**중화인민공화국 인터넷 안보법(초안)**

목　　차

　　제1장 총칙

　　제2장 인터넷 안보 전략, 계획 및 촉진

　　제3장 네트워크 운영 안보

　　　　제1절 일반 규정

　　　　제2절 핵심 정보 인프라의 운영 안보

　　제4장 인터넷 정보 안보

　　제5장 모니터링·조기경보 및 긴급조치

　　제6장 법률책임

제7장 부칙

**제1장 총칙**

1. 인터넷 안보을 보장하고 인터넷 공간의 주권과 국가안전, 사회공공이익을 수호하며 공민, 법인과 기타 조직의 합법적 권익을 보호하고 경제사회 정보화의 건전한 발전을 촉진시키기 위하여 이 법을 제정한다.
2. 중화인민공화국 경내에서의 네트워크 구축, 운영, 유지보수와 인터넷 안보에 대한 감독관리는 이 법의 관할을 받는다.
3. 국가는 인터넷 안보과 정보화 발전을 동시에 중요시하는 원칙을 고수하고 적극 활용, 과학적인 발전, 법에 따른 관리, 안전 보장의 방침을 따르며 인터넷 인프라의 구축을 촉진시키고 인터넷 기술의 혁신과 응용을 격려하며 인터넷 안보 보장시스템을 구축완비하고 인터넷 안보 보호능력을 강화한다.
4. 국가는 신의성실하고 건전·문명한 온라인 행위를 창도하고 조치를 취하여 사회의 전반적인 인터넷 안보 의식과 수준을 강화하며 사회 전체가 공동으로 인터넷 안보에 참여하고 인터넷 안보을 촉진시키는 양호한 환경을 조성한다.
5. 국가는 인터넷 공간 관리, 인터넷 기술의 연구개발과 표준의 제정, 인터넷 범죄 단속 등 분야에서의 국제교류와 협력을 적극 추진하고 평화롭고 안전하며 개방적이고 협력하는 인터넷 공간의 구축을 촉진시킨다.
6. 국가인터넷안보및정보화부서가 인터넷 안보 사업과 관련 감독관리 업무를 총괄 및 조율한다. 국무원 공업및정보화부서, 공안부서와 기타 관련 부서는 이 법과 관련 법률, 행정법규의 규정에 따라 각자의 직책 범위 내에서 인터넷 안보 및 감독관리 업무를 담당한다.

현급 이상 지방인민정부 관련 부서의 인터넷 안보 및 감독관리 지책은 국가의 관련 규정에 따라 확정한다.

1. 네트워크를 구축, 운영하거나 네트워크를 통해 서비스를 제공함에 있어 법률, 법규의 규정과 국가표준, 업계표준의 강제성 요구에 따라 기술적인 조치와 기타 필요한 조치를 취함으로써 네트워크의 안전적, 안정적인 운영을 보장하고 인터넷 안보 사건에 효율적으로 대응하며 인터넷 범죄 활동을 방비하고 네트워크 데이터의 온전성, 비밀성 및 사용가능성을 유지해야 한다.
2. 인터넷 관련 업계조직은 정관에 따라 업계의 자율성을 강화하고 인터넷 안보 행위 규범을 제정하며 회원을 지도하여 법에 따라 인터넷 안보을 강화하고 인터넷 안보 수준을 제고시킴으로써 업계의 건전한 발전을 촉진시킨다.
3. 국가는 공민, 법인과 기타 조직이 법에 따라 네트워크를 사용할 수 있는 권리를 보호하며 네트워크 접속의 보급을 촉진시키고 네트워크 서비스 수준을 제고시켜 사회를 위하여 안전하고 편리한 네트워크 서비스를 제공하고 인터넷 정보의 적법하고 질서있는 유동을 보장한다.

그 어떠한 개인과 조직도 네트워크를 이용함에 있어 헌법과 법률을 준수하고 공공질서를 지키며 사회공중도덕을 존중해야 하고 인터넷 안보을 침해하거나 네트워크를 이용하여 국가안전 침해, 테러주의와 극단주의 홍보, 민족원한과 민족차별 선양, 색정음란정보 전파, 타인 모욕·비방, 사회질서 교란, 공공이익 침해, 타인의 지적재산권과 기타 합버적 권익 침해 등 활동에 종사해서는 아니된다.

1. 그 어떠한 개인과 조직도 인터넷안보및정보화부서, 공업및정보화부서, 공안부서 등 부서에 인터넷 안보을 해하는 행위를 제보할 수 있다. 제보를 받은 부서는 지체없이 법에 따라 처리해야 하며; 본 부서의 관할이 아닌 경우 지체없이 처리권한이 있는 부서로 이송해야 한다.

**제2장 인터넷 안보 전략, 계획 및 촉진**

1. 국가는 인터넷 안보 전략을 제정하여 인터넷 안보 보장의 기본 요구와 주요 목표를 명확히 하고 인터넷 안보 보장시스템 보완, 인터넷 안보 능력 강화, 인터넷 안보 기술 및 산업의 발전 촉진, 인터넷 안보 유지보수 사업에 대한 사회의 공동참여 추진 등 정책조치를 출범한다.
2. 국무원 통신, 라디오·TV, 에너지, 교통, 수리, 금융 등 업계 주관부서와 국무원 기타 관련 부서는 국가 인터넷 안보 전략에 의거하여 국가안보, 국계민생과 연관된 중점 업종, 중점 분야의 인터넷 안보 계획을 수립하고 실시한다.
3. 국가는 인터넷 안보 표준 시스템을 구축 및 보완한다. 국무원 표준화행정주관부서와 국무원 기타 관련 부서는 각자의 직책에 근거하여 인터넷 안보 관리, 네트워크 제품·서비스 및 운영 안전과 관련된 국가표준, 업계표준을 제정하고 적시에 개정한다.

국가는 기업이 인터넷 안보 국가표준, 업계표준의 제정에 참여하는 것을 지원하고 기업이 국가표준, 업계표준보다 엄격한 기업표준을 제정하는 것을 격려한다.

1. 국무원과 성·자치구·직할시 인민정부는 통합적으로 계획하고 투자를 확대하여 인터넷 안보 기술 산업과 프로젝트를 중점적으로 후원하고 인터넷 안보 기술의 연구개발, 응용과 홍보를 지원하며 네트워크 기술의 지적재산권을 보호하고 과학연구기구, 고등교육기관 및 기업이 국가 인터넷 안보기술 혁신 프로젝트에 참여하는 것을 지원해야 한다.
2. 각 급 인민정부와 그 관련 부서는 인터넷 안보 홍보교육을 주기적으로 진행하고 관련 업체가 인터넷 안보 홍보교육을 차질없이 진행하도록 지도 및 촉구해야 한다.

매스미디어는 사회대중에 대해 지향적인 인터넷 안보 홍보교육을 진행해야 한다.

1. 국가는 기업과 고등교육기관, 직업학교 등 교육훈력기구가 인터넷 안보 관련 교육훈련을 실시하여 다양한 방식으로 인터넷 안보 기술인재를 육성하고 인터넷 안보 기술인재 교류를 촉진하는 것을 지원한다.

**제3장 네트워크 운영 안보**

**제1절 일반 규정**

1. 국가는 인터넷 안보 등급화 제도를 시행한다. 네트워크 운영자는 인터넷 안보 등급화 제도의 요구에 따라 다음 각 호의 안보 의무를 이행하여 네트워크 교란, 침해 또는 무권한 접근을 방지하고 네트워크 데이터의 유출 또는 도난, 변조를 방지한다.
2. 내부 안보관리제도와 운영매뉴얼을 제정하고 인터넷 안보 담당자를 확정하여 사이보 안보 책임을 차질없이 이행해야 한다.
3. 컴퓨터 바이러스 및 인터넷 공격, 인터넷 침입 등 인터넷 안보 침해 행위를 방어하는 기술조치를 취해야 한다.
4. 네트워크 운영상황 기록 및 추적, 인터넷 안보 사건 모니터링 및 기록 등 기술조치를 취하고 규정에 따라 네트워크 운영일지를 보관해야 한다.
5. 데이터 분류, 중요 데이터 백업, 암호화 등 조치를 취해야 한다.
6. 법률, 행정법규에 규정한 기타 의무.

인터넷 안보 등급화의 세부 규정은 국무원이 정한다.

1. 네트워크 제품·서비스는 관련 국가표준, 업계표준에 부합되어야 한다. 네트워크 제품·서비스 제공자는 악성 프로그램을 설치해서는 아니되고; 이용자 정보 수집 기능이 있는 제품·서비스의 경우 이용자에게 그 기능을 명시하여 동의를 득해야 하며; 그 네트워크 제품·서비스에 안보상의 결함 등 위험이 있을 경우 지체없이 이용자에게 고지하고 구제조치를 취해야 한다.

네트워크 제품·서비스 제공자는 그 제품·서비스를 위한 안보 유지보수 서비스를 지속적으로 제공해야 하며; 규정된 기간 내에 또는 당사자가 약정한 기간 내에 안보 유지보수 서비스를 중단해서는 아니된다.

1. 네트워크 핵심설비와 인터넷 안보 전문제품은 관련 국가표준, 업계표준의 강제성 요구에 따라 자격을 구비한 기구의 안보 인증 또는 안보 측정을 통과한 후에야 판매가 가능한다. 국가인터넷안보및정보화부서는 국무원 관련 부서와 회동하여 네트워크 핵심설비 및 인터넷 안보 전문제품 목록을 제정, 공표하고 안보 인증결과 및 안보 측정결과의 상호인정을 추진함으로써 중복적인 인증, 측정을 모면해야 한다.
2. 네트워크 운영자는 이용자에게 네트워크 접속 서비스, 도메인 등록 서비스를 제공하고 유선전화, 휴대전화 가입수속을 처리하거나 이용자에게 정보발표 서비스를 제공함에 있어 이용자와 계약서를 체결하거나 서비스의 제공을 확인할 때 진실한 신분정보의 제공을 이용자에게 요구해야 한다. 이용자가 진실한 신분정보를 제공하지 아니할 경우 네트워크 운영자는 그에게 관련 서비스를 제공해서는 아니된다.

국가는 안전하고 편리한 전자신분 인증기술의 연구개발을 지원하며 서로 다른 전자신분 인증기술의 상호인정과 통용화를 추진한다.

1. 네트워크 운영자는 인터넷 안보 사건 긴급대비책을 제정해야 하며 시스템 결함, 컴퓨터 바이러스, 인터넷 침입, 인터넷 공격 등 안보상의 위험을 지체없이 처리해야 한다. 인터넷 안보을 침해하는 사건이 발생한 경우 즉시 긴급대비책을 가동하여 해당 구제조치를 취하고 규정에 따라 관련 주관부서에 보고해야 한다.
2. 그 어떠한 조직과 개인도 타인의 네트워크 침입, 타인의 정상적인 네트워크 기능 방해, 네트워크 데이터 절취 등 인터넷 안보을 해치는 활동에 종사해서는 아니되고; 네트워크 침입, 정상적인 네트워크 기능 방해, 네트워크 데이터 절취 등 인터넷 안보 침해 수단과 제조방법을 제공해서는 아니되며; 타인이 실시하는 인터넷 안보 침해 활동을 위하여 기술지원, 광고·홍보, 지급·정산 등 도움을 제공해서는 아니된다.
3. 국가안보과 범죄수사의 수요가 있을 경우 수사기관은 법률 규정에 따라 네트워크 운영자게 필요한 지원과 협조를 요청할 수 있다.
4. 국가는 네트워크 운영자 간에 인터넷 안보 정보의 수집, 분석, 통보 및 긴급대응 등 분야의 협력을 추진하여 네트워크 운영자의 안보 보장 능력을 강화하는 것을 지원한다.

관련 업계조직은 해당 업계의 인터넷 안보 규범과 협력 매커니즘을 구축완비하고 인터넷 안보 위험에 대한 분석평가를 강화하며 정기적으로 회원에게 위험을 경고하고 회원의 인터넷 안보 위험 대응을 지원, 협조한다.

**제2절 핵심 정보 인프라의 운영 안보**

1. 국가는 공공통신·라디오/TV 전송 등 서비스를 제공하는 기초정보망, 에너지·교통·수리·금융 등 중요한 업종과 전기/용수/가스공급·의료위생·사회보장 등 공공서비스 분야의 중요한 정보시스템, 군사망, 구(區)가 설치되어 있는 시(市)급 이상의 국가기관 등 정무 시스템, 이용자를 많이 확보하고 있는 네트워크 서비스 제공자가 소유하고 있거나 관리하는 네트워크와 시스템(이하 '핵심 정보 인프라'로 약칭)을 중점적으로 보호한다. 핵심 정보 인프라 안보방법은 국무원이 제정한다.
2. 국무원 통신, 라디오·TV, 에너지, 교통, 수리, 금융 등 업계 주관부서와 국무원 기타 관련 부서(이하 '핵심 정보 인프라 안보업무 담당부서'로 약칭)는 국무원이 규정한 직책에 따라 핵심 정보 인프라의 운영 안보 업무에 대한 지도와 감독을 각각 담당한다.
3. 핵심 정보 인프라를 구축함에 있어 업무의 안정적, 지속적 운영를 지원하는 성능을 확보하도록 하고 안보기술조치의 동시 계획, 동시 구축, 동시 사용을 보장해야 한다.
4. 이 법 제17조의 규정 이외에 핵심 정보 인프라 운영자는 다음 각 호의 안보 의무를 이행해야 한다.
5. 안보관리 전문기구와 안보관리 담당자를 설치하고 그 담당자와 핵심 직무 담당인력에 대한 안보배경 심사를 실시해야 한다.
6. 정기적으로 종업원에 대한 인터넷 안보 교육, 기술교육 및 기능평가를 실시해야 한다.
7. 재해복구를 대비하여 중요한 시스템과 데이터베이스를 백업해야 한다.
8. 인터넷 안보 사건 긴급대비책을 제정하고 정기적으로 시물레이션을 실시해야 한다.
9. 법률, 행정법규에 규정한 기타 의무.
10. 핵심 정보 인프라 운영자는 네트워크 제품·서비스 구매시 납품자자와 안보계약을 체결하여 안보 및 비밀유지 의무와 책임을 명확히 해야 한다.
11. 핵심 정보 인프라 운영자의 네트워크 제품 또는 서비스 구매가 국가안보에 영향을 미칠 우려가 있을 경우 국가인터넷안보및정보화부서가 국무원 관련부서와 회동하여 실시하는 안전심사를 통과해야 한다. 구체적인 방법은 국무원이 규정한다.
12. 핵심 정보 인프라 운영자는 운영 과정에서 수집 및 발생한 공민의 개인정보 등 중요한 데이터를 중화인민공화국 경내에 저장해야 하며; 업무의 수요로 인해 해외에 저장할 필요가 있거나 해외 조직 또는 개인에게 제공해야 하는 경우 국가인터넷안보및정보화부서가 제정한 방법에 따라 안보평가를 실시해야 한다. 법률, 행정법규에 별도의 규정이 있을 경우 그 규정에 따른다.
13. 핵심 정보 인프라 운영자는 스스로 또는 전문기구에 의뢰하여 그 네트워크의 잠재적 안보 위험에 대한 측정평가를 매년 1회 이상 실시해야 하며 검사평가 상황과 그가 취한 개선조치에 대한 인터넷 안보 보고서를 작성하여 핵심 정보 인프라 안보 업무 담당부서에 보고해야 한다.
14. 국가사이보안보및정보화부서는 관련부서를 조율하여 협력 매커니즘을 구축해야 한다. 핵심 정보 인프라에 대해 다음 각 호의 안보조치를 취할 수 있다.
15. 핵심 정보 인프라의 안보 위험에 대해 추출검사와 측정을 실시하고 개선조치를 제안하며 필요한 경우 전문검사측정기구에 의뢰하여 네트워크에 대한 안보 위험 측정평가를 실시한다.
16. 정기적으로 핵심 정보 인프라 운영자를 조직하여 인터넷 안보 비상대응 시물레이션을 추진하고 핵심 정보 인프라의 사이보 안보 사건 대응능력과 협력능력을 강화한다.
17. 관련 부서, 핵심 정보 인프라 운영자 및 인터넷 안보 서비스 기구, 관련 연구기관 등 사이의 인터넷 안보 정보 공유를 촉진시킨다.
18. 인터넷 안보 사건의 긴급대응 및 복구 등에 대해 기술지원을 제공하고 협조한다.

**제4장 인터넷 정보 안보**

1. 네트워크 운영자는 이용자 정보 보호제도를 구축완비하여 이용자의 개인정보, 프라이버시 및 상업비밀에 대한 보호를 강화해야 한다.
2. 네트워크 운영자는 공민의 개인정보를 수집하고 사용함에 있어 적법성, 정당성, 필요성의 원칙을 준수해야 하고 정보 수집·사용의 목적, 방식과 범위를 명시해야 하며 수집 대상자의 동의를 득해야 한다.

네트워크 운영자는 제공하는 서비스와 무관한 공민의 개인정보를 수집해서는 아니되고 법률, 행정법규의 규정과 양자간의 약정을 어기고 공민의 개인정보를 수집·사용해서는 아니되며 법률, 행정법규의 규정 또는 이용자와의 약정에 따라 그가 보관한 개인정보를 처리해야 한다.

네트워크 운영자는 공민의 개인정보를 수집·사용함에 있어 수집·사용 규칙을 공개해야 한다.

1. 네트워크 운영자는 그가 수집한 공민 개인정보의 비밀성을 유지해야 하고 유출, 변조, 훼손해서는 아니되며 매각하거나 불법으로 타인에 제공해서는 아니된다.

네트워크 운영자는 기술조치와 기타 필요한 조치를 취하여 공민 개인정보의 안보을 확보하고 그가 수집한 공민의 개인정보가 유출, 훼손, 분실되는 것을 방지해야 한다. 정보의 유출, 훼손, 분실이 우려될 경우 즉시 구제조치를 취하고 영향을 받을 가능성이 있는 이용자에게 고지하며 규정에 따라 관련 주관부서에 보고해야 한다.

1. 공민은 네트워크 운영자가 법률, 행정법규의 규정 또는 양자간의 약정을 어기고 자신의 개인정보를 수집·사용한 사실을 발견한 경우 네트워크 운영자에게 그 개인정보의 삭제를 요구할 권리가 있으며; 네트워크 운영자가 수집·저장한 자신의 개인정보에 오류가 있음을 발견한 경우 네트워크 운영자에게 정정을 요구할 권리가 있다.
2. 그 어떠한 개인과 조직도 공민의 개인정보를 절취하거나 기타 불법적인 방식으로 획득해서는 아니되며 공민의 개인정보를 매각하거나 불법으로 타인에게 제공해서는 아니된다.
3. 법에 의거하여 인터넷 안보 감독관리 직책을 담당하는 부서는 직책 이행 과정에서 알게된 공민의 개인정보, 프라이버시 및 상업비밀의 비밀성을 유지해야 하며 유출, 매각하거나 불법으로 타인에게 제공해서는 아니된다.
4. 네트워크 운영자는 그 이용자가 발표하는 정보에 대한 관리를 강화해야 하며 법률, 행정법규에 의해 발표 또는 전송이 금지된 정보를 발견항 경우 즉시 당해 정보의 전송을 중단하고 삭제 등 처리조치를 취하여 정보의 확산을 막아야 하며 관련 기록을 보관하고 관련 주관부서에 보고해야 한다.
5. 전자정보 발송자가 발송하는 전자정보와 응용 소프트웨어 제공자가 제공하는 응용 소프트웨어 악성 프로그램을 설치해서는 아니되며 법률, 행정법규에 의해 발표 또는 전송이 금지된 정보가 포함되어서는 아니된다.

전자정보 발송 서비스 제공자와 응용 소프트웨어 다운로드 서비스 제공자는 안보관리 의무를 이행해야 하며 전자정보 발송자, 응용 소프트웨어 제공자가 전 항에 규정한 행위를 행한 사실을 발견한 경우 즉시 서비스 제공을 중단해야 하며 삭제 득 처리조치를 취하고 관련 기록을 보고하며 관련 주관부서에 보고해야 한다.

1. 네트워크 운영자는 인터넷 정보 안보 신고·제보 팰랫폼을 구축하고 신고·제보방식 등 정보를 공표하며 인터넷 정보 안보 신고와 제보를 지체없이 접수 및 처리해야 한다.
2. 국가인터넷안보및정보화부서와 관련 부서는 법에 따라 인터넷 안보 감독관리 직책을 이행하고 법률, 행정법규에 의해 발표 또는 전송이 금지된 정보를 발견한 경우 네트워크 운영자에게 전송을 중단하고 삭제 등 처리조치를 취하며 관련 기록을 보관할 것을 요구해야 한다. 상기 정보의 출처가 중환인민공화국 경외인 경우 기술조치 및 기타 필요한 조치를 취하여 정보의 전파를 차단하도록 관련 기구에 통보한다.

**제5장 모니터링·조기경보 및 긴급처치**

1. 국가는 인터넷 안보 모니터링·조기경보 및 정보통보제도를 구축한다. 국가인터넷안보및정보화부서는 관련 부서와 회동하여 인터넷 안보 정보의 수집, 분석 및 통보 업무를 강화하고 규정에 따라 인터넷 안보 모니터링·조기경보 정보를 통일적으로 발표한다.
2. 핵심 정보 인프라 안보 업무를 담당한 부서는 본 업계, 본 분야의 인터넷 안보 모니터링·조기경보 및 정보통보제도를 구축완비해야 하며 규정에 따라 인터넷 안보 모니터링·조기경보 정보를 보고해야 한다.
3. 국가인터넷안보및정보화부서는 관련 부서와 회동하여 인터넷 안보 긴급대응 업무제도를 구축완비하고 인터넷 안보 사건 긴급대비책을 제정하며 정기적으로 시물레이션을 실시한다.

핵심 정보 인프라 안보 업무를 담당한 부서는 본 업계, 본 분야의 인터넷 안보 사건 긴급대비책을 제정하고 정기적으로 시물레이션을 실시해야 한다.

인터넷 안보 사건 긴급대비책은 사건 발생 후의 피해정도, 영향범위 등 요인에 따라 인터넷 안보 사건의 등급을 확정하고 상응하는 긴급대비조치를 규정해야 한다.

1. 인터넷 안보 사건이 발생 직전이거나 발생 위험이 증대된 경우 현급 이상 인민정부의 관련 부서는 관련 법률, 행정법규와 국무원이 규정한 권한, 절차에 따라 해당 등급의 조기경보 정보를 발표하고 곧 발생하게 될 사건의 특성과 초래 가능한 피해에 근거하여 다음 조치를 취해야 한다.
2. 관련 부서, 기구 및 인원에게 지체없이 관련 정보를 수집, 보고하고 인터넷 안보 사건의 발생·발전 상황에 대한 모니터링을 강화할 것을 요구한다.
3. 관련 부서, 기구 및 전문인력을 조직하여 인터넷 안보 사건 정보를 분석 및 평가하여 사건 발생 가능성, 영향범위 및 피해정도를 예측한다.
4. 대중과 관련한 예측정보 및 분석평가 결과를 사회에 공표한다.
5. 규정에 따라 사회에 인터넷 안보 사건의 피해를 받을 위험이 있음을 알리는 경고를 발표하고 피해를 모면하거나 줄일 수 있는 조치를 공개한다.
6. 인터넷 안보 사건이 발생하는 경우 현급 이상 인민정부의 관련 부서는 인터넷 안보 사건 긴급대비책을 가동하여 인터넷 안보 사건을 조사·평가하고 네트워크 운영자에게 기술조치 및 기타 필요한 조치를 취하여 잠재적인 안보 우환을 제거하고 피해의 확산을 방지할 것을 요구해야 하며 지체없이 대중과 관련된 경고 정보를 사회에 발표해야 한다.
7. 인터넷 안보 사건으로 인해 돌발사건 또는 안전생산사고가 발생한 경우 <중화인민공화국 돌발사건 긴급대응법>, <중화인민공화국 안전생산법> 등 관련 법률의 규정에 따라 처리해야 한다.
8. 국가안전 및 사회공공질서의 유지와 중대한 돌발 사회안전사건 처리에 필요한 경우 국무원 또는 성·자치구·직할시 인민정부는 국무원의 비준을 득한 후 일부 지역에서 네트워크 통신 제한 등 임시조치를 취할 수 있다.

**제6장 법률책임**

1. 네트워크 운영자가 이 법 제17조, 제21조에 규정한 인터넷 안보 의무를 이행하지 아니한 경우 관련 주관부서가 시정을 명하고 경고를 주며; 시정을 거부하거나 인터넷 안보에 피해를 초래한 경우 1만위안 이상 10만위안 이하의 과태료를 부과하고; 직접 담당한 주관자에게 5,000위안 이상 5만위안 이하의 과태료를 부과한다.

핵심 정보 인프라 운영자가 이 법 제27조~제29조, 제32조에 규정한 인터넷 안보 의무를 이행하지 아니한 경우 관련 주관부서가 시정을 명하고 경고를 주며; 시정을 거부하거나 인터넷 안보에 피해를 초래한 경우 10만위안 이상 100만위안 이하의 과태료를 부과하고; 직접 담당한 주관자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.

1. 네트워크 제품·서비스 제공자, 전자정보 발송자, 응용 소프트웨어 제공자가 이 법의 규정을 어기고 다음 각 호의 어느 하나에 해당되는 행위를 행하였을 경우 관련 주관부서가 시정을 명하고 경고를 주며; 시정을 거부하거나 인터넷 안보에 피해를 초래한 경우 5만위안 이상 50만위안 이하의 과태료를 부과하고; 직접 담당한 주관자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.
2. 악성 프로그램을 설치한 경우;
3. 그 제품·서비스에 이용자 정보 수집 기능이 있음에도 불구하고 이용자에게 명시하여 동의를 득하지 아니한 경우;
4. 그 제품·서비스에 존재하는 안보결함 등 위험을 지체없이 이용자에게 고지하고 구제조치를 취하지 아니한 경우;
5. 그 제품·서비스에 대한 안보 유지보수를 무단 중단한 경우.
6. 네트워크 운영자가 이 법의 규정을 어기고 이용자에게 진실한 신분정보의 제공을 요구하지 않았거나 진실한 신분정보를 제공하지 않은 이용자에게 관련 서비스를 제공한 경우 관련 주관부서가 시정을 명하고; 시정을 거부하거나 경위가 심각한 경우 5만위안 이상 50만위안 이하의 과태료를 부과함과 더불어 관련 주관부서가 관련 업무 일시 중단, 휴업정돈, 사이트 폐쇄, 관련 업무 허가증 또는 영업허가증 취소 처벌을 내릴 수 있으며; 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.
7. 네트워크 운영자가 이 법의 규정을 어기고 공민의 개인정보를 보호받을 권리를 침해한 경우 관련 주관부서가 시정을 명하고 경위에 따라 경고, 불법소득 몰수, 불법소득 10배 이하의 과태료 부과 처벌 중의 하나를 부과하거나 병과할 수 있으며 불법소득이 없을 경우에는 50만위안 이하의 과태료를 부과한다. 경위가 심각한 경우 업무 일시 중단, 휴업정돈, 사이트 폐쇄, 관련 업무 허가증 또는 영업허가증 취소 처벌을 내릴 수 있으며; 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.

이 법의 규정을 어기고 공민의 개인정보를 절취하거나 기타 불법적인 방식으로 획득, 매각하거나 불법으로 타인에게 제공하였으나 범죄를 구성하지 아니할 경우 공안기관이 불법소득을 몰수하고 불법소득의 1배 이상 10배 이하에 상당하는 과태료를 병과하며, 불법소득이 없을 경우에는 5만위안 이하의 과태료를 부과한다.

1. 핵심 정보 인프라 운영자가 이 법 제30조의 규정을 어기고 안보 심사를 거치지 않았거나 안보 심사를 통과하지 못한 네트워크 제품 또는 서비스를 사용한 경우 관련 주관부서가 사용 중단을 명하고 구매금액의 1배 이상 10배 이하에 상당하는 과태료를 부과하며; 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.
2. 핵심 정보 인프라 운영자가 이 법의 규정을 어기고 해외에 네트워크 데이터를 저장하거나 안보평가를 거치지 않고 해외 조직 또는 개인에게 네트워크 데이터를 제공한 경우 관련 주관부서가 시정을 명하고 경고를 주며 불법소득을 몰수하고 5만위안 이상 50만위안 이하의 과태료를 부과하며 이와 더불어 업무 일시 중단, 휴업정돈, 사이트 폐쇄, 관련 업무 허가증 또는 영업허가증 취소 처벌을 내릴 수 있다. 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.
3. 네트워크 운영자가 이 법의 규정을 어기고 법률, 행정법규에 의해 발표 또는 전송이 금지된 정보에 대해 전송 중단, 삭제 등 조치를 취하지 않고 관련 기록을 보관하지 아니한 경우 관련 주관부서가 시정을 명하고 경고를 주며 불법소득을 몰수한다. 시정을 거부하거나 경위가 심각한 경우 10만위안 이상 50만위안 이하의 과태료를 부과함과 더불어 업무 일시 중단, 휴업정돈, 사이트 폐쇄, 관련 업무 허가증 또는 영업허가증 취소 처벌을 내릴 수 있으며; 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 2만위안 이상 20만위안 이하의 과태료를 부과한다.

전자정보 발송 서비스 제공자, 응용 소프트웨어 다운로드 서비스 제공자가 이 법에 규정한 안보 의무를 이행하지 아니하였을 경우 전 항의 규정에 따라 처벌한다.

1. 법률, 행정법규에 의해 발표 또는 전송이 금지된 정보를 발표 또는 전송한 경우 관련 법률, 행정법규의 규정에 따라 처벌한다.
2. 네트워크 운영자가 이 법의 규정을 어기고 다음 각 호의 어느 하나에 해당되는 행위를 행하였을 경우 관련 주관부서가 시정을 명하고; 시정을 거부하거나 경위가 심각한 경우 5만위안 이상 50만위안 이하의 과태료를 부과하며; 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.
3. 인터넷 안보 위험, 인터넷 안보 사건을 관련 주관부서에 보고하지 아니한 경우;
4. 관련 부서가 법에 따라 실시하는 감독검사를 거부, 방해한 경우;
5. 필요한 지원 또는 협조의 제공을 거부한 경우.
6. 이 법 제22조에 규정한 인터넷 안보 파괴 행위를 행하였지만 범죄를 구성하지 아니하거나 이 법의 규정에 위배되는 기타 행위를 행하여 치안관리법 위반에 해당되는 경우 법에 따라 치안관리 처벌을 내린다.
7. 국가기관 정무 시스템 운영자가 이 법에 규정한 인터넷 안보 의무를 이행하지 아니한 경우 그 상급기관 또는 관련 기관이 시정을 명하고; 법에 따라 직접 담당한 주관자와 기타 직접적 책임이 있는 자에게 처분을 내린다.
8. 법에 따라 인터넷 안보 감독관리 직책을 담당하는 부서의 업무인력이 직무를 소홀히 하고 직권을 남용하거나 사리를 도모하는 부정행위를 행하였으나 범죄를 구성하지 아니할 경우 법에 따라 행정처분을 내린다.
9. 이 법의 규정을 어기고 타인에게 손해를 초래한 경우 법에 따라 민사책임을 진다.
10. 이 법의 규정을 위반하여 범죄를 구성한 경우 법에 따라 형사책임을 추궁한다.

**제7장 부칙**

1. 이 법에 사용한 용어의 의미는 다음과 같다.
2. 인터넷라 함은 검퓨터 또는 기타 정보단말기 및 관련 설비로 구성되었고 일정한 규칙과 절차에 따라 정보를 수집, 저장, 전송, 교환, 처리하는 네트워크와 시스템을 지칭한다.
3. 인터넷 안보이라 함은 필요한 조치를 통하여 인터넷에 대한 공격, 침입, 교란, 파괴, 불법사용과 우발사고를 방비하고 네트워크의 안정적인 운영 상태를 유지시키며 온라인으로 저장, 전송, 처리한 정보의 온전성, 비밀성, 사용가능성을 보장할 수 있는 능력을 지칭한다.
4. 네트워크 운영자라 함은 네트워크의 소유자, 관리자 및 타인이 소유 또는 관리하는 네트워크를 이용하여 관련 서비스를 제공하는 네트워크 서비스 제공자를 지칭하며 기초통신 운영자, 네트워크 정보 서비스 제공자, 중요 정보시스템 운영자 등을 포함한다.
5. 네트워크 데이터라 함은 네트워크를 통해 수집, 저장, 전송, 처리되고 발생하는 각 종의 전자 데이터를 지칭한다.
6. 공민의 개인정보라 함은 전자 또는 기타 방식으로 기록한 공민의 성명, 출생년월일, 신분증 번호, 개인 생체인식정보, 직업, 주소, 전화번호 등 개인의 신분정보와 기타 단독으로 또는 다른 정보와 결합하여 공민 개인의 신분을 식별할 수 있는 각 종 정보를 지칭한다.
7. 국가비밀정보의 저장, 처리와 연관된 네트워크 운영 안보은 이 법의 규정을 준수해야 하는 것 외에 비밀유지 관련 법률, 행정법규의 규정도 준수해야 한다.
8. 군사용 네트워크 및 정보 안보 방법은 중앙군사위원회가 제정한다.
9. 이 법은 년 월 일부터 시행한다.