

# 网络产品和服务安全审查办法（试行）

**第一条** 为提高网络产品和服务安全可控水平，防范网络安全风险，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

**第二条** 关系国家安全的网络和信息系统的采购的重要网络产品和服务，应当经过网络安全审查。

**第三条** 坚持企业承诺与社会监督相结合，第三方评价与政府持续监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对网络产品和服务及其供应链进行网络安全审查。

**第四条** 网络安全审查重点审查网络产品和服务的安全性、可控性，主要包括：

（一）产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；

（二）产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；

（三）产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险；

（四）产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险；

（五）其他可能危害国家安全的风险。

**第五条** 国家互联网信息办公室会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。

网络安全审查办公室具体组织实施网络安全审查。

**第六条** 网络安全审查委员会聘请相关专家组成网络安全审查专家委员会，在第三方评价基础上，对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估。

**第七条** 国家依法认定网络安全审查第三方机构，承担网络安全审查中的第三方评价工作。

**第八条** 网络安全审查办公室按照国家有关要求、根据全国性行业协会建议和用户反映等，按程序确定审查对象，组织第三方机构、专家委员会对网络产品和服务进行网络安全审查，并发布或在一定范围内通报审查结果。

**第九条** 金融、电信、能源、交通等重点行业和领域主管部门，根据国家网络安全审查工作要求，组织开展本行业、本领域网络产品和服务安全审查工作。

**第十条** 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，应当通过网络安全审查。产品和服务是否影响国家安全由关键信息基础设施保护工作部门确定。

**第十一条** 承担网络安全审查的第三方机构，应当坚持客观、公正、公平的原则，按照国家有关规定，参照有关标准，重点从产品和服务及其供应链的安全性、可控性，安全机制和技术的透明性等方面进行评价，并对评价结果负责。

**第十二条** 网络产品和服务提供者应当对网络安全审查工作予以配合，并对提供材料的真实性负责。

第三方机构等相关单位和人员对审查工作中获悉的信息等承担安全保密义务，不得用于网络安全审查以外的目的。

**第十三条** 网络安全审查办公室不定期发布网络产品和服务安全评估报告。

**第十四条** 网络产品和服务提供者认为第三方机构等相关单位和人员有失客观公正，或未能对审查工作中获悉的信息承担安全保密义务的，可以向网络安全审查办公室或者有关部门举报。

**第十五条** 违反本办法规定的，依照有关法律法规予以处理。

**第十六条** 本办法自 2017 年 6 月 1 日起实施。