|  |  |  |
| --- | --- | --- |
| **온라인 안전검열방법**  국가인터넷정보판공실, 국가발전과개혁위원회, 공업과정보화부 등 령 제6호  국가인터넷정보판공실, 국가발전과개혁위원회, 공업과정보화부, 공안부, 국가안전부, 재정부, 상무부, 중국인민은행, 국가시장감독관리총국, 국가라디오방송총국, 국가비밀보장국, 국가암호관리국은 공동으로 <인터넷 안전검열방법>을 제정하였으며, 이를 공포한다.  국가인터넷정보판공실 주임 장영문  국가발전과개혁위원회 주임 하입봉  공업과정보화부 부장 묘 우  공안부 부장 조극지  국가안전부 부장 진문청  재정부 부장 유 곤  상무부 부장 종 산  중국인민은행 행장 이 강  국가시장감독관리총국 국장 초아경  국가라디오방송총국 국장 섭진석  국가비밀보장국 국장 전 정  국가암호관리국 국장 이조종  2020년 4월 13일  **제1조** 핵심정보 기초시설 공급사슬 안전을 확실히 보장하고, 국가안전을 수호하기 위해서 <중화인민공화국 국가안전법>, <중화인민공화국 온라인 안전법>에 근거하여 본 방법을 제정한다.  **제2조** 핵심정보 기초시설 운영자(이하 ‘운영자’)가 온라인 제품과 서비스를 구매할 때 국가안전에 영향을 주거나 줄 가능성이 있을 경우에는 본 방법에 따라 온라인 안전검열을 진행하여야 한다.  **제3조** 온라인 안전검열은 온라인 안전 위험 예방과 선진기술 응용 촉진을 결합하고, 공정하고 투명한 과정과 지식재산권 보호를 결합하며, 사전검열과 지속적인 관리감독을 결합하고, 기업승낙과 사회감독을 결합하는 것을 유지하며, 제품과 서비스의 안정성, 국가 안전 위험을 초래할 수 있는 등의 방면에서 검열을 진행한다.  **제4조** 중앙 온라인 안전과정보화 위원회의 지도 하에 국가인터넷정보판공실은 중화인민공화국 국가발전과개혁위원회, 중화인민공화국 공업과정보화부, 중화인민공화국 공안부, 중화인민공화국 국가안전부, 중화인민공화국 재정부, 중화인민공화국 상무부, 중국인민은행, 국가시장감독관리총국, 국가라디오방송총국, 국가비밀보장국, 국가암호관리국과 함께 국가 온라인 안전검열 업무체제를 구축한다.  온라인 안전검열판공실은 국가인터넷정보판공실에 설치하고 온라인 안전검열 관련 제도규범을 제정하고, 온라인 안전검열을 조직한다.  **제5조** 운영자가 온라인 제품과 서비스를 구매할 때, 해당 제품과 서비스를 사용한 후에 초래될 수 있는 국가 안전 위험을 사전에 판단하여야 한다. 국가 안전에 영향을 주거나 줄 수 있는 경우, 온라인 안전검열판공실에 온라인 안전검열을 신고하여야 한다.  핵심정보 기초시설 보호업무 부처는 본 업종, 본 영역의 사전판단가이드를 제정할 수 있다.  **제6조** 온라인 안전검열을 신고하는 구매활동에 대해서 운영자는 구매문건, 협의서 등을 통해 제품과 서비스 제공자에게 온라인 안전검열에 협조할 것을 요구하고, 제품과 서비스를 제공하기 위한 편리한 조건을 이용하지 않고, 사용자 데이터를 불법으로 취득하지 않으며, 사용자 설비를 불법으로 통제하고 조종하지 않고, 정당한 이유 없이 제품 공급이나 필요한 기술지원 서비스 등을 중단하지 않음을 승낙한다.  **제7조** 운영자가 온라인 안전검열을 신고할 경우에는 아래 서류를 제출하여야 한다.  7.1 신고서  7.2 국가 안전에 영향에 주거나 줄 수 있는 것에 관한 분석 보고서  7.3 구매문건, 협의서, 체결할 예정인 계약서 등  7.4 온라인 안전검열 업무에 필요한 기타서류  **제8조** 온라인 안전검열판공실은 검열 신고서류를 수령한 날로부터 10 업무일 내 검열 필요 여부를 확정하여, 운영자에게 서면으로 통지한다.  **제9조** 온라인 안전검열은 중점적으로 온라인 제품과 서비스 구매에 따른 국가 안전 위험성 초래 가능성에 대해 평가하고, 주요 고려요인은 다음과 같다.  9.1 제품과 서비스 사용 후 핵심정보 기초시설이 불법으로 통제되고 간섭이나 파괴되거나 중요한 데이터가 도난, 폭로, 훼손되는 위험  9.2 제품과 서비스 공급 중단으로 핵심정보 기초시설 업무 연속성에 대한 위해(危害)  9.3 제품과 서비스의 안전성, 개방성, 투명성, 출처의 다양성, 공급채널의 신뢰성 및 정치, 외교, 무역 등 요인으로 인해 공급이 중단되는 위험  9.4 제품과 서비스 제공자가 중국 법률, 행정법규, 부처 규장을 준수하는 상황  9.5 기타 핵심정보 기초시설 안전과 국가 안전에 해를 끼칠 가능성이 있는 요인  **제10조** 온라인 안전검열판공실이 온라인 안전검열 전개가 필요하다고 여길 경우, 운영자에게 서면통지서를 발송한 날로부터 30 업무일 내 기초검열을 완료하고, 작성한 검열 결론 건의와 검열 결론 건의를 온라인 안전검열 업무 체제 구성원 단위 및 관련 핵심정보 기초시설 보호업무 부처에 발송하여 의견을 구한다. 상황이 복잡할 경우에는 15 업무일을 연장할 수 있다.  **제11조** 온라인 안전검열 업무체제 구성원 단위와 핵심정보 기초기설 보호업무 부처 관계자는 검열 결론 건의를 받은 날로부터 15 업무일 내 서면으로 의견을 회신하여야 한다.  온라인 안전검열 업무체제 구성원 단위와 핵심정보 기초기설 보호업무 부처 관계자의 의견이 일치할 경우, 온라인 안전검열판공실은 서면으로 검열 결론을 운영자에게 통지한다. 의견이 불일치할 경우에는 특별검열절차에 따라 처리하고, 이를 운영자에게 통지한다.  **제12조** 특별검열절차에 따라 처리하는 경우, 온라인 안전검열판공실은 관련 부처와 단위의 의견을 청취하고, 깊이 있게 분석 평가를 진행해 검열 결론 건의를 다시 작성하여, 온라인 안전검열 업무체제 구성원 단위와 핵심정보 기초기설 보호업무 부처 관계자의 의견을 구해 절차대로 중앙 온라인 안전과정보화 위원회에 보고하여 승인을 득한 후, 검열 결론을 내려 운영자에게 서면으로 통지한다.  **제13조** 특별검열절차는 일반적으로 45 업무일 내 완성해야 하고, 상황이 복잡한 경우에는 적절하게 연장할 수 있다.  **제14조** 온라인 안전검열판공실이 보충서류 제출을 요구하는 경우, 운영자와 제품과 서비스 제공사는 이에 협조하여야 한다. 보충서류 제출시간은 검열기간에 포함되지 않는다.  **제15조** 온라인 안전검열 업무체제 구성원 단위가 국가 안전에 영향을 주거나 줄 가능성이 있는 온라인 제품과 서비스라고 여길 경우, 온라인 안전검열판공실은 절차에 따라 중앙 온라인 안전과정보화 위원회에 보고하여 승인을 득한 후, 본 방법 규정에 따라 검열을 진행한다.  **제16조** 온라인 안전검열에 참여한 관련 부처와 인원은 엄격히 기업 비즈니스 기밀과 지식재산권을 보호하고, 운영자와 제품과 서비스 제공자가 제출한 미공개서류 및 검열업무 중 알게 된 기타 미공개정보에 대한 비밀유지의무를 책임져야 한다. 정보 제공자의 동의를 구하지 않고, 관련 없는 자에게 이를 공개하거나 검열 이외의 목적으로 사용할 수 없다.  **제17조** 운영자 또는 온라인 제품과 서비스 제공자가 검열 인원이 객관적인 공정성을 잃었거나 또는 검열업무 중 알게 된 정보에 대한 비밀유지의무를 다하지 못한다고 여길 경우, 온라인 안전검열판공실이나 유관부처에 신고할 수 있다.  **제18조** 운영자는 제품과 서비스 제공자가 안전검열을 이행하면서 이를 승낙하도록 독촉한다.  온라인 안전검열판공실은 신고 접수 등의 방식을 통해 사전∙사중∙사후 감독을 강화한다.  **제19조** 운영자가 본 방법 규정을 위반한 경우, <중화인민공화국 온라인 안전법> 제65조 규정에 따라 처리한다.  **제20조** 본 방법에서의 핵심정보 기초시설 운영자는 핵심정보 기초시설 보호업무 부처가 인정한 운영자를 의미한다.  본 방법에서 일컫는 온라인 제품과 서비스는 주로 핵심 온라인 설비, 고성능 컴퓨터와 서버, 대용량 저장설비, 대형 데이터베이스와 응용 소프트웨어, 온라인 안전설비, 클라우드 서비스 및 기타 핵심정보 기초기설 안전에 대해 중요한 영향을 끼치는 온라인 제품과 서비스를 뜻한다.  **제21조** 국가 기밀 정보와 관련된 경우, 국가 유관 비밀유지 규정에 의거 집행한다.  **제22조** 본 방법은 2020년 6월 1일부터 실시하며, <온라인 제품과 서비스 안전검열방법(시범시행)>은 동시에 폐지한다. |  | **网络安全审查办法**  国家互联网信息办公室、国家发展和改革委员会、工业和信息化部等令第 6 号  国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局联合制定了《网络安全审查办法》，现予公布。  国家互联网信息办公室主任 庄荣文  国家发展和改革委员会主任 何立峰  工业和信息化部部长 苗　圩  公安部部长 赵克志  国家安全部部长 陈文清  财政部部长 刘　昆  商务部部长 钟　山  中国人民银行行长 易　纲  国家市场监督管理总局局长 肖亚庆  国家广播电视总局局长 聂辰席  国家保密局局长 田　静  国家密码管理局局长 李兆宗  2020年4月13日  **第一条** 为了确保关键信息基础设施供应链安全，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》，制定本办法。  **第二条** 关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。  **第三条** 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。  **第四条** 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局建立国家网络安全审查工作机制。  网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。  **第五条** 运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。  关键信息基础设施保护工作部门可以制定本行业、本领域预判指南。  **第六条** 对于申报网络安全审查的采购活动，运营者应通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。  **第七条** 运营者申报网络安全审查，应当提交以下材料：  （一）申报书；  （二）关于影响或可能影响国家安全的分析报告；  （三）采购文件、协议、拟签订的合同等；  （四）网络安全审查工作需要的其他材料。  **第八条** 网络安全审查办公室应当自收到审查申报材料起，10个工作日内确定是否需要审查并书面通知运营者。  **第九条** 网络安全审查重点评估采购网络产品和服务可能带来的国家安全风险，主要考虑以下因素：  （一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；  （二）产品和服务供应中断对关键信息基础设施业务连续性的危害；  （三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；  （四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；  （五）其他可能危害关键信息基础设施安全和国家安全的因素。  **第十条** 网络安全审查办公室认为需要开展网络安全审查的，应当自向运营者发出书面通知之日起30个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门征求意见；情况复杂的，可以延长15个工作日。  **第十一条** 网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门应当自收到审查结论建议之日起15个工作日内书面回复意见。  网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门意见一致的，网络安全审查办公室以书面形式将审查结论通知运营者；意见不一致的，按照特别审查程序处理，并通知运营者。  **第十二条** 按照特别审查程序处理的，网络安全审查办公室应当听取相关部门和单位意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知运营者。  **第十三条** 特别审查程序一般应当在45个工作日内完成，情况复杂的可以适当延长。  **第十四条** 网络安全审查办公室要求提供补充材料的，运营者、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。  **第十五条** 网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。  **第十六条** 参与网络安全审查的相关机构和人员应严格保护企业商业秘密和知识产权，对运营者、产品和服务提供者提交的未公开材料，以及审查工作中获悉的其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或用于审查以外的目的。  **第十七条** 运营者或网络产品和服务提供者认为审查人员有失客观公正，或未能对审查工作中获悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。  **第十八条** 运营者应当督促产品和服务提供者履行网络安全审查中作出的承诺。  网络安全审查办公室通过接受举报等形式加强事前事中事后监督。  **第十九条** 运营者违反本办法规定的，依照《中华人民共和国网络安全法》第六十五条的规定处理。  **第二十条** 本办法中关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者。  本办法所称网络产品和服务主要指核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。  **第二十一条** 涉及国家秘密信息的，依照国家有关保密规定执行。  **第二十二条** 本办法自2020年6月1日起实施，《网络产品和服务安全审查办法（试行）》同时废止。 |