|  |  |  |
| --- | --- | --- |
| **중화인민공화국 사이버 안보법**  중화인민공화국 주석 령 제53호  <중화인민공화국 사이버 안보법>이 2016년 11월 7일의 중화인민공화국 제12기 전국인민대표대회 상무위원회 제24차 회의에서 통과되어 이에 공표하며, 2017년 6월 1일부터 시행한다.  중화인민공화국 주석 시진핑  2016년 11월 7일  목　차  제1장 총 칙  제2장 인터넷 안보 지지 및 촉진  제3장 인터넷 운영 안전  제1절 일반 규정  제2절 핵심 정보 인프라의 운영 안전  제4장 인터넷 정보 안전  제5장 모니터링 조기경보 및 긴급조치  제6장 법률책임  제7장 부 칙  제1장 총 칙  제1조 인터넷 안보 보장을 위하여, 인터넷 공간의 주권과 국가안보, 사회공공이익을 수호하고 공민, 법인과 기타 조직의 합법적 권익을 보호하고 경제사회의 정보화의 건전한 발전을 촉진시키기 위하여 이 법을 제정한다.  제2조 중화인민공화국 경내에서의 인터넷 구축, 운영, 유지보수와 인터넷 안보에 대한 감독관리는 이 법을 적용한다.  제3조 국가는 인터넷 안보와 정보화 발전을 동시에 중요시하는 원칙을 고수하고 적극 활용, 과학적인 발전, 법에 따른 관리, 안보 보장의 방침을 따르며 인터넷 인프라의 구축과 상호간 연결을 촉진시키고 인터넷 기술의 혁신과 응용을 장려하고 인터넷안보 인재의 양성을 지원하고 인터넷안보 보장시스템을 구축하고 완벽히 함으로써 인터넷안보 능력을 강화한다.  제4조 국가는 인터넷안보 전략을 제정하고 부단히 완벽히 하여 인터넷안보를 보장하는 기본요구와 주요목표를 명확히 함으로써 중점분야의 인터넷안보 정책, 임무 및 조치를 제시한다.  제5조 국가는 조치를 취하여 중화인민공화국 경내외의 인터넷안보리스크와 위협을 모니터링, 예방 및 처리하므로써 핵심정보 인프라의 공격, 칩입, 교란 및 파괴를 받지 않도록 보호하고 법에 따라 인터넷 불법 범죄활동을 징벌하며, 인터넷공간의 안보와 질서를 유지한다.  제6조 국가는 신의성실하고 건강하고 문명한 온라인 행위를 창도하고 사회주의 핵심가치관을 전파시키며, 조치를 취하여 사회의 전반적인 인터넷안보 의식과 수준을 강화시키며, 사회 전체가 공동으로 인터넷안보에 참여함으로써 인터넷안보을 촉진시키는 양호한 환경을 조성한다.  제7조 국가는 인터넷 공간에 대한 관리, 인터넷 기술의 연구개발과 표준 제정, 인터넷 범죄 단속 등 분야에서의 국제교류와 협력을 적극 추진하고, 평화롭고 안전하고 개방적이고 협력적인 인터넷공간을 구축함으로써 다차원, 민주, 투명적인 인터넷공간 관리 체계를 구축한다.  제8조 국가 인터넷안보 및 정보화부서가 인터넷안보 사업과 관련된 감독관리 업무를 총괄하고 조율한다. 국무원 전신주관부서, 공안부서 및 기타 유관부서는 이 법과 관련 법률, 행정법규의 규정에 따라 각자의 직책 범위 내에서 인터넷안보 및 감독관리 업무를 담당한다.  현급 이상 지방인민정부 유관부서의 인터넷안보 및 감독관리 직무는 국가의 관련 규정에 따라 확정한다.  제9조 인터넷 운영자가 경영과 서비스활동을 전개할 시에는 반드시 법률, 행정법규를 준수하고 사회윤리를 존중시하고 상업의식을 지키고 신의성실하고 인터넷안보 의무를 이행해야 하며, 아울러 정부와 사회의 감독을 받고 사회에 대한 책임을 진다.  제10조 인터넷을 구축, 운영하거나 인터넷을 통해 서비스를 제공함에 있어 법률, 행정법규의 규정과 국가표준의 강제성 요구에 따라 기술적인 조치와 기타 필요한 조치를 취함으로써 인터넷 안보와 그 안정적인 운영을 보장하고 인터넷안보 사건에 효율적으로 대응함으로써 인터넷 범죄 활동을 방비하고 인터넷 데이터의 완벽성과 비밀성, 사용가능성을 유지해야 한다.  제11조 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.  제12조 국가는 공민, 법인과 기타 조직이 법에 따라 인터넷을 사용할 수 있는 권리를 보장하며 인터넷 접속의 보급을 촉진시키고 인터넷 서비스 수준을 제고시켜 사회에 안전하고 편리한 인터넷 서비스를 제공함으로써 인터넷 정보의 적법적이고 질서있는 유동을 보장한다.  그 어떠한 개인과 조직도 인터넷을 이용함에 있어 헌법과 법률을 준수하고 공공질서를 지키며 사회공중윤리를 존중시해야 하며, 인터넷 안보을 위해하거나 인터넷를 이용하여 국가안보, 영예와 이익을 해치고 국가정권의 전복을 선동하고, 사회주의 제도를 반대하고, 국가분열을 선동하고, 국가통일을 파괴하고, 테러주의와 극단주의를 선양하고, 민족원한과 민족차별시를 선양하고, 폭력과 색정음란정보를 전파하고, 허위정보를 날조하거나 전파하여 경제질서와 사회질서를 교란하고 타인의 명예와 프라이버시, 지적재산권과 기타 합법적 권익을 침해하는 등의 활동에 종사해서는 아니된다.  제13조 국가는 미성년자의 건강한 성장에 이로운 인터넷제품과 서비스 연구, 개발을 지지하며, 법에 따라 인터넷을 이용하여 미성년자의 심신건강을 해롭히는 활동을 징벌함으로써 미성년자에게 안전하고 건강한 인터넷 환경을 제공한다.  제14조 그 어떠한 개인과 조직도 인터넷안보 및 정보화부서, 전신부서, 공안부서 등 부서에 인터넷 안보를 해롭히는 행위를 제보할 수 있다. 제보를 받은 부서는 지체없이 법에 따라 처리해야 하며, 본 부서의 관할이 아닌 경우 지체없이 관할권한이 있는 부서로 이송해야 한다.  유관부서는 제보자가 제공한 관련 정보에 대한 비밀를 고수함으로써 제보자의 합법적 권익을 보호한다.  제2장 인터넷 안보 지지 및 촉진  제15조 국가는 인터넷 안보 표준 시스템을 구축 및 완벽히 한다. 국무원 표준화행정주관부서와 국무원 기타 유관부서는 각자의 직무에 근거하여 인터넷 안보 관리, 인터넷 제품, 서비스 및 운영 안전과 관련된 국가표준, 업계표준을 제정하고 적시에 개정한다.  국가는 기업과 연구기관, 대학교, 인터넷 관련 업계조직이 인터넷 안보 국가표준, 업계표준의 제정에 참여하는 것을 지원한다.  제16조 국무원과 성, 자치구, 직할시 인민정부는 통일적으로 계획하고 투자를 증가하여 인터넷 안보 기술 산업과 프로젝트를 중점적으로 지원하고 인터넷 안보 기술의 연구개발과 응용을 지원하고 안전하고 믿음성 있는 인터넷제품과 서비스를 보급시키며, 인터넷 기술의 지적재산권을 보호하고 기업과 연구기관, 대학교 등에서 국가의 인터넷 안보 기술혁신프로젝트에 참여하는 것을 지원해야 한다.  제17조 국가는 인터넷 사회화 서비스체계 건설을 추진하며, 관련 기업, 기구에서 인터넷안보 인증, 검사, 리스크평가 등 안보서비스를 전개하는 것을 장려한다.  제18조 국가는 인터넷데이터 안보와 이용기술의 개발을 장려하며, 공공데이터자원의 개방을 촉진시켜 기술혁신과 경제사회발전을 촉진시킨다.  국가는 인터넷안보 관리방식의 혁신과 인터넷 신기술의 운용을 지원함으로써 인터넷안보 수준을 제고시킨다.  제19조 각 급 인민정부 및 유관부서는 인터넷 안보 홍보교육을 주기적으로 진행하고 관련 업체가 인터넷 안보 홍보교육을 차질없이 진행하도록 지도 및 독촉해야 한다.  매스미디어는 사회대중에 대한 지향적인 인터넷 안보 홍보교육을 진행해야 한다.  제20조 국가는 기업과 대학교, 직업학교 등 교육기구가 인터넷 안보 관련 교육을 실시하여 다양한 방식으로 인터넷 안보 기술인재를 양성하고 인터넷 안보 기술인재 교류를 촉진하는 것을 지원한다.  제3장 인터넷 운영 안전  제1절 일반 규정  제21조 국가는 인터넷 안보 등급 보호제도를 실시한다. 인터넷 운영자는 인터넷 안보 등급 보호제도의 요구에 따라 다음 각 호의 안보 의무를 이행하여 인터넷 교란, 침해 또는 무권한 접근을 방지하고 인터넷 데이터의 유출 또는 도난, 변조를 방지한다.  (1) 내부 안보관리제도와 운영매뉴얼을 제정하고 인터넷 안보 담당자를 지정하여 인터넷 안보 책임을 차질없이 이행해야 한다.  (2) 컴퓨터 바이러스 및 인터넷 공격, 인터넷 침입 등 인터넷 안보 침해 행위를 방어하는 기술조치를 취해야 한다.  (3) 인터넷 운영상태, 인터넷 안보사건을 모니터링, 기록하는 기술조치를 취하며, 규정에 따라 인터넷 운영일지를 최저 6개월 보관해야 한다.  (4) 데이터 분류, 중요 데이터 백업, 암호화 등 조치를 취해야 한다.  (5) 법률, 행정법규에 규정한 기타 의무.  제22조 인터넷 제품•서비스는 관련 국가표준의 강제성 요구에 부합되어야 한다. 인터넷 제품, 서비스 제공자는 악성 프로그램을 설치해서는 아니되며, 그 인터넷 제품과 서비스에 안보결함, 약점이 있는 것을 발견한 경우에는 지체없이 보완조치를 취함과 아울러 규정에 따라 이용자에게 고지하고 유관주관부서에 보고해야 한다.  인터넷 제품, 서비스 제공자는 그 제품, 서비스에 대한 안보 유지보수 서비스를 지속적으로 제공해야 하며, 규정된 기간 내에 또는 당사자가 약정한 기간 내에 안보 유지보수 서비스를 중단해서는 아니된다.  인터넷 제품, 서비스가 이용자의 정보를 수집하는 기능이 있는 경우 그 제공자는 이용자에게 이를 명시하여 동의를 얻어야 하며, 개인의 정보와 관련되는 경우에는 본 법과 관련 법률, 행정법규상 개인정보보호 관련 규정도 준수해야 한다.  제23조 인터넷 핵심설비와 인터넷 안보 전용제품은 관련 국가표준의 강제성 요구에 따라 자격을 구비한 기구의 안보 인증에 합격되거나, 또는 안보 검측을 거쳐 요구에 부합되는 경우에야 판매를 하거나 제공할 수 있다. 국가 인터넷안보 및 정보화부서는 국무원 유관부서와 회동하여 인터넷 핵심설비 및 인터넷 안보 전용제품 목록을 제정, 공표하며 안보 인증결과와 안보 검측결과의 상호인정을 추진함으로써 중복 인증, 검측을 모면해야 한다.  제24조 인터넷 운영자는 이용자에게 인터넷 접속 서비스, 도메인 등록 서비스를 제공하고 유선전화, 휴대전화 가입수속을 처리하거나 이용자에게 정보발표, 메시지 등 서비스를 제공함에 있어 이용자와 계약서를 체결하거나 서비스의 제공을 확인할 때 진실한 신원정보를 제공하도록 요구해야 한다. 이용자가 진실한 신원정보를 제공하지 아니할 경우 인터넷 운영자는 그에게 관련 서비스를 제공해서는 아니된다.  국가는 확실한 인터넷 신원전략을 실시하며, 안전하고 편리한 전자신원 인증기술의 연구개발을 지원하며, 서로 다른 전자신원 인증기술의 상호인정과 통용화를 추진한다.  제25조 인터넷 운영자는 인터넷 안보 사건 긴급대비책을 제정해야 하며 시스템 결함, 컴퓨터 바이러스, 인터넷 공격, 인터넷 침입 등 안보상의 리스크를 지체없이 처리해야 한다. 인터넷 안보에 해로운 사건이 발생한 경우 즉시 긴급대비책을 가동하여 해당 구제조치를 취하고 규정에 따라 유관주관부서에 보고해야 한다.  제26조 인터넷 안보 인증, 검측, 리스크평가 등 활동을 전개하는 경우에는 사회에 시스템 결함, 컴퓨터 바이러스, 인터넷공격, 인터넷침입 등 인터넷 안보정보를 공개해야 하며, 아울러 국가의 관련 규정을 준수해야 한다.  제27조 그 어떠한 조직과 개인도 타인의 인터넷 침입, 타인의 정상적인 인터넷 기능 방해, 인터넷 데이터 절취 등 인터넷 안보을 해치는 활동에 종사해서는 아니되며, 인터넷 침입, 정상적인 인터넷 기능 방해 및 방어조치, 인터넷 데이터 절취 등 인터넷 안보를 침해하는 프로그램과 수단을 제공해서는 아니되며, 타인의 인터넷 안보 침해 활동을 분명이 알면서도 그에 대한 기술지원, 광고홍보, 지불정산 등에 협조를 해서는 아니된다.  제28조 인터넷 운영자는 국가안보와 범죄수사와 관련되는 공안기관, 국가안보기관의 법적 활동에 기술지원과 협조를 제공해야 한다.  제29조 국가는 인터넷 운영자 간에 인터넷 안보 정보의 수집, 분석, 통보 및 긴급대응 등 분야의 협력을 추진하여 인터넷 운영자의 안보 보장 능력을 강화하는 것을 지원한다.  관련 업계조직은 해당 업계의 인터넷 안보 규범과 협력 메커니즘을 구축완비하고 인터넷 안보 리스크에 대한 분석평가를 강화하고 정기적으로 회원에게 리스크 경고를 하고 회원의 인터넷 안보 리스크 대응을 지원하고 협조한다.  제30조 인터넷 안보 및 정보화부서와 유관부서가 인터넷안보 직무를 이행하는 중에서 획득한 정보는 인터넷안보 유지의 필요에만 사용해야 하며, 기타 용도에 사용해서는 아니된다.  제2절 핵심 정보 인프라의 운영 안전  제31조 국가는 공공통신과 정보서비스, 에너지, 교통, 수력, 금융, 공공서비스, 전자정무 등 중요한 업종과 분야, 그리고 일단 파괴되거나 기능상실 또는 데이터 누설로 인해 국가안보, 국가경제와 국민의 생활, 공공이익이 심각한 위해가 초래되는 기타의 핵심 정보인프라는 인터넷안보 등급보호제도의 기초상 중점보호를 실시한다. 핵심 정보인프라의 구체적 범위와 안보방법은 국무원이 제정한다.  국가는 핵심 정보인프라 이외의 인터넷 운영자가 자율적으로 핵심 정보인프라 보호체계에 참여하는 것을 권장한다.  제32조 국무원이 규정한 업무분공에 따라 핵심 정보인프라 안보업무를 담당한 부서는 본 업계, 본 분야의 핵심 정보인프라 안보계획을 작성 및 실행하고 핵심 정보인프라의 운영 안보 업무를 지도하고 감독한다.  제33조 핵심 정보 인프라의 구축은 업무의 안정적, 지속적 운영를 지원하는 성능을 보장해야 하며, 안보기술조치의 동시 계획, 동시 구축, 동시 사용을 보장해야 한다.  제34조 이 법 제21조 규정 이외에 핵심 정보 인프라 운영자는 다음 각 호의 안보 의무를 이행해야 한다.  (1) 안보관리 전문기구와 안보관리 담당자를 설치하고 그 담당자와 핵심 직무 담당직원에 대한 안보배경 심사를 실시해야 한다.  (2) 정기적으로 종업원에 대한 인터넷 안보 교육, 기술교육 및 기능평가를 실시해야 한다.  (3) 재해복구를 대비하여 중요한 시스템과 데이터베이스를 백업해야 한다.  (4) 인터넷 안보 사건 긴급대비책을 제정하고 정기적으로 시물레이션을 실시해야 한다.  (5) 법률, 행정법규에 규정한 기타 의무.  제35조 핵심 정보 인프라 운영자가 인터넷 제품, 서비스를 구매함에 있어 국가안보에 영향이 미칠 수 있는 경우에는 국가 인터넷안보 및 정보화부서가 국무원 유관부서와 공동으로 실시한 국가안보 심사에 통과되어야 한다.  제36조 핵심 정보인프라 운영자가 인터넷제품•서비스를 구매 시에는 규정에 따라 제공자와 안보계약을 체결함으로써 안보, 비밀보호 의무 및 책임을 명확히 약정해야 한다.  제37조 핵심 정보 인프라 운영자는 중화인민공화국 경내 운영 과정에서 수집 및 생성된 개인정보와 중요한 데이터를 마땅히 경내에 저장해야 한다. 업무의 수요로 인해 해외에 저장할 필요가 있는 경우에는 국가 인터넷안보 및 정보화부서가 국무원 유관부서와 공동으로 제정한 방법에 따라 안보평가를 받아야 한다. 법률, 행정법규에 별도의 규정이 있을 경우는 그 규정에 따른다.  제38조 핵심 정보 인프라 운영자는 스스로 또는 인터넷안보서비스기구에 의뢰하여 그 인터넷의 안보와 존재할 수 있는 리스크에 대한 검측 평가를 매년 1회 이상 실시해야 하며, 검측평가 상황과 개선조치를 핵심 정보인프라 안보 업무를 담당하는 유관부서에 보고해야 한다.  제39조 국가 인터넷안보 및 정보화부서는 유관부서를 조율하여 핵심 정보인프라에 대해 다음 각 호의 안보조치를 취해야 한다.  (1) 핵심 정보인프라의 안보 리스크에 대해 추출검사를 실시하고 개선조치를 제안하며 필요시에는 인터넷안보서비스기구에 의뢰하여 인터넷에 대한 안보 리스크 검측평가를 실시한다.  (2) 정기적으로 핵심 정보인프라 운영자를 동원하여 인터넷 안보 비상대응 시물레이션을 추진하고 인터넷안보 사건 대응능력과 협동 협조능력을 강화한다.  (3) 유관 부서, 핵심 정보 인프라 운영자 및 인터넷 안보 서비스기구, 유관 연구기관 등 지간의 인터넷 안보 정보 공유를 촉진시킨다.  (4) 인터넷 안보 사건의 긴급대응 및 인터넷 기능복구 등에 대해 기술지원을 제공하고 협조한다.  제4장 인터넷 정보 안전  제40조 인터넷 운영자는 그가 수집한 이용자 정보에 대해 엄격히 비밀에 붙여야 하며, 아울러 이용자 정보보호제도를 구축하고 완벽히 해야 한다.  제41조 인터넷 운영자는 개인정보를 수집하고 사용함에 있어 적법성, 정당성, 필요성의 원칙을 준수하고 수집과 사용규칙을 공개해야 하며, 정보 수집, 사용의 목적, 방식과 범위를 명시함과 아울러 수집 대상자의 동의를 득해야 한다.  인터넷 운영자는 그가 제공하는 서비스와 무관한 개인정보를 수집해서는 아니되며 법률, 행정법규의 규정과 양자간의 약정을 어기고 개인정보를 수집, 사용해서는 아니되며 법률, 행정법규의 규정과 이용자간의 약정에 따라 그가 보관한 개인정보를 관리해야 한다.  제42조 인터넷 운영자는 그가 수집한 개인정보를 유출, 변조, 훼손해서는 아니되며, 수집 대상자의 동의를 득하지 않고서는 타인에게 개인정보를 제공해서는 아니된다. 다만, 처리를 거쳐 특정 개인을 식별하기 어렵고 또한 원상복구가 불가능한 경우는 예외로 한다.  인터넷 운영자는 기술조치와 기타 필요한 조치를 취하여 그가 수집한 개인정보의 안전을 보장함으로써 정보의 유출, 훼손, 분실을 방지해야 하며, 개인정보의 유출, 훼손, 분실이 발생되거나 우려될 경우에는 즉시 구제조치를 취하고 지체없이 규정에 따라 이용자에게 고지하는 동시에 유관주관부서에 보고해야 한다.  제43조 개인이 인터넷 운영자가 법률, 행정법규의 규정 또는 양자간의 약정을 어기고 자신의 개인정보를 수집, 사용한 사실을 발견한 경우 인터넷 운영자에게 그 개인정보를 삭제하도록 요구할 권리가 있으며, 인터넷 운영자가 수집, 저장한 자신의 개인정보에 오류가 있음을 발견한 경우 인터넷 운영자에게 정정하도록 요구할 권리가 있다. 인터넷 운영자는 삭제 또는 정정의 조치를 취해야 한다.  제44조 그 어떠한 개인과 조직도 개인정보를 절취하거나 기타 불법적인 방식으로 획득해서는 아니되며 개인정보를 불법으로 매각하거나 타인에게 제공해서도 아니된다.  제45조 법에 의거하여 인터넷 안보 감독관리 직책을 담당하는 부서와 그 업무직원은 직무 이행 과정에서 알게된 개인정보, 프라이버시 및 상업비밀에 비밀을 유지해야 하며 유출, 매각하거나 불법으로 타인에게 제공해서는 아니된다.  제46조 그 어떠한 개인과 조직도 인터넷 사용행위에 대한 책임을 져야 하며, 사기, 범죄방법 전수, 금지물품이나 관제물품의 제작, 판매 등 불법 범죄활동을 실시하는 사이트, 통신그룹을 설립해서는 아니되며, 인터넷을 이용하여 사기, 금지물품이나 관제물품의 제작 또는 판매, 그리고 기타 불법 범죄행위를 실시하는 정보를 발표해서는 아니된다.  제47조 인터넷 운영자는 그 이용자가 발표하는 정보에 대한 관리를 강화해야 하며 법률, 행정법규에 의해 발표 또는 전송이 금지되는 정보를 발견한 경우 즉시 당해 정보의 전송을 중단시키고 삭제 등 처리조치를 취하여 정보의 확산을 막아야 하며 관련 기록을 보관하고 유관주관부서에 보고해야 한다.  제48조 어떠한 개인이나 조직도 발송한 전자정보, 제공한 응용소프트웨어는 악성 프로그램을 설치해서는 아니되며, 법률, 행정법규에 의해 발표 또는 전송이 금지되는 정보가 포함되어서는 아니된다.  전자정보 발송 서비스 제공자와 응용 소프트웨어 다운로드 서비스 제공자는 안보관리 의무를 이행해야 하며, 그 이용자가 전항에서 규정한 행위가 있는 것을 알고 있는 경우에는 서비스 제공을 중단하고 삭제 등 조치를 취하고 관련 기록을 보존해야 하며, 아울러 유관주관부서에 보고해야 한다.  제49조 인터넷 운영자는 인터넷 정보안전에 대한 신고, 제보 제도를 구축하고 신고,제보방식 등 정보를 공표하며 인터넷 정보안전 신고와 제보를 지체없이 접수 및 처리해야 한다.  인터넷 운영자는 인테냇안보 및 정보화부서와 유관부서가 법에 따라 실시하는 감독검사에 협조해야 한다.  제50조 국가 인터넷안보 및 정보화부서와 유관부서는 법에 따라 인터넷정보 감독관리 직무를 수행하고 법률, 행정법규에 의해 발표 또는 전송이 금지되는 정보를 발견한 경우 인터넷 운영자에게 전송을 중단시키고 삭제 등 처리조치를 취하고 관련 기록을 보관하도록 요구해야 한다. 상기 정보의 출처가 중환인민공화국 경외인 경우에는 기술조치 및 기타 필요한 조치를 취하여 전파를 차단하도록 유관기구에 통보해야 한다.  제5장 모니터링 조기경보 및 긴급조치  제51조 국가는 인터넷 안보 모니터링•조기경보 및 정보 통보제도를 구축한다. 국가 인터넷안보 및 정보화부서는 유관부서와 회동하여 인터넷 안보 정보의 수집, 분석 및 통보 업무를 강화하고 규정에 따라 인터넷 안보 모니터링 조기경보 정보를 통일적으로 발표한다.  제52조 핵심 정보인프라 안보 업무를 담당한 부서는 본 업계, 본 분야의 인터넷 안보 모니터링 조기경보 및 정보 통보제도를 구축완비해야 하며 규정에 따라 인터넷 안보 모니터링 조기경보 정보를 보고해야 한다.  제53조 국가 인터넷안보 및 정보화부서는 유관 부서와 회동하여 인터넷 안보 리스크평가와 긴급대응 업무기제를 구축하고 완벽히 하며, 인터넷 안보 사건 긴급대비책을 제정하며 정기적으로 시물레이션을 실시한다.  핵심 정보 인프라 안보 업무를 담당한 부서는 본 업계, 본 분야의 인터넷 안보 사건 긴급대비책을 제정하여 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.  제54조 인터넷 안보 사건이 발생하는 리스크가 증대된 경우 성급 이상 인민정부 유관부서는 규정한 권한, 절차에 따라, 아울러 인터넷안보 리스크의 특성과 초래 가능한 피해에 근거하여 다음 조치를 취해야 한다.  (1) 유관부서, 기구 및 인원에게 지체없이 관련 정보를 수집, 보고하고 인터넷 안보 사건의 리스크에 대한 모니터링을 강화하도록 요구한다.  (2) 유관부서, 기구 및 전문인력을 동원하여 인터넷 안보 사건 정보를 분석 및 평가하여 사건 발생 가능성, 영향범위 및 피해정도를 예측한다.  (3) 사회에 인터넷 안보 사건 리스크경보를 발표하고 피해를 모면하거나 줄일 수 있는 조치를 공개한다.  제55조 인터넷 안보 사건이 발생하는 경우에는 즉시 인터넷 안보 사건 긴급대비책을 가동하여 인터넷 안보 사건을 조사•평가하고 인터넷 운영자에게 기술조치 및 기타 필요한 조치를 취하여 잠재적인 안보 우환을 제거하고 피해의 확산을 방지하도록 요구해야 하며 지체없이 대중과 관련된 경고 정보를 사회에 발표해야 한다.  제56조 성급 이상 인민정부 유관부서가 인터넷 안보 감독관리 직무를 이행하는 과정에서 인터넷에 비교적 큰 안보리스크를 발생했거나 안보사건이 발생한 경우 규정된 권한과 절차에 따라 당해 인터넷 운영자의 법정대표자 또는 주요책임자와 면담을 진행할 수 있다. 인터넷 운영자는 요구에 따라 조치를 취하여 시정 정돈을 실시하여 우환을 제거해야 한다.  제57조 인터넷 안보 사건으로 인해 돌발사건 또는 안전생산사고가 발생한 경우 <중화인민공화국 돌발사건 긴급대응법>, <중화인민공화국 안전생산법> 등 관련 법률, 행정법규의 규정에 따라 처리해야 한다.  제58조 국가안보 및 사회공공질서의 유지와 중대한 돌발 사회안보사건 처리에 필요한 경우 국무원의 결정이나 비준을 득한 후 일부 지역에서 인터넷 통신 제한 등 임시조치를 취할 수 있다.  제6장 법률책임  제59조 인터넷 운영자가 이 법 제21조, 제25조에 규정한 인터넷 안보 의무를 이행하지 아니한 경우 유관주관부서가 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 제33조, 제34조, 제36조, 제38조에 규정한 인터넷 안보 의무를 이행하지 아니한 경우 유관 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.  제60조 이 법 제22조 1항, 2항, 제48조 1항의 규정을 어기고 다음 각 호의 어느 하나에 해당되는 행위를 행하였을 경우 유관주관부서가 시정을 명하고 경고를 주며; 시정을 거부하거나 인터넷 안보에 피해를 초래한 경우 5만위안 이상 50만위안 이하의 과태료를 부과하며, 직접 담당한 주관자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.  (1) 악성 프로그램을 설치한 경우  (2) 그 제품•서비스에 존재하는 안보결함 등 리스크는 지체없이 구제조치를 취하지 아니하거나 또는 규정에 따라 지체없이 이용자에게 고지함과 아울러 유관주관부서에 보고하지 아니한 경우  (3) 그 제품•서비스에 대한 안보 유지보수를 무단 중단한 경우.  제61조 인터넷 운영자가 이 법 제24조 1항의 규정을 어기고 이용자에게 진실한 신원정보의 제공하도록 요구하지 않았거나 진실한 신원정보를 제공하지 않은 이용자에게 관련 서비스를 제공한 경우 유관주관부서가 시정을 명하고; 시정을 거부하거나 사안이 심각한 경우 5만위안 이상 50만위안 이하의 과태료를 부과함과 더불어 유관 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.  제62조 이 법 제26조의 규정을 어기고 인터넷 안보인증, 검측, 리스크평가ㅏ 등 활동을 전개하거나, 또는 사회에 시스템 결함, 컴퓨터 바이러스, 인터넷 공격, 인터넷 침입 등 인터넷 안보정보를 발표한 경우 유관주관부서는 시정하도록 명령하고 경고를 주며, 시정을 거절하거나 사안이 심각한 경우 1만 위안 이상 10만 위안 이하의 과태료를 부과함과 아울러 유관주관부서는 당분간 영업 중지, 조업정지 정돈, 사이트 폐쇄, 관련 업무허가증이나 영업허가증 등기말소를 할 수 있으며, 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 5천위안 이상 5만 위안 이하의 과태료를 부과한다.  제63조 이 법 제27조의 규정을 어기고 인터넷 안보에 피해를 주는 활동에 종사하거나, 또는 인터넷 안보 위해활동에 전문 사용되는 프로그램, 수단을 제공하거나, 또는 타인의 인터넷 안보 위해활동에 기술적 지원, 광고, 지불결제 등의 협조를 제공하고 범죄 구성에는 이르지 아니한 경우 공안기관은 불법 소득을 몰수하고 5일 이하의 구속에 처하는 동시에 5만 위안 이상 50만 위안 이하의 과태료를 부과할 수 있으며, 사안이 심각한 경우 5일 이상 15일 이하의 구속을 처하는 동시에 10만 위안 이상 100만 위안 이하의 과태료를 부과할 수 있다.  관련 업체에 전항의 행위가 있는 경우 공안기관은 그 불법소득을 몰수하고 10만 위안 이상 100만 위안 이하의 벌금을 부과하며, 동시에 직접 담당하는 주관자와 기타 직적접 책임이 있는 자에게 전항의 규정에 따라 처벌을 가한다.  이 법 제27조의 규정을 어기고 치안관리 처벌을 받은 자는 5년 내에 인터넷 안보관리와 인터넷 운영 관건 일자리에 임해서는 아니되며, 형서처분을 받은 자는 종신토록 인터넷 안보관리와 인터넷 운영 관건 일자리에 임해서는 아니된다.  제64조 인터넷 운영자, 인터넷 제품이나 서비스 제공자가 이 법 제22조 3항, 제41조~제43조의 규정을 어기고 개인정보를 보호받을 권리를 침해한 경우 유관주관부서가 시정을 명하고 경위에 따라 경고, 불법소득 몰수, 불법소득의 1배 이상 10배 이하의 과태료 부과 등 처벌 중의 하나를 처하거나 병과할 수 있으며 불법소득이 없을 경우에는 100만위안 이하의 과태료를 부과하고 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다. 사안이 심각한 경우 업무의 일시 중단, 휴업정돈, 사이트 폐쇄, 관련 업무 허가증 또는 영업허가증 취소 처벌을 내릴 수 있다.  이 법 제44조의 규정을 어기고 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 100만위안 이하의 과태료를 부과한다.  제65조 핵심 정보 인프라 운영자가 이 법 제35조의 규정을 어기고 안보 심사를 거치지 않았거나 안보 심사를 통과하지 못한 인터넷 제품 또는 서비스를 사용한 경우 유관주관부서가 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.  제66조 핵심 정보 인프라 운영자가 이 법 제37조의 규정을 어기고 해외에 인터넷 데이터를 저장하거나 안보평가를 거치지 않고 해외 조직 또는 개인에게 인터넷 데이터를 제공한 경우 유관 주관부서가 시정을 명하고 경고를 주며 불법소득을 몰수하고 5만위안 이상 50만위안 이하의 과태료를 부과하며 이와 더불어 업무 일시 중단, 휴업정돈, 사이트 폐쇄, 관련 업무허가증 또는 영업허가증 취소 처벌을 내릴 수 있으며, 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.  제67조 이 법 제46조의 규정을 어기고 불법 범죄활동에 종사하는 사이트, 통인그룹를 설립하거나, 또는 인터넷을 이용하여 불법 범죄활동 관련 정보를 발표하였으나 범죄 구성에는 이르지 아니한 경우 공안기관은 5일 이하의 구속을 처하며, 동시에 1만 위안 이상 10만 위안 이하의 과태료를 부과한다. 사안이 심각한 경우에는 5일 이상 15일 이하의 구속을 처하는 동시에 5만 위안 이상 50만 위안 이하의 과태료를 부과하며, 불법 범죄활동에 종사하는 사이트, 통신그룹을 폐쇄한다.  업체에 전항의 행위가 있는 경우 공안기관은 10만 위안 이상 50만 위안 이하의 과태료를 주과하고 동시에 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 전항의 규정에 따라 처벌한다.  제68조 인터넷 운영자가 이 법 제47조의 규정을 어기고 법률, 행정법규에 의해 발표 또는 전송이 금지된 정보에 대해 전송 중단, 삭제 등 조치를 취하지 않고 관련 기록을 보관하지 아니한 경우 유관 주관부서가 시정을 명하고 경고를 주며 불법소득을 몰수한다. 시정을 거부하거나 사안이 심각한 경우 10만위안 이상 50만위안 이하의 과태료를 부과함과 더불어 업무 일시 중단, 휴업정돈, 사이트 폐쇄, 관련 업무허가증 또는 영업허가증 취소 처벌을 내릴 수 있으며, 직접 담당하는 주관자와 기타 직접적 책임이 있는 자에게 1만위안 이상 10만위안 이하의 과태료를 부과한다.  전자정보 발송 서비스 제공자, 응용 소프트웨어 다운로드 서비스 제공자가 이 법 제48조 2항에 규정한 안보 관리의무를 이행하지 아니하였을 경우 전 항의 규정에 따라 처벌한다.  제69조 인터넷 운영자가 이 법의 규정을 위반하고 다음 행위 중의 하나가 있는 경우 유관주관부서는 시정하도록 명하며, 시정을 거부하거나 사안이 심각한 경우 5만 위안 이상 50만 위안 이하의 벌금을 부과하고 직접 담당한 주관자와 기타 직접적 책임이 있는 자에게 1만 위안 이상 10만 위안 이하의 관태료를 부과한다.  (1) 법률, 행정법규가 발표 또는 전송을 금지하는 정보를 유관부서의 요구에 따라 전송 중지, 제거 등 처분 조치를 취하지 아니한 경우  (2) 유관부서가 법에 따라 실시하는 감독검사를 거부, 저애하는 경우  (3) 공안기관, 국가안보기관에 기술지원과 협조 제공을 거부하는 경우.  제70조 이 법 제12조 2항과 기타 법률, 행정법규에 의해 발표 또는 전송이 금지된 정보를 발표 또는 전송한 경우 관련 법률, 행정법규의 규정에 따라 처벌한다.  제71조 이 법에 규정한 인터넷 안보 불법 행위가 있는 경우 관련 법률, 행정법규의규정에 따라 신용보존서류에 기록하고 이를 공시한다.  제72조 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.  제73조 인터넷 안보 및 정보화부서와 유관부서가 이 법 제30조의 규정을 어기고 인터넷 안보 직무를 수행하는 과정에서 획득한 정보를 기타 용도에 사용한 경우 법에 다라 직접 담당한 주관자와 기타 직법적 책임있는 자를 처벌한다.  인터넷 안보 및 정보화부서 업무직원이 직무를 소홀히 하고 직권을 남용하거나 사리를 도모하는 부정행위를 행하였으나 범죄에 이르지 아니할 경우 법에 따라 처벌한다.  제74조 이 법의 규정을 어기고 타인에게 손해를 초래한 경우 법에 따라 민사상 책임을 진다.  이 법의 규정을 어기어 치안관리 위반행위를 구성한 경우 법에 따라 치안관리 처벌을 주며, 범죄를 저지른 경우에는 법에 따라 형사상 책임을 추궁한다.  제75조 경외 기구, 조직, 개인이 중화인민공화국의 핵심정보 인프라를 공격, 침입, 파괴 활동에 종사하여 심각한 결과를 초래한 경우 법에 따라 법적 책임을 추궁하며, 국무원 공안부서와 유관부서는 당해 기구, 조직, 개인에 대한 재산 동결 또는 기타 필요한 제재조치를 가할 있다.  제7장 부 칙  제76조 이 법에 사용한 용어의 의미는 다음과 같다.  (1) 인터넷라 함은 검퓨터 또는 기타 정보단말기 및 관련 설비로 구성되었고 일정한 규칙과 절차에 따라 정보를 수집, 저장, 전송, 교환, 처리하는 시스템을 지칭한다.  (2) 인터넷 안보라 함은 필요한 조치를 통하여 인터넷에 대한 공격, 침입, 교란, 파괴, 불법사용과 우발사고를 방비하여 인터넷의 안정적인 운영 상태를 유지시키고 인터넷 데이터의 완벽성, 비밀성, 사용가능성을 보장할 수 있는 능력을 지칭한다.  (3) 인터넷 운영자라 함은 인터넷의 소유자, 관리자 및 인터넷 서비스 제공자를 지칭한다.  (4) 인터넷 데이터라 함은 인터넷를 통해 수집, 저장, 전송, 처리되고 발생하는 각 종의 전자 데이터를 지칭한다.  (5) 개인정보라 함은 전자 또는 기타 방식으로 기록한, 단독으로 또는 기타 정보와 결합하여 자연인 개인의 신원을 식별할 수 있는 각종 정보를 지칭하며, 이에는 자연인의 성명, 출생년월일, 신분증번호, 개인의 생물인식정보, 주소, 전화번호 등이 포함되나 이에 국한되지는 아니한다.  제77조 국가비밀정보의 저장, 처리와 연관된 인터넷 운영 안보는 이 법의 규정을 준수해야 하는 것 외에 비밀유지 관련 법률, 행정법규의 규정도 준수해야 한다.  제78조 군사용 인터넷안보는 중앙군사위원회가 별도로 제정한다.  제79조 이 법은 2017년 6월 1일부터 시행한다. |  | **中华人民共和国网络安全法**  中华人民共和国主席令第五十三号  《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。  中华人民共和国主席 习近平  2016年11月7日  目 录  第一章 总 则  第二章 网络安全支持与促进  第三章 网络运行安全  第一节 一般规定  第二节 关键信息基础设施的运行安全  第四章 网络信息安全  第五章 监测预警与应急处置  第六章 法律责任  第七章 附 则  第一章 总 则  第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。  第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。  第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。  第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。  第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。  第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。  第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。  第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。  县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。  第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。  第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。  第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。  第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。  任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。  第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。  第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。  有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。  第二章 网络安全支持与促进  第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。  国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。  第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。  第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。  第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。  国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。  第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。  大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。  第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。  第三章 网络运行安全  第一节 一般规定  第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照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六个月；  （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。  第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。  网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。  网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。  第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。  第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。  国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。  第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。  第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。  第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。  第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。  第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。  有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。  第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。  第二节 关键信息基础设施的运行安全  第三十一条 国家对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、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。  国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。  第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。  第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。  第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：  （一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；  （二）定期对从业人员进行网络安全教育、技术培训和技能考核；  （三）对重要系统和数据库进行容灾备份；  （四）制定网络安全事件应急预案，并定期进行演练；  （五）法律、行政法规规定的其他义务。  第三十五条 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，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。  第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。  第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。  第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。  第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：  （一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；  （二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；  （三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；  （四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。  第四章 网络信息安全  第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。  第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。  网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。  第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。  网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。  第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。  第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。  第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。  第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。  第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。  第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。  电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。  第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。  网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。  第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。  第五章 监测预警与应急处置  第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。  第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。  第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。  负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。  网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。  第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：  （一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；  （二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；  （三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。  第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。  第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。  第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。  第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。  第六章 法律责任  第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。  关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。  第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：  （一）设置恶意程序的；  （二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；  （三）擅自终止为其产品、服务提供安全维护的。  第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。  第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。  第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。  单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。  违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。  第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。  违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。  第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。  第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。  第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。  单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。  第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。  电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。  第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：  （一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；  （二）拒绝、阻碍有关部门依法实施的监督检查的；  （三）拒不向公安机关、国家安全机关提供技术支持和协助的。  第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。  第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。  第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。  第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。  网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。  第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。  违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。  第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。  第七章 附 则  第七十六条 本法下列用语的含义：  （一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。  （二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。  （三）网络运营者，是指网络的所有者、管理者和网络服务提供者。  （四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。  （五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。  第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。  第七十八条 军事网络的安全保护，由中央军事委员会另行规定。  第七十九条 本法自2017年6月1日起施行。 |