

《中华人民共和国密码法》颁布施行五周年来

**密码新政策办法**

2024年12月

**金融和重要领域**

**前 言**

2019年10月26日，《中华人民共和国密码法》（简称《密码法》）正式颁布，自2020年1月1日起正式施行。密码应用在金融、公安、社保、交通、能源、水利、教育、广电、税务等领域不断向纵深拓展。

同时，5G、物联网、云计算、大数据、人工智能、区块链、量子通信、数字经济等新技术新业态正与密码紧密融合。密码持续发挥着在保障国家网络与信息安全中的重要作用。

以下为《密码法》颁布施行五年来，我国金融和重要领域新出台的部分公开的密码相关政策办法。

**目 录**

**[一、金融领域密码应用 1](#_Toc14505)**

**[二、基础设施网络密码应用 4](#_Toc28728)**

[（一）基础信息网络密码应用 4](#_Toc16979)

[（二）交通运输网络密码应用 5](#_Toc412)

[（三）能源基础设施网络密码应用 9](#_Toc803)

[（四）资源信息化网络密码应用 11](#_Toc24539)

[（五）城市基础设施网络密码应用 13](#_Toc1916)

**[三、密码与数字经济融合应用 15](#_Toc29229)**

[（一）现代农业密码应用 15](#_Toc31891)

[（二）先进制造业密码应用 15](#_Toc28771)

[（三）现代服务业及新兴产业密码应用 17](#_Toc17564)

**[四、信息惠民密码应用 22](#_Toc16103)**

[（一）电子政务密码应用 22](#_Toc16103)

[（二）社会治理密码应用 24](#_Toc6483)

[（三）民生保障密码应用 24](#_Toc25491)

**[五、密码科技创新和基础支撑能力 28](#_Toc6137)**

1. 金融领域密码应用

《国家金融监督管理总局关于印发银行保险机构数据安全管理办法的通知》

金规〔2024〕24号，自2024年12月27日起施行

第二十八条　银行保险机构应当按照“业务必要授权”原则，对敏感级及以上数据严格实施授权管理，制定数据访问闭环管理机制，并对数据访问行为实施审计。确因业务需要从生产环境提取数据的，应当建立严格的审批程序，并明确数据使用或者保存期限。

银行保险机构利用互联网等信息网络开展数据处理活动时，要落实网络安全等级保护、关键信息基础设施安全保护、密码保护等制度要求。  
<https://www.gov.cn/zhengce/zhengceku/202412/content_6995081.htm>

《中国人民银行 国家发展改革委 工业和信息化部 金融监管总局 中国证监会 国家数据局 国家外汇局关于印发＜推动数字金融高质量发展行动方案＞的通知》  
银发〔2024〕200号，发文时间：2024年11月21日

　　（十七）加强数据和网络安全防护。指导金融机构严格落实数据保护法律法规和标准规范，完善数据安全管理体系，强化数据安全的商用密码保护，建立健全全流程数据安全管理机制。

<http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/5519902/index.html>

《证券期货业网络和信息安全管理办法》  
中国证券监督管理委员会令（第218号），自2023年5月1日起施行  
　　第二十六条　核心机构应当对交易、行情、开户、结算、风控、通信等重要信息系统具有自主开发能力，掌握执行程序和源代码并安全可靠存放。

　　经营机构应当根据自身发展需要，加强自主研发能力建设，持续提升自主可控能力。

　　核心机构和经营机构应当按照国家及中国证监会有关要求，开展信息技术应用创新以及商用密码应用相关工作。

<https://www.gov.cn/gongbao/2023/issue_10526/202306/content_6887131.html>

《银行保险机构消费者权益保护管理办法》  
中国银行保险监督管理委员会令2022 年第9号，自2023年3月1日起施行

　　第四十五条　银行保险机构应当在消费者授权同意等基础上与合作方处理消费者个人信息，在合作协议中应当约定数据保护责任、保密义务、违约责任、合同终止和突发情况下的处置条款。

　　合作过程中，银行保险机构应当严格控制合作方行为与权限，通过加密传输、安全隔离、权限管控、监测报警、去标识化等方式，防范数据滥用或者泄露风险。

<https://www.gov.cn/gongbao/content/2023/content_5753317.htm>  
  
  
《中国人民银行 市场监管总局 银保监会 证监会关于印发＜金融标准化“十四五”发展规划＞的通知》  
银发〔2022〕18号，成文日期为2022年1月23日  
　　·健全金融业网络安全与数据安全标准体系。建立健全金融业关键信息基础设施保护标准体系，支持提升安全防护能力。加强金融网络安全能力评估、风险排查、安全防御、漏洞管理等标准建设，助力提升网络安全威胁发现、监测预警、应急处置、攻击溯源能力。推动金融信息科技外包服务评价、金融机构安全运营中心建设、金融数据分级、生命周期安全与评估、商用密码应用等标准供给与实施。  
<http://www.gov.cn/xinwen/2022-02/09/5672688/files/babb8d6995b14c5e9f1ffac89c6fd999.pdf>

《中国人民银行关于加强支付受理终端及相关业务管理的通知》  
银发〔2021〕259号，成文日期为2021年10月12日  
　　·清算机构、收单机构应当按照《中国人民银行关于强化银行卡受理终端安全管理的通知》（银发〔2017〕21号）规定，对银行卡受理终端采取密码识别技术等有效手段，确保银行卡受理终端序列号不被篡改。  
<http://www.gov.cn/zhengce/zhengceku/2022-02/25/content_5675558.htm>

《理财公司理财产品销售管理暂行办法》  
中国银行保险监督管理委员会令2021年第4号，自2021年6月27日起施行  
　　第七条　理财产品销售机构从事理财产品销售业务活动，应当持续具备下列条件：  
　　……

　　（四）具备完善的防火墙、入侵检测、数据加密以及灾难恢复等信息安全管理体系和设施；  
　　……  
<https://www.gov.cn/gongbao/content/2021/content_5625997.htm>  
  
  
《证券基金经营机构信息技术管理办法》  
中国证券监督管理委员会令第179号，自2021年1月15日起修正施行  
 第三十一条　证券基金经营机构应当完善网络隔离、用户认证、访问控制、数据加密、数据备份、数据销毁、日志记录、病毒防范和非法入侵检测等安全保障措施，保护经营数据和客户信息安全，防范信息泄露与损毁。  
<https://www.gov.cn/gongbao/content/2021/content_5600087.htm>

《中国银保监会关于印发监管数据安全管理办法（试行）的通知》

银保监发〔2020〕43号，自2020年9月23日起施行  
　　·本办法所称监管数据安全是指监管数据在采集、处理、存储、使用等活动（以下简称监管数据活动）中，处于可用、完整和可审计状态，未发生泄露、篡改、损毁、丢失或非法使用等情况。  
　　·银保监会建立健全监管数据安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。  
<http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=959801&itemId=928&generaltype=0>

《中国银保监会办公厅关于预防银行业保险业从业人员金融违法犯罪的指导意见》  
银保监办发﹝2020﹞18号，成文日期为2020年2月24日

·银行保险机构要制定内部网络安全管理制度和操作规程，建立监督制约机制，确保制度得到刚性执行。加强数据安全管理，严格控制数据授权范围，实现数据分类、重要数据备份和加密。  
<http://www.gov.cn/zhengce/zhengceku/2020-03/24/content_5494985.htm>

# 二、基础设施网络密码应用

## （一）基础信息网络密码应用

《工业和信息化部等十二部门关于印发＜5G规模化应用“扬帆”行动升级方案＞的通知》

工信部联通信〔2024〕227号，成文日期为2024年11月22日

　　（五）筑牢5G应用安全防护屏障

　　完善通信网络安全防护管理，加快新兴行业5G终端安全、网络设备安全、数据安全、密码安全等关键技术研究，推动研制具备虚拟化、智能化、自适应能力的安全产品。发挥5G应用安全创新推广中心集智攻关优势，打造5G应用安全产业核心竞争力。面向重点行业开展5G应用安全标杆锻造，提炼30项以上原子化5G应用安全能力。  
<https://www.gov.cn/zhengce/zhengceku/202411/content_6989412.htm>

《工业和信息化部关于印发“十四五”信息通信行业发展规划的通知》  
工信部规〔2021〕164号，成文日期为2021年11月1日

　　·健全行业网络安全审查体系，推进网络关键设备安全检测认证，建立供应商网络安全成熟度认证等供应链风险管理制度，稳妥有序推进商用密码应用，提升网络基础设施安全保障水平。  
<http://www.gov.cn/zhengce/zhengceku/2021-11/16/content_5651262.htm>

《工业和信息化部、中央网络安全和信息化委员会办公室 、科学技术部 、生态环境部、住房和城乡建设部 、农业农村部、国家卫生健康委员会、国家能源局关于印发＜物联网新型基础设施建设三年行动计划（2021—2023年）＞的通知》  
工信部联科〔2021〕130号，成文日期为2021年9月10日

　　·强化安全支撑保障。加快物联网领域商用密码技术和产品的应用推广，建设面向物联网领域的密码应用检测平台，提升物联网领域商用密码安全性和应用水平。  
<http://www.gov.cn/zhengce/zhengceku/2021-09/29/content_5640204.htm>

《工业和信息化部 中央网络安全和信息化委员会办公室 国家发展和改革委员会 教育部 财政部 住房和城乡建设部 文化和旅游部 国家卫生健康委员会 国务院国有资产监督管理委员会 国家能源局关于印发＜5G应用“扬帆”行动计划（2021-2023年）＞的通知》  
工信部联通信〔2021〕77号，成文日期为2021年7月5日  
　　·开展5G应用安全示范推广。在5G应用中推广使用商用密码，做好密码应用安全性评估。  
<http://www.gov.cn/zhengce/zhengceku/2021-07/13/content_5624610.htm>

## （二）交通运输网络密码应用

《铁路关键信息基础设施安全保护管理办法》

中华人民共和国交通运输部令2023年第20号，自2024年2月1日起施行  
　　第十七条  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铁路关键信息基础设施，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每年至少开展一次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铁路关键信息基础设施安全检测和风险评估、网络安全等级测评制度相衔接，避免重复评估、测评。  
<https://xxgk.mot.gov.cn/2020/jigou/fgs/202401/t20240104_3980678.html>  
  
  
《公路水路关键信息基础设施安全保护管理办法》  
中华人民共和国交通运输部令（2023年第4号），2023年6月1日起施行  
　　第十八条　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公路水路关键信息基础设施，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每年至少开展一次商用密码应用安全性评估。  
<https://www.gov.cn/gongbao/2023/issue_10566/202307/content_6890791.html>

《交通运输部 国家铁路局 中国民用航空局 国家邮政局 中国国家铁路集团有限公司关于印发＜加快建设交通强国五年行动计划（2023-2027年）＞的通知》

交规划发〔2023〕21号，发文日期为2023年3月29日

　　·开展网络和数据安全能力提升行动。组织实施网络安全实网攻防演练，加强商用密码应用推广。  
  
  
《交通运输部办公厅关于印发＜道路运输电子证照运行服务规范（试行）＞的通知》

交办运函〔2022〕1606号，成文日期为2022年11月21日  
　　·省级交通运输主管部门应加强电子证照的数据安全保护，严防非法授权访问、非法数据出库等行为，防止数据泄露，保障数据安全。加强国产密码应用和安全性评估。

<https://xxgk.mot.gov.cn/2020/jigou/ysfws/202211/t20221121_3712703.html>

《工业和信息化部办公厅关于印发车联网网络安全和数据安全标准体系建设指南的通知》

工信厅科〔2022〕5号，成文日期为2022年2月25日  
　　·总体与基础共性标准是车联网网络安全和数据安全的总体性、通用性和指导性标准，包括术语和定义、总体架构、密码应用等3类标准。其中，密码应用标准主要规范车联网密码应用通用要求，明确数字证书格式、数字证书应用、设备密码应用等要求。

<https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_e36a55c43a3346c9a4b31e534b92be44.html>

《交通运输部 科学技术部关于印发〈交通领域科技创新中长期发展规划纲要（2021—2035年）〉的通知》  
交科技发〔2022〕11号，成文日期为2022年1月24日  
　　·围绕全面提升智慧交通发展水平，集中攻克交通运输专业软件和专用系统，加快移动互联网、人工智能、区块链、云计算、大数据等新一代信息技术及空天信息技术与交通运输融合创新应用，推动交通运输领域商用密码创新应用，加快发展交通运输新型基础设施。  
<http://www.gov.cn/zhengce/zhengceku/2022-04/06/content_5683595.htm>

《工业和信息化部关于大众消费领域北斗推广应用的若干意见》  
工信部电子〔2022〕5号，成文日期为2022年1月17日  
　　·加快推进高精度、低功耗、低成本、小型化的北斗芯片及关键元器件研发和产业化，形成北斗与5G、物联网、车联网等新一代信息技术融合的系统解决方案。鼓励应用商用密码，保障产品安全。  
<http://www.gov.cn/zhengce/zhengceku/2022-01/29/content_5671098.htm>

国家邮政局、国家发展和改革委员会、交通运输部联合印发《“十四五”邮政业发展规划》  
发布日期为2021年12月28日  
　　·加强网络数据安全。严格落实网络安全工作责任制，完善行业网络安全、数据安全有关标准规范。在网络建设和运营过程中，同步规划、建设、使用有关安全保护措施，严格落实国家关于等保、关保、密评等有关要求。加强行业关键信息基础设施保护,组织编制相关规划，强化行业指导和监督。加强行业重要数据和个人信息保护。  
<https://www.spb.gov.cn/gjyzj/c100009/c100012/202201/f7f90da54b10432bb5cff518b4c7ebae.shtml>  
  
  
《交通运输部关于印发＜数字交通“十四五”发展规划＞的通知》  
交规划发〔2021〕102号，成文日期为2021年12月22日  
　　·健全国家综合交通运输信息平台基础支撑和网络安全防护体系，加强关键信息基础设施保护和商用密码技术应用。  
　　·推动安全可信服务和产品应用。完善行业网络身份认证和设备安全接入认证体系，加强商用密码技术应用、接入检测、监督检查等。强化网络安全产品供应链管理。推进重要信息系统密码技术应用，完善行业密码服务基础设施。  
<https://xxgk.mot.gov.cn/2020/jigou/zhghs/202112/t20211222_3632469.html>

《工业和信息化部关于加强车联网网络安全和数据安全工作的通知》

工信部网安〔2021〕134号，成文日期为2021年9月15日  
　　·认定为关键信息基础设施的，要落实《关键信息基础设施安全保护条例》有关规定，并按照国家有关标准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。  
<http://www.gov.cn/zhengce/zhengceku/2021-09/16/content_5637709.htm>  
  
  
《交通运输部关于印发＜交通运输领域新型基础设施建设行动方案（2021—2025年）＞的通知》  
交规划发〔2021〕82号，成文日期为2021年8月31日  
　　·加强网络安全保护。严格落实等级保护制度，加强关键信息基础设施保护，强化态势感知能力建设，保障数据共享安全可控。建立健全数据安全保护制度，加强基础设施数据全生命周期管理和分级分类保护，落实数据容灾备份措施。推进商用密码技术应用。  
<http://www.gov.cn/zhengce/zhengceku/2021-09/29/content_5639987.htm>

《工业和信息化部办公厅关于开展车联网身份认证和安全信任试点工作的通知》

工信厅网安函〔2021〕148号，成文日期为2021年6月8日

为贯彻落实《新能源汽车产业发展规划（2021-2035年）》《智能汽车创新发展战略》和车联网产业发展专委会第四次全体会议工作任务要求，加快推进车联网网络安全保障能力建设，构建车联网身份认证和安全信任体系，推动商用密码应用，保障蜂窝车联网（C-V2X）通信安全，现开展车联网身份认证和安全信任试点工作。  
<https://www.gov.cn/zhengce/zhengceku/2021-06/10/content_5616843.htm>  
  
  
《交通运输部办公厅关于印发＜城市轨道交通自动售检票系统运营技术规范（试行）＞的通知》  
交办运〔2022〕27号，成文日期为2021年5月27日  
　　·自动售检票系统的应用软件具有应用软件操作权限管理功能，操作员账户和密码采用加密形式存储，并满足日常定期修改密码要求，支持对轨道交通专用票、二维码车票密钥的统一管理，主要包括密钥制作、密钥下发、数据验签和第三方密钥管理。轨道交通专用票、二维码车票、一卡通卡等密钥的使用和管理符合国家网络安全及商用密码管理的相关法律法规和标准要求。  
　　·自动售检票系统的数据安全管理应具有灾难备份及数据恢复功能，所有敏感数据在存储和传输时采用高安全加密方式。  
　　·互联网票务的密钥使用和管理应符合国家网络安全及商用密码管理的相关法律法规，并保证支付安全。  
<https://xxgk.mot.gov.cn/2020/jigou/ysfws/202206/t20220609_3658774.html>

《交通运输部办公厅关于加快推广应用道路运输电子证照提升数字化服务与监管能力的通知》

交办运〔2021〕25号，成文日期为2021年3月16日  
　　·统一开发电子证照系统。根据相关标准规范要求，采用国产密码算法技术，建设开发部级电子证照系统，同时推进与部级运政系统、网上便民运政系统、部移动客户端和微信公众号、国家政务服务平台等相关信息系统的对接工作。统一开发省级电子证照系统基础软件。  
<http://www.gov.cn/zhengce/zhengceku/2021-04/02/content_5597486.htm>

《交通运输部关于推动交通运输领域新型基础设施建设的指导意见》

交规划发〔2020〕75号，成文日期为2020年8月3日  
　　·加强关键信息基础设施保护。建设集态势感知、风险预警、应急处置和联动指挥为一体的网络安全支撑平台，加强信息共享、协同联动，形成多层级的纵深防御、主动防护、综合防范体系，加强威胁风险预警研判，建立风险评估体系。切实推进商用密码等技术应用，积极推广可信计算，提高系统主动免疫能力。

<http://www.gov.cn/zhengce/zhengceku/2020-08/06/content_5532842.htm>

《交通运输部办公厅关于充分发挥全国道路货运车辆公共监管与服务平台作用支撑行业高质量发展的意见》  
交办运〔2020〕18号，成文日期为2020年4月26日  
　　·加强网络安全管理。货运平台建设运维单位要根据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》等有关法律规定，做好网络运行安全和网络信息安全工作，完善安全等保三级系统的网络安全保护体系，建立健全网络安全防范、监测、通报、响应和处置机制。同时，运用自主可控密码技术，实现数据及传输安全管理。各级交通运输主管部门应严格管理数据应用，有效保证信息安全。  
<https://xxgk.mot.gov.cn/2020/jigou/ysfws/202006/t20200623_3316089.html>

《交通运输部关于印发＜推进综合交通运输大数据发展行动纲要（2020—2025年）＞的通知》  
交科技发〔2019〕161号，成文日期为2019年12月9日

　　·完善数据安全保障措施。推进交通运输领域数据分类分级管理，加强重要数据和个人信息安全保护，制定数据分级安全管理、数据脱敏等制度规范。推进重要信息系统密码技术应用和重要软硬件设备自主可控。  
<https://www.mot.gov.cn/zhengcejiedu/ytddxsqtdzhjtysdsjfz/xiangguanzhengce/201912/t20191213_3430331.html>  
  
（三）能源基础设施网络密码应用

《电力监控系统安全防护规定》

中华人民共和国国家发展和改革委员会令第27号，自2025年1月1日起施行

**第十一条** 生产控制区与电力监控专用网络的广域网之间的联接处应当设置电力专用纵向加密认证装置或者加密认证网关。

**第十二条** 电力调度机构应当依照电力调度管理体制建立基于数字证书等技术的分布式电力调度认证机制。生产控制区处理重要业务过程中应当采用应用层端到端加密认证机制，其中与电力调度机构交互业务数据应当纳入电力调度认证机制，保障数据传输的完整性和真实性。

<https://www.ndrc.gov.cn/xxgk/zcfb/fzggwl/202412/t20241211_1394960_ext.html>

《国家能源局关于加快推进能源数字化智能化发展的若干意见》

国能发科技〔2023〕27号，制发日期为2023年3月28日  
　　（十六）推动能源数据分类分级管理与共享应用。推动能源行业数据分类分级保护制度建设，加强数据安全治理。对于安全敏感性高的数据，提高数据汇聚融合的风险识别与防护水平，强化数据脱敏、加密保护和安全合规评估；对于安全敏感性低的数据，健全确权、流通、交易和分配机制，有序推动数据在产业链上下游的共享，推进数据共享全过程的在线流转和在线跟踪，支持数据便捷共享应用。加强行业大数据中心数据安全监管，强化数据安全风险态势监测，规范数据使用。充分结合全国一体化大数据中心体系建设，推动算力资源规模化集约化布局、协同联动，提高算力使用效率。  
<https://zfxxgk.nea.gov.cn/2023-03/28/c_1310707122.htm>

《国家能源局综合司关于印发＜2023年电力安全监管重点任务＞的通知》  
国能综通安全〔2023〕4号，成文日期为2023年1月17日

　　·推进电力行业网络与信息安全工作。组织开展网络安全五年行动计划中期评估，持续推进电力行业网络安全“明目”“赋能”“强基”行动。加强网络安全态势感知能力建设，推进国家级电力网络安全靶场建设，组织开展年度攻防演练。修订行业网络安全事件应急预案，建立完善网络安全监督管理技术支撑体系， 推动量子计算、北斗、商用密码等在电力行业的应用。

<http://zfxxgk.nea.gov.cn/2023-01/17/c_1310693609.htm>

《能源局关于印发＜电力行业网络安全等级保护管理办法＞的通知》

国能发安全规〔222〕101号，2022年11月16日起施行，有效期5年

**第二十一条**　电力企业采用密码进行等级保护的，应当遵照《中华人民共和国密码法》等有关法律法规和国家密码管理部门制定的网络安全等级保护密码技术标准执行。

**第二十二条**　电力企业网络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。运用密码技术进行网络安全等级保护建设与整改时，应当采用商用密码检测、认证机构检测认证合格的商用密码产品和服务。涉及商用密码进口的，还应当符合国家商用密码进口许可有关要求。

**第二十三条**　电力企业应当按照有关法律法规要求，开展商用密码应用安全性评估工作。  
<https://www.gov.cn/gongbao/content/2023/content_5743639.htm>

《国家能源局关于印发＜电力行业网络安全管理办法＞的通知》

国能发安全规〔2022〕100号，成文日期为2022年11月16日

　　·电力企业应当按照国家有关规定开展商用密码应用安全性评估等工作，未达到要求的应当及时进行整改；

　　·电力行业关键信息基础设施运营者应当于每年11月1日前，将当年关键信息基础设施安全保护工作的专项总结报行业部门，总结内容应当包括但不限于网络产品和服务采购情况、密码使用情况、下一年度安全保护计划等。  
<http://zfxxgk.nea.gov.cn/2022-11/16/c_1310683245.htm>

《国家能源局关于印发＜电力行业网络安全等级保护管理办法＞的通知》

国能发安全规〔2022〕101号，成文日期为2022年11月16日

　　·单独设置“网络安全等级保护的密码管理”章节，要求电力企业应当按照有关法律法规要求，开展商用密码应用安全性评估工作  
<http://zfxxgk.nea.gov.cn/2022-11/16/c_1310683235.htm>  
  
  
《工业和信息化部 国家发展和改革委员会 科学技术部 生态环境部 应急管理部 国家能源局关于“十四五”推动石化化工行业高质量发展的指导意见》  
工信部联原〔2022〕34号，成文日期为2022年3月28日  
　　·实施石化行业工业互联网企业网络安全分类分级管理，推动商用密码应用，提升安全防护水平。  
<http://www.gov.cn/zhengce/zhengceku/2022-04/08/content_5683972.htm>

《国家能源局关于印发＜2022年能源工作指导意见＞的通知》

国能发规划〔2022〕31号，成文日期为2022年3月17日

　　·加快能源系统数字化升级。积极开展煤矿、油气田、管网、电网、电厂等领域设备设施、工艺流程的智能化升级。推动分布式能源、微电网、多能互补等智慧能源与智慧城市、园区协同发展。加强北斗系统、5G、国密算法等新技术和“互联网+安全监管”智能技术在能源领域的推广应用。  
<http://zfxxgk.nea.gov.cn/2022-03/17/c_1310534134.htm>

《国家发展改革委 国家能源局关于印发＜“十四五”现代能源体系规划＞的通知》

发改能源〔2022〕210号，成文日期为2022年1月29日  
　　·网络安全管控。加快推进电力监控系统安全防护体系完善工程、电力信息系统密码基础设施建设工程、北斗时空基础设施应用及智能化运营体系工程建设，开展北斗时频网建设，推进重点企业电力北斗综合服务平台建设和终端应用试点。建成电力行业网络安全态势感知平台和全业务、分布式、高仿真的电力行业网络安全仿真验证环境。  
<https://www.ndrc.gov.cn/xxgk/zcfb/ghwb/202203/t20220322_1320016.html?state=123&code=&state=123>

（四）资源信息化网络密码应用

《水利部关于推进水库、水闸、蓄滞洪区运行管理数字孪生的指导意见》

水运管〔2024〕269号，成文日期为2024年10月14日  
　　（五）加强网络信息安全保障  
　　落实网络信息安全管理主体责任，严格执行国家和水利行业网络信息安全和保密管理规定，构建完善的网络安全组织管理体系、安全技术体系和安全运营体系，加强数据安全保护，全面保障数字孪生水利工程数据安全。落实工控系统分区分域、设备自主可控、国产商用密码保护、网络可信准入等要求。  
<https://www.gov.cn/gongbao/2024/issue_11726/202411/content_6989758.html>

《水利部关于印发＜水利建设市场经营主体信用信息管理办法＞的通知》

水建设〔2024〕201号，成文日期为2024年7月27日

    第二十八条　全国水利监管平台应加强信用信息安全基础设施和安全防护能力建设，保障信息安全。按照保护水利建设市场经营主体权益的要求，明确信息查询使用权限和程序，依据《信息安全等级保护管理办法》做好系统备案和安全保护等级确定，对重要信息加密保护，完善信息查询使用登记和审查制度，防止信息被窃取或泄露。  
<https://www.gov.cn/gongbao/2024/issue_11606/202409/content_6976921.html>

《自然资源部关于印发＜关于加强自然资源领域基础研究的若干举措＞的通知》

自然资发〔2024〕118号，成文日期为2024年6月30日

　　九、发展需求-数据-知识驱动的科研范式

　　以自然资源数据为基础，以专业领域知识为引导，以地球系统模拟为场景，推动大数据、人工智能、商用密码等先进技术在自然资源系统性复杂性问题研究上的创新应用，催生新的自然资源研究方向，提升自然资源创新效能。

<https://www.gov.cn/zhengce/zhengceku/202407/content_6960890.htm>

《自然资源部关于印发＜自然资源领域数据安全管理办法＞的通知》

自然资发〔2024〕57号，成文日期为2024年3月22日

　　第十二条 数据处理者应当对数据处理活动安全负主体责任,对各类数据实行分级防护，不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护，确保数据持续处于有效保护和合法利用的状态。  
　　……  
　　（三）利用互联网等信息网络开展数据处理活动时，要落实网络安全等级保护、关键信息基础设施安全保护、密码保护和保密等制度要求；  
　　……  
　　第二十三条 数据处理者应当在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志，并采用商用密码技术保护日志的完整性。其中，一般数据的日志留存时间不少于六个月，涉及重要数据安全事件处置、溯源的，相关日志留存时间不少于一年；涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间不少于三年。涉及核心数据安全事件处置、溯源的相关日志留存时间不少于三年。

<https://www.gov.cn/zhengce/zhengceku/202403/content_6942232.htm>

《自然资源部关于印发〈自然资源数字化治理能力提升总体方案〉的通知》

自然资发〔2024〕33号，成文时间为2024年2月5日

　　·要求健全密码应用保障体系，构建以密码技术为核心的自然资源数据安全防护体系，统筹国土、海洋、测绘、地调等已建商用密码平台，打造部级密码平台，利用商用密码技术和产品，为关键信息基础设施和重要信息系统提供统一的密码技术支撑。

<https://www.gov.cn/zhengce/zhengceku/202402/content_6931049.htm>

《自然资源部关于加快测绘地理信息事业转型升级更好支撑高质量发展的意见》  
自然资发〔2023〕158号，成文日期为2023年8月22日  
　　·加强地理信息安全监管。以安全应用为核心，完善测绘地理信息法规政策，建立测绘地理信息数据分类分级保护制度，研究制定地理信息数据流通和交易负面清单。推进保密处理技术研发应用，推动国产密码技术融合应用。加强卫星导航定位基准站安全管理，规范基准站备案、建设、运维和服务。  
<https://www.gov.cn/zhengce/zhengceku/202308/content_6899855.htm>

[《水利部办公厅关于印发2023年水利网信工作要点的通知》](http://www.mwr.gov.cn/zwgk/gknr/202303/t20230317_1649867.html" \o "《水利部办公厅关于印发2023年水利网信工作要点的通知》" \t "_blank)

[办信息〔2023〕73号，成文日期为2023年3月14日](http://www.mwr.gov.cn/zwgk/gknr/202303/t20230317_1649867.html" \o "《水利部办公厅关于印发2023年水利网信工作要点的通知》" \t "_blank)

　　·持续推进数字孪生海河建设。深入开展流域数据治理，完善海河流域水利一张图1.0并推广应用。初步搭建模型管理平台，开展模型库建设。强化数据安全防护，建设数据安全基础防护设施，加大密码技术应用。

　　·推进商用密码应用。开展以商用密码技术为核心的水利部数据安全治理平台项目建设，大力推进商用密码在小浪底水利枢纽、大藤峡水利枢纽等水利工程关键信息基础设施的应用，坚持数字孪生水利建设与密码应用“同步规划、同步建设、同步运行”原则，持续将商用密码应用落实情况统筹纳入水利网络安全监督检查范围，推动密码应用与网络安全、数据安全融合发展。

<http://www.mwr.gov.cn/zwgk/gknr/202303/t20230317_1649867.html>  
  
  
《自然资源部办公厅 国家林业和草原局办公室关于强化业务协同加快推进林权登记资料移交 数据整合和信息共享的通知》

自然资办发〔2023〕2号，成文日期为2023年1月12日  
　　四、健全林权登记与林业管理信息共享机制

各地自然资源和林草部门，应当立足本地信息化建设实际，通过多种方式、多种渠道，积极推进林业管理和林权登记信息互通共享，能够通过信息共享获取的材料，不得要求群众重复提交。  
　　（三）保障信息共享安全。各地要建立安全的信息共享物理环境、网络环境、数据加密与传输机制，保障共享数据安全。要制定信息共享安全制度，共享信息仅用于林业管理和林权登记工作，防止数据外泄，确保信息安全。  
<https://www.gov.cn/zhengce/zhengceku/2023-01/19/content_5737927.htm>  
  
  
《水利部关于印发〈“十四五”水利科技创新规划〉的通知》  
水国科〔2021〕416号，成文日期为2021年12月31日  
　　·开展水利关键信息基础设施网络安全防护体系研究,构建网络安全监控平台,研制安全可控的水利关键信息基础设施核心装备,并基于国产密码技术开展数据安全防护研究。  
<http://www.mwr.gov.cn/zwgk/gknr/202201/t20220117_1559761.html>  
  
  
（五）城市基础设施网络密码应用  
  
《住房城乡建设部关于印发＜城市数字公共基础设施标准体系＞的通知》

建标〔2024〕79号，成文日期为2024年10月25日  
　　9.安全与保障

　　规范信息技术应用创新、安全与保障等方面的要求，为网络基础设施、感知基础设施、算力基础设施、融合基础设施、公共数字底座、应用支撑、建设与运营提供安全支撑，包括网络安全、数据安全、密码应用安全和其他4个子类标准。  
　　（3）密码应用安全

　　规范城市数字公共基础设施的物理与环境、网络与通信、设备与计算、应用与数据等国产密码应用的安全要求。  
<https://www.gov.cn/zhengce/zhengceku/202411/content_6984542.htm>

《住房和城乡建设部等部门关于加快发展数字家庭 提高居住品质的指导意见》

建标〔2021〕28号，成文日期为2021年04月06日  
　　·强化网络和数字安全保障。数字家庭系统应同步规划、同步建设、同步使用网络安全技术。按照法律法规规定和国家强制性标准要求，采取技术等必要措施，保障数字家庭系统安全稳定运行，防止信息泄露、损毁、丢失，确保收集、产生数据和个人信息安全。遵守密码应用规定，形成安全可控完整的产业生态系统。  
<http://www.gov.cn/zhengce/zhengceku/2021-04/17/content_5600311.htm>

《国家发展改革委办公厅关于加快落实新型城镇化建设补短板强弱项工作有序推进县城智慧化改造的通知》

发改办高技〔2020〕530号，成文日期为2020年7月9日  
　　·建全网络安全防护体系，做好网络安全与智慧化改造一体化推进。落实网络安全工作责任制要求，完善智慧化改造网络安全管理制度规范。认真落实国家网络安全等级保护、网络安全审查、云计算采购服务、国家密码管理等有关规定，采购部署安全可靠的软硬件产品，具备与智慧化水平相匹配的体系化安全防护能力。  
<http://www.gov.cn/zhengce/zhengceku/2020-07/29/content_5530869.htm>

三、密码与数字经济融合应用  
  
《国务院关于印发“十四五”数字经济发展规划的通知》

国发〔2021〕29号，成文日期为2021年12月12日  
　　·提升网络安全应急处置能力，加强电信、金融、能源、交通运输、水利等重要行业领域关键信息基础设施网络安全防护能力，支持开展常态化安全风险评估，加强网络安全等级保护和密码应用安全性评估。  
<http://www.gov.cn/zhengce/zhengceku/2022-01/12/content_5667817.htm>

（一）现代农业密码应用  
  
《农业农村部关于印发＜“十四五”全国农业农村信息化发展规划＞的通知》  
农市发〔2022〕4号，成文日期为2022年2月22日  
　　·安全可控，有序推进。坚持发展和安全并重，强化网络安全和数据安全保障能力，守住安全底线，全面提升发展的持续性和稳定性。坚持数量服从质量、进度服从实效、求好不求快，科学规划、试点先行，因地制宜推进农业农村信息化建设。  
<http://www.moa.gov.cn/nybgb/2022/202204/202206/t20220607_6401745.htm>

（二）先进制造业密码应用

《工业和信息化部关于印发工业控制系统网络安全防护指南的通知》

工信部网安〔2024〕14号，成文日期为 2024年1月19日

　　·在工业控制系统中使用加密协议和算法时应符合相关法律法规要求，鼓励优先采用商用密码，实现加密网络通信、设备身份认证和数据安全传输。

　　·定期梳理工业控制系统运行产生的数据，结合业务实际，开展数据分类分级，识别重要数据和核心数据并形成目录。围绕数据收集、存储、使用、加工、传输、提供、公开等环节，使用密码技术、访问控制、容灾备份等技术对数据实施安全保护。

<https://www.gov.cn/zhengce/zhengceku/202402/content_6929643.htm>

《工业和信息化部 国家发展和改革委员会 生态环境部关于促进钢铁工业高质量发展的指导意见》  
工信部联原〔2022〕6号，成文日期为2022年1月20日  
　　·大力发展智能制造。开展钢铁行业智能制造行动计划，推进5G、工业互联网、人工智能、商用密码、数字孪生等技术在钢铁行业的应用。

　　·落实网络安全主体责任，大力提高商用密码应用安全，提升工业控制系统安全防护水平，制定应急响应预案，积极应对新兴技术融合带来的安全挑战。  
<http://www.gov.cn/zhengce/zhengceku/2022-02/08/content_5672513.htm>

《工业和信息化部 科技部 自然资源部关于印发“十四五”原材料工业发展规划的通知》

工信部联规〔2021〕212号，成文日期为2021年12月21日  
　　·深化实施原材料生产企业工业互联网网络安全分类分级管理，推动商用密码技术应用，提升重点行业企业工业互联网安全防护能力。  
<http://www.gov.cn/zhengce/zhengceku/2021-12/29/content_5665166.htm>

《工业和信息化部 国家发展和改革委员会 教育部 科技部 财政部 人力资源和社会保障部 国家市场监督管理总局 国务院国有资产监督管理委员会关于印发＜“十四五”智能制造发展规划＞的通知》  
工信部联规〔2021〕207号，成文日期为2021年12月21日  
　　·加强安全保障。加强智能制造安全风险研判，同步推进网 络安全、数据安全和功能安全，推动密码技术深入应用。实施 企业网络安全分类分级管理，督促企业落实网络安全主体责 13 任。完善国家、地方、企业多级工控信息安全监测预警网络， 加快建设工业互联网安全技术监测服务体系。  
<http://www.gov.cn/zhengce/zhengceku/2021-12/28/content_5664996.htm>

《工业和信息化部关于发布“十四五”民用爆炸物品行业安全发展规划的通知》  
工信部规〔2021〕183号，成文日期为2021年11月15日

　　·探索建立民爆行业智能制造标准体系，与民爆产品、安全等标准优化协同，形成面向 智能制造典型应用场景的标准群，在行业内开展应用试点。协同推进网络安全、信息安全和功能安全，加强商用密码在数字化智能化生产、仓储、运输体系中的应用，充分发挥基础保障作用。

<http://www.gov.cn/zhengce/zhengceku/2021-12/04/content_5655830.htm>

《国务院办公厅关于印发新能源汽车产业发展规划（2021—2035年）的通知》

国办发〔2020〕39号，成文日期为2020年10月20日  
　　·打造网络安全保障体系。健全新能源汽车网络安全管理制度，构建统一的汽车身份认证和安全信任体系，推动密码技术深入应用，加强车载信息系统、服务平台及关键电子零部件安全检测，强化新能源汽车数据分级分类和合规应用管理，完善风险评估、预警监测、应急响应机制，保障“车端—传输管网—云端”各环节信息安全。  
<http://www.gov.cn/zhengce/zhengceku/2020-11/02/content_5556716.htm>

《工业和信息化部办公厅关于印发＜建材工业智能制造数字转型行动计划（2021-2023年）＞的通知》

工信厅原〔2020〕39号,成文日期为2020年9月16日  
　　·构建网络、平台、安全三大功能体系，鼓励企业积极探索“5G+工业互联网”，促进工业互联网与建材工业深度融合。推动建材行业工业互联网标识解析二级节点建设，深化标识解析应用。大力发展建材行业工业互联网创新应用平台，加快开发建材工业APP，推动建材企业和设备上云上平台，实现制造资源和制造能力互联互通。构建工业互联网密码支撑体系，加快商用密码在建材行业深度应用。  
<http://www.gov.cn/zhengce/zhengceku/2020-09/21/content_5545222.htm>

《工业和信息化部关于工业大数据发展的指导意见》

工信部信发〔2020〕67号，成文日期为2020年4月28日  
六、强化数据安全

（十五）加强工业数据安全产品研发。开展加密传输、访问控制、数据脱敏等安全技术攻关，提升防篡改、防窃取、防泄漏能力。加快培育安全骨干企业，增强数据安全服务，培育良好安全产业生态。  
<https://www.gov.cn/gongbao/content/2020/content_5530364.htm>

（三）现代服务业及新兴产业密码应用  
  
  
《财政部关于印发＜会计软件基本功能和服务规范＞的通知》

财会〔2024〕12号，自2025年1月1日起施行

　　第三十七条　会计软件采用密码技术的，应当遵循国家密码主管部门的有关规定。

<https://www.gov.cn/gongbao/2024/issue_11606/202409/content_6976924.html>

《财政部关于印发＜会计信息化工作规范＞的通知》

财会〔2024〕11号，自2025年1月1日起施行

第三十八条　单位应当加强会计数据安全风险防范，采取数据加密传输技术等有效措施，保证会计数据处理与应用的安全合规，避免会计数据在生成、传输、处理、存储等环节的泄露、篡改及损毁风险。

单位应当对电子会计资料进行备份，规定备份信息的备份方式、备份频率、存储介质、保存期等，确保会计资料的安全、完整和可用。

鼓励单位结合内部数据管理要求建立会计数据安全分类分级管理体系，加强对重要数据和核心数据的保护。

<https://www.gov.cn/gongbao/2024/issue_11586/202409/content_6975086.html>

《财政部 国家网信办关于印发＜会计师事务所数据安全管理暂行办法＞的通知》

财会〔2024〕6号，自2024年10月1日起施行

**第十二条**　会计师事务所应当明确数据传输操作规程。核心数据、重要数据传输过程中应当采用加密技术，保护传输安全。

**第十三条**　审计工作底稿应当按照法律、行政法规和国家有关规定存储在境内。相关加密设备应当设置在境内并由境内团队负责运行维护，密钥应当存储在境内。

**第十六条**　会计师事务所应当采用网络隔离、用户认证、访问控制、数据加密、病毒防范、非法入侵检测等技术手段，及时识别、阻断和溯源相关网络攻击和非法访问，保障数据安全。  
<https://www.gov.cn/gongbao/2024/issue_11386/202406/content_6955750.html>  
  
  
《中共中央办公厅 国务院办公厅关于数字贸易改革创新发展的意见》

成文日期为2024年8月17日  
　　（十七）加强知识产权保护。研究构建数据知识产权保护规则。加强对源代码、算法、加密密钥、商业秘密以及其他专有信息的法律保护。加快推动数字产品标识化。加强数字贸易领域知识产权公共服务。加强涉及数字贸易的商标注册和保护。拓宽知识产权海外维权和争议解决渠道。

<https://www.gov.cn/gongbao/2024/issue_11766/202412/content_6993326.html>  
  
  
《快递市场管理办法》  
中华人民共和国交通运输部令2023年第22号，自2024年3月1日起施行  
　　第三十六条　经营快递业务的企业应当建立快递运单（含电子运单）制作、使用、保管、销毁等管理制度和操作规程，采取加密、去标识化等安全技术措施保护快递运单信息安全。

　　经营快递业务的企业应当建立快递运单码号使用、销毁等管理制度，实行码号使用信息、用户信息、快递物品信息关联管理，保证快件可以跟踪查询。

任何单位和个人不得非法使用、倒卖快递运单。  
<https://www.gov.cn/gongbao/2024/issue_11206/202403/content_6937896.html>  
  
  
《产业结构调整指导目录（2024年本）》  
中华人民共和国国家发展和改革委员会令第7号，自2024年2月1日起施行  
　　第一类　鼓励类  
　　五十、网络安全

　　1.网络安全产品：端点安全产品、设施安全产品、应用安全产品、数据安全产品、身份安全产品、安全管理产品等

　　2.网络安全服务：安全咨询、设计与开发，安全集成、安全运营、信息的安全处理和存储、测评认证、灾难备份与恢复、网络安全审计、应急响应、实训基础设施服务、教育培训、安全众测、网络安全保险等

　　3.网络安全技术的研发与转让

　　4.网络安全检测工具：源代码审计工具、软件负载压力测试工具、网络性能测试仪、漏洞扫描与验证工具、安全配置核查工具、网络流量分析工具、模糊测试工具、渗透测试工具、协议一致性验证工具、流量仿真工具等

　　5.网络安全基础设施建设与改造升级：网络安全基础平台设施、网络安全产业园区等

6.数据安全技术产品研发与产业化应用，数据安全服务发展（包括检测评估、认证、教育培训等）  
<https://www.gov.cn/gongbao/2024/issue_11206/202403/content_6937897.html>

《交通运输部关于修改〈邮政业寄递安全监督管理办法〉的决定》

中华人民共和国交通运输部令2023年第24号，2023年12月20日修改施行

　　第二十二条　邮政企业、快递企业应当按照国家网络安全等级保护制度的要求，履行下列安全保护义务，保障其网络免受干扰、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6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。

<https://www.gov.cn/gongbao/2024/issue_11226/202403/content_6940051.html>  
  
  
《工业和信息化部办公厅关于组织开展网络安全保险服务试点工作的通知》

工信厅网安函〔2023〕356号，成文日期为2023年12月14日  
　　三、试点对象及内容

　　结合我国网络安全保险发展实际，试点内容包括面向电信和互联网、工业互联网、车联网等重点行业的企业类保险和网络安全产品、信息技术产品，以及网络安全服务类保险，主要试点内容如下。  
　　（一）企业类

　　以企业法人为被保险方，主要保障网络安全事件对其造成的财产损失或赔偿责任。

　　2.工业互联网企业。面向联网工业企业、工业互联网平台企业、标识解析企业等工业互联网企业，针对因网络攻击或内部人员操作不当造成的联网工业设备或工业控制系统运行故障、自动化生产线停止运行、重要数据被加密锁定等风险场景，主要承保营业中断损失、数据资产重置费用、应急处置费用等。面向原材料工业、装备工业、消费品工业和电子信息制造业等重要行业企业，针对因网络攻击或操作不当造成的生产制造系统运行故障，办公自动化等系统运行中断、管理数据损坏等风险场景，主要承保营业中断损失、数据资产重置费用、应急处置费用等。

3.车联网企业。面向整车生产制造企业、车辆电子系统制造企业、电子零部件企业、智能车辆运营企业等车联网相关企业，针对因网络攻击、系统设计缺陷、操作不当等导致的装配线等生产制造系统运行故障、车辆设计敏感数据被泄露等风险场景，主要承保车主、车上人员以及第三方的索赔损失、数据资产重置费用、硬件改善成本、营业中断损失、应急处置费用等。  
<https://www.gov.cn/zhengce/zhengceku/202312/content_6921869.htm>  
  
  
《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》

工信部信管函〔2023〕26号，成文日期为2023年2月6日  
　　二、提升全链条管理能力，营造健康服务生态

　　(一)落实APP开发运营者主体责任

　　1.完善内部管理机制。明确用户服务和权益保护的牵头管理部门和负责人，建立全生命周期个人信息保护机制，健全考核问责制度，将相关法规政策要求落实到产品研发、推广和运营各环节，不断提高合规水平。定期对个人信息保护措施及执行情况等进行合规审计，有效防范风险隐患。

2.增强技术保障能力。采取访问控制、技术加密、去标识化等安全技术措施，加强前端和后端安全防护。主动监测发现个人信息泄露、窃取、篡改、毁损、丢失、非法使用等风险威胁，及时响应处置要求。  
<https://www.gov.cn/zhengce/zhengceku/2023-03/02/content_5744106.htm>  
  
  
《商务部 中央网信办 发展改革委关于印发＜“十四五”电子商务发展规划＞的通知》  
商电发〔2021〕191号，成文日期为2021年10月09日  
　　·探索建立电子商务平台网络安全防护和金融风险预警机制，支持电子商务相关企业研究多属性的安全认证技术，充分发挥密码在保障网络信息安全方面的作用。加强电子商务企业数据全生命周期管理，建立相应管理制度及安全防护措施，保障网上购物的个人信息和重要数据安全。开展数据出境安全评估能力建设，保障电子商务领域重要数据、个人信息的有序安全流动。指导电子商务企业树牢安全生产意识，完善安全风险治理体系，提升安全生产工作水平。  
<http://www.gov.cn/zhengce/zhengceku/2021-10/27/content_5645853.htm>

《国家知识产权局关于印发知识产权公共服务“十四五”规划的通知》

国知发服字〔2021〕39号，成文日期为2021年12月31日  
　　·全面落实《网络安全法》《数据安全法》《个人信息保护法》《密码法》等法律法规和网络安全等级保护制度，加强网络安全等级保护第三级及以上网络、信息系统和重要数据的安全防护。  
　　·加强对云计算、大数据、区块链、人工智能等新技术新应用的安全防护，确保其技术、产品、服务和供应链安全。积极推进国产密码技术和产品应用，提升使用密码技术保障网络与数据安全的水平。  
<http://www.gov.cn/zhengce/zhengceku/2022-01/09/content_5667251.htm>

《国家新闻出版署关于印发＜出版业“十四五”时期发展规划＞的通知》  
国新出发〔2021〕20号，成文日期为2021年12月31日  
　　·出版领域区块链技术创新应用工程: 推动智能合约、共识算法、加密算法、分布式系统等区块链技术在出版产业中的创新应用, 以联盟链为重点, 发展区块链服务平台, 完善数字资产与供应链管理, 健全行业监管机制, 提高出版(版权)管理水平。  
<https://www.nppa.gov.cn/nppa/contents/279/102953.shtml>

《住房和城乡建设部等部门关于推动物业服务企业加快发展线上线下生活服务的意见》

建房〔2020〕99号，成文日期为2020年12月4日  
　　·保障平台安全运营。严格落实网络和数据安全法律法规和政策标准，建立健全安全管理制度，采用国产密码技术，增强安全可控技术和产品应用，加强日常监测和安全演练，确保智慧物业管理服务平台网络和数据安全。  
<http://www.gov.cn/zhengce/zhengceku/2020-12/19/content_5571261.htm>  
  
  
《工业和信息化部关于印发“十四五”软件和信息技术服务业发展规划的通知》

工信部规〔2021〕180号，成文日期为2021年11月15日  
　　·加快区块链共识算法、加密算法、高效安全智能合约、分布式系统 等关键技术研发。支持区块链底层技术平台、区块链服务平台等建设。加强金融 科技、供应链管理、政府服务等重点领域应用。  
<http://www.gov.cn/zhengce/zhengceku/2021-12/01/content_5655205.htm>  
  
  
《邮政业寄递安全监督管理办法》  
中华人民共和国交通运输部令2020年第1号，自2020年2月15日起施行  
　　第二十二条　邮政企业、快递企业应当按照国家网络安全等级保护制度的要求，履行下列安全保护义务，保障其网络免受干扰、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：

……  
（四）采取数据分类、重要数据备份和加密等措施；

……  
<https://www.gov.cn/gongbao/content/2020/content_5509721.htm>

四、信息惠民密码应用

## （一）电子政务密码应用

《电子档案管理办法》  
国家档案局令第22号公布，自2024年11月1日起施行

　　第八条　电子档案管理的全过程应当符合国家网络安全、数据安全、个人信息保护、保密管理、密码管理等相关法律法规要求，确保电子档案的安全。  
　　第十七条　电子文件形成部门应当在电子文件形成、办理、收集过程中完成保管期限鉴定、分类、命名等工作，确保电子文件符合归档要求，并且完整采集描述电子文件内容、结构和背景信息的元数据及其整个管理过程元数据。

　　电子文件及其元数据归档不得采用非开放的压缩、加密等技术措施。

党政机关电子公文归档，应当去除电子印章的数字签名信息，只保留印章图形。其他组织机构电子文件归档可以参照处理。  
<https://www.gov.cn/gongbao/2024/issue_11746/202412/content_6991650.html>

《中共中央办公厅 国务院办公厅关于加快公共数据资源开发利用的意见》

发文时间：2024年9月21日  
　　（十六）增强支撑能力。加快建立数据产权归属认定、市场交易、权益分配、利益保护制度。统筹数据领域标准体系建设管理，组织开展相关标准研制、宣传、执行和评价。依托国家重点研发计划、国家科技重大专项等，开展数据加密、可信流通、安全治理等关键技术研究和攻关。加强数据领域人才队伍建设，将提高做好数据工作的能力纳入干部教育培训内容。积极参与国际交流合作，推动公共数据国际治理规则、国际标准制定。

<https://www.gov.cn/gongbao/2024/issue_11666/202410/content_6983475.html>

《国务院办公厅关于印发＜政务服务电子文件归档和电子档案管理办法＞的通知》

国办发〔2023〕26号，自2023年7月30日起施行  
　　第九条　政务服务电子文件归档格式应当符合国家标准规范，并且通用、开放、不绑定软硬件。加密的政务服务电子文件应当解除加密技术手段后归档。

　　政务服务电子文件归档一般采用在线实时归档方式，不具备在线归档条件的，可以采用离线归档方式，归档时间最迟不能超过办理完毕后的第二年6月底。  
　　第十一条　各级政务服务机构应当做好本单位政务服务电子档案安全管理工作，定期开展电子档案备份，做好电子档案登记、日常检查、转换、迁移、鉴定、销毁等工作。政务服务电子文件办理过程中应当按照国家有关法律法规要求，规范使用密码技术进行保护。  
<https://www.gov.cn/gongbao/2023/issue_10686/202309/content_6902579.html>  
  
  
《国务院关于加强数字政府建设的指导意见》  
国发〔2022〕14号，成文日期为2022年6月6日

　　·加强关键信息基础设施安全保护和网络安全等级保护，建立健全网络安全、保密监测预警和密码应用安全性评估的机制，定期开展网络安全、保密和密码应用检查，提升数字政府领域关键信息基础设施保护水平。  
<http://www.gov.cn/zhengce/zhengceku/2022-06/23/content_5697299.htm>

《国务院办公厅关于加快推进电子证照扩大应用领域和全国互通互认的意见》

国办发〔2022〕3号，成文日期为2022年1月20日  
　　·建立健全涵盖电子证照应用业务、数据、技术、管理、安全等的标准体系，制定电子证照签章、电子印章密码应用等规范，完善电子证照在移动服务、自助服务等领域的使用规范。  
　　·加强电子证照签发、归集、存储、使用等各环节安全管理，严格落实网络安全等级保护制度等要求，强化密码应用安全性评估，探索运用区块链、新兴密码技术、隐私计算等手段提升电子证照安全防护、追踪溯源和精准授权等能力。  
<http://www.gov.cn/zhengce/zhengceku/2022-02/22/content_5674998.htm>

《国务院办公厅关于印发全国一体化政务服务平台移动端建设指南的通知》

国办函〔2021〕105号，成文日期为2021年9月29日  
　　·各地区和国务院有关部门要综合利用密码技术、安全审计等手段强化本地区本部门政务服务平台移动端安全保障和风险防控能力，构建全方位、多层次、一致性的防护体系，切实保障全国一体化平台移动端安全平稳高效运行。  
<http://www.gov.cn/zhengce/zhengceku/2021-11/12/content_5650485.htm>

《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》

国办发〔2019〕57号，成文日期为2019年12月30日

　　·项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。  
　　·对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。  
<http://www.gov.cn/zhengce/zhengceku/2020-01/21/content_5471256.htm>

《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》  
公网安〔2020〕1960号，印发时间为2020年7月22日  
　　·落实密码安全防护要求。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。  
<https://www.mps.gov.cn/n6557558/c7369310/content.html>

（二）社会治理密码应用

《民政部关于印发＜“十四五”民政信息化发展规划＞的通知》  
民发〔2021〕104号，成文日期为2021年12月23日  
　　·全面开展国产商用密码应用，构建民政统一的密码应用基础服务平台，提供统一的数据传输、存储加密和身份认证管理等相关服务，提升密码使用和管理水平。  
<http://www.gov.cn/zhengce/zhengceku/2021-12/30/content_5665421.htm>

（三）民生保障密码应用

《国家中医药管理局关于印发＜中医医院信息与数字化建设规范（2024版）＞的通知》

国中医药规财函〔2024〕259号，发文时间为2024年12月5日

　　第五十条 中医医院应当按照《密码法》等有关法律法规使用商用密码保护信息系统和网络设施，同步规划、同步建设、同步运行商用密码保障系统，定期委托商用密码检测机构开展商用密码应用安全性评估。http://www.natcm.gov.cn/guicaisi/zhengcewenjian/2024-12-13/35452.html

《教育部关于发布＜直播类在线教学平台安全保障要求＞教育行业标准的通知》  
教科信函〔2022〕59号，成文日期为2022年12月9日  
　　JY/T 0651-2022《直播类在线教学平台安全保障要求》明确，直播教学平台应依据GB/T 39786-2021及《商用密码应用安全性评估管理办法(试行)》等标准和政策文件的要求，使用商用密码进行保护，定期委托检测机构开展密码应用安全性评估，并提供密码应用安全性评估报告。  
<http://www.moe.gov.cn/srcsite/A16/s3342/202301/t20230113_1039260.html>  
  
  
《住房和城乡建设部关于加快住房公积金数字化发展的指导意见》

建金〔2022〕82号，成文日期为2022年12月7日  
　　·切实保障数据和网络安全。落实数据分类分级保护制度，明确数据使用权限、适用范围、安全保障措施等，建立健全数据安全内控机制，加大数据保护力度。加强数据全生命周期安全管理，强化安全监测、数据加密、数据脱敏、授权访问等技术保护措施。严格执行网络安全等级保护制度，定期组织开展网络安全、密码应用等安全自查和检测评估。加强网络安全基础设施建设，充分运用智能感知、威胁预测等技术，强化日常监测，不断提高网络安全防护能力。  
<https://www.gov.cn/zhengce/zhengceku/2023-01/10/content_5735961.htm>  
  
  
《国家卫生健康委、国家中医药局、国家疾控局＜关于印发“十四五”全民健康信息化规划＞的通知》

国卫规划发〔2022〕30号，成文日期为2022年11月7日

　　·构建卫生健康行业网络可信体系。建设一批医疗卫生机构商用密码应用示范，全面推广商用密码应用，完善卫生健康行业商用密码应用体系。建设各类医疗卫生机构、人员和患者可信数字身份管理系统，实现医患可信身份电子认证和电子签名，保证访问、处理数据的用户身份真实，确保网络行为可管、可控、可溯源。完善卫生健康行业电子认证服务体系，实现电子认证服务跨区域互信互认。

<http://www.nhc.gov.cn/guihuaxxs/s3585u/202211/49eb570ca79a42f688f9efac42e3c0f1.shtml>

国家卫生健康委、国家中医药局、国家疾控局《关于印发医疗卫生机构网络安全管理办法的通知》  
国卫规划发〔2022〕29号，成文日期为2022年8月8日  
　　·各医疗卫生机构应按照《密码法》等有关法律法规和密码应用相关标准规范，在网络建设过程中同步规划、同步建设、同步运行密码保护措施，使用符合相关要求的密码产品和服务。  
<http://www.gov.cn/zhengce/zhengceku/2022-08/30/content_5707404.htm>

《国家药监局关于印发＜药品监管网络安全与信息化建设“十四五”规划＞的通知》

国药监综〔2022〕23号，成文日期为2022年4月24日  
　　·完善网络安全保障体系，健全网络安全管理制度，开展信息系统安全等级保护备案与信息安全等级保护测评、关键信息基础设施安全保护、密码应用安全性评估等工作。  
　　·结合药监云平台服务的建设实际和业务应用的密码需求，进一步建设完善网络安全信任体系。根据各业务系统中密码应用特点，逐步完善国家局密码资源服务能力，满足相关法律法规和管理条例的要求，实现系统和数据的主动安全保护。

　　·建设统一认证服务系统，提升密码服务基础水准，扩大密码服务种类，提高密码服务可用性，从服务形态、部署方式、访问接口到运维管理等方面加强密码服务统一管理，为药监云平台建设提供技术先进、方案完备、高效可用的密码安全防护能力。  
<https://www.nmpa.gov.cn/xxgk/fgwj/gzwj/gzwjzh/20220511110329171.html>  
  
  
《教育部等六部门关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》

教科信〔2021〕2号，成文日期为2021年7月1日  
　　·推动建设教育系统密码基础设施和支撑平台，建立完善全国统一的身份认证体系，推动移动终端的多因子认证。利用国产商用密码技术推动数据传输和存储加密，提升数据保障能力。

<http://www.gov.cn/zhengce/zhengceku/2021-07/22/content_5626544.htm>

《教育部关于加强新时代教育管理信息化工作的通知》

教科信函〔2021〕13号，成文日期为2021年3月10日  
　　·构建数字认证体系。完善教育数字认证基础支撑体系总体规划，建立统一的教育系统密码基础设施和支撑平台。建设基于“一校一码、一人一号”的数字认证互联互通互认体系，实现跨平台的单点登录。推动以智能终端为载体的多因子认证，探索手机短信、移动协同签名等多种认证方式，提升服务体验。数字认证使用的密码技术和产品应符合国家密码管理部门要求。探索推动区块链技术在招生考试、学历认证、学分互认、求职就业等领域的应用，提高数字认证可信性。

<http://www.moe.gov.cn/srcsite/A16/s3342/202103/t20210322_521669.html>

《关于加快推进卫生健康行业电子证照建设与应用的指导意见》  
国卫办规划发〔2020〕17号，成文日期为2020年10月16日  
　　·强化电子证照系统安全保障。各级卫生健康行政部门要强化风险防控能力，建立安全制度，规范系统应用，依法依规使用卫生健康行业电子证照，建立卫生健康行业电子证照系统国产密码应用保障体系和安全制度，对涉及国家安全、公共安全、个人隐私等数据提供安全支撑。做好卫生健康行业电子证照数据备份工作，保障系统安全互联、信息安全共享。  
<http://www.nhc.gov.cn/guihuaxxs/gongwen12/202010/64d370e60e6647709d847300fec16abe.shtml>  
  
  
《关于加强全民健康信息标准化体系建设的意见》  
国卫办规划发〔2020〕14号，成文日期为2020年09月27日  
　　·完善行业网络安全标准体系。贯彻《中华人民共和国网络安全法》，推进网络安全等级保护、商用密码应用、关键信息基础设施保护等制度在行业落地实施，研究编制卫生健康行业网络安全技术、医疗卫生机构安全能力评估、关键信息基础设施识别认定和保护等标准。  
<http://www.nhc.gov.cn/guihuaxxs/pqt/202010/4114443b613546148b275f191da4662b.shtml>  
  
  
《国家卫生健康委办公厅关于做好信息化支撑常态化疫情防控工作的通知》  
国卫办规划函〔2020〕506号，成文日期为2020年6月28日  
　　·加大网络安全投入。各级卫生健康部门要按照中央网信办要求提高信息化建设中网络安全投入的比例，提升信息化产品和服务安全可控水平，推进商用密码应用的深度和广度。  
<http://www.nhc.gov.cn/guihuaxxs/s10743/202006/5a2bc24e181a43a6b242a86706c361a3.shtml>

# 五、密码科技创新和基础支撑能力

《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》

工信部联网安﹝2022﹞182号，成文日期为2023年1月3日  
　　·加强核心技术攻关。推进新型计算模式和网络架构下数据安全基础理论和技术研究，支持后量子密码算法、密态计算等技术在数据安全产业的发展应用。优化升级数据识别、分类分级、数据脱敏、数据权限管理等共性基础技术，加强隐私计算、数据流转分析等关键技术攻关。研究大数据场景下轻量级安全传输存储、隐私合规检测、数据滥用分析等技术。  
<https://www.gov.cn/zhengce/zhengceku/2023-01/15/content_5737026.htm>

《工业和信息化部关于印发＜工业和信息化领域数据安全管理办法（试行）＞的通知》

工信部网安〔2022〕166号，成文日期为2022年12月8日

　　第十五条 工业和信息化领域数据处理者应当按照法律、行政法规规定和用户约定的方式、期限进行数据存储。存储重要数据和核心数据的，应当采用校验技术、密码技术等措施进行安全存储，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。

　　第十七条 工业和信息化领域数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据和核心数据的，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。  
<https://www.gov.cn/zhengce/zhengceku/2022-12/14/content_5731918.htm>

《工业和信息化部关于印发“十四五”大数据产业发展规划的通知》

工信部规〔2021〕179号，成文日期为2021年11月15日  
　　·推动数据安全产业发展。支持重点行业开展数据安全技术手段建设，提升数据安全防护水平和应急处置能力。加强数据安全产品研发应用，推动大数据技术在数字基础设施安全防护中的应用。加强隐私计算、数据脱敏、密码等数据安全技术与产品的研发应用，提升数据安全产品供给能力，做大做强数据安全产业。  
<http://www.gov.cn/zhengce/zhengceku/2021-11/30/content_5655089.htm>

《工业和信息化部 中央网络安全和信息化委员会办公室关于加快推动区块链技术应用和产业发展的指导意见》

工信部联信发〔2021〕62号，成文日期为2021年5月27日  
　　·构建底层平台。在分布式计算与存储、密码算法、共识机制、智能合约等重点领域加强技术攻关，构建区块链底层平台。支持利用传感器、可信网络、软硬件结合等技术加强链上链下数据协同。推动区块链与其他新一代信息技术融合，打造安全可控、跨链兼容的区块链基础设施。

<https://www.miit.gov.cn/jgsj/xxjsfzs/wjfb/art/2021/art_aac4af17ec1f4d9fadd5051015e3f42d.html>