

解读《关键信息基础设施安全 保护条例》

《关键信息基础设施安全保护条例》共六章51条，自2021年9月1日起施行。

第一章	总则
第二章	关键信息基础设施认定
第三章	运营者责任义务
第四章	保障和促进
第五章	法律责任
第六章	附则

The screenshot shows the Baidu Encyclopedia interface. At the top, the Baidu logo and search bar are visible, with the search term '关键信息基础设施安全保护条例' (Regulations on the Security Protection of Key Information Infrastructure). Below the search bar, there are navigation links for '首页' (Home), '秒懂百科' (Quick Understanding Encyclopedia), '特色百科' (Special Encyclopedia), '知识专题' (Knowledge Special Topics), '加入百科' (Join Encyclopedia), '百科团队' (Encyclopedia Team), '权威合作' (Authoritative Cooperation), '下载百科APP' (Download Encyclopedia APP), and '个人中心' (Personal Center). The main content area features the title '关键信息基础设施安全保护条例' in large white text on a blue background, with sub-headers for '国务院发布的条例' (Regulations issued by the State Council) and '法律百科' (Law Encyclopedia). There are also icons for '播报' (Broadcast), '讨论' (Discussion), and '上传视频' (Upload Video). Below the title, there is a section for '收藏' (Favorites) with 0 items, and a section for '正文' (Main Text) with 0 items. The main text area contains the following content:

《关键信息基础设施安全保护条例》旨在建立专门保护制度，明确各方责任，提出保障促进措施^[4]，保障关键信息基础设施安全及维护网络安全，根据《中华人民共和国网络安全法》，制定的条例。^[5]

2021年4月27日，经国务院第133次常务会议通过，2021年7月30日，国务院总理李克强签署中华人民共和国国务院令745号^[6]，公布《关键信息基础设施安全保护条例》，自2021年9月1日起施行。^[2]

At the bottom right, there is a Windows watermark: '激活 Windows 转到“设置”以激活 Windows.'

Q1.什么是关键信息基础设施?

第二条 本条例所称关键信息基础设施，是指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等。

Q 2.关键信息基础设施如何管理?

1

三同步（**第十二条** 安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。）

2

八职责（**第十五条** 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：）

- 1) 建立健全网络安全制度；
- 2) 开展网络安全监测、检测和评估；
- 3) 具备网络安全事件应急能力；
- 4) 组织网络安全工作考核；
- 5) 开展网络安全教育、培训；
- 6) 履行个人信息和数据安全保护责任；
- 7) 对设计、建设、运行、维护等服务实施安全管理；
- 8) 报告网络安全事件和重要事项。

3

三注意

- 1) 注意优先采购安全可信的网络产品和服务，采购网络产品和服务可能影响国家安全的，应当按照网络安全规定通过安全审查； **(第十九条)**
- 2) 注意与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任的履行情况进行监督； **(第二十条)**
- 3) 注意运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。 **(第二十一条)**

两不准

- 1) **第三十条** 网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。
- 2) **第三十一条** 未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。

三鼓励

1) **第三十二条** 国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。

能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全运行提供重点保障。

2) **第三十五条** 国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。

3) **第三十六条** 国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。



附则

第五十条 存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。