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任。

第五章 附 则

第四十二条 国家密码管理部门依照法律、行政法规的规定，制定密码管理规章。

第四十三条 中国人民解放军和中国人民武装警察部队的密码工作管理办法，由中央军事委员会根据本法制定。

第四十四条 本法自 2020 年 1 月 1 日起施行。

中华人民共和国网络安全法

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改:

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任;

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月;

（四）采取数据分类、重要数据备份和加密等措施;

（五）法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据

等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条 的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务:

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查;

（二）定期对从业人员进行网络安全教育、技术培训和技能考核;

（三）对重要系统和数据库进行容灾备份;

（四）制定网络安全事件应急预案，并定期进行演练;

（五）法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施:

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估;

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力;

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享;

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章 网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测;

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度;

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条 、第二十五条 规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条 第一款、第二款和第四十八条 第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条 第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、

停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条 违反本法第二十六条 规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条 规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条 规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条 第三款、第四十一条 至第四十三条 规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条 规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条 规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条 规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条 违反本法第四十六条 规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条 网络运营者违反本法第四十七条 规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条 第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条 第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十三条 网信部门和有关部门违反本法第三十条 规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果

的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自 2017 年 6 月 1 日起施行。

中华人民共和国计算机信息系统安全保护条例

中华人民共和国国务院令

（147号）

现发布《中华人民共和国计算机信息系统安全保护条例》，自发布之日起施行。

总理 李鹏

1994年2月18日

中华人民共和国计算机信息系统安全保护条例

第一章 总则

第一条 为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定本条例。

第二条 本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第四条 计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

第五条 中华人民共和国境内的计算机信息系统的安全保护，适用本条例。未联网的微型计算机的安全保护办法，另行制定。

第六条 公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

第七条 任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

第二章 安全保护制度

第八条 计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。

第九条 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。

第十条 计算机机房应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。

第十一条 进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

第十二条 运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。

第十三条 计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

第十四条 对计算机信息系统中发生的案件，有关使用单位应当在２４小时内向当地县级以上人民政府公安机关报告。

第十五条 对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

第十六条 国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

第三章 安全监督

第十七条 公安机关对计算机信息系统安全保护工作行使下列监督职权:

（一）监督、检查、指导计算机信息系统安全保护工作;

（二）查处危害计算机信息系统安全的违法犯罪案件;

（三）履行计算机信息系统安全保护工作的其他监督职责。

第十八条 公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

第十九条 公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

第四章 法律责任

第二十条 违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿:

（一）违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的;

（二）违反计算机信息系统国际联网备案制度的;

（三）不按照规定时间报告计算机信息系统中发生的案件的;

（四）接到公安机关要求改进安全状况的通知后，在限期内拒不改进的;

（五）有危害计算机信息系统安全的其他行为的。

第二十一条 计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

第二十二条 运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的，由海关依照《中华人民共和国海关法》和本条例以及其他有关法律、法规的规定处理。

第二十三条 故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 15000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

第二十四条 违反本条例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚条例》的有关规定处罚；构成犯罪的，依法追究刑事责任。

第二十五条 任何组织或者个人违反本条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

第二十六条 当事人对公安机关依照本条例所作出的具体行政行为不服的，可以依法申请行政复议或者提起行政诉讼。

第二十七条 执行本条例的国家公务员利用职权，索取、收受贿赂或者有其他违法、失职行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，给予行政处分。

第五章 附则

第二十八条 本条例下列用语的含义：

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

第二十九条 军队的计算机信息系统安全保护工作，按照军队的有关法规执行。

第三十条 公安部可以根据本条例制定实施办法。

第三十一条 本条例自发布之日起施行。

中华人民共和国计算机信息网络国际联网管理暂行规定

中华人民共和国国务院令

（第 195 号）

《中华人民共和国计算机信息网络国际联网管理暂行规定》，已经 1996 年 1 月 23 日国务院第 42 次常务会议通过，现予发布施行。

总理 李鹏

1996 年 2 月 1 日

第一条 为了加强对计算机信息网络国际联网的管理，保障国际计算机信息交流的健康发展，制定本规定。

第二条 中华人民共和国境内的计算机信息网络进行国际联网，应当依照本规定办理。

第三条 本规定下列用语的含义是:

（一）计算机信息网络国际联网（以下简称国际联网），是指中华人民共和国境内的计算机信息网络为实现信息的国际交流，同外国的计算机信息网络相联接。

（二）互联网络，是指直接进行国际联网的计算机信息网络；互联单位，是指负责互联网络运行的单位。

（三）接入网络，是指通过接入互联网络进行国际联网的计算机信息网络；接入单位，是指负责接入网络运行的单位。

第四条 国家对国际联网实行统筹规划，统一标准、分级管理、促进发展的原则。

第五条 国务院经济信息化领导小组（以下简称领导小组）负责协调、解决有关国际联网工作中的重大问题。领导小组办公室按照本规定制定具体管理办法，明确国际出入口信息提供单位、互联单位、接入单位和用户的权利、义务和责任，并负责对国际联网工作的检查监督。

第六条 计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行建立或者使用其他信道进行国际联网。

第七条 已经建立的互联网络，根据国务院有关规定调整后，分别由邮电部、电子工业部，国家教育委员会和中国科学院管理。新建互联网络，必须报经国务院批准。

第八条 接入网络必须通过互联网络进行国际联网。

拟建立接入网络的单位，应当报经互联单位的主管部门或者主管单位审批；办理审批手续时，应当提供其计算机信息网络的性质、应用范围和所需主机地址等资料。

第九条 接入单位必须具备下列条件:

（一）是依法设立的企业法人或者事业法人;

（二）具有相应的计算机信息网络、装备以及相应的技术人员和管理人员;

（三）具有健全的安全保密管理制度和技术保护措施;

（四）符合法律和国务院规定的其他条件。

第十条 个人、法人和其他组织（以下统称用户）使用的计算机或者计算机信息网络，需要进行国际联网的，必须通过接入网络进行国际联网。前款规定的计算机或者计算机信息网络，需要接入接入网络的，应当征得接入单位的同意，并办理登记手续。

第十一条 国际出入口信道提供单位、互联单位和接入单位，应当建立相应的网络管理中心，依照法律和国家有关规定加强对本单位及其用户的管理，做好网络信息安全管理工作，确保为用户提供良好、安全的服务。

第十二条 互联单位与接入单位，应当负责本单位及其用户有关国际联网的技术培训和管理教育工作。

第十三条 从事国际联网业务的单位和个人，应当遵守国家有关法律、行政法规，严格执行安全保密制度，不得利用国际联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息。

第十四条 违反本规定第六条、第八条和第十条规定的，由公安机关或者公安机关根据国际出入口信道提供单位、互联单位、接入单位的意见，给予警告、通报批评、责令停止联网，可以并处１．５万元以下的罚款。

第十五条 违反本规定，同时触犯其他有关法律、行政法规的，依照有关法律、行政法规的规定予以处罚；构成犯罪的，依法追究刑事责任。

第十六条 与台湾、香港、澳门地区的计算机信息网络的联网，参照本规定执行。

第十七条 本规定自发布之日起施行。

中华人民共和国计算机信息系统安全保护条例

中华人民共和国国务院令

（第 147 号）

第一章 总则

第一条 为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定本条 例。

第二条 本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第四条 计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

第五条 中华人民共和国境内的计算机信息系统的安全保护，适用本条 例。

未联网的微型计算机的安全保护办法，另行制定。

第六条 公安部主管全国计算机信息系统安全保护工作。

国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

第七条 任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

第二章 安全保护制度

第八条 计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。

第九条 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。

第十条 计算机机房应当符合国家标准和国家有关规定。

在计算机机房附近施工，不得危害计算机信息系统的安全。

第十一条 进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

第十二条 运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。

第十三条 计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

第十四条 对计算机信息系统中发生的案件，有关使用单位应当在24小时内向当地县级以上人民政府公安机关报告。

第十五条 对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

第十六条 国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

第三章 安全监督

第十七条 公安机关对计算机信息系统安全保护工作行使下列监督职权:

（一）监督、检查、指导计算机信息系统安全保护工作;

（二）查处危害计算机信息系统安全的违法犯罪案件;

（三）履行计算机信息系统安全保护工作的其他监督职责。

第十八条 公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

第十九条 公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

第四章 法律责任

第二十条 违反本条 例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿:

（一）违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的;

（二）违反计算机信息系统国际联网备案制度的;

（三）不按照规定时间报告计算机信息系统中发生的案件的;

（四）接到公安机关要求改进安全状况的通知后，在限期内拒不改进的;

（五）有危害计算机信息系统安全的其他行为的。

第二十一条 计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

第二十二条 运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的，由海关依照《中华人民共和国海关法》和本条 例以及其他有关法律、法规的规定处理。

第二十三条 故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 1　 5 万元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

第二十四条 违反本条 例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚法》的有关规定处罚；构成犯罪的，依法追究刑事责任。

第二十五条 任何组织或者个人违反本条 例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

第二十六条 当事人对公安机关依照本条 例所作出的具体行政行为不服的，可以依法申请行政复议或者提起行政诉讼。

第二十七条 执行本条 例的国家公务员利用职权，索取、收受贿赂或者有其他违法、失职行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，给予行政处分。

第五章 附则

第二十八条 本条 例下列用语的含义：

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

第二十九条 军队的计算机信息系统安全保护工作，按照军队的有关法规执行。

第三十条 公安部可以根据本条 例制定实施办法。

第三十一条 本条 例自发布之日起施行。

教育部办公厅关于印发《教育行业网络安全综合治理行动方案》的通知

(教技厅[2017]3号)

各省、自治区、直辖市教育厅(教委),新疆生产建设兵团教育局,部属各高等学校,部内各司局、各直属单位,中国教育和科研计算机网网络信息中心:

为全面贯彻党中央、国务院关于网络安全的统筹部署，落实《网络安全法》,迎接党的十九大胜利召开,按照教育部网络安全和信息化领导小组的统一部署,教育部将于3月至8月开展以“治乱、堵漏、补短、规范”为目标的网络安全综合治理行动。现将《教育行业网络安全综合治理行动方案》印发给你们,请遵照执行。

联系人:科技司,潘润恺,010-66096823

教育部办公厅

2017年3月15日

教育行业网络安全综合治理行动方案

教育行业网络安全是国家网络安全的重要组成部分。近年来,按照国家网络安全的总体部署,在全行业共同努力下,教育行业网络安全意识显著提高,形势明显好转，工作机制基本建立,防护能力不断加强。但也要看到,教育行业机构多、系统多、数据多影响面广,网络安全工作仍存在许多问题，主要表现在:安全责任不落实、管理不规范、安全隐患修复不及时、监测预警和应急响应能力不足、网络安全事件时

有发生等问题。这些问题给教育行业不仅造成了不良影响,同时危害到师生的切身利益。为全面贯彻党中央、国务院关于网络安全的统筹部署,落实《网络安全法》,迎接党的十九大胜利召开,按照教育部网络安全和信息化领导小组的统一部署，自 2017 年 3 月至 8 月，教育部将在全行业开展以“治乱、堵漏、补短、规范”为目标的网络安全综合治理行动,综合治理行动方案如下:

一、工作目标

面向各级教育行政部门及其直属单位、高等学校(以下简称各单位),坚持以问题导向、突出重点、完善机制、狠抓落实,重点加强对网站乱象的治理、堵塞安全漏洞、补齐等保短板、规范安全管理。同时,兼顾近期与长远、综合治理与源头治理相结合，全面提升教育行业网络安全水平,增强信息系统防护能力,有效防范和抵御安全风险隐患，切实保障信息系统(网站)稳定运行和数据安全。

二、工作内容

(一)治理网站乱象,强化主体责任。

1.进一步落实网站统一标识工作。各级教育行政部门及其直属单位应按照《党政机关网站开办审核、资格复核和网站标识管理办法》和各地要求,尽快到各地机构编制部门完成网站开办审核、资格复核和挂标工作。如未按期完成,将根据有关职能部门要求对网站主管单位予以督办。(2017 年 5 月底前完成)

2.加强教育行业网站信息发布管理。各单位应全面检查网站信息发布情况,如有发布的信息中存在法律和行政法规禁止发布或传输的信息、涉及个人隐私和单位秘密的信息,应采取删除或更正等措施立

即整改。加强对电子邮箱的管理,对非在职人员电子邮箱账号予以注销,对使用简单密码的应采取有效措施要求更换并建立定期更新密码的制度。(2017 年 5 月底前完成)

3.开展教育机构网站域名清理工作。中国教育和科研计算机网网络信息中心根据教育机构名录核对注册 edu.cn 域名的机构情况,根据实际情况对非教育机构的网站使用该域名的进行清理。教育部研究加强对教育机构网上名称的管理,规范教育机构域名,提升教育机构网站的公信力和权威性。(2017 年 8 月底完成)

(二)堵塞安全漏洞,增强防护能力。

1.全面监测网络安全威胁。各级教育行政部门及其有条件的直属单位、高校应对本地区、本单位主管的信息系统(网站)开展常态化监测,发现存在漏洞、后门、暗链、弱口令等安全威胁的信息系统(网站),应及时通报、限时修复、跟踪核查整改结果,尽快消除安全隐患。持续推进。

2.检测应用软件安全风险。教育部深入分析支撑教育行业重要业务管理、教育教学活动中使用范围较广的应用软件产品的安全性,通过测试发掘软件存在的安全缺陷、漏洞等风险隐患,告知开发单位及时采取补救措施,并尽快协助教育行业用户完成对软件的升级和修复。持续推进。

(三)补齐等保短板,履行安全保护义务。

1.加快完成定级备案。各单位应清楚掌握主管的信息系统(网站)情况,按照《教育部 公安部关于全面推进教育行业信息安全等级保护工作的通知》(以下简称《通知》)的要求,建立信息系统安全等级保

护制度和程序,尽快完成信息系统(网站)等级保护定级工作,并到当地公安机关进行备案。新建系统应在正式上线前完成信息系统定级备案和测评整改。(2017 年 5 月底完成)

2.有序推进测评整改。各单位应按照《通知》要求,对主管的信息系统(网站)开展网络安全等级测评整改工作。重点加强对主管的关键信息基础设施的保护,明确安全管理负责人,制订专门应急预案，完成年度测评工作,深入查找薄弱环节并迅速整改。(2017 年 6 月底完成)

（四）规范安全管理,提升治理水平

1.加强和规范数据管理。教育部加快制定出台《教育部教育数据管理办法》,各省级教育行政部门参照制定相应的数据管理办法,各单位应规范数据采集、存储、使用和开放共享,推进对重要数据的加密存储和传输,及其容灾备份。(2017 年 8 月底前完成)2.加强关键信息基础设施规范管理。各单位应开展关键信息基础设施专项检查和安全评估，研究制定关键信息基础设施管理和防护规范,明确产品和服务采购、人员管理工作要求,指导、监督关键信息基础设施的运行安全。(2017 年底前完成)

3.健全网络安全事件应急响应机制。各单位应研究制定信息技术安全应急预案,建立安全事件分级响应、跨部门协同处置的工作机制。加强应急处置队伍建设，落实 24 小时值守，并定期开展安全演练,提高教育信息系统(网站)应急处置水平。(2017 年底前完成)

三、工作要求

(一)提高思想认识,加强组织领导。教育部负责统筹部署本次综合治理行动,省级教育行政部门负责统筹本地区的综合治理行动。各单

位应充分认识开展综合治理行动的重要性和紧迫性将工作纳入重要议事日程予以部署,明确主管领导、牵头部门和责任人,提供必要的工作保障,确保各项工作落到实处。

(二)加强协调配合,形成工作合力。各单位应加强与网信部门、公安机关、工信部门等网络安全职能部门的沟通配合,在打击网络违法行为、处置网络安全事件等方面形成合力。探索与网络安全专业机构、安全企业建立合作机制或购买第三方服务,在信息共享、技术支持、教育培训等方面开展多方位的合作。

(三)加强监督检查,完善通报机制。各单位应在每月底报送当月工作进展情况,填写《教育行业网络安全综合治理行动进展统计表》(见附件)。教育部将综合治理行动纳入教育信息化工作月报内容定期通报。同时,将网络安全工作纳入校园及周边治安综合治理工作考核评价体系和网络安全生产大检查,建立网络安全长效监督机制。

(四)开展宣传教育,提升安全意识。各单位应组织开展网络安全宣传教育,面向网络安全管理人员和技术人员开展专题培训切实提高网络安全意识、管理水平和防护能力。利用新生入学教育、网络安全宣传周等契机,通过形势政策课、讲座、报告会等方式面向广大师生开展网络安全宣传教育,提高网络安全意识和素养。

附件:教育行业网络安全综合治理行动进展统计表

教育行业网络安全综合治理行动进展统计表

单位名称:

<table>
<tr><td colspan="8">一、单位基本情况</td></tr>
<tr><td>主管领导</td><td></td><td>职务</td><td></td><td>联系方式</td><td colspan="3"></td></tr>
<tr><td>职能部门</td><td></td><td>责任人</td><td></td><td>职务</td><td colspan="3"></td></tr>
<tr><td>移动电话</td><td></td><td>电子邮箱</td><td colspan="3"></td><td></td></tr>
<tr><td colspan="8">二、月度工作部署情况</td></tr>
<tr><td colspan="8">部署综合治理行动的会议、发文情况；完善综合治理行动的工作机制情况；推进本月工作完成综合治理行动相关工作的措施；综合治理行动的创新或可资借鉴的经验案例。</td></tr>
<tr><td colspan="8">三、月度工作进展情况</td></tr>
<tr><td colspan="8">（一）网站规范管理工作</td></tr>
<tr><td colspan="3">本单位信息系统数量</td><td></td><td colspan="3">完成信息发布整改数量</td><td></td></tr>
<tr><td colspan="3">完成网站开办审核工作</td><td></td><td colspan="3">完成网站挂标工作</td><td></td></tr>
<tr><td colspan="3">事业单位门户网站数量</td><td></td><td colspan="3">完成网站挂标工作数量</td><td></td></tr>
<tr><td colspan="8">（二）安全威胁处置工作</td></tr>
<tr><td colspan="2">是否开展检测工作</td><td colspan="2"></td><td colspan="2">开展监测的工作方式</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="3">发现的安全威胁数量</td><td>漏洞</td><td></td><td colspan="2" rowspan="3">完成整改的数量</td><td>漏洞</td><td></td></tr>
<tr><td>后门</td><td></td><td>后门</td><td></td></tr>
<tr><td>暗链</td><td></td><td>暗链</td><td></td></tr>
<tr><td colspan="8">（三）网络安全等级保护工作</td></tr>
<tr><td></td><td>系统总数</td><td>一级</td><td>二级</td><td>三级</td><td>四级</td><td colspan="2">未定级</td></tr>
<tr><td>定级备案</td><td></td><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td>测评整改</td><td></td><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="3">关键信息基础设施数量</td><td></td><td colspan="2">已完成测评数量</td><td colspan="2"></td></tr>
</table>

备注：1.省级教育行政部门、部直属单位需填写网站开办审核、挂标工作完成情况

2.如本单位未开展监测工作，则无需填写安全威胁处置工作栏目的相关内容；发现和完成整改的安全威胁数量，仅需填写本单位监测工作涉及的相关数据

3.开展监测的方式包括自行组织、专业机构合作、购买第三方服务等。

教育部办公厅关于印发《教育信息化专项-教育业务管理信息系统建设子项目管理细则(试行)》的通知

(教技厅函[2017]4号)

部内各司局、各直属单位:

为贯彻落实《教育信息化十年发展规划（2010-2020年）》，规范信息系统建设、运维全过程管理，规范财政专项资金使用，根据《教育信息化项目管理暂行办法》（教技厅函〔2016〕37号）和《教育信息化专项资金管理办法》（教财厅函〔2016〕38号）的要求，我部研究制定了《教育信息化专项-教育业务管理信息系统子项目管理细则（试行）》。现印发给你们，请认真贯彻执行。

联系人：教育部科技司 潘润恺 010-66096823

教育部办公厅

2017年1月16日

教育信息化专项-教育业务管理信息系统子项目管理细则（试行）

第一章 总则

第一条 为规范教育信息化专项-教育业务管理信息系统子项目（以下简称子项目）的建设与运维管理，规范中央财政预算资金申请与使用，明晰信息系统及数据管理与安全权责，提高服务教育管理核心业务的水平，参照《国家电子政务工程建设项目管理暂行办法》（国家发改委第55号令），根据《教育信息化项目管理暂行办法》

（教技厅函〔2016〕37号，以下简称《项目管理办法》）和《教育信息化专项资金管理办法》（教财厅函〔2016〕38号，以下简称《资金管理办法》），制定本细则。

第二条 本细则所称子项目是指使用中央财政“教育信息化专项”资金建设、运维，通过互联网提供服务，支持教育部本级管理核心工作的教育业务管理信息系统（以下简称信息系统）项目。不在互联网运行的信息系统，管理办法由相关单位另行制定。

第三条 子项目建设、运维坚持“统筹规划、有限目标；分工协作、需求首责；集成共享、安全可靠；服务业务、绩效考评”原则。

第二章 组织管理

第四条 教育部网络安全和信息化领导小组办公室（挂靠科技司，以下简称教育部网信办）是子项目组织单位，负责总体规划、统筹协调及子项目立项、验收与资金需求管理等。具体包括：研究制定子项目建设总体规划、组织审定信息系统总体运维规划；组织子项目需求建议征集与综合评审，组织子项目建设方案综合评审，批复子项目预立项和正式立项，组织子项目的项目验收；组织子项目所需工程监理服务；协助财务司组织子项目预算申报等。

第五条 部内司局、直属单位（以下简称业务单位）是子项目的责任单位和子项目建设形成的信息系统的主管单位，在信息系统全生命周期内（从需求提出到停止使用）对信息系统的需求、建设、预算、运维、安全、应用及数据管理等工作负首要责任。具体包括：提出需

求建议，组织编制建设方案、系统开发服务招标、第三方测试、安全等级保护定级备案和测评整改、上线评估、部署和试运行、自验收；提出子项目的项目验收申请，接受项目验收，负责验收通过后信息系统正式运行、应用实施和维护的组织管理；制定子项目预算、负责预算执行、接受相关审计等。

第六条 教育部教育管理信息中心（以下简称信息中心）是子项目的技术管理、支撑服务单位和信息系统公共支撑环境的建设、运维单位，也是信息系统的运维服务单位。具体职责包括：负责信息系统公共支撑硬件、软件环境的建设与运维；负责信息系统的系统集成（包括门户集成和数据集成），负责统一门户和基础数据库的建设、运行与维护，实现信息系统间数据共享和互联互通；负责制定子项目建设、集成、运维的技术标准规范，信息系统总体运维规划，提供运行支撑服务；为业务单位提供技术支持、协助进行技术管理与建设方案编制；协助业务单位组织开展子项目第三方测试；参与子项目需求建议综合评审、建设方案综合评审和验收等工作。

第七条 教育部密码工作领导小组办公室是子项目商用密码的统筹和管理单位，负责商用密码在子项目中的应用、推广，对子项目涉及商用密码的环节进行审核，参与子项目建设方案综合评审、使用商用密码子项目的验收等工作。

第八条 发展规划司是子项目数据的统筹管理单位，负责制定数据管理办法，统筹协调子项目数据的采集、存储、共享、公开和安全等

工作，并对有关工作内容进行审核，参与子项目需求建议的综合评审、建设方案综合评审和验收等工作。

第九条 财务司是子项目预算资金的管理单位，按照《资金管理办法》规定对子项目经费进行管理，参与子项目需求建议的综合评审、建设方案综合评审、验收等工作。

第十条 教育管理信息化专家组是子项目专家咨询机构，受教育部网信办委托，对子项目建设总体规划、信息系统总体运维规划、信息系统管理及技术规范等提出意见建议，负责子项目立项、建设、验收过程有关专家评审等工作。

第十一条 子项目建设实行监理制度。子项目监理主要负责协助业务单位对信息系统建设的质量、进度和投资进行监督，对子项目合同和文档资料进行管理，并协调有关单位间的工作关系。

第三章 子项目需求确定

第十二条 需求建议征集。每年 1 月，教育部网信办研究提出子项目年度重点支持范围，报教育部网络安全和信息化领导小组（以下简称教育部网信领导小组）审定同意后，发布子项目需求建议征集通知。

第十三 条需求建议提出。每年 2 月，业务单位根据子项目需求建议征集通知，依照子项目需求建议编制要求，在子项目重点支持范围内提出子项目需求建议报教育部网信办。如子项目涉及多个业务单位

的，由参与单位协商确定牵头单位，并由牵头单位提出子项目需求建议。

第十四条 需求建议综合评审。教育部网信办组织相关单位开展子项目需求建议综合评审，主要包括子项目建设的必要性和可行性，数据采集的合规性和必要性等，教育部网信办根据综合评审结果汇总形成子项目支持建议，报教育部网信领导小组审定。

第十五条 子项目预立项。每年 2 月底前，教育部网信办根据教育部网信领导小组审定的子项目支持建议，向相关业务单位下达子项目预立项通知。

第四章 子项目建设方案编制

第十六条 建设方案编制。各业务单位收到预立项通知后，应根据子项目建设方案编制要求和子项目建设技术标准规范，开展详细需求分析，会同信息中心组织相关单位编制子项目建设方案（含投资概算）。重要信息系统的建设方案必须将国产密码应用纳入整体规划，同时按照《教育行业信息系统安全等级保护定级工作指南》（教技厅函〔2014〕74 号）等文件要求，完成信息系统安全等级保护自主定级和专家评审，并于 4 月底前将建设方案正式函报教育部网信办。

第十七条 建设方案综合评审。教育部网信办收到业务单位报来的建设方案后，组织相关单位对建设方案进行初审，审核内容包括：业务需求的确定性，数据采集、存储、共享、公开和安全管理等的合规性、必要性，商用密码应用的合规性，系统集成方案的合规性、可行

性，系统安全方案的合规性，系统所采用技术标准和规范的科学性，技术方案的可行性，预算的合理性等。教育部网信办将各单位意见汇总后反馈业务单位，业务单位根据初审意见修改建设方案，并于15个工作日内重新提交教育部网信办。每年5月底前，教育部网信办组织相关单位及专家对重新提交的建设方案进行会议评审，形成终审意见。终审未通过的子项目，本年度不纳入教育部预算申请方案。

第十八条 第三方造价评估。建设方案审核通过后，业务单位需招标或委托具有相关专业资质的第三方组织开展第三方造价评估，形成评估报告，并根据造价评估报告修改建设方案的投资概算部分，形成最终建设方案。

第五章 子项目立项

第十九条 子项目预算申报。每年6月底前，业务单位需将最终建设方案及子项目计划任务书（含分年预算安排）一并提交教育部网信办。教育部网信办综合延续性子项目，汇总形成下一年度子项目及预算安排方案，报教育部网信领导小组审定后送财务司。

第二十条 子项目立项。财政部批复预算后，财务司按《资金管理办法》下达预算资金，同时函告教育部网信办。部网信办接财务司子项目年度预算批复通知后，向获得年度财政预算的业务单位下达子项目正式立项通知。未获得年度财政预算的子项目本年度暂不正式立项。

第二十一条 子项目年度实施计划书编制。子项目年度预算批复下达后，业务单位根据财政批复年度预算数，编制子项目年度实施计划书，报财务司、教育部网信办备案。

第六章 子项目过程管理

第二十二条 项目监理与技术助理入场。子项目正式立项后，教育部网信办向各子项目派驻项目监理，协助业务单位开展项目管理有关工作；信息中心向子项目派驻技术助理，协助业务单位完成子项目的技术管理工作，并负责组织信息系统的系统集成等工作。

第二十三条 系统开发服务采购。项目监理与技术助理入场后，业务单位即可根据《项目管理办法》和《资金管理办法》的规定实施子项目系统开发服务政府采购。采购合同签订后，合同文本及附件应报教育部网信办备案并抄送信息中心，作为子项目项目验收、绩效考核和公共软硬件支撑环境建设的重要依据。

第二十四条 合同款拨付。为保证子项目实施进度与质量，系统开发服务合同款可参照以下方式进行拨付：签订合同时拨付总金额的20%、详细设计方案确认后拨付总金额的30%、上线评估通过后拨付总金额的30%、完成自验收后拨付总金额的20%。为保证三年维保服务质量，建议业务单位在上线评估完成后，要求系统开发单位出具合同总金额10%的履约保函。

第二十五条 信息系统第三方测试。信息系统开发完成后，业务单位会同信息中心组织开展第三方测试。测试内容应包括功能测试、性能测试、安全测试和集成测试等。

第二十六条 信息系统安全等级保护定级备案和测评整改。信息系统第三方测试完成后，业务单位应完成信息系统安全等级保护备案和测评整改工作。

第二十七条 信息系统上线自评估。信息系统第三方测试、安全等级保护备案和测评整改完成后，业务单位应对信息系统的功能实现情况进行评估，并组织信息中心对系统集成、运行安全等情况进行评估。

第二十八条 信息系统部署及试运行。信息系统上线自评估通过后，业务单位向信息中心提出试运行申请，开展信息系统部署和试运行工作，同时将评估报告报教育部网信办备案。信息系统试运行时间一般不得少于 6 个月。试运行结束后，业务单位提交用户报告，说明信息系统使用情况；信息中心出具试运行报告，说明信息系统是否符合正式运行的技术要求。用户报告和试运行报告是子项目验收的必要材料。

第七章 子项目验收

第二十九条 子项目验收。子项目验收工作包括自验收和项目验收两个阶段。自验收由业务单位自行组织，应在信息系统试运行结束后的 20 个工作日内完成。项目验收由教育部网信办组织，在自验收完

成 20 个工作日内，由业务单位向教育部网信办提出验收申请，同时提交子项目验收材料。教育部网信办在收到验收申请后 20 个工作日内组织完成子项目的项目验收。子项目项目验收通过后方可正式运行。

第三十条 子项目延期验收。对无法按项目执行期完成项目验收的子项目，业务单位应向教育部网信办提交项目延期申请。经同意后，业务单位继续组织子项目实施；延期时间原则上不得超过一年。

第三十一条 子项目实施终止。子项目因故无法实施，业务单位应及时总结子项目执行情况，严格按照相关要求清理账目和资产，编制资金决算及资产清单，形成子项目终止报告，经分管部领导同意后，报教育部网信办、财务司。

第八章 附 则

第三十二条 根据本细则的有关规定，教育部网信办组织制定相应的工作流程和规范。

第三十三条 本细则由教育部网信办负责解释与修订。

第三十四条 本细则自公布之日起实施。

信息安全等级保护备案实施细则

(公信安〔2007〕1360号)

第一条 为加强和指导信息安全等级保护备案工作，规范备案受理、审核和管理等工作，根据《信息安全等级保护管理办法》制定本实施细则。

第二条 本细则适用于非涉及国家秘密的第二级以上信息系统的备案。

第三条 地市级以上公安机关公共信息网络安全监察部门受理本辖区内备案单位的备案。隶属于省级的备案单位，其跨地（市）联网运行的信息系统，由省级公安机关公共信息网络安全监察部门受理备案。

第四条 隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由公安部公共信息网络安全监察局受理备案，其他信息系统由北京市公安局公共信息网络安全监察部门受理备案。

隶属于中央的非在京单位的信息系统，由当地省级公安机关公共信息网络安全监察部门（或其指定的地市级公安机关公共信息网络安全监察部门）受理备案。

跨省或者全国统一联网运行并由主管部门统一定级的信息系统在各地运行、应用的分支系统（包括由上级主管部门定级，在当地有应

用的信息系统），由所在地地市级以上公安机关公共信息网络安全监察部门受理备案。

第五条 受理备案的公安机关公共信息网络安全监察部门应该设立专门的备案窗口，配备必要的设备和警力，专门负责受理备案工作，受理备案地点、时间、联系人和联系方式等应向社会公布。

第六条 信息系统运营、使用单位或者其主管部门（以下简称“备案单位”）应当在信息系统安全保护等级确定后 30 日内，到公安机关公共信息网络安全监察部门办理备案手续。办理备案手续时，应当首先到公安机关指定的网址下载并填写备案表，准备好备案文件，然后到指定的地点备案。

第七条 备案时应当提交《信息系统安全等级保护备案表》（以下简称《备案表》）（一式两份）及其电子文档。第二级以上信息系统备案时需提交《备案表》中的表一、二、三；第三级以上信息系统还应当在系统整改、测评完成后 30 日内提交《备案表》表四及其有关材料。

第八条 公安机关公共信息网络安全监察部门收到备案单位提交的备案材料后，对属于本级公安机关受理范围且备案材料齐全的，应当向备案单位出具《信息系统安全等级保护备案材料接收回执》；备案材料不齐全的，应当当场或者在五日内一次性告知其补正内容；对不属于本级公安机关受理范围的，应当书面告知备案单位到有管辖权的公安机关办理。

第九条 接收备案材料后，公安机关公共信息网络安全监察部门应当对下列内容进行审核:

（一）备案材料填写是否完整，是否符合要求，其纸质材料和电子文档是否一致;

（二）信息系统所定安全保护等级是否准确。

第十条 经审核，对符合等级保护要求的，公安机关公共信息网络安全监察部门应当自收到备案材料之日起的十个工作日内，将加盖本级公安机关印章（或等级保护专用章）的《备案表》一份反馈备案单位，一份存档；对不符合等级保护要求的，公安机关公共信息网络安全监察部门应当在十个工作日内通知备案单位进行整改，并出具《信息系统安全等级保护备案审核结果通知》。

第十一条 《备案表》中表一、表二、表三内容经审核合格的，公安机关公共信息网络安全监察部门应当出具《信息系统安全等级保护备案证明》（以下简称《备案证明》）。《备案证明》由公安部统一监制。

第十二条 公安机关公共信息网络安全监察部门对定级不准的备案单位，在通知整改的同时，应当建议备案单位组织专家进行重新定级评审，并报上级主管部门审批。

备案单位仍然坚持原定等级的，公安机关公共信息网络安全监察部门可以受理其备案，但应当书面告知其承担由此引发的责任和后果，经上级公安机关公共信息网络安全监察部门同意后，同时通报备案单位上级主管部门。

第十三条 对拒不备案的，公安机关应当依据《中华人民共和国计算机信息系统安全保护条例》等其他有关法律、法规规定，责令限期整改。逾期仍不备案的，予以警告，并向其上级主管部门通报。

依照前款规定向中央和国家机关通报的，应当报经公安部公共信息网络安全监察局同意。

第十四条 受理备案的公安机关公共信息网络安全监察部门应当及时将备案文件录入到数据库管理系统，并定期逐级上传《备案表》中表一、表二、表三内容的电子数据。上传时间为每季度的第一天。

受理备案的公安机关公共信息网络安全监察部门应当建立管理制度，对备案材料按照等级进行严格管理，严格遵守保密制度，未经批准不得对外提供查询。

第十五条 公安机关公共信息网络安全监察部门受理备案时不得收取任何费用。

第十六条 本细则所称“以上”包含本数（级）。

第十七条 各省（区、市）公安机关公共信息网络安全监察部门可以依据本细则制定具体的备案工作规范，并报公安部公共信息网络安全监察局备案。

信息安全等级保护管理办法

(公通字〔2007〕43号)

第一章 总则

第一条 为规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规，制定本办法。

第二条 国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

第三条 公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

第四条 信息系统主管部门应当依照本办法及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

第五条 信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。

第二章 等级划分与保护

第六条 国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

第七条 信息系统的安全保护等级分为以下五级:

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第八条 信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级，信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级，信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

第三章 等级保护的实施与管理

第九条 信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。

第十条 信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。有主管部门的，应当经主管部门审核批准。

跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。

对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。

第十一条 信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

第十二条 在信息系统建设过程中，运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）、《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）、《信息安全技术数据库管理系统安全技术要求》（GB/T20273-2006）、《信息安全技术 服务器技术要求》、《信息安全技术终端计算机系统安全等级技术要求》（GA/T671-2006）等技术标准同步建设符合该等级要求的信息安全设施。

第十三条 运营、使用单位应当参照《信息安全技术 信息系统安全管理要求》（GB/T20269-2006）、《信息安全技术信息系统安全工程管理要求》（GB/T20282-2006）、《信息系统安全等级保护基本要求》等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。

第十四条 信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。

第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。

信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据特殊安全需求进行自查。

经测评或者自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

第十五条 已运营（运行）的第二级以上信息系统，应当在安全保护等级确定后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

新建第二级以上信息系统，应当在投入运行后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。

第十六条 办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料:

（一）系统拓扑结构及说明;

（二）系统安全组织机构和管理制度;

（三）系统安全保护设施设计实施方案或者改建实施方案;

（四）系统使用的信息安全产品清单及其认证、销售许可证明;

（五）测评后符合系统安全保护等级的技术检测评估报告;

（六）信息系统安全保护等级专家评审意见;

（七）主管部门审核批准信息系统安全保护等级的意见。

第十七条 信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，应当在收到备案材料之日起的 10 个工作日内颁发信息系统安全等级保护备案证明；发现不符合本办法及有关标准的，应当在收到备案材料之日起的 10 个工作日内通知备案单位予以纠正；发现定级不准的，应当在收到备案材料之日起的 10 个工作日内通知备案单位重新审核确定。

运营、使用单位或者主管部门重新确定信息系统等级后，应当按照本办法向公安机关重新备案。

第十八条 受理备案的公安机关应当对第三级、第四级信息系统的运营、使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次，对第四级信息系统每半年至少检查一次。对跨省或者全国统一联网运行的信息系统的检查，应当会同其主管部门进行。

对第五级信息系统，应当由国家指定的专门部门进行检查。

公安机关、国家指定的专门部门应当对下列事项进行检查:

（一）信息系统安全需求是否发生变化，原定保护等级是否准确;

（二）运营、使用单位安全管理制度、措施的落实情况;

（三）运营、使用单位及其主管部门对信息系统安全状况的检查情况;

（四）系统安全等级测评是否符合要求;

（五）信息安全产品使用是否符合要求;

（六）信息系统安全整改情况;

（七）备案材料与运营、使用单位、信息系统的符合情况;

（八）其他应当进行监督检查的事项。

第十九条 信息系统运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导，如实向公安机关、国家指定的专门部门提供下列有关信息安全保护的信息资料及数据文件:

（一）信息系统备案事项变更情况;

（二）安全组织、人员的变动情况;

（三）信息安全管理制度、措施变更情况;

（四）信息系统运行状况记录;

（五）运营、使用单位及主管部门定期对信息系统安全状况的检查记录;

（六）对信息系统开展等级测评的技术测评报告;

（七）信息安全产品使用的变更情况;

（八）信息安全事件应急预案，信息安全事件应急处置结果报告;

（九）信息系统安全建设、整改结果报告。

第二十条 公安机关检查发现信息系统安全保护状况不符合信息安全等级保护有关管理规范和技术标准的，应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求，按照管理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案。必要时，公安机关可以对整改情况组织检查。

第二十一条 第三级以上信息系统应当选择使用符合以下条件的信息安全产品：

（一）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；

（二）产品的核心技术、关键部件具有我国自主知识产权；

（三）产品研制、生产单位及其主要业务、技术人员无犯罪记录；

（四）产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；

（五）对国家安全、社会秩序、公共利益不构成危害；

（六）对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

第二十二条 第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：

（一）在中华人民共和国境内注册成立（港澳台地区除外）；

（二）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

（三）从事相关检测评估工作两年以上，无违法记录；

（四）工作人员仅限于中国公民;

（五）法人及主要业务、技术人员无犯罪记录;

（六）使用的技术装备、设施应当符合本办法对信息安全产品的要求;

（七）具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度;

（八）对国家安全、社会秩序、公共利益不构成威胁。

第二十三条 从事信息系统安全等级测评的机构，应当履行下列义务:

（一）遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果;

（二）保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险;

（三）对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

第四章 涉及国家秘密信息系统的分级保护管理

第二十四条 涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。

非涉密信息系统不得处理国家秘密信息。

第二十五条 涉密信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密三个等级。

涉密信息系统建设使用单位应当在信息规范定密的基础上，依据涉密信息系统分级保护管理办法和国家保密标准 BMB17-2006《涉及国家秘密的计算机信息系统分级保护技术要求》确定系统等级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定保护等级。

保密工作部门和机构应当监督指导涉密信息系统建设使用单位准确、合理地进行系统定级。

第二十六条 涉密信息系统建设使用单位应当将涉密信息系统定级和建设使用情况，及时上报业务主管部门的保密工作机构和负责系统审批的保密工作部门备案，并接受保密部门的监督、检查、指导。

第二十七条 涉密信息系统建设使用单位应当选择具有涉密集成资质的单位承担或者参与涉密信息系统的设计与实施。

涉密信息系统建设使用单位应当依据涉密信息系统分级保护管理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。

第二十八条 涉密信息系统使用的信息安全保密产品原则上应当选用国产品，并应当通过国家保密局授权的检测机构依据有关国家保密标准进行的检测，通过检测的产品由国家保密局审核发布目录。

第二十九条 涉密信息系统建设使用单位在系统工程实施结束后，应当向保密工作部门提出申请，由国家保密局授权的系统测评机构依

据国家保密标准 BMB22-2007《涉及国家秘密的计算机信息系统分级保护测评指南》，对涉密信息系统进行安全保密测评。

涉密信息系统建设使用单位在系统投入使用前，应当按照《涉及国家秘密的信息系统审批管理规定》，向设区的市级以上保密工作部门申请进行系统审批，涉密信息系统通过审批后方可投入使用。已投入使用的涉密信息系统，其建设使用单位在按照分级保护要求完成系统整改后，应当向保密工作部门备案。

第三十条 涉密信息系统建设使用单位在申请系统审批或者备案时，应当提交以下材料:

（一）系统设计、实施方案及审查论证意见;

（二）系统承建单位资质证明材料;

（三）系统建设和工程监理情况报告;

（四）系统安全保密检测评估报告;

（五）系统安全保密组织机构和管理制度情况;

（六）其他有关材料。

第三十一条 涉密信息系统发生涉密等级、连接范围、环境设施、主要应用、安全保密管理责任单位变更时，其建设使用单位应当及时向负责审批的保密工作部门报告。保密工作部门应当根据实际情况，决定是否对其重新进行测评和审批。

第三十二条 涉密信息系统建设使用单位应当依据国家保密标准 BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》，加强涉密信息系统运行中的保密管理，定期进行风险评估，消除泄密隐患和漏洞。

第三十三条 国家和地方各级保密工作部门依法对各地区、各部门涉密信息系统分级保护工作实施监督管理，并做好以下工作:

（一）指导、监督和检查分级保护工作的开展;

（二）指导涉密信息系统建设使用单位规范信息定密，合理确定系统保护等级;

（三）参与涉密信息系统分级保护方案论证，指导建设使用单位做好保密设施的同步规划设计;

（四）依法对涉密信息系统集成资质单位进行监督管理;

（五）严格进行系统测评和审批工作，监督检查涉密信息系统建设使用单位分级保护管理制度和技术措施的落实情况;

（六）加强涉密信息系统运行中的保密监督检查。对秘密级、机密级信息系统每两年至少进行一次保密检查或者系统测评，对绝密级信息系统每年至少进行一次保密检查或者系统测评;

（七）了解掌握各级各类涉密信息系统的管理使用情况，及时发现和查处各种违规违法行为和泄密事件。

第五章 信息安全等级保护的密码管理

第三十四条 国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度，被保护对象的安全防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。

信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

第三十五条 信息系统安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。

第三十六条 信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码管理局审批，密码的设计、实施、使用、运行维护和日常管理等，应当按照国家密码管理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码管理 例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码管理机构备案。

第三十七条 运用密码技术对信息系统进行系统等级保护建设和整改的，必须采用经国家密码管理部门批准使用或者准于销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

第三十八条 信息系统中的密码及密码设备的测评工作由国家密码管理局认可的测评机构承担，其他任何部门、单位和个人不得对密码进行评测和监控。

第三十九条 各级密码管理部门可以定期或者不定期对信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评，对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和

测评。在监督检查过程中，发现存在安全隐患或者违反密码管理相关规定或者未达到密码相关标准要求的，应当按照国家密码管理的相关规定进行处置。

第六章 法律责任

第四十条 第三级以上信息系统运营、使用单位违反本办法规定，有下列行为之一的，由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，并及时反馈处理结果：

（一）未按本办法规定备案、审批的；

（二）未按本办法规定落实安全管理制度、措施的；

（三）未按本办法规定开展系统安全状况检查的；

（四）未按本办法规定开展系统安全技术测评的；

（五）接到整改通知后，拒不整改的；

（六）未按本办法规定选择使用信息安全产品和测评机构的；

（七）未按本办法规定如实提供有关文件和证明材料的；

（八）违反保密管理规定的；

（九）违反密码管理规定的；

（十）违反本办法其他规定的。

违反前款规定，造成严重损害的，由相关部门依照有关法律、法规予以处理。

第四十一 信息安全监管部门及其工作人员在履行监督管理职责中，玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第七章 附则

第四十二 已运行信息系统的运营、使用单位自本办法施行之日起180日内确定信息系统的安全保护等级；新建信息系统在设计、规划阶段确定安全保护等级。

第四十三 本办法所称“以上”包含本数（级）。

第四十四 本办法自发布之日起施行，《信息安全等级保护管理办法（试行）》（公通字[2006]7号）同时废止。

关于信息安全等级保护工作的实施意见

(公通字〔2004〕66 号)

信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。实行信息安全等级保护制度，能够充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到有效保护的目的，增强安全保护的整体性、针对性和实效性，使信息系统安全建设更加突出重点、统一规范、科学合理，对促进我国信息安全的发展将起到重要推动作用。

为了进一步提高信息安全的保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

一、开展信息安全等级保护工作的重要意义

近年来，党中央、国务院高度重视，各有关方面协调配合、共同努力，我国信息安全保障工作取得了很大进展。但是从总体上看，我国的信息安全保障工作尚处于起步阶段，基础薄弱，水平不高，存在以下突出问题：信息安全意识和安全防范能力薄弱，信息安全滞后于信息化发展；信息系统安全建设和管理的目标不明确；信息安全保障工作的重点不突出；信息安全监督管理缺乏依据和标准，监管措施有待到位，监管体系尚待完善。随着信息技术的高速发展和网络应用的迅速普及，我国国民经济和社会信息化进程全面加快，信息系统的基础性、全局性作用日益增强，信息资源已经成为国家经济建设和社会发展的重要战略资源之一。保障信息安全，维护国家安全、公共利益和社会稳定，是当前信息化发展中迫切需要解决的重大问题。

实施信息安全等级保护，能够有效地提高我国信息和信息系统安全建设的整体水平，有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调；有利于为信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务，有效控制信息安全建设成本；有利于优化信息安全资源的配置，对信息系统分级实施保护，重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全；有利于明确国家、法人和其他组织、公民的信息安全责任，加强信息安全管理；有利于推动信息安全产业的发展，逐步探索出一条适应社会主义市场经济发展的信息安全模式。

二、信息安全等级保护制度的原则

信息安全等级保护的核心是对信息安全分等级、按标准进行建设、管理和监督。信息安全等级保护制度遵循以下基本原则:

（一）明确责任，共同保护。通过等级保护，组织和动员国家、法人和其他组织、公民共同参与信息安全保护工作; 各方主体按照规范和标准分别承担相应的、明确具体的信息安全保护责任。

（二）依照标准，自行保护。国家运用强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行定级、自行保护。

（三）同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相适应。因信息和信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

（四）指导监督，重点保护。国家指定信息安全监管职能部门通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。国家重点保护涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统，主要包括: 国家事务处理信息系统（党政机关办公系统）; 财政、金融、税务、海关、审计、工商、社会保障、能源、交通运输、国防工业等关系到国计民生的信息系统; 教育、国家科研等单位的信息系统; 公用通信、广播电视传输等基础信

息网络中的信息系统；网络管理中心、重要网站中的重要信息系统和其他领域的重要信息系统。

三、信息安全等级保护制度的基本内容

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

信息系统是指由计算机及其相关和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。

根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度；遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；针对信息的保密性、完整性和可用性要求及信息系统必须要达到的基本的安全保护水平等因素，信息和信息系统的安全保护等级共分五级：

1.第一级为自主保护级，适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益。

2.第二级为指导保护级，适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害。

3. 第三级为监督保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害。

4. 第四级为强制保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害。

5. 第五级为专控保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。

国家通过制定统一的管理规范和技术标准，组织行政机关、公民、法人和其他组织根据信息和信息系统的不同重要程度开展有针对性的保护工作。国家对不同安全保护级别的信息和信息系统实行不同强度的监管政策。第一级依照国家管理规范和技术标准进行自主保护；第二级在信息安全监管职能部门指导下依照国家管理规范和技术标准进行自主保护；第三级依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行监督、检查；第四级依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行强制监督、检查；第五级依照国家管理规范和技术标准进行自主保护，国家指定专门部门、专门机构进行专门监督。

国家对信息安全产品的使用实行分等级管理。

信息安全事件实行分等级响应、处置的制度。依据信息安全事件对信息和信息系统的破坏程度、所造成的社会影响以及涉及的范围，确定

事件等级。根据不同安全保护等级的信息系统中发生的不同等级事件制定相应的预案，确定事件响应和处置的范围、程度以及适用的管理制度等。信息安全事件发生后，分等级按照预案响应和处置。

四、信息安全等级保护工作职责分工

公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。

在信息安全等级保护工作中，涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。

信息和信息系统的主管部门及运营、使用单位按照等级保护的管理规范和技术标准进行信息安全建设和管理。

国务院信息化工作办公室负责信息安全等级保护工作中部门间的协调。

五、实施信息安全等级保护工作的要求

信息安全等级保护工作要突出重点、分级负责、分类指导、分步实施，按照谁主管谁负责、谁运营谁负责的要求，明确主管部门以及信息系统建设、运行、维护、使用单位和个人的安全责任，分别落实等级保护措施。实施信息安全等级保护应当做好以下六个方面工作:

（一）完善标准，分类指导。制定系统完整的信息安全等级保护管理规范和技术标准，并根据工作开展的实际情况不断补充完善。信息安

全监管职能部门对不同重要程度的信息和信息系统的安全等级保护工作给予相应的指导，确保等级保护工作顺利开展。

（二）科学定级，严格备案。信息和信息系统的运营、使用单位按照等级保护的管理规范和技术标准，确定其信息和信息系统的安全保护等级，并报其主管部门审批同意。

对于包含多个子系统的信息系统，在保障信息系统安全互联和有效信息共享的前提下，应当根据等级保护的管理规定、技术标准和信息系统内各子系统的重要程度，分别确定安全保护等级。跨地域的大系统实行纵向保护和属地保护相结合的方式。

国务院信息化工作办公室组织国内有关信息安全专家成立信息安全保护等级专家评审委员会。重要的信息和信息系统的运营、使用单位及其主管部门在确定信息和信息系统的安全保护等级时，应请信息安全保护等级专家评审委员会给予咨询评审。

安全保护等级在三级以上的信息系统，由运营、使用单位报送本地区地市级公安机关备案。跨地域的信息系统由其主管部门向其所在地的同级公安机关进行总备案，分系统分别由当地运营、使用单位向本地地市级公安机关备案。

信息安全产品使用的分等级管理以及信息安全事件分等级响应、处置的管理办法由公安部会同保密局、国密办、信息产业部和认监委等部门制定。

（三）建设整改，落实措施。对已有的信息系统，其运营、使用单位根据已经确定的信息安全保护等级，按照等级保护的管理规范和技

术标准，采购和使用相应等级的信息安全产品，建设安全设施，落实安全技术措施，完成系统整改。对新建、改建、扩建的信息系统应当按照等级保护的管理规范和技术标准进行信息系统的规划设计、建设施工。

（四）自查自纠，落实要求。信息和信息系统的运营、使用单位及其主管部门按照等级保护的管理规范和技术标准，对已经完成安全等级保护建设的信息系统进行检查评估，发现问题及时整改，加强和完善自身信息安全等级保护制度的建设，加强自我保护。

（五）建立制度，加强管理。信息和信息系统的运营、使用单位按照与本系统安全保护等级相对应的管理规范和技术标准的要求，定期进行安全状况检测评估，及时消除安全隐患和漏洞，建立安全制度，制定不同等级信息安全事件的响应、处置预案，加强信息系统的安全管理。信息和信息系统的主管部门应当按照等级保护的管理规范和技术标准的要求做好监督管理工作，发现问题，及时督促整改。

（六）监督检查，完善保护。公安机关按照等级保护的管理规范和技术标准的要求，重点对第三、第四级信息和信息系统的安全等级保护状况进行监督检查。发现确定的安全保护等级不符合等级保护的管理规范和技术标准的，要通知信息和信息系统的主管部门及运营、使用单位进行整改；发现存在安全隐患或未达到等级保护的管理规范和技术标准要求的，要限期整改，使信息和信息系统的安全保护措施更加完善。对信息系统中使用的信息安全产品的等级进行监督检查。

对第五级信息和信息系统的监督检查，由国家指定的专门部门、专门机构按照有关规定进行。

国家保密工作部门、密码管理部门以及其他职能部门按照职责分工指导、监督、检查。

六、信息安全等级保护工作实施计划

计划用三年左右的时间在全国范围内分三个阶段实施信息安全等级保护制度。

（一）准备阶段。为了保障信息安全等级保护制度的顺利实施，在全面实施等级保护制度之前，用一年左右的时间做好下列准备工作:

1.加强领导，落实责任。在国家网络与信息安全协调小组的领导下，地方各级人民政府、信息安全监管职能部门、信息系统的主管部门和运营、使用单位要明确各自的安全责任，建立协调配合机制，分别制定详细的实施方案，积极推进信息安全等级保护制度的建立，推动信息安全管理运行机制的建立和完善。

2.加快完善法律法规和标准体系。法律规范和技术标准是推广和实施信息安全等级保护工作的法律依据和技术保障。为此，《信息安全等级保护管理办法》和《信息安全等级保护实施指南》、《信息安全等级保护评估指南》等法规、规范要加紧制定，尽快出台。

加快信息安全等级保护管理与技术标准的制定和完善，其他现行的相关标准规范中与等级保护管理规范和技术标准不相适应的，应当进行调整。

3.建设信息安全等级保护监督管理队伍和技术支撑体系。信息安全监管职能部门要建立专门的信息安全等级保护监督检查机构，充实力

量，加强建设，抓紧培训，使监督检查人员能够全面掌握信息安全等级保护相关法律规范和管理规范及技术标准，熟练运用技术工具，切实承担信息安全等级保护的指导、监督、检查职责。同时，还要建立信息安全等级保护监督、检查工作的技术支撑体系，组织研制、开发科学、实用的检查、评估工具。

4.进一步做好等级保护试点工作。选择电子政务、电子商务以及其他方面的重点单位开展等级保护试点工作，并在试点工作的基础上进一步完善等级保护实施指南等相关的配套规范、标准和工具，积累信息安全等级保护工作实施的方法和经验。

5.加强宣传、培训工作。地方各级人民政府、信息安全监管职能部门和信息系统的主管部门要积极宣传信息安全等级保护的相关法规、标准和政策，组织开展相关培训，提高对信息安全等级保护工作的认识和重视，积极推动各有关部门、单位做好开展信息安全等级保护工作的前期准备。

（二）重点实行阶段。在做好前期准备工作的基础上，用一年左右的时间，在国家重点保护的涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统中实行等级保护制度。经过一年的建设，使基础信息网络和重要信息系统的核心要害部位得到有效保护，涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统的保护状况得到较大改善，结束目前基本没有保护措施或保护措施不到位的状况。

在工作中，如发现等级保护的管理规范和技术标准以及检查评估工具等存在问题，及时组织有关部门进行调整和修订。

（三）全面实行阶段。在试行工作的基础上，用一年左右的时间，在全国全面推行信息安全等级保护制度。已经实施等级保护制度的信息和信息系统的运营、使用单位及其主管部门，要进一步完善信息安全保护措施。没有实施等级保护制度的，要按照等级保护的管理规范和技术标准认真组织落实。

经过三年的努力，逐步将信息安全等级保护制度落实到信息安全规划、建设、评估、运行维护等各个环节，使我国信息安全保障状况得到基本改善。

二、学校相关政策文件

中国地质大学学校办公室文件

地大学校办发〔2022〕49号

中国地质大学（武汉）学校办公室
关于印发《校园网络设施建设与管理办法
（试行）》的通知

各单位:

现将《中国地质大学（武汉）校园网络设施建设与管理办法（试行）》印发给你们，请认真执行。

中国地质大学（武汉）学校办公室

2022年10月9日

中国地质大学（武汉）
校园网络设施建设与管理办法（试行）

第一章　总　则

第一条　为进一步规范校园网络设施的统筹建设和规范管理，避免重复建设和浪费，确保建设和管理工作协调有序进行，推动信息化工作科学发展，根据国家有关规定，结合学校实际，制定本办法。

第二条　本办法所称校园网络设施由校园网络与网络配套设施组成。校园网络指学校校园内由学校管理的用于向师生提供网络服务的有线网口、无线访问接入点（AP）、交换机、通信线缆等计算机网络设备和线路等；网络配套设施指与校园网络配套的设备用房和通信管道（孔）等。

第三条　校园网络设施实行统筹规划、统一建设和统一管理。

第二章　职责分工

第四条　信息化工作办公室是校园网络设施总体统筹单位。负责校园网络设施的标准制定和技术支撑；参与校园网络设施建设过程的方案设计、材料选型定样、材料进场验收送检、施工过程监督、竣工验收等全部过程；负责校园网络的建设和管理的规划和协调；负责协调电信运营商开展互联网业务的建设和管理。

第五条　学校基本建设管理部门（校园规划与基建处、新

校区建设指挥部等）是校园网络设施建设的主体单位。负责校园公共区域通信管道(孔)的综合布线布局规划、施工建设和协调，负责新建和扩建楼宇与区域的通信管道(孔)、设备用房和综合布线的设计和施工建设；单独实施的校园网络改造工程原则上由信息化工作办公室牵头实施。校园网络设施的实施方案、技术图纸等资料同时报学校基本建设管理部门和信息化工作办公室备案。

第六条 后勤保障部是南望山校区网络配套设施管理的主体单位，未来城校区管理办公室是未来城校区网络配套设施管理的主体单位。

第七条 各单位根据本单位职责，协同做好校园网络设施的相关管理工作。

第三章 校园网络建设和管理

第八条 校园网络建设按照规定流程进行管理。建设单位将综合布线设计及实施方案提交信息化工作办公室审查，经批准后方可施工；校园网络建设所采用的设备及材料，须符合国家相关质量标准，施工方需将设备性能报告、工程材料（线材、模块、面板等）样品及检测报告等提交信息化工作办公室核验；工程竣工并验收合格后，向信息化工作办公室和学校基本建设单位提交施工图纸、测试报告和验收资料等书面文档，并按照档案管理要求进行资料归档，相应资产向信息化工作办公室移交。

第九条 校园网络建设涉及保密区域、单位和人员的，同时报学校保密办公室审批。

第十条 校园网络实行分级管理。校园网络所用的网络设备（包括交换机、路由器、机柜、接口模块、无线 AP 等）和线路（包括光纤、双绞线、跳线等）由信息化工作办公室负责管理和维护，其他单位和个人不得私自进行配置和调整；接入校园网的用户设备和线路，由各使用单位及个人自行管理和维护。

第十一条 任何单位和个人用户不得更改校园网网络线路，不得自行接入网络交换设备，所有接入端口仅供端口所在房间的末端设备接入。

第十二条 所有接入校园网络的交换设备须符合校园网络管理规定，以确保网络稳定畅通。对于接入校园网络的所有网络设备，不论产权归属，信息化工作办公室均具有配置管理权限。

第四章 网络配套设施建设和管理

第十三条 网络配套设施在建设和使用中实施集约化建设原则，具备共建、共享条件的，原则上不再新建。校内外各单位因学校师生业务服务需要，需在校内新建通信管道(孔)和网络机房等网络配套设施的，必须向信息化工作办公室提交需求申请报告及设计方案，由信息化工作办公室进行技术论证和审核，提交学校基本建设管理部门批准后，方可进行施工建设。

第十四条 校内室外公共区域应建设地下综合管沟或专用管道连接各个楼宇，每幢楼宇都应配置独立的设备间和网络布线桥架等设施。新建区域由学校基本建设管理部门在规划设计中落实，已建区域由学校基本建设管理部门在改造调整中逐步落实。

第十五条 网络配套设施管理单位负有消防和安防等管理责任，保证设备运行环境的安全、整洁和通风，设备间不得挪作它用。

第十六条 校内各类网络配套设施均为学校资产，校内外各单位需要使用上述资产必须按程序提交申请，由信息化工作办公室作技术方案审核、后勤保障部或未来城校区管理办公室审批，任何单位和个人不得私自使用。校外单位如需使用，需按规定签订合同并缴纳相应费用。

第五章 附 则

第十七条 本办法由信息化工作办公室负责解释，自发布之日起施行。

中国地质大学（武汉）学校办公室 2022年10月9日印发

中国地质大学学校办公室文件

地大学校办发〔2022〕53号

中国地质大学（武汉）学校办公室
关于印发《网络安全和信息化工作
管理办法》的通知

各单位:

现将《中国地质大学（武汉）网络安全与信息化工作管理办法》印发给你们，请认真执行。

中国地质大学（武汉）学校办公室

2022年11月8日

中国地质大学（武汉）
网络安全和信息化工作管理办法

第一章　总　则

第一条　为进一步加强和规范学校网络安全和信息化工作，全面提高学校网络安全和信息化工作水平，促进学校网络安全和信息化工作可持续发展，确保学校网络安全和信息化工作科学、规范、合理、有序推进，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中国教育现代化 2035》等精神结合学校实际，制定本办法。

第二条　学校网络安全和信息化工作涵盖全校信息化基础设施（包括但不限于物理环境、网络设备、云计算与存储资源）、信息化资源、应用系统、网络安全等的规划、建设、运行维护、终止的全过程。网络安全和信息化工作目标是构建安全稳定的网络环境，推进信息互通和资源共享，推动学校加速迈向治理现代化和教育现代化，为学校事业改革发展提供全面、高效的网络支撑和信息保障，打造智慧校园。

第三条　网络与信息安全管理遵循“统筹规划、同步建设、集中管理、分级负责”的工作思路，实行“涉密不上网上网不涉密”“谁主管谁负责，谁主办谁负责，谁使用谁负责”的管理原则。

第四条　本办法适用于全校范围内各单位新建、购置的与

网络安全和信息化工作相关的各类设施、设备、数字资源与信息系统等的建设与运行管理，适用于学校所有单位、个人以及使用学校校园网或信息资源的其他单位的人员。

第二章　工作机制和职责分工

第五条　建立健全统筹有力、权责明晰、协同高效的网络安全和信息化工作管理体制，形成学校网络安全和信息化工作领导小组（以下简称网信领导小组）统筹决策、学校网络安全和信息化工作专家组（以下简称网信专家组）技术咨询、网络安全和信息化工作领导小组办公室（以下简称网信办）统一协调、信息化工作办公室（以下简称信息化办）统一管理和统筹推进、各二级单位积极参与和配合、学校数据中心提供统一数据共享、服务大厅提供“一网通办”“一次办好”的网络安全和信息化工作机制。

第六条　网信领导小组统一领导全校网络安全和信息化工作，其主要职责包括:

（一）审定学校网络安全和信息化工作发展战略、重大政策和专项规划;

（二）审定网络安全和信息化工作有关文件规范和技术标准等;

（三）研究学校网络安全和信息化工作中的有关重大事项。

第七条　网信专家组是学校网络安全和信息化工作重要技术问题与专项规划的决策咨询机构，其主要职责包括:

（一）对学校网络安全和信息化工作发展战略、总体规划、专项计划、项目实施等提出政策法规和专业技术方面的咨询意

见;

（二）对学校网络安全和信息化工作中有关重大技术问题提供解决方案、工作建议等方面专业技术咨询。

第八条 网信办是网信领导小组开展工作的执行机构，人员由学校办公室、信息化工作办公室、党委宣传部负责人组成，设在信息化办。其主要职责包括:

（一）协调网络安全和信息化建设工作中需要协调的事项;

（二）协调和督促学校网络安全事件处置，开展网络安全教育活动;

（三）协调与上级单位、主管部门的业务关系，开展对网络安全和信息化工作的指导;

（四）承办网信领导小组交办的其他工作。

第九条 信息化办是学校网络安全和信息化规划设计、统筹建设、管理运维、安全监督的管理部门，也是学校网络安全和信息化工作的技术支持部门。其主要职责包括:

（一）建立和健全学校网络安全和信息化工作的各项管理规章制度;

（二）制定学校网络安全和信息化工作规划、实施方案和标准规范;

（三）负责学校网络安全和信息化工作项目规划、建设、管理、运行维护及技术支持工作;

（四）负责学校涉密信息系统、信息设备和存储设备保密归口管理;

（五）落实国家网络安全等级保护制度工作要求，定期对

校园网络及各级各类信息系统（网站）进行安全检查，发布安全状况评估报告。

第十条 健全和完善职责明确、分工协同的网络安全和信息化工作机制。学校办公室负责信息化建设的联动推进、学校主页规划建设、二级单位网站考评及相关协调工作；党委宣传部负责涉校舆情管理和网络文化建设；安全保卫部负责协助公安机关对网络安全事件调查取证；图书档案与文博部负责数字档案的归档管理；各二级单位负责本单位的网站建设、信息审核发布、业务系统建设与日常运行管理工作。

第十一条 加强网络安全管理，落实信息化日常工作。各二级单位需明确 1 名负责人（处级干部）具体负责本单位网络安全和信息化工作；同时安排 1 名工作人员作为本单位网络安全和信息化工作专员（以下简称网信员），负责本单位信息化基础设施的日常管理，承担本单位相关业务系统及单位网站的规划建设、升级改造、日常维护，保证信息的准确性、实时性、完整性和系统安全。

第三章 网络安全管理

第十二条 学校网络安全管理工作包括信息化基础设施安全、系统安全和数据信息安全。信息化基础设施安全是指校园网络、云资源等基础设施和物理环境的安全；系统安全是指承载信息系统的服务器、软件运行环境以及应用系统的安全；数据信息安全是指各业务系统产生的数据、通过信息服务方式发布的各种信息内容的安全。

第十三条 各单位主要负责人是本单位网络安全和信息化

工作的第一责任人。信息化办保障校园网络和各业务系统的技防安全，定期对校园内各个系统和网站进行安全检测，对存在安全隐患的系统和网站提出整改要求和建议，并提供必要的技术支持，督促整改；各单位负责本单位信息系统和网站的系统安全、数据信息安全，切实做好数据信息日常维护、定期备份和及时归档工作。

第十四条 校园网用户必须遵守国家有关法律法规，不得利用校园网从事违反国家法律法规和学校规章制度的活动。信息化办遵照国家的网络安全管理规定，记录用户上网行为，并配合公安机关要求，提供用户上网记录。

第十五条 校园网用户应妥善保管自己的统一身份认证账号和上网账号，以免造成个人信息泄露，防止他人盗用后在网上从事非法活动。因管理不善导致密码泄露，账号所有者负全部责任，对网络安全造成严重危害的，应追究当事人责任。

第十六条 学校对上网信息实行分级分类审核。学校保密委员会办公室负责对涉密单位网站建设的审查审批；学校办公室、党委宣传部负责审核学校网络平台发布的文件类和宣传报道类信息；各单位主要负责人负责审核本单位的发布信息。重要信息需报分管校领导或主要领导同意，信息审核实施台账管理，未经审核的信息不得擅自在网上发布。对于信息审核不严，造成学校声誉受到影响的单位负责人按学校相关规定实行责任追究。

第四章 信息化基础设施建设与管理

第十七条 校园信息化基础设施是指校园范围内建设的各

类通信管线、管沟、通信电缆光缆、楼内弱电线路机房、网络主机房及各类服务器存储设备、有线无线网络设备、网络接入设备、安防监控设备等。

第十八条 校园信息化基础设施由信息化办、后勤保障部、安全保卫部协同管理。各电信运营商独立或与学校合作建设的设施和设备中数据通信类设施设备由信息化办统一管理，语音通信类设施设备由后勤保障部、未来城校区管理办公室统一管理，安防监控类设施设备由安全保卫部统一管理。

第十九条 为避免重复建设、违规建设，新建、扩建、改建楼宇时或道路、管网、景观、绿化等校园基础设施涉及校园信息化基础设施的工程项目，建设单位应向校园规划委员会报告，批准后方可执行。原则上信息化办应全程参与其前期调研、方案设计、建设实施和工程验收，并就有关事项提出专业指导意见。

第五章 信息化资源管理

第二十条 学校信息化资源包含数字教学资源、数字文献资源、数字博物馆资源、数字档案资源、正版化软件资源、科研资源、文化资源、管理服务资源、业务系统数据及运行数据等，是学校的数据资产，归学校所有。

第二十一条 信息化资源采用集中存储，归口管理。数字教学资源管理及平台建设由本科生院、研究生院、远程与继续教育学院负责，各教学单位、教师参与教学资源内容建设；数字文献资源、数字博物馆资源、数字档案资源管理、平台和内容建设由图书档案与文博部负责，各有关单位参与数字档案资

源内容建设；正版化软件和公共服务性软件资源建设由信息化办负责，专业性软件资源由各业务单位负责；相关业务系统数据及信息资源统一接入学校数据中心，由信息化办负责日常管理，提供统一的数据共享和数据服务。

第二十二条 网信办审批和发布全校唯一的数据标准、信息标准和信息共享、交换及数据服务标准，信息化办负责相关标准的制定、统一管理和规范实施，保障信息化资源的合理配置、有效共享和授权使用。各单位须严格执行学校相关标准，确保数据的唯一性和准确性。

第六章 信息化项目管理

第二十三条 信息化项目包括各类教学、科研、管理及服务工作的信息系统建设，智慧校园公共服务平台的开发和集成，校园网络安全体系构建、信息化基础设施建设。

第二十四条 根据“硬件集群、数据集中、应用集成”的建设原则，各单位的信息化建设项目须通过信息化办审核、备案或审批。应用系统登记备案并通过安全审核后才允许上线运行，原则上部署在学校提供的统一云资源平台上，数据汇总到学校数据中心，应用服务纳入学校信息门户。

各单位不得再为信息化项目独立建设机房，购置网络设备、安全设备、服务器设备、存储设备等硬件设备。未经信息化办允许，严禁私设服务器对外提供服务，包括对内网、外网用户提供访问服务。一经发现未经许可私设服务器，信息化办有权立刻关停服务。

第二十五条 信息化建设项目要符合学校信息化建设中长

期规划的要求，确保在规划总体框架内实现业务协同和信息共享。软件系统项目须符合国家网络安全等级保护规范，信息数据必须明确唯一的数据来源，保持数据的一致性和完整性，遵循学校统一的规范和标准。

第二十六条 信息化办负责对所有信息系统开展常年定期安全检查，存在高、中危漏洞的信息系统，关闭外网访问权限并通告信息系统责任单位限期整改。限期内，整改合格后开放外网访问权限，关闭整改仍未达到合格要求的信息系统。对新建和升级改造信息系统除进行安全扫描外，还需进行数据标准查验，对未达到学校明确的安全标准或不符合学校统一发布的数据和信息标准的信息系统，将不予验收。

第二十七条 信息化办对所有信息化建设项目实行统筹管理和全程监管。每年 11 月底前受理下一年度部门信息化建设项目申请，组织专家评审，评审通过的项目报请网信领导小组审批；审批通过的项目由建设单位按学校有关规定实施项目采购并签订项目合同；项目完成后，项目建设单位按照合同约定和学校有关规定组织项目验收工作。

第二十八条 信息化建设项目的建设方案、实施方案、需求文档、系统安装文档及安装盘、应用系统源代码、数据库结构与数据字典、测试报告、验收报告等需在在建设单位存档并在信息化办留存备案。

第七章 绩效管理

第二十九条 学校不定期开展网络安全和信息化工作绩效考评，单位采用评价性考核，信息化项目和个人采用选拔式评

优。单位主要考核内容包括：各单位提供网上师生服务的满意程度、系统日常运行管理水平、部门业务信息化程度、数据维护的效率和质量、网络安全管理与应急处置能力等。

第三十条 考评工作根据考核内容采取网上评审、会议评审或两者相结合的方式进行；考评专家由校内外技术专家、业务部门代表和师生代表组成；考评工作由网信办组织实施。

第三十一条 单位考评结果按优秀、合格、不合格方式进行评价。网信办对于考评优秀的单位、信息化项目和个人，报请网信领导小组审批，学校发文进行表彰奖励。对于不合格单位实行督促整改。

第八章 附 则

第三十二条 本办法由信息化工作办公室负责解释，自发布之日起施行。

第三十三条 《中国地质大学（武汉）网络安全和信息化工作管理办法（试行）》（地大校办发〔2020〕37号）同时废止。各单位应参照本办法制定网络安全和信息化工作实施细则。

中国地质大学（武汉）学校办公室 2022年11月8日印发

中国地质大学学校办公室文件

地大学校办发〔2022〕54号

中国地质大学（武汉）学校办公室关于印发《信息系统建设与运行管理办法》的通知

各单位:

现将《中国地质大学（武汉）信息系统建设与运行管理办法》印发给你们，请认真执行。

中国地质大学（武汉）学校办公室

2022年11月12日

中国地质大学（武汉）
信息系统建设与运行管理办法

第一章　总　则

第一条　为有序推进学校信息化建设，保障全校信息系统建设和运行管理工作规范、有效，根据《中国地质大学（武汉）网络安全和信息化工作管理办法》精神，按照“统一规划，统一标准，分工运维，消除孤岛”工作原则，结合学校实际情况，制订本办法。

第二条　信息系统是指为满足学校教学、科研、管理和服务等工作而建设的信息收集、传递、存储、加工、维护和使用的人机交互系统。学校信息系统主要包括各类教学、科研、管理及服务的业务系统和公共服务系统，原则上在校内使用，服务对象为学校师生。

第三条　本办法适用于学校所有信息系统的建设和运行管理。

第二章　职责划分

第四条　网络安全和信息化工作领导小组负责信息系统等信息化项目的建设计划的审定；信息化工作办公室负责信息化项目的立项受理和项目验收的组织工作。

第五条　信息化工作办公室应按照信息系统与网络安全“同步设计、同步建设、同步使用”原则，全程参与信息系统项目的立项审核、过程监督与项目验收，负责确认系统的技术

要求和验收规范，对项目建设过程、系统安全和运行管理予以监督。

第六条 各部门负责信息系统的需求调研、建设实施、日常运行、安全维护，确保系统除满足自身业务需求外，还须遵循学校相关信息化标准，满足学校数据交换、数据共享及安全的要求。

第三章 项目立项与项目实施

第七条 信息化工作办公室于每年12月草拟下一年度学校信息化建设计划，并提交网络安全和信息化工作领导小组审核。

第八条 各部门按照建设项目计划和经费预算进行招标采购，合理组织人力资源和技术团队进行实施工作，实施过程中的技术支持工作由信息化工作办公室负责。

第九条 信息系统建设的技术要求包含但不限于:

（一）遵循《中国地质大学（武汉）数据标准》《中国地质大学（武汉）信息标准编码规则与代码集》和《中国地质大学（武汉）数据管理办法》等标准规范;

（二）采用符合学校信息化要求的技术架构，支持统一的云部署;

（三）通过学校数据中心平台进行数据交换和共享，提供与学校数据中心平台对接的标准接口;

（四）须与学校统一身份认证中心进行认证集成；须与学校统一通信平台对接，提供短信、微信、邮件等消息发送和管理;

（五）须与学校信息门户进行单点登录集成；面向师生服

务的业务流程须与学校网上厅一站式服务集成，支持统一的移动应用。

第十条 信息系统建设项目实行项目负责人制，项目负责人应为建设单位在编人员，负责具体信息系统建设项目的组织实施；如项目负责人发生变更，应及时向信息化工作办公室提交变更备案。

第十一条 信息系统原则上部署到学校提供的公共服务平台上，项目负责人向信息化工作办公室申请系统需要的资源，并登记备案。

第四章 项目验收与材料归档

第十二条 信息系统建成后原则上应试运行不少于3个月，方可申请验收，由信息化工作办公室对验收材料进行审核，审核通过后才能组织项目验收。

第十三条 提交审核的验收材料主要有:

（一）用户需求文档：应含需求总体描述、业务需求、数据需求、运行环境、系统对接需求和系统管理需求等;

（二）系统设计文档：应含系统架构设计、功能设计、数据库设计、接口设计、安全设计等;

（三）系统运行维护文档：应含系统安装部署说明书、系统维护手册、系统使用手册、系统接口手册等;

（四）测试报告：含系统功能单元测试、集成测试、性能测试和安全检测等;

（五）验收报告及验收意见：含系统建设、系统部署及试运行情况说明，用户使用情况报告及建设单位是否同意验收的

意见;

（六）产品厂家或开发商《售后服务承诺书》。

第十四条 项目采用专家审查等方式进行验收，形成验收评价意见，未尽事宜需形成备忘录，作为约定时间或质保期内整改依据。

第十五条 项目验收会后，建设单位一周内将经审核的验收材料、专家验收意见、招标及投标文件、源代码和安装包（提供光盘或U盘，不涉及商家商业秘密的源代码）、项目归档材料清单等材料报信息化工作办公室备案存档，并按相关规定向档案馆归档。

第十六条 建设单位需确保信息系统正常运行，信息化工作办公室每年将组织对信息系统的实施情况和运行效果进行评估，评估结果作为后续同类项目立项审核的参考依据。

第五章 系统运行与终止

第十七条 信息系统上线运行前，信息化工作办公室将按照学校网络安全和信息化工作有关管理办法的规定对系统进行安全检查，对于安全检查不符合学校规定要求的信息系统必须整改，符合要求方可上线正式运行。

第十八条 建设单位对信息系统的维护与管理，应定岗、定人、定责，制定工作制度，建立工作机制，确保运行维护工作的持续性和有效性；必须安排专人负责系统的日常运行维护及管理，遵守国家、行政主管部门和学校各级管理规定。

第十九条 各部门运行的信息系统应根据业务性质、重要程度等确定安全等保等级，定期进行安全检测。同时接受信息

化工作办公室定期开展的安全技术检测和信息系统年审，对发现的安全漏洞及时整改，避免出现网络安全事件。

第二十条 信息系统在运行使用过程中，必须遵守国家法律法规或学校相关规定。

第二十一条 信息系统终止运行时，应向信息化工作办公室提出申请，在处理好历史数据，做好数据留存归档后方可终止系统运行。

第六章 经费管理

第二十二条 信息系统建设经费由学校财务部门纳入预算管理，由信息化工作办公室统筹使用。各单位自筹经费的建设项目，执行过程仍纳入信息化工作办公室监督管理。

第二十三条 建设单位须接受学校财务管理部门和审计部门对经费使用和管理情况进行的监督检查。

第七章 附 则

第二十四条 信息系统建设项目中涉及安全保密、知识产权和档案管理等问题的，按国家法律法规和学校相关规定执行。

第二十五条 本办法由信息化工作办公室负责解释，自发布之日起施行。《中国地质大学（武汉）信息系统建设与运行管理办法（试行）》（地大校办发〔2020〕40号）同时废止。

中国地质大学（武汉）学校办公室 2022年11月12日印发

中国地质大学学校办公室文件

地大学校办发〔2022〕55号

中国地质大学（武汉）学校办公室
关于印发《网络安全事件应急预案》的通知

各单位:

现将《中国地质大学（武汉）网络安全事件应急预案》印发给你们，请认真执行。

中国地质大学（武汉）学校办公室

2022年11月12日

中国地质大学（武汉）网络安全事件应急预案

第一章　总　则

第一条　为健全学校网络安全事件应急处置工作机制，规范网络安全事件应急处置工作流程，提高学校网络安全事件应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校网络安全稳定，根据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规，《国家突发公共事件总体应急预案》《突发事件应急预案管理办法》和学校《网络安全和信息化建设管理办法》等精神，制定本预案。

第二条　本预案适用于学校和校内各单位发生网络安全事件的应急处置。本预案所称网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害、数据泄露等学校信息化基础设施或相关信息系统造成危害，对社会造成负面影响的事件，一般可分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件、舆情事件、信息内容类事件和其他事件。

第三条　根据学校网络系统情况，结合网络安全事件可能造成的危害和发展蔓延的趋势等因素，学校将网络安全事件划分为“重大”和“一般”两个等级。

符合下列情形之一的为校园重大网络安全事件:

（一）全校大量用户无法正常上网，不包括正常报备后的

升级改造、施工、停电或其它特殊情况引起的网络中断。

（二）重要业务信息系统（网站）遭受重大系统损失或非法篡改等，明显影响系统效率和业务处理能力，或造成重大不良社会影响。

（三）网络病毒在全校范围内广泛传播。

（四）重要业务信息系统（网站）的信息或数据发生丢失或被窃取、篡改、假冒。

（五）其他对学校网络安全稳定和正常秩序构成较大威胁，造成重大影响的网络安全事件。

除上述情形之外，对学校网络安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为校园一般网络安全事件。

第四条 学校网络安全事件应急处置工作应符合以下基本原则:

（一）统一指挥、密切协同。学校网络安全和信息化工作领导小组（以下简称网信领导小组）统筹协调全校网络安全应急指挥工作，建立健全与上级和地方政府有关主管部门、二级单位和相关专业服务机构等多方参与、协调联动的闭环管理应急机制，加强网络安全事件预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

（二）分级管理、强化责任。按照“谁主管谁负责，谁使用谁负责，谁运维谁负责”的原则，各二级单位对本单位建设、使用、维护的各类信息系统和网站的网络安全和应急处置工作

承担主体责任。各单位党政主要负责人是网络安全和应急处置工作第一责任人。

（三）预防为主、平战结合。坚持日常预防和事件处置工作相结合，做好网络安全事件预防、预判、预警工作，抓早抓小，争取早发现、早报告、早控制、早解决，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，严控网络安全事件风险等级和影响范围。

第二章　组织架构与职责

第五条　学校网信领导小组统筹协调全校网络安全事件应急工作，指导学校网络安全事件应急处置；发生校园重大网络安全事件时，成立网络安全事件应急工作组，负责组织指挥和协调事件处置。

第六条　根据学校网络安全和信息化工作机制与相关部门职能分工要求，各有关单位在网络安全事件应急处置工作的职责如下:

（一）学校网络安全和信息化工作领导小组办公室（以下简称网信办）负责网络安全应急管理事务性工作，对接教育部、省教育厅等主管部门，向学校网信领导小组报告网络安全事件情况，提出校园重大网络安全事件、校园一般网络安全事件的应对措施建议和意见，统筹组织学校网络安全监测工作;

（二）学校办公室牵头组织重大敏感时期、重要活动、重要会议期间发生的网络安全事件的协调处置；维稳（综治）办

公室统筹危及校园安全的行为和活动的监测与处置；保密办公室负责涉密网络安全事件的处理。

（三）党委宣传部负责学校舆情监测和信息内容安全类事件的处置，对涉及师生思想政治和意识形态工作方面的预警性、倾向性、苗头性网络安全问题，加强分析研判并妥善有效应对。

（四）安全保卫部密切联系国家相关部门，负责涉及人为破坏类网络安全事件的处置，配合重大安全事件的处置。

（五）信息化工作办公室（以下简称信息化办）负责校园基础网络及公共服务信息系统安全工作，保证校园网络信息服务不中断；负责网络攻击、设备故障类网络安全事件的处置；负责全校网络与信息安全事件处置的技术支持工作；每年组织一次应急演练，并将年度演练情况按要求上报。同时根据演练情况对预案进行修改完善；定期组织网络安全业务培训，提高网络安全管理人员和技术人员的风险防范意识和应急处置技能。

第三章　监测与预警

第七条　事件监测。党委宣传部通过多种渠道和技术手段密切监测全校舆情；信息化办通过多种渠道和技术手段密切监测全校信息系统运行，对发现的网络安全事件采取相应的措施及时处置，并将掌握的情况立即上报网信领导小组并通知相关单位。各单位对本单位信息系统（网站）的运行情况进行密切监测，一旦发生网络安全事件，应当立即通过电话、短信等方

式上报信息化办，不得迟报、谎报、瞒报和漏报。

第八条 威胁监测。党委宣传部组织对全校信息内容安全威胁进行监测，信息化办组织对全校信息系统和网站的网络安全威胁进行监测，建立多方协作的信息共享机制，通过多种途径监测、汇聚漏洞、病毒、网络攻击等网络安全威胁信息，对发生的威胁及时通知相关单位，并督促其及时进行处置、整改和上报。

第九条 预警研判和发布。党委宣传部、信息化办对所负责监测的有关信息进行综合研判，对发生网络安全事件的可能性及其可能造成的影响进行分析评估:

（一）认为属于能引发校园一般网络安全事件需要立即采取防范措施的情况，及时通知校内相关单位;

（二）认为属于能引发校园重大网络安全事件的信息，应立即向学校网信领导小组报告并采必要的应对措施;

（三）认为属于涉及行业领域重大隐患的信息，应经学校网信领导小组批准及时向上级主管部门报告。

第四章 应急处置和响应

第十条 发生网络安全事件时，由学校网信领导小组授权，学校办公室、党委宣传部、信息化办、保密办公室等部门和责任单位立即组建应急工作组。根据网络安全事件类型和等级，应急工作组在网信领导小组统一指挥下，采取科学有效的应急处置措施应对，并保存网络攻击、网络入侵、网络病毒或不当

舆情等证据，严禁冷处理、拖延处理。

第十一条 校园重大网络安全事件应急处置流程与措施:

（一）责任单位须第一时间关停应用、切断外网等有效措施，立即将有关情况报网信办，力争将损害和影响降低到最小范围;

（二）网信办第一时间报网信领导小组和责任单位分管校领导，成立应急工作组，对于存在人为破坏活动的情况同时报安全保卫部;

（三）责任单位在应急工作组的指导下根据专项应急预案开展应急处置工作，并于 12 小时内以书面报告形式向网信办报送《网络安全事件情况报告》(附件 1)，在安全事件处置完毕后 3 个工作日内以书面报告的形式向网信办报送《网络安全事件整改报告》(附件 2);

（四）网信办实时向网信领导小组汇报事件应急处置进度。事件处置完毕后，网信领导小组会同相关部门对整改结果进行审核并按照相关规定向上级主管部门汇报。

第十二条 校园一般网络安全事件应急处置流程与措施:

（一）责任单位须第一时间采取关停应用、删除问题文档等有效措施，立即将有关情况报网信办，及时消除不良影响，控制事态蔓延。

（二）责任单位在整改完成后向网信办报送《网络安全事件整改报告》(附件 2)，并接受网信办对安全事件整改结果的审核。

第五章　工作保障

第十三条　筑牢基层防线。各单位应落实网络安全应急工作责任制，建立本单位网络安全事件应急处置工作机构，明确分管责任人和工作专员，建立健全相关应急工作机制。

第十四条　加强技术支撑。信息化办作为全校网络安全应急技术支撑单位，应加强网络安全技术队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、技术支撑工作。

第十五条　建设专家队伍。成立学校网络安全专家组，为全校网络安全事件的预防和处置提供技术咨询和决策建议。

第十六条　促进信息共享与应急合作。加强与上级和地方政府有关主管部门、校内各单位、周边高校、网络安全专业机构等单位的日常工作沟通和应急处置合作，积极探索建立网络安全事件信息共享机制和网络安全事件的快速发现和协同处置机制。

第十七条　强化经费保障。学校每年提供专项经费，用于网络安全应急技术支撑队伍建设、专家队伍建设、监测通报、宣传教育培训、预案演练、物资保障等工作开展。

第十八条　责任与奖惩。对在网络安全事件应急管理工作中做出突出贡献的先进单位和个人给予表彰和奖励；对在应急管理工作中有失职、渎职行为的，依照相关规定追究有关单位和有关人员责任。

第六章　附　则

第十九条 本预案原则上每年评估一次，根据实际情况适时修订。

第二十条 本预案由信息化工作办公室负责解释，自发布之日起施行。《中国地质大学（武汉）网络安全事件应急预案（试行）》（地大校办发〔2020〕38号）同时废止。

附件：1.网络安全事件情况报告

2.网络安全事件整改报告

附件 1

网络安全事件情况报告

单位名称：（需加盖公章）　　事发时间：　年　月　日　分

<table>
<tr><td rowspan="2">联系人姓名</td><td rowspan="2"></td><td>手机</td><td></td></tr>
<tr><td>电子邮箱</td><td></td></tr>
<tr><td>事件分类</td><td colspan="3">☐有害程序事件☐ 网络攻击事件
☐信息破坏事件☐设备设施故障
☐灾害事件　☐舆情事件
☐信息内容类事件☐其他_____</td></tr>
<tr><td>事件分级</td><td colspan="3">☐ 校园一般网络安全事件
☐ 校园重大网络安全事件</td></tr>
<tr><td>信息系统的基本情况（如涉及请填写）</td><td colspan="3">系统名称：_____
系统网址和 IP 地址：_____
系统主管单位/部门：_____
系统运维单位/部门：_____
系统主要用途：_____</td></tr>
<tr><td>事件概况</td><td colspan="3">（包括：事件发现、处置、原因、危害、采取的紧急措施等）</td></tr>
<tr><td>党政主要负责人意见（签字）</td><td colspan="3"></td></tr>
</table>

附件 2

网络安全事件整改报告

单位名称：（需加盖公章）　　报告时间：　年　月　日

联系人姓名		手机	
		电子邮箱	
事件分类	☐ 有害程序事件☐ 网络攻击事件 ☐信息破坏事件☐设备设施故障 ☐灾害事件　☐舆情事件 ☐信息内容类事件 ☐其他_____		
事件分级	☐ 校园一般网络安全事件 ☐ 校园重大网络安全事件		
信息系统的基本情况(如涉及请填写)	系统名称：_____ 系统网址和 IP 地址：_____ 系统主管单位/部门：_____ 系统运维单位/部门：_____ 系统主要用途：_____		
事件报告	（包括：事件原因、整改措施、影响、恢复情况等）		
党政主要负责人意见（签字）			

中国地质大学（武汉）学校办公室　　2022 年 11 月 12 日印发

中国地质大学学校办公室文件

地大学校办发〔2022〕57号

中国地质大学（武汉）学校办公室
关于印发《电子印章管理办法》的通知

各单位:

现将《中国地质大学（武汉）电子印章管理办法》印发给你们，请认真执行。

中国地质大学（武汉）学校办公室

2022年11月14日

中国地质大学（武汉）电子印章管理办法

第一章　总　则

第一条　为加快学校信息化建设，规范电子印章管理，确保电子印章合法、安全、可靠使用，提高办事效率，根据《中华人民共和国电子签名法》《国务院关于国家行政机关和企业事业单位社会团体印章管理的规定》《全国一体化在线政务服务平台电子印章管理办法（试行）》精神，结合学校实际，制定本办法。

第二条　电子印章是应用数字密码技术，结合数字证书和模拟传统实物印章的图形化电子签名，能够按国家标准传输、审验、显示及打印，是一种可存储在专用 USBKEY 或印章服务器中的电子数据。电子印章的使用可确保用户身份及印章的真实性、访问权限的有效性以及信息的完整性和不可抵赖性。

第三条　本办法所指电子印章主要分为电子公章、电子专用章和电子签名章。电子公章是指由学校统一审批和发放，在一定期限内用以证明校内部门机构身份的电子印章。电子专用章是指由学校统一审批和发放，在印章上注明范围内使用的业务专用电子印章。电子签名章是指由学校统一审批和发放，在一定期限内用以证明校领导和各二级单位主要负责人身份的电子印章。电子公章和电子专用章的图形化特征，应与实物印章的印模完全一致。电子签名章的图形化特征，应与印章持有人签名完全一致。

第四条　电子印章的管理、使用与实物印章相同，且与实

物印章具有等同效力。

第二章　电子印章使用范围

第五条　学校电子印章具体使用范围:

（一）学校电子公章在湖北省电子政务内网平台使用。主要办理电子公文处理和学校信息报送等业务。

（二）部门电子公章和电子签名章在学校内部办公平台各系统使用。如办理公文流转、发送校内电子公文等审核类业务。

（三）电子专用章在学校各二级单位办公业务平台使用。主要办理学生成绩单、相关证明等证明类业务。

学校合同、协议、委托书、工作介绍信等对外信函或资料中暂不使用电子印章。

第六条　电子印章仅限于被授权人在电子政务专用网络以及学校办公局域网络环境下使用。

第三章　电子印章申请及制发

第七条　学校办公室负责学校电子印章的使用审批、管理和监督工作；信息化工作办公室负责学校电子印章的制作、授权发放、注销、电子签章认证平台管理等技术支持和安全防护工作。

第八条　电子印章申请。印章使用单位通过学校“网上办事大厅”发起申请，按照服务流程完成申请。

第九条　印章信息审核。电子印章申请信息经学校办公室审核同意后，由信息化工作办公室对印章申请相关材料进行存档备案。

第十条 电子印章制作。信息化工作办公室依据学校办公室审核同意后的申请材料制作数字证书、电子印章，同时在相应管理系统中完成对电子印章使用人员的业务授权。

第十一条 电子印章授权变更。因人员变动需要对电子印章重新授权时，在学校“网上办事大厅”提交申请，信息化工作办公室办理授权变更手续。

第四章 电子印章使用及保管

第十二条 电子印章使用。被授权使用人员限在学校信息化系统中对应的网上办事业务、电子公文审核发布和归档中使用电子印章。

第十三条 电子印章注销。使用单位因发生业务调整或机构变更、人员变动、印章废止等情况时，应通过“网上办事大厅”申请，按照服务流程完成注销。

第十四条 电子印章变更。使用单位因实物印章损坏、丢失，重新申办印章后，应按照本办法的电子印章申领程序重新制作电子印章。信息化工作办公室同时将原电子印章注销。

第十五条 电子印章管理遵循“按需发放，授权应用”“谁持有，谁使用，谁负责”原则。电子印章按照实物印章管理要求进行管理。电子公章、电子专用章对学校及各二级单位指定使用人员进行业务授权，在业务授权范围内使用。

第十六条 实行电子印章被授权人登记备案制度。电子印章被授权人因事假、病假、休假等原因不在岗位时，可进行业务委托，授权他人代办该业务，或申请变更被授权人。

第五章　电子印章安全管理

第十七条　信息化工作办公室建立统一的电子印章系统，提供电子印章申请、制作、备案、查询、变更、注销、签章、验章和使用审计管理等功能，并制定相关接口规范，学校各个应用系统都可以根据该规范接入应用。各二级单位不再新建电子印章系统，已建电子印章系统的，应与学校统一的电子印章系统进行对接，并实现互通互认。

第十八条　电子印章系统建设应采用具有国家商用密码型号的产品，支持国产密码算法和文档格式标准。电子印章系统建设应符合《GM/T 38540-2020 信息安全技术 安全电子签章密码技术规范》《GA/T1106-2013 信息安全技术电子签章产品安全技术要求》《GB/T33481-2016 党政机关电子印章应用规范》等规定。电子印章系统应具备完善的信息安全防护措施，至少应符合计算机信息系统安全保护等级三级要求。

第十九条　电子印章系统应采取集中存储，分级授权、制发、管理，统一验证的模式部署，并建立可靠的数据存储、备份、恢复、审计机制，确保数据安全。电子印章数据应当存放在指定服务器上，并由信息化工作办公室指定专人管理。

第二十条　涉及国家秘密的信息系统确需使用电子印章时，应按照国家保密管理相关规定执行。

第六章　责任追究

第二十一条　电子印章被授权人因委托他人代审、代办业务，造成管理不当、审核差错并造成损失的，由电子印章被授

权人承担责任。

第二十二条 电子印章系统管理员违规提供电子公章，由此产生的后果，由违规的系统管理员承担责任。

第二十三条 对伪造、变造、冒用、盗用电子印章的行为，学校根据情节轻重追究当事人的责任；构成犯罪的，依法追究刑事责任；给他人造成损失的，依法承担民事责任。

第二十四条 电子印章使用管理中发生的违规违纪行为，由学校纪检监察部门调查处理，学校办公室配合，信息化工作办公室提供技术支持。

第七章 附 则

第二十五条 本办法由信息化工作办公室负责解释。

第二十六条 本办法自发布之日起施行。《中国地质大学（武汉）电子印章管理办法（试行）》（地大校办发〔2020〕2号）同时废止。

中国地质大学（武汉）学校办公室 2022年11月14日印发

中国地质大学学校办公室文件

地大学校办发〔2022〕66号

中国地质大学（武汉）学校办公室
关于印发《网站建设运行管理办法》的通知

各单位:

现将《中国地质大学（武汉）网站建设运行管理办法》印发给你们，请认真执行。

中国地质大学（武汉）学校办公室

2022年12月20日

中国地质大学（武汉）网站建设运行管理办法

第一章　总　则

第一条　为提高学校网站建设、管理、应用水平，充分发挥网站服务师生、对外宣传交流的窗口作用，助力学校建设地球科学领域国际知名研究型大学，根据《中国地质大学（武汉）章程》等规定，结合学校工作实际，制定本办法。

第二条　本办法所指网站包括学校中英文官方网站和各二级单位中英文网站。

第二章　职责分工

第三条　学校统一部署中英文网站建设工作。各二级单位应建设并完善中文网站，各人才培养单位、教学科研单位原则上应建设英文网站，其他单位根据需要建设英文网站。

第四条　学校办公室负责全校网站的统筹管理，负责中文官网建设与管理、英文官网运行监督等工作。信息化工作办公室负责全校网站技术支撑平台的建设和管理，提供网站信息安全和相关的技术服务，负责网站备案登记、网站数据备份等工作。党委宣传部负责全校网站意识形态、学校标识等内容的监督指导工作。国际合作处负责英文官网日常管理运行工作，包括翻译、校对、审核及信息发布等。各二级单位负责本单位网站建设、更新和维护工作；相关单位负责学校中英文官网固定栏目信息更新与维护。

第三章　总体要求

第五条　严格执行“谁建设、谁主管、谁负责”原则。各单位应建立本单位中英文网站管理规章制度，明确分管领导和网站管理员，落实先审批后发布的工作要求，未经审批的信息严禁上网。

第六条　根据《中国地质大学（武汉）章程》规定，学校中文名称为：中国地质大学（武汉），英文名称为：China University of Geosciences，中文简称：地大，英文缩写：CUG。学校中文官网地址：http://www.cug.edu.cn，英文官网地址：http://en.cug.edu.cn/。

第七条　各二级单位中英文网站应规范使用国家机关、学校及本单位中英文名称、缩写，遵循学校《校名、校标、校徽、校誉管理暂行办法》及视觉形象识别系统有关要求，规范使用校标、校徽等学校标识。

第四章　学校中文官网管理

第八条　学校中文官网主要发布面向师生或社会公开、反映学校改革建设情况的综合性信息、重要专题信息等，主要包含学校概况、组织机构、教育教学、师资队伍、学科建设、科学研究等固定板块，地大要闻、图片新闻、学术动态、通知公告、教学科研、媒体地大、地大人等新闻版块，师生服务大厅、专题聚焦等链接版块。

第九条　学校中文官网各版块信息更新来源及要求如下：

1.固定版块。校情数据以发展规划与学科建设处提供的教育事业综合统计调查表为准，其他信息由相应管理服务单位负责编辑、校对，经学校办公室审核后发布。

2.新闻版块。地大要闻、教学科研、媒体地大和地大人栏的信息主要来自地大新闻网，学术动态栏信息来自各教学科研单位，图片新闻由党委宣传部、学校办公室制作发布。新闻版块信息来源单位严格执行审批流程，确保信息的准确性、及时性、有效性。

3.链接版块。学校办公室负责链接版块的规划和调整，各链接网站责任单位负责网站建设、更新和维护。

第五章　学校英文官网管理

第十条　学校英文官网采用信息来源单位负责制，固定版块中学校内容（学校简介、学院信息、科学研究、国际合作、校园介绍、校友简介、捐赠和联系方式等）的更新频率与中文官网保持一致，国际教育等内容（招生、招聘、就业等）的更新频率与国际教育学院网站保持一致。新闻和科研学术等版块应及时更新相关信息,重大外宣新闻的发布应不晚于中文官网 2 天。

第十一条　学校英文官网新闻按照内容分为 3 类，由相关单位提供图文素材，国际教育学院翻译、校审后发布上网。

1.外事类新闻，由国际合作处负责撰写或从中文官网挑选，包括国外高校或研究机构等来校调研、校领导出国访问、留学生重要活动等内容。

2.常规外宣新闻，由党委宣传部负责撰写或从中文官网挑选，包括学校重大活动、重要成果、荣获奖励或称号、杰出人物等内容，并提供图片等素材。

3.科技学术类新闻，由科学技术发展院负责挑选我校发表的高水平论文、具有国际影响力的学术事件和著名学者讲座报道等内容，并提供图片等素材。

第六章　二级单位中英文网站管理

第十二条　二级单位中文网站注重时效性、实用性和服务性，贴近学校教学科研和师生生活，并建立完善的内容更新机制。建设有英文网站的二级单位，应参考世界一流大学院系英文网站和学校英文官网，做到版块合理、内容详实、更新及时。

第十三条　网站栏目设置应包含但不仅限于以下内容。

1.各单位中文网站，包括单位简介、组织机构、规章制度、新闻报道、相关办事流程、联系方式等信息。各版块信息完整，结构层次分类合理，链接明确、导航清晰。

2.教学单位英文网站，包括单位简介、学科建设、课程设置、师资队伍、新闻报道、联系方式等信息。各版块信息完整，结构层次分类合理，链接明确、导航清晰。

3.科研单位英文网站，包括单位简介、著名学者、新闻报道、国际合作等信息。

4.其他二级单位英文网站，包括单位简介、主要职责、新闻报道、联系方式等信息。

第十四条　对未按照此办法运行管理或考评不合格的二级

单位中英文网站，学校将相关情况纳入对二级单位及班子成员综合考核管理。

第七章　中英文网站安全管理

第十五条　学校所有网站遵循合法、规范、真实、及时的原则发布信息，不得发布违反国家法律法规和各项规章制度的信息，不得发布侵犯他人合法权益的信息，不得传播有害信息。

第十六条　严格执行“涉密不上网，上网不涉密”原则，涉密信息、内部资料、不宜公开事宜均不得上网发布。

第十七条　保密要害部门建设网站时，应严格遵守国家保密相关法规，网站内容必须经过学校保密委员会办公室审核通过后方能发布上网。

第八章　附　则

第十八条　本办法由学校办公室负责解释。

第十九条　本办法自发布之日起施行。《中国地质大学（武汉）网站建设运行管理办法（试行）》（地大校办发〔2020〕1号）同时废止。

中国地质大学（武汉）学校办公室　　2022年12月20日印发

中国地质大学校长办公室文件

地大校办发〔2020〕39 号

中国地质大学（武汉）校长办公室
关于印发《数据管理办法（试行）》的通知

各学院、各处（室）、各直属单位：

现将《中国地质大学（武汉）数据管理办法（试行）》印发给你们，请认真执行。

中国地质大学（武汉）校长办公室

2020 年 7 月 28 日

中国地质大学（武汉）数据管理办法（试行）

第一章　总　则

第一条　为贯彻落实教育部对于高校信息化的相关要求，实现学校信息化数据的统一管控，为学校教学、科研、管理、服务及相关决策提供安全、完整和便捷的数据服务，根据《国务院关于印发促进大数据发展行动纲要的通知》（国发〔2015〕50号）、《教育部机关及直属事业单位教育数据管理办法》（教厅发〔2018〕1号）等文件精神，按照相关法律法规和制度要求，结合学校实际，制定本办法。

第二条　本办法中提到的数据是指学校内部各类信息化基础环境设施和信息系统所产生、保存和利用的相关数据，包括但不限于：管理信息系统产生的业务数据、使用计算机编制的数据、网站数据、教学资源（含多媒体视频、图片、课件等）、用户服务支持系统产生的数据、电子化处理的印刷品数据等，分为结构化数据和非结构化数据。

第三条　本办法旨在建立学校数据管理体系，规范权威数据生产、维护、交换、共享、使用与归档等环节的管理流程。构建安全、稳定、高效运行的数据环境，将学校各类数据资源进行有机整合，保证信息化数据的一致性、实时性、有效性、安全性和高效性，实现权威数据集中管理。

第四条　信息化数据是学校的无形资产和战略资源，是提

升学校教学、科研、管理水平的重要基础。数据管理应遵循以下原则：

（一）统一规范原则。信息系统采集和处理的数据应符合学校制定的数据标准，相同业务类型的数据使用统一数据源。

（二）全程管控原则。建立数据从采集、处理、维护、共享的全过程管控体系，相关业务部门对所管理的数据承担相应管理职责，对其权限范围内所负责的数据进行定期检查，重点保证数据采集的真实性、准确性、完整性和及时性。

（三）安全可控原则。建立健全学校信息安全保障体系，完善数据共享安全机制、数据防灾备份机制，确保数据安全。

（四）数据归档原则。建立完善数据归档机制，各类数据按学校相关规定及时向档案馆归档。

第二章　数据管理机构与职责

第五条　网络与信息中心是学校的数据管理机构，负责统筹规划全校信息化数据管理工作。具体职责包括：确定各类数据对应的权威数据生产部门，建立全校的数据标准、编码标准、技术规范、管理规范，对各系统建设时数据标准的执行情况进行监督，负责学校数据中心平台的运行维护、提供公共数据服务，保障学校数据安全和数据及时归档。

第六条　各业务部门是相应权威数据生产部门，负责本部门信息化数据生产的准确性和及时性，确保数据质量。具体职责包括：确保本部门信息化数据与学校数据中心平台的联通，

及时完成数据维护、更新和归档，按学校统一数据标准向数据中心平台提供生产数据、获取共享数据。

第七条 各业务部门主要负责人是本部门数据管理第一责任人，网络安全和信息化工作分管领导是本部门数据管理直接责任人。

第三章 学校数据中心平台

第八条 学校数据中心平台是各业务部门生产数据的汇聚地，是进行数据交换、发布和共享的公共服务平台。它不生产数据，采用统一的接口为其它信息系统提供数据服务。

第九条 各业务系统生产的数据应及时进入学校数据中心平台，及时向数据中心平台归档。

第十条 网络与信息中心应及时对学校数据中心平台数据进行收集、整理、归档，形成权威数据，对业务系统进行数据的授权共享。

第十一条 各业务部门的数据原则上只允许通过学校数据中心平台进行数据交换和共享。

第四章 数据生产和运维

第十二条 数据生产主要包括数据采集、录入和审核三个环节。各业务部门应按照本部门业务需求以及学校数据标准和规范生产数据，满足数据的真实性、完整性、规范性和时效性要求。

（一）真实性：各业务部门业务系统生产的数据必须真实、

准确、可靠，须经本部门业务人员审核后才能进入到学校数据中心平台。

（二）完整性：各业务部门须确保业务系统相关数据完整、齐全，避免数据缺失。

（三）规范性：各业务部门在进行数据采集、录入、审核时须保证数据的规范可用，符合《中国地质大学（武汉）数据标准》和《中国地质大学（武汉）信息标准编码规则与代码集》要求。

（四）时效性。各业务部门须及时进行数据维护，防止产生无效数据、过时数据。

第十三条 学校各业务部门在进行数据生产时，除法律法规另有规定以外，应当遵循“一数一源”的原则。凡属于学校数据中心平台可以获取的数据，禁止各业务部门向其它部门或师生重复采集。

第十四条 业务部门生产的数据均为学校所有，各业务部门有义务向数据中心平台提供可共享的数据，同时依据管理授权进行共享。

第十五条 数据运维是指学校各业务部门在业务操作过程中，对其信息化数据所进行的补充、修正、更新和删除等操作。学校各业务部门须依照其业务数据运维的权限和职责，明确数据的修正、补充、更新、删除等操作流程。

第五章 数据共享与使用

第十六条 数据按共享类型分为两类：

（一）基础数据：具有基础性、基准性、标识性的信息化数据。

（二）有条件共享数据：数据内容敏感、按照规定不宜进行大范围公开、泄露后会对集体或个人产生严重影响只能按特定条件提供给需求方的数据。

第十七条 学校各业务部门须向网络与信息中心提出申请，获取基础数据的使用权，网络与信息中心提供数据共享接口。

第十八条 学校数据信息主要用于本校教学、科研、管理和服务等，数据使用部门要按照“谁使用，谁负责”的原则，加强对共享数据使用的全过程管理，申请使用数据的部门必须保护相关数据的安全，不得将数据信息用于申请应用范围之外。除上级主管部门要求上报的数据外，学校业务系统数据不得与校外信息系统进行交换。

第六章 数据质量

第十九条 数据生命周期质量管理是对生产、处理、存储、应用、归档、备份整个数据生命周期的各个环节数据进行精确管理。为保证数据管理的科学性、保证数据提供的准确性、及时性、便于利用，各数据生产部门必须采取有效手段保障生产数据质量。

第二十条 遵循“谁生产，谁维护；谁使用，谁反馈”的

原则，建立疑义、错误数据快速校核机制和数据结构变化反馈机制。数据使用部门对于发现的数据质量问题及时反馈至网络与信息中心，网络与信息中心协助和督促数据生产部门进行数据质量整改。

第二十一条 加强数据修改和共享环节管控。为保证全校数据的一致性，数据使用部门对于从学校数据中心平台获取的权威数据，只能进行引用和衍生，不能增加、删除和修改；数据生产部门进行数据质量整改和维护时方可授权进行数据修正。

第二十二条 网络与信息中心是数据质量的监管部门，各业务部门可以就其他业务部门所提供数据是否准确、及时、完整和规范等情况向网络与信息中心提出工作意见和建议。

第七章 数据安全

第二十三条 各业务部门应遵守国家相关法律法规，采取必要的管理和技术措施保证数据安全，避免数据丢失或被破坏、更改和泄露，严禁使用来源不明的数据。

第二十四条 使用数据时应注意保护个人隐私、限定数据使用范围，不得将获得的数据公开，不得直接或以改变数据形式等方式提供给除数据申请部门外的第三方，也不得用于或变相用于其他目的。

第二十五条 学校各业务部门应定期对本部门负责的数据进行巡检，对数据及日志进行备份，确保数据安全可靠。

第八章　附　则

第二十六条　本办法由网络安全和信息化工作领导小组办公室负责解释，自发布之日起施行。

中国地质大学（武汉）学校办公室　　2020年7月28日印发

二、其他相关资料

新赛道、新优势、新突破
纵深推进国家教育数字化战略行动

教育部党组成员、副部长　吴岩

2023年11月7日

中华人民共和国教育部
Ministry of Education of the People's Republic of China

培训目标

- **教育数字化不仅是工具和手段，更是思维和理念。**教育部高度重视思想引领的作用，自2013年以来每年举办培训班，以训代会，提升领导干部对教育数字化工作的理解和认识。
- 今年**开拓性地举办**高等学校教育数字化专题研讨班，目标是总结高等教育数字化的工作成效，宣贯国家教育数字化战略行动的理念举措，凝聚高等学校推动教育数字化的思想共识，以教育数字化支撑引领高等教育高质量发展，发挥高等教育在推进教育现代化，建设教育强国的龙头作用。

一　开辟新赛道，深刻认识高等教育数字化战略意义

二　塑造新优势，系统总结高等教育数字化思路成效

三　形成新突破，扎实推进高等教育数字化重点任务

一 开辟新赛道，深刻认识高等教育数字化战略意义

党中央高度重视网信工作

教育数字化是教育发展的新赛道

高等教育要在教育数字化上勇立潮头

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

1.1 党中央高度重视网信工作

党的十八大以来，党中央从进行伟大斗争、建设伟大工程、推进伟大事业、实现伟大梦想的全局和战略高度出发，加快建设网络强国、数字中国

2014年
党中央决策成立中央网络安全和信息化领导小组，习近平总书记亲自担任组长

2016年
习近平主持召开网络安全和信息化工作座谈会并发表重要讲话

2018年
中央网络安全和信息化领导小组升级成为中央网络安全和信息化委员会，首次全国网信工作会议召开

2021年
国家“十四五”规划首次对数字中国建设进行了专篇部署

2022年
中共中央、国务院印发《数字中国建设整体布局规划》提出新时代数字中国建设的整体战略

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

1.1 党中央高度重视网信工作| 习近平总书记对网信工作作出了系列的论述

没有信息化就没有现代化
—— 习近平在中央网络安全和信息化领导小组第一次会议上讲话（2014年2月）

过不了互联网这一关，就过不了长期执政这一关
—— 习近平在全国网络安全和信息化工作会议上的讲话（2018年4月）

信息化为中华民族带来了千载难逢的机遇
—— 习近平在全国网络安全和信息化工作会议上的讲话（2018年4月）

加快数字中国建设，就是要适应我国发展新的历史方位，全面贯彻新发展理念，以信息化培育新动能，用新动能推动新发展，以新发展创造新辉煌。
——习近平致首届数字中国建设峰会的贺信（2018年4月）

1.1 党中央高度重视网信工作| 数字教育是数字中国的重要组成部分

“十四五”规划和2035远景目标纲要

明确聚焦**教育**等重点领域，推动**数字化服务普惠应用**。推进**学校**等**公共服务机构资源数字化，加大开放共享和应用力度**。

数字中国建设整体布局规划

将数字教育作为数字中国的重要组成部分进行部署，提出“**大力实施国家教育数字化战略行动，完善国家智慧教育平台**”。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

1.2 教育数字化是教育发展的新赛道

党的二十大

- 教育、科技、人才是全面建设社会主义现代化国家的**基础性、战略性支撑**。
- 推进教育数字化，建设全民终身学习的**学习型社会、学习型大国**。

中央政治局第五次集体学习

- 教育数字化是我国开辟教育发展**新赛道**和塑造教育发展**新优势**的**重要突破口**。
- 进一步推进数字教育，为**个性化学习、终身学习、扩大优质教育资源覆盖面和教育现代化**提供有效支撑。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

1.2 教育数字化是教育发展的新赛道| 教育数字化支撑教育高质量发展

支撑教育均衡

我们将通过教育信息化，**逐步缩小区域、城乡数字差距**，大力促进教育公平，让亿万孩子同在蓝天下共享优质教育、通过知识改变命运。

——习近平致国际教育信息化大会的贺信（2015年5月）

支撑教育变革

要总结应对新冠肺炎疫情以来大规模在线教育的经验，**利用信息技术更新教育理念、变革教育模式。**

——习近平在教文卫体育领域专家代表座谈会的讲话（2020年9月）

支撑个性学习

充分发挥人工智能优势，加快发展**伴随**每个人一生的教育、**平等**面向每个人的教育、**适合**每个人的教育、更加**开放**灵活的教育。

——习近平致国际人工智能与教育大会的贺信（2019年5月）

支撑终身学习

因应信息技术的发展，推动教育变革和创新，构建网络化、数字化、个性化、终身化的教育体系，建设“**人人皆学、处处能学、时时可学**”的学习型社会。

——习近平致国际教育信息化大会的贺信（2015年5月）

1.3 高等教育要在教育数字化上勇立潮头

重要标志

高等教育发展水平是一个国家发展水平和发展潜力的重要标志
——2016全国高校思政会

两个事关

办好高等教育事关国家发展事关民族未来
——2016年致清华大学建校105周年贺信

两个更为迫切

党和国家事业发展对高等教育的需要，对科学知识和优秀人才的需要，比以往任何时候都更为迫切
——2021年考察清华大学座谈会

龙头

教育强国建设龙头是高等教育
——2023年中央政治局第五次集体学习

高等教育是教育强国建设的“龙头”，应当在数字化应用中起到示范引领的作用

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

1.3 高等教育要在教育数字化上勇立潮头

从教育大国到教育强国是一个系统性跃升和质变，必须以改革创新为动力

——习近平在中央政治局第五次集体学习时的讲话
（2023年5月29日）

要坚持系统观念，统筹推进

- 育人方式改革
- 办学模式改革
- 管理体制改革
- 保障机制改革
- 教育评价改革

要充分发挥数字技术**“突破口”**的作用，促进数字技术与教育教学的深度融合，推动高等教育的高质量发展，实现高教发展的**“变轨超车”**，回答好**“强国建设、教育何为”**的时代之问。

互联网　区块链　大数据　人工智能

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

二　塑造新优势，系统总结高等教育数字化思路成效

有底蕴	有理念	有基础	有应用	有自信
起步蓄能期 快速发展期 变革引领期	工作理念 工作原则 重大关系	硬件基础（云网端） 软件基础（平台资源）	疫情防控 慕课西行 虚拟实训 就业创业	世界大会 理论成果 平台获奖

建设教育强国

高教战线**敢为人先、敢于担当、善于创新**，在**基础设施建设、平台应用创新、服务提质增效**等方面开展了大量工作，开拓出了一条具有**中国特色的教育数字化发展之路**，国际层面上已颇具影响力，甚至在部分领域实现了领跑。

我们有能力、有信心也有决心将教育数字化打造成为中国教育的靓丽名片！

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.1有底蕴

起步蓄能期	快速发展期	变革引领期
(1978年-2011年)	(2012年-2021年)	(2022年至今)
阶段一	阶段二	阶段三

教育数字化的三个阶段

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.1有底蕴|起步蓄能期

1978年
全国教育工作会议

小平同志提出，要制订加速发展电视、广播等现代化教育手段的措施，这是多快好省发展教育事业的重要途径，必须引起充分的重视。

1978年
中央广播电视大学成立

国家批准，教育部成立中央广播电视大学，也就是国家开放大学的前身，第一家面向全国开展远程开放教育的新型高等学校应运而生。

1984年
计算机教育普及

小平同志在参观上海微电子技术应用汇报展览会上指出，计算机的普及要从娃娃做起，推动计算机进入教育教学领域。

1994年
互联网进入校园

清华大学等10所高校承担“中国教育和科研计算机网示范工程”建设项目，建成了我国第一个大型骨干网络，高等学校成为我国第一批互联网用户。

口2.1有底蕴|起步蓄能期

1999年，教科网实现了全国**31个省**全覆盖，成为了高教数字化的**标志工程**

第一个电子杂志

神州学人
(1996)

第一个搜索引擎

天网搜索引擎
(1996)

第一个网络论坛

水木清华截图
(2004年)

第一个数字图书馆

CALIS（中国高等教育文献保障系统，1998）和CADAL（大学数字图书馆国际合作计划，2001）

教科网诞生了第一批的互联网应用，**高等学校**成为了我国互联网发展的**先锋力量**

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.1有底蕴|快速发展期

党的十八大以来，我国教育信息化进入了快车道

2012年

《教育信息化十年发展规划(2011-2020)》发布，**第一次**全国教育信息化工作电视电话会议召开，提出**建设“三通两平台”**

2015年

国际教育信息化大会召开，习近平主席致贺信。提出**“坚持不懈推进教育信息化”**

2015年

第二次全国教育信息化工作电视电话会议召开。指出**“三通两平台”取得突破性进展**

2018年

《教育信息化2.0行动计划》发布，基本实现**“三全两高一大”**的建设目标

2019年

国际人工智能与教育大会召开，习近平主席致贺信。强调**“积极推动人工智能和教育深度融合，促进教育变革创新”**

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.1有底蕴|快速发展期

慕课是快速发展的缩影，反映了我国高等数字化发展的蓬勃景象

- 2012年是慕课元年，2013年，我们迅速跟进，截止目前已上线慕课数量超过**7.26万**门，注册用户**4.4亿**，学习人数达到**12.1亿**人次，在校生获得慕课学分认定达**3.52亿**人次，覆盖国家**174个**，慕课数量与学习人数均为**世界第一!**

口2.1有底蕴|变革引领期

在2022年全国教育工作会议上，提出实施**国家教育数字化战略行动**，以**国家智慧教育平台**为重要抓手，利用数字技术全面赋能**学生学习、教师教学、学校治理、教育创新和国际合作**，推动教育数字化发展进入新阶段。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口 2.1 有底蕴|变革引领期

组 长	怀进鹏 部党组书记、部长	副组长	吴岩 部党组成员、副部长	王光彦 部党组成员、副部长

办公室	办公厅 统筹协调应用和示范		科技司 公共支撑、标准规范、安全运行		工作专班
	规划司	人事司	财务司	机关党委	驻部纪检监察组
其他成员	教材局	基教司	校外监管司	职成司	高教司
	督导局	教师司	思政司	学生司	新闻办

调整教育部网信工作领导小组，实行“双牵头”机制，强化网信工作的组织领导

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.1有底蕴|变革引领期

部党组书记、部长怀进鹏同志**亲自谋划、亲自部署、亲自推动**教育数字化工作，推动教育信息化发展进入数字化**新阶段**。

11次	**38**次	**93**项
网信领导小组会	**信息化专班会议**	**战略行动要点任务**

口2.2有理念 | “3C”

联结为先 Connection

互联网的本质是联结，而互联网三大定律之一的**麦特卡夫定律**告诉我们，网络价值同网络用户数量的平方成正比，**联结越多、覆盖越广，能量越大、价值越高**。因此，我们推进教育数字化工作，要做到**应联尽联**，推动更多**用户在线、平台互联、数据互通**，在联结中发挥互联网的倍增、溢出效应。

联结为先的本质是强化流量意识，通过活跃的应用，积累海量的数据，充分发挥数据的效能，推动教育数字化转型。在数字时代，流量越大，数据越丰富，画像越准确，潜在价值就越高。因此，流量是数字时代的黄金法则。

facebook TikTok

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.2有理念 | “3C”

内容为本 Content

要通过优质的内容增强平台的**吸引力、影响力**，进而提高用户的**活跃度、忠诚度**。内容是平台的灵魂，没有好的内容，平台将失去生命力。因此，我们要集中优势力量，用**最好的学校、最好的老师**，打造“永不落幕”的金课堂，以内容作为智慧教育平台的核心竞争力。

线上一流课程

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.2有理念 | “3C”

合作为要 Cooperation

众人拾柴火焰高，要充分发挥各方力量，形成协同推进教育数字化的蓬勃动力。因此，要加强**部内协同、部省合作和部际联动**，充分调动广大师生和社会主体的积极性，构建多元参与的教育数字化发展生态。

事实证明，仅靠政府供给，是难以满足师生多元化需求的。必须构建多元参与的资源供给生态，才能维持资源动态更新，持续提高质量。

口2.2 有理念| “四个坚持”

应用为王

秉持**“方法重于技术、组织创新重于技术创新”**工作理念，把业务应用摆在优先突出位置，不盲目追求技术先进，强调**每个人都可以做数字化的专家**。以应用需求驱动数字化建设，将**业务司局挺在一线抓应用**，团结更多力量参与，避免业务工作和数字化工作**“两张皮”**。

基教司
优质精品课程资源上线中小学平台应用首批省级专家指导团队建设

职成司
指导建设终身教育平台推动职教大脑建设，统筹教学和管理数据

高教司
高校教师教学组织和教学发展体系建设
智慧高教平台资源推广

学生司
提供精准就业服务
开拓就业服务平台岗位资源供给

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.2有理念| “四个坚持”

服务至上

贯彻以**人民为中心**的发展思想，严把**质量关**，以面向**广大师生的服务**作为主攻方向，解决师生的**痛点、难点、堵点**，让广大师生在共享互联网发展成果上有更多获得感，**让数据多跑路、师生少跑腿**。

服务立德树人
提供海量思政类的资源，打造大学生的思政阵地，做好网络育人工作。

实现一网通办
提供**26项**政务服务，全部实现线上办理，累计办件量超**6000万**。

开展教师研修
去年起，寒暑假开展教师研修，浏览超过**2.2亿**次，培训教师**4000万**人次。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.2有理念| “四个坚持”

简洁高效

怀进鹏部长反复强调不要搞重复建设，不盲目追求高端，把宝贵资金用在发展紧要处。我们建设国家智慧教育平台，就是充分**利用现有基础**，把散落在不同领域的**“珍珠”串成“项链”**，花了小钱、办了大事。

强化标准规范
建立系列的标准规范，规范项目、平台、数据、安全的管理，并对平台接入、版本更迭等方面提出明确要求。

强化集成整合
提出实现统一命名域名、统一用户认证、统一平台要素、统一运行监测，推动各方整合为一个有机整体。

强化运行监测
对国家智慧教育平台及外链平台进行监测，了解平台访问和应用情况，为平台资源优化提出工作建议。

口2.2有理念| “四个坚持”

安全运行

网络安全和信息化是一体之两翼，驱动之双轮。要以“时时放心不下”的责任感，统筹发展和安全，守牢网络安全底线，强化**内容安全、技术安全、数据安全、算法安全，**健全内容审核、数据保障、产权保护机制，确保产权清晰无争议、安全运行有保障。

内容安全

建立内容审核管理规范，开展国家智慧教育平台的内容安全专项治理，做好“**上线必审、更新必审、审必到位**”。

技术安全

落实网络安全**等保制度**，健全安全**监测通报机制**，开展网络安全**攻防演习**，提高抵御有组织网络攻击的能力。

数据安全

落实数据**分类分级制度**，重点保障师生**个人信息**，健全**数据全生命周期**保障机制，探索开展数据安全评估。

算法安全

开展GPT的**专项研究**，掌握生成式人工智能对教育的影响；参与大模型备案工作，探索建立教育系统**算法备案**制度。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.2有理念 | 四个数字

若**数字教育**是一辆车，**数字科技**是发动机，**数字人文**是方向盘，**数字伦理**是刹车器。

新型教育生态

教育结构重组 教育流程再造 教育文化重塑

数字教育 • 纽带

数字科技 • 动能

新的科技手段和新的思维方式
实现教育泛在化、个性化、精准化
打造无边界教学

数字人文 • 方向

强调坚持科学精神与人文情怀并重
构建和谐人技关系
厚植人文精神

数字伦理 • 底线

守住数字伦理的底线，关键看素养
重视数字伦理教育，提升高校师生数字素养

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.3有基础|硬件条件

中国教育和科研计算机网是我国研究**下一代互联网技术、开发重大应用、推动下一代互联网产业发展**的重要基础试验设施。

3万公里光纤传输网

3Tb网络总带宽

1873个高校和科研单位

2000万IPv4用户规模

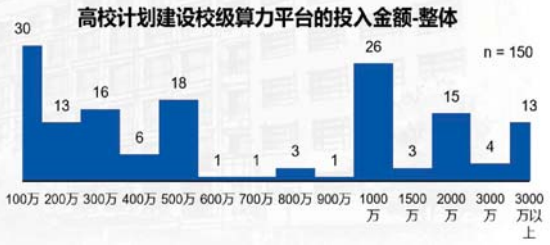
1000万IPv6用户规模

口2.3有基础|硬件条件

算力是数字时代的重要驱动力，高校是算力的高地

超算资源：2022年全球超级计算机排行榜TOP 500中，部署在大学的超级计算系统超过**50**个，中国高校**上海交大、中南大学、清华大学、南京大学、南方科技大学**入选。**北大、清华、北航**等**17所**高校建有超算中心。

普通算力：1981所学校建设校级数据中心，**58**所高校的计划投入金额规模达到**千万级**以上。浙江和**阿里**、上交大和**腾讯**、苏州大学和**华为云**进行深度合作，建立算力联盟。

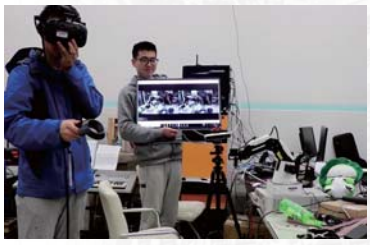


智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.3有基础|硬件条件

数字校园建设上，教育部印发了《高等学校数字校园规范》，提出了数字校园建设的要求。各高校对标规范要求，结合本单位特点，打造了一批**智慧教室、虚拟实训室**等，构建了未来学习环境。

四川大学华西校区



清华大学虚拟实训室

华中师范大学整体推进智慧校园

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.3有基础 | 软件条件

国家智慧教育公共服务平台

2022年3月，国家智慧教育公共服务平台上线。
一年多来，平台从分散**走向**集成**（2022.3）**，从中央**走向**地方**（2022.7）**，从线上**走向**线下**（2022.11）**，从国内**走向**国外**（2023.2）**，从校园**走向**社会**（2023.3）**，覆盖范围不断拓展，打造了数字教育发展的新坐标。

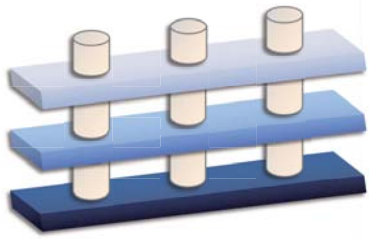
349.3亿次
平台浏览量

24.05亿人次
平台访客量

1.5年11次
平台迭代更新

口2.3有基础|软件条件

构建以基础教育、职业教育、高等教育为“三横”，德育、智育、体美劳育为“三纵“的“**三横三纵**”的资源服务格局，支撑课前备课、课堂教学、课后服务等教育全环节。



国家中小学智慧教育平台

- **53个**栏目
- **8.8万条**资源
- 资源较上线前增长**4倍**

国家职业教育智慧教育平台

- **10381门**在线精品课
- **2213门**视频公开课
- 覆盖**19个**专业大类**467个**专业

国家高等教育智慧教育平台 Smart Education of China · Higher Education

- **2.7万门**优质课程
- **1804条**国家一流课程
- 覆盖**13个**学科门类**93个**专业

打造世界最大的数字教育资源库，支撑世界最大规模的教育

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.3有基础 | 软件条件

- **集成21个慕课平台和各类资源，建设上线全球最大国家高等教育智慧教育平台**
- **一年来，用户覆盖174个国家和地区**

- **汇聚资源：覆盖13个学科门类、93个专业类**
- **五育并举：德、智、体、美、劳**
- **横向联通：课内教育与课外教育**
- **纵向贯通：本科、研究生教育**

成为覆盖高等教育人才培养全过程的综合服务平台

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.4有应用|支撑疫情期间大规模在线教育

服务“停课不停教，停课不停学”

全区域
全覆盖
全方位

- **授课教师：108万人**
- **在线学习：35亿人次**
- **在线课程：1719万门次**

- **全国高校课程开出率91%**
- **教师在线教学认可度80%**
- **学生在线教学满意度85%**

- 组织37家基础好、实力强的在线课程平台和技术平台
- 带动110余家社会和高校平台积极主动参与

学堂在线 xuetangx.com　爱课程 iCourse　超星　好大学在线　人卫慕课 PMPHMOOC.COM

口2.4有应用|汇聚优质资源促进区域教育协调发展

慕课西行

慕课西行推动**更有质量的公平**。教育部启动实施了**“慕课西部行计划”**，运用信息技术赋能教育、连接东西，通过成千上万个慕课、基于慕课应用的线上线下混合式教学、“同步课堂”等方式，**帮助西部高校提升教学质量**。

19.22万门
定制课程

4.95亿人次
学生学习

446.77万门次
混合教学

183.24万人次
教师应用

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.4有应用|提高高校实验教学质量

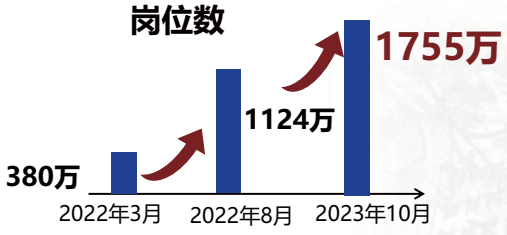
虚拟仿真实验平台“实验空间”汇集了**3488门**课程，**174所**中西部高校参与共建**810门**虚拟仿真实验教学课程，其中**196门**被评为国家级一流课程。**179所**中西部高校利用“实验空间”已有虚拟仿真实验课程开设在线实验课程，组建了**2615个**教学班。

南航和西北工大、贵州理工体验我国自主研制的C919大型客机“装配”过程

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

口2.4有应用|支撑服务大学生创业就业

24365 一职为你 国家大学生就业服务平台
2 4 3 6 5 校 园 招 聘 服 务



累计19.3万家用人单位面向2023届高校毕业生提供招聘专场102场，汇集就业岗位信息达1755万条。

智慧高教平台设立“创课平台”板块，遴选近500门创新创业慕课、微课和虚拟仿真实验以及100家创新创业实践教育基地等优质资源。

□2.5有自信|世界数字教育大会

时任国务院副总理
孙春兰出席会议并致辞

教育部部长怀进鹏
作主旨演讲

全球超过**130个**国家和地区的代表参会
相关报道及转载总计**13500余篇**

世界数字教育大会成果

- ◆ 发布中国智慧教育蓝皮书和智慧教育发展指数
- ◆ 发布智慧教育平台标准规范
- ◆ 发布成立世界数字教育联盟的倡议
- ◆ 发布世界数字教育发展合作倡议
- ◆ 与三大电信运营商举行战略合作签约仪式

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□2.5 有自信|哈马德国王奖

国家智慧教育平台 获**2022年度联合国教科文组织**哈马德·本·伊萨·阿勒哈利法国王**教育信息化奖**。

共有58个教科文组织会员国的98个项目申报该奖项，中国“国家智慧教育平台”项目凭借“**通过数字学习平台促进公众的知识获取**”方面的突出成绩获奖。中国**第三次**获得该奖项，**成为世界上获奖次数最多的国家**。

教科文组织认为：

2022年推出的中国“**国家智慧教育平台**”**包罗万象**，提供大量与课程匹配的学习资源，包括8万项涵盖各年级和学科的基础教育内容、1.9万项职业教育内容，以及2.7万项高等教育线上课程。该平台还包括**丰富的课外材料供学生全面学习**，此外，项目还涵盖数字能力建设—**为逾千万教师提供培训**，**惠及偏远和农村地区学生**—进而提高**中国教育**的**质量**和**公平性**。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□2.5有自信|世界慕课与在线教育大会

2019年
中国慕课大会

发布《中国慕课行动宣言》

2020年
世界慕课大会

发布《慕课发展北京宣言》

2021年
世界慕课与在线教育大会

推介慕课建用学管中国范式

2022年
世界慕课与在线教育大会

发布《世界高等教育数字化发展报告》和《世界高等教育数字化发展指数》

2023年
世界慕课与在线教育大会（米兰）

实现数字教育的理论引领和实践引领

口 2.5有自信 | 慕课出海

世界慕课联盟于2020年12月11日正式成立，由清华大学发起，并发布了《慕课发展北京宣言》。2021年12月9日，世界慕课联盟更名为**“世界慕课与在线教育联盟”**。

上线了**icourse**和**xuetangX**两个英文平台，包括英语、法语等**14种语言**的**1000余门**国际化课程资源。能够为全球学习者免费提供配套教学服务，覆盖**177个国家和地区。**

中国慕课与**印度尼西亚**国家平台签署合作协议，**中国34所大学**为印尼提供**104门**高水平慕课，支持印尼**300多所高校**学生的在线学习。

慕课出海1.0
慕课大会、慕课联盟
课程出海、平台出海

慕课出海2.0
资源出海、活动出海
服务出海、标准出海

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

三 形成新突破，扎实推进高等教育数字化重点任务

教育数字化是我国开辟教育发展新赛道和塑造教育发展新优势的重要突破口。“突破口”就是要攻坚克难、开疆拓土、引领发展，回答“教育强国建设、数字化何为”的时代命题。

改变学生学习	改变教师教学	改变教育治理	改变教育生态
更加公平地学	教师减负增效	促进高效管理	教育组织形式
更加智慧地学	打造数字课堂	促进便捷服务	教育教学模式
更加高效地学	教师队伍建设	促进科学决策	教育评价机制

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

- **横向比较**，要有自信，我国教育数字化发展已经处于世界前列；
- **纵向比较**，相较基础教育、职业教育而言，我们仍有不少值得学习的地方。
- 自去年年底分管教育数字化工作以来，我到湖南、宁夏等地调研教育数字化工作，看了一些地方和学校，他们利用数字化**手段之强、覆盖之广、应用之深、效果之好**，超乎我的想象。


宁夏“西海固”地区调研


湖南常德特殊学校调研


湖南中小学调研

□3.1 重点工作一：以数字化改变学生学习

- 数字时代，学生知识获取变得更加容易，学习门槛大大降低
- 对学生的综合素质提出了更高的要求，更注重沟通能力、整合能力、创新能力
- 运用数字技术改变学生的学习，构建适应数字时代的学习生态

实现更加公平地学　**实现更加智慧地学**　**实现更加高效地学**

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.1 以数字化改变学生学习 | 更加公平地学

形势分析

中西部和东部学校的差距客观存在
中西部在高校、教师、学生数量上，均占了普通高校的半壁江山
振兴中西部高等教育事关教育强国整体战略，事关中国式现代化总体进程

行动方向

慕课西部行2.0

拓围　**深化**　**创新**

更优组织、更具智慧、更加创新、更加持续

福建工程学院与新疆农业大学、喀什大学、巴音郭楞职业技术学院等新疆高校携手打造“福建—新疆”高校融合式同步云上课程

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.1 以数字化改变学生学习 | 更加智慧地学

变革学生学习模式，建设一批未来学习中心

新型学习组织	智慧学习空间	新学习生态
整合高校图书馆各类线上线下资源，支撑学习方式变革和知识创新创造。	虚实融合，集信息服务中心、学习支持中心、教学支持中心为一体。	立足提高知识创新、转化和终身学习能力，培育融合创新的学习新生态。

在2023年全国教育数字化现场推进会上，武汉理工大学利用图书馆，融合虚拟现实等技术，打造未来学习中心，展示了从读纸质的书转变为读VR的书。

未来学习中心

□3.1 以数字化改变学生学习 | 更加高效地学

形势分析

知识大爆炸的时代，时刻保持学习才能满足社会需求

人口负增长的时代，必须尽快将“人口红利”转化为“人才红利”

行动方向

推动高教优质资源向社会开放，为更多学习者提供学习机会

利用高校文献资源共建共享体系，扩大优质学术资源覆盖面

上线国家智慧教育读书平台

发布智慧教育App

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.2 重点工作二：以数字化改变教师教学

- 数字技术与教育教学深度融合，将改变传统的教学模式，对教师的数字素养和教学能力提出全面的要求
- 教师工作效率大大提升•课堂呈现形式大大丰富•教师队伍建设大大强化

支撑	支撑	支撑
教师减负增效	打造数字课堂	教师队伍建设

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.2 以数字化改变教师教学 | 支撑教师减负增效

形势分析

让教师从简单而重复的劳动中解放

有更多精力投入到钻研教学方法、创新教育模式、打造精品课堂

行动方向

普及智能教学系统、智能教学助手等工具，提供丰富的教育资源，减轻教师备课的压力

研制学科知识图谱，结合用户行为大数据，助力实现因材施教、个性化教学

华中师大打造小雅智能教学平台
多样化教学资源、AI赋能教学、教师分层分组教学
过程性数据、课程画像和师生画像

□3.2 以数字化改变教师教学 | 支撑打造数字课堂

形势分析

部分高校实验教学条件仍有短板，
无法高质量开展实验教学
高危或极端环境
高成本、高消耗、不可逆操作

行动方向

建设虚拟仿真实验课程
沉浸性、融合性、互动性强
“网上做实验”和“虚拟做真实验”

福州软件职业技术学院课程元宇宙

高校借助沉浸式虚拟现实等技术创设数字孪生校园，学生身在其中，开展数字化学习活动。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.2 以数字化改变教师教学 | 支撑教师队伍建设

形势分析

受空间地域限制，学科专业归属影响
教师交流受限、教研合作较少

行动方向

建设一批跨学科、跨校际、动态开放的虚拟教研室
- 创新教研形态
- 加强教学研究
- 共建优质资源
- 开展教师培训

启动虚拟教研室建设试点项目

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.3 重点工作三：以数字化改变教育治理

要运用大数据提升国家治理现代化水平，实现政府决策科学化、社会治理精准化、公共服务高效化。

—— 习近平在十九届中共中央政治局第二次集体学习时讲话（2017年12月）

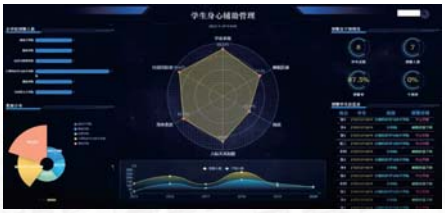
- 以管理流程为主的线性范式逐渐向以数据为中心的扁平化、平台化范式转变。
- 教育管理由“**粗放式**”向“**精准化**”转变。
- 高校应把握大方向，推进学校治理能力的提质升级，提高教育治理现代化水平。

促进高效管理　**促进便捷服务**　**促进科学决策**

□3.3 以数字化改变教育治理 | 促进高效管理

形势分析

经过多年发展，当前高校基本**实现核心业务的数字化支撑全覆盖**。但是不少系统**只是将线下的流程机械地搬到线上**，反而增加了管理负担。



西安电子科技大学学生身心辅助管理

行动方向

一方面，通过数字技术改变行政办公模式，**推动流程再造，提高管理效率，降低行政成本，提高办公灵活度**。

另一方面，通过大数据技术可以及时掌握校园环境和学生动态，根据学生个性情况实施**精准管理**，及时处理突发事件，提高管理的效能。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.3 以数字化改变教育治理 | 促进便捷服务

形势分析

近年来，各地政府陆续出台了“只进一扇门”、“最多跑一次”、“不见面审批”等改革措施。高校积极改革，推动“**一网通办**”实现数据多跑路、群众少跑腿。

行动方向

高校要深化面向师生的服务改革，重点围绕师生关注的**难点堵点**问题和**高频办理**事项，以数字技术优化服务流程、提升服务体验，**争取从“最多跑一次”到“一次都不跑”**。

智慧北航 “一网通办”

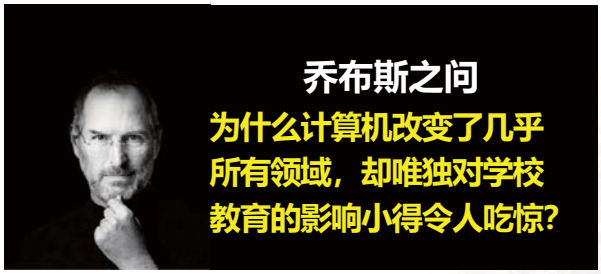
智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.3 以数字化改变教育治理 | 促进科学决策

武汉理工大学通过“大屏汇报、数据说话”，展示了何为数据支撑下的科学决策机制

学校要充分发挥**数据效能**，构建教育**科学决策**机制，聚焦学校改革发展的重点任务，因需汇聚**业务数据**，结合经济发展等**外部数据**，构建大数据分析**决策指标**，实时汇聚、系统分析、深入挖掘数据价值，推动教育决策由经验驱动向数据驱动转变，提升教育治理的智能化水平。

3.4 重点工作四：以数字化改变教育生态



- 所有改变都有量变到质变的过程，当前我们已经看到了以数字化推动教育深层次变革的曙光
- 敢为天下先。以数字技术变革教育组织形式、教育教学模式和教育评价机制

变革	变革	变革
教育**组织形式**	教育**教学模式**	教育**评价机制**

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

3.4 以数字化改变教育生态 | 变革教育组织形式

高起点建设国家数字大学

- 创新现代大学的组织形式，打造**数字时代新型大学**。
- 探索开放灵活的学分认定和学历学位授予机制，颁发**微学分、微证书**，支撑构建**人人皆学、处处能学、时时可学**的学习型社会。
- 推动优质课程向海外开放，通过**在线学习**的方式，给留学生颁发证书，打造**“留学中国”数字教育品牌**。

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

3.4 以数字化改变教育生态 | 变革教育教学模式

以GPT为代表的人工智能应用将对教育带来深层次的变化

改变教学模式	改变教学要求	改变专业布局

“师生机”三元交互教学新模式

依靠简单脑力劳动的工作将被替代，特别是律师、医生等高知识附加值的职业，被取代的可能性越大。
因此，要及时调整专业布局，以应对人工智能带来的挑战。

□3.4 以数字化改变教育生态 | 变革教育评价机制

- 改进**结果评价**，强化**过程评价**，探索**增值评价**，健全**综合评价**，利用信息技术，提高教育评价的科学性、专业性、客观性。
- **改变学生评价：**构建从入学到就业的动态跟踪机制，全面评价学生的综合素质。
- **改变教师评价：**利用数据科学评价教师发展，共享教师排查教师违法问题。
- **改变学校评价：**利用大数据支撑教学成果评估、学科评估等工作。

长沙市以网络学习空间人人通为载体和纽带，全面收集教学行为数据和学生成长数据，形成大数据成长档案

西安电子科技大学构建学习过程大数据采集流程，绘制学生数字画像，颁发线上线下学习双证书

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

□3.4 以数字化改变教育生态 | 变革教育评价机制

中国GPT的机遇和挑战

教育场景	师生、生生 →	人际+人机	教育环境	信息化 →	智能化
教学内容	静态的学科知识 →	动态的综合任务	变 教学模式	以教为主 →	以学为主
学习方式	人际协作 →	人技协同	育人理念	知识为主 →	能力为重 价值为先

人的培养目标	教育的基本理论
不变	
立德树人的根本任务	教学的原则

智慧教育 Smart Education of China
中华人民共和国教育部 Ministry of Education of the People's Republic of China

各级教育部门
发挥好“**战略指挥部**”的职能
- 综合协调、政策引导，汇聚各方力量
- 服务中心、思想中心、组织中心和指挥中心

高校领导干部
发挥好“**前线指挥员**”的权责
- 一把手带头抓数字化，从嘴上落到脚下
- 带头抓、带头干、带头改

广大教师
发挥好“**一线战斗员**”的作用
- 投入足够的精力、投入足够的时间
- 数字技术武装头脑、武装课堂、武装教学

谢谢

中华人民共和国教育部
Ministry of Education of the People's Republic of China