中華人民共和国ネットワーク安全法

（2016 年 11 月 7 日第 12 期全国人民代表大会常務委員会第 24 回会議採択
2025 年 10 月 28 日第 14 期全国人民代表大会常務委員会第 18 回会議「『中華人民共和国ネットワーク安全法』の改正に関する決定」に基づき改正、2026 年 1 月 1 日施行）

目次

第 1 章　総則

第 1 条　ネットワーク安全を保障し、ネットワーク空間の主権並びに国家の安全及び社会公共の利益を維持し、公民、法人及びその他の組織の適法な権益を保護し、経済・社会の情報化の健全な発展を促進するため、本法を制定する。

第 2 条　中華人民共和国国内におけるネットワークの構築、運営、メンテナンス及び使用並びにネットワーク安全に係る監督管理に、本法を適用する。

第 3 条　ネットワーク安全業務では、中国共産党の指導を堅持し、総体的国家安全観を貫徹し、発展及び安全を統一的に計画し、ネットワーク強国建設を推進する。

第 4 条　国は、ネットワーク安全と情報化の発展の両立を堅持し、積極的な利用・科学的な発展・法による管理・安全の確保という方針に則って、ネットワークインフラの建設及び相互接続を推進し、ネットワーク技術のイノベーション及び応用を奨励し、ネットワーク安全人材の育成を支持し、ネットワーク安全保障体制を確立して健全化し、ネットワーク安全保護能力を向上させる。

第 5 条　国は、ネットワーク安全戦略を制定し、かつ、絶えず完全化し、ネットワーク安全の保障に係る基本要求及び主たる目標を明確にし、重点領域のネットワーク安全政策、作業任務及び措置を打ち出す。

第 6 条　国は、措置を講じて、中華人民共和国国内外に由来するネットワーク安全上のリスク及び脅威についてモニタリング、防御及び対処をし、重要な情報インフラが攻撃、

侵入、妨害及び破壊を受けることがないよう保護し、ネットワーク違法犯罪活動を法により処罰し、ネットワーク空間の安全及び秩序を維持する。

第 7 条　国は、信義誠実が守られ、健全でマナーをわきまえたオンライン行為を提唱し、社会主義核心的価値観の伝播を推し進め、措置を講じて社会全体のネットワーク安全に係る意識及び水準を向上させ、ネットワーク安全の促進に社会全体が共に参加する良好な環境を形成する。

第 8 条　国は、ネットワーク空間のガバナンス、ネットワーク技術の研究開発及び標準制定、ネットワーク違法犯罪の取締り等の面における国際交流及び協力を積極的に展開し、平和で安全かつ開放的・協力的なネットワーク空間の構築を推し進め、多国間の民主的で透明性あるネットワークガバナンス体制を確立する。

第 9 条　国のネット情報部門は、ネットワーク安全業務及び関連する監督管理業務の統一的な計画・調整に責任を負う。国務院の電信主管部門、公安部門及びその他の関係機関は、本法及び関係する法律・行政法規の規定により、各自の職責の範囲内において、ネットワーク安全に係る保護及び監督管理業務に責任を負う。

県級以上の地方人民政府の関係部門のネットワーク安全に係る保護及び監督管理の職責は、国の関係規定に従って確定する。

第 10 条　ネットワーク運営者は、経営及びサービス活動を展開する場合には、法律・行政法規を遵守し、社会公徳を尊重し、商業道徳を遵守し、誠実に信義を守り、ネットワーク安全保護義務を履行し、政府及び社会の監督を受け入れ、社会的責任を負わなければならない。

第 11 条　ネットワークを構築・運営し、又はネットワークを通じてサービスを提供する場合には、法律・行政法規の規定及び国家標準の強制的要求により、技術的措置及びその他の必要な措置を講じ、ネットワークの安全かつ安定的な運行を保障し、効果的にネットワーク安全インシデントに対応し、ネットワーク違法犯罪活動を予防し、ネットワークデータの完全性、機密性及び可用性を維持しなければならない。

第 12 条　ネットワーク関連の業界組織は、規約に従って、業界の自己規律性を強化し、ネットワーク安全行為規範を制定し、会員を指導してネットワーク安全保護を強化させ、ネットワーク安全保護水準を向上させ、業界の健全な発展を促進する。

第 13 条　国は、公民、法人及びその他の組織がネットワークを法により使用する権利を保護し、ネットワーク接続の普及を促進し、ネットワークサービスの水準を引き上げ、安全かつ便利なネットワークサービスを社会に提供し、ネットワーク情報の法による秩序立った自由な流通を保障する。

いかなる個人及び組織も、ネットワークを使用する場合には、憲法・法律を遵守し、公の秩序を遵守し、社会公徳を尊重しなければならず、ネットワーク安全に危害を及ぼしてはならず、国家の安全、栄誉及び利益に危害を及ぼし、国家政権の転覆・社会主義制度の打倒を扇動し、国家の分裂・国家統一の破壊を扇動し、テロリズム・過激主義を喧伝し、民族憎悪・民族差別を喧伝し、暴力・わいせつポルノ情報を流布し、虚偽の情報を捏造・流布して経済秩序及び社会秩序を攪乱し、並びに他人の名誉、プライバシー、知的財産権及びその他の適法な権益を侵害する等の活動に、ネットワークを利用して従事してはならない。

第 14 条　国は、未成年者の健全な成長に資するネットワーク製品及びサービスの研究開発

を支持し、ネットワークを利用して未成年者の心身の健康に危害を及ぼす活動に従事することを法により処罰し、未成年者のために安全かつ健全なネットワーク環境を提供する。

第 15 条　いずれの個人及び組織も、ネットワーク安全に危害を及ぼす行為について、ネット情報、電信、公安等の部門に通報する権利を有する。通報を受けた部門は、遅滞なく法により処理をしなければならず、当該部門の職責に属さないものについては、処理の権限を有する部門に遅滞なく移送しなければならない。

関係部門は、通報者の関連情報について秘密を保持し、通報者の適法な権益を保護しなければならない。

第 2 章　ネットワーク安全の支持及び促進

第 16 条　国は、ネットワーク安全の標準体系を確立及び完全化する。国務院の標準化行政主管部門及び国務院のその他の関係部門は、各自の職責に基づき、ネットワーク安全の管理並びにネットワーク製品・サービス及び運行の安全に関する国家標準・業界標準の制定を組織し、かつ、適時改訂する。

国は、企業、研究機構、高等教育機関及びネットワーク関連の業界組織がネットワーク安全に係る国家標準・業界標準の制定に関与することを支持する。

第 17 条　国務院及び省・自治区・直轄市人民政府は、統一的に計画し、投入を増やして、重点ネットワーク安全技術産業及びプロジェクトを支援し、ネットワーク安全技術の研究開発及び応用を支持し、安全で信頼性の高いネットワーク製品及びサービスを普及させ、ネットワーク技術の知的財産権を保護し、企業、研究機構及び高等教育機関等が国のネットワーク安全技術イノベーションプロジェクトに参加することを支持しなければならない。

第 18 条　国は、ネットワーク安全に係る社会化サービス体系の構築を推進し、関係企業・機構がネットワーク安全認証・検証及びリスク評価等の安全サービスを展開することを奨励する。

第 19 条　国は、ネットワークデータの安全保護及び利用技術の開発を奨励し、公共データ資源のオープン化を促進し、技術イノベーション及び経済・社会の発展を推し進める。

第 20 条　国は、人工知能の基礎理論の研究及びアルゴリズム等の重要技術の研究開発を支持し、トレーニングデータ資源、計算能力等のインフラ建設を推進し、AI 倫理規範を完全化し、リスクのモニタリング・評価及び安全監督管理を強化し、人工知能の応用及び健全な発展を促進する。

国は、ネットワーク安全に係る管理方式のイノベーションを支持し、人工知能等の新技術を活用して、ネットワーク安全保護水準を引き上げる。

第 21 条　各級人民政府及びその関係部門は、日常的なネットワーク安全宣伝教育を組織・展開し、かつ、関係単位がネットワーク安全宣伝教育業務を適切に行うよう指導及び督促しなければならない。

マスメディアは、対象を明確に打ち出し、社会に向けてネットワーク安全宣伝教育を行わなければならない。

第 22 条　国は、企業及び高等教育機関、職業学校等の教育研修機構がネットワーク安全関

連の教育及び研修を展開し、様々な方式を採用してネットワーク安全人材を育成し、ネットワーク安全人材の交流を促進することを支持する。

第 3 章　ネットワーク運行の安全

第 1 節　一般規定

第 23 条　国は、ネットワーク安全等級保護制度を実行する。ネットワーク運営者は、ネットワーク安全等級保護制度の要求に従い、次の各号に掲げる安全保護義務を履行して、ネットワークが妨害、破壊又は不正アクセスを受けることがないよう保障し、ネットワークデータが漏洩すること又は窃取・改ざんされることを防止しなければならない。

（一）　内部安全管理制度及び操作規程を制定し、ネットワーク安全責任者を確定し、ネットワーク安全保護責任を遂行する。

（二）　コンピュータウイルス及びサイバー攻撃、ネットワーク侵入等、ネットワーク安全に危害を及ぼす行為を予防する技術的措置を講ずる。

（三）　ネットワークの運行状態及びネットワーク安全インシデントをモニタリング及び記録する技術的措置を講じ、かつ、規定に従って、関連するウェブログを 6 か月以上保管する。

（四）　データ分類、重要データのバックアップ及び暗号化等の措置を講ずる。

（五）　法律・行政法規に定めるその他の義務

第 24 条　ネットワーク製品・サービスは、関連する国家標準の強制的要求に適合しなければならない。ネットワーク製品・サービスの提供者は、悪意のあるプログラムを組み込んではならず、そのネットワーク製品・サービスに安全上の欠陥、脆弱性等のリスクが存在することを発見した場合には、直ちに救済措置を講じ、規定に従って遅滞なくユーザーに告知し、かつ、関係主管部門に報告しなければならない。

ネットワーク製品・サービスの提供者は、その製品・サービスのためにセキュリティメンテナンスを継続的に提供しなければならず、所定の、又は当事者が約定した期限内に、セキュリティメンテナンスの提供を終了してはならない。

ネットワーク製品・サービスがユーザー情報の収集機能を有する場合には、その提供者は、これをユーザーに明示し、かつ、同意を取得しなければならず、ユーザーの個人情報に関わる場合には、本法及び関係する法律・行政法規の個人情報保護に関する規定も遵守しなければならない。

第 25 条　ネットワーク重要設備及びネットワーク安全専用製品は、関連する国家標準の強制的要求に従って、資格を具備する機構による安全認証に合格し、又は安全検証において要求に適合した後に限り、販売又は提供することができる。国のネット情報部門は、国務院の関係部門と共同して、ネットワーク重要設備及びネットワーク安全専用製品目録を制定及び公布し、かつ、安全認証及び安全検証の結果の相互承認を推し進め、重複認証・検証を回避する。

第 26 条　ネットワーク運営者は、ユーザーのためにネットワーク接続若しくはドメイン登録サービスをし、固定電話、移動電話等の加入手続をし、又はユーザーに情報発信、インスタントメッセージング等のサービスを提供する場合には、ユーザーとの合意締結又

は提供サービスの確認の際に、真実の身分情報を提供するようユーザーに要求しなければならない。ユーザーが真実の身分情報を提供しない場合には、ネットワーク運営者は、その者に関連サービスを提供してはならない。

国は、CTID（Cyber Trusted Identity）戦略を実施し、安全で手軽な電子身分認証技術の研究開発を支持し、異なる電子身分認証間の相互承認を推し進める。

第 27 条　ネットワーク運営者は、ネットワーク安全インシデント緊急時対応計画を制定し、システム脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入等の安全リスクに遅滞なく対処しなければならず、ネットワーク安全に危害を及ぼすインシデントが発生した場合には、直ちに緊急時対応計画を始動させ、相応の救済措置を講じ、かつ、規定に従って関係主管部門に報告する。

第 28 条　ネットワーク安全認証・検証、リスク評価等の活動を展開し、システム脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入等のネットワーク安全情報を社会に発信する場合には、国の関係規定を遵守しなければならない。

第 29 条　いかなる個人及び組織も、他人のネットワークに不法に侵入し、他人のネットワークの正常機能を妨害し、ネットワークデータを窃取する等、ネットワーク安全に危害を及ぼす活動に従事してはならず、ネットワークへの侵入、ネットワークの正常機能及び防護措置への妨害、ネットワークデータの窃取等、ネットワーク安全に危害を及ぼす活動への従事に専ら用いられるプログラム及びツールを提供してはならない。他人がネットワーク安全に危害を及ぼす活動に従事していることを明らかに知っている場合には、その者のために技術サポート、広告宣伝、支払決済等の幇助をしてはならない。

第 30 条　ネットワーク運営者は、法により国家の安全を維持し、及び犯罪を捜査するという公安機関・国家安全機関の活動のために、技術サポート及び協力を与えなければならない。

第 31 条　国は、ネットワーク安全情報の収集、分析、周知及び緊急時対処等の面においてネットワーク運営者間で協力が行われることを支持し、ネットワーク運営者の安全保障能力を向上させる。

関係する業界組織は、当該業界のネットワーク安全に係る保護規範及び連携の仕組みを確立して健全化し、ネットワーク安全リスクに対する分析評価を強化し、定期的に会員に対してリスク警告を行い、ネットワーク安全リスクへの会員の対応に支持及び協力をする。

第 32 条　ネット情報部門及び関係部門がネットワーク安全保護職責の履行中に取得した情報は、ネットワーク安全の維持に係る必要にのみ用いることができ、その他の用途に用いてはならない。

第 2 節　重要な情報インフラの運行の安全

第 33 条　国は、公共通信及び情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務等の重要な業界及び領域、並びにその他ひとたび破壊、機能喪失又はデータ漏洩に遭うと、国家の安全、国家経済・国民生活及び公共の利益に著しい危害を及ぼす可能性のある重要な情報インフラに対し、ネットワーク安全等級保護制度の基礎の上において、重点的な保護を実行する。重要な情報インフラの具体的な範囲及び安全保護

の方法については、国務院が制定する。

国は、重要な情報インフラ以外のネットワーク運営者が重要な情報インフラ保護体制に任意で加わることを奨励する。

第 34 条　国務院が定める職責分担に従い、重要な情報インフラの安全保護業務に責任を負う部門は、当該業界・当該領域の重要な情報インフラの安全計画をそれぞれ作成し、かつ、組織・実施し、重要な情報インフラの運行の安全保護業務を指導及び監督する。

第 35 条　重要な情報インフラを建設する場合には、それが業務の安定的かつ持続的な運行をサポートする性能を有するよう確保し、かつ、安全に係る技術的措置の同時計画・同時建設・同時使用を保証しなければならない。

第 36 条　本法第 23 条の規定のほか、重要な情報インフラの運営者は、次の各号に掲げる安全保護義務も履行しなければならない。

（一）　専門の安全管理機構及び安全管理責任者を置き、かつ、当該責任者及び重要部署の人員に対し安全背景審査を行う。

（二）　定期的に業務従事者に対してネットワーク安全教育、技術研修及び技能評価を行う。

（三）　重要なシステム及びデータベースに対して耐災害性バックアップを行う。

（四）　ネットワーク安全インシデント緊急時対応計画を制定し、かつ、定期的に訓練を行う。

（五）　法律・行政法規に定めるその他の義務

第 37 条　重要な情報インフラの運営者がネットワーク製品及びサービスを調達する場合において、国家の安全に影響する可能性があるときは、国のネット情報部門が国務院の関係部門と共同して組織する国家安全審査を通過しなければならない。

第 38 条　重要な情報インフラの運営者は、ネットワーク製品及びサービスを調達する場合には、規定に従って提供者と安全秘密保持合意を締結し、安全及び秘密保持に係る義務及び責任を明確にしなければならない。

第 39 条　重要な情報インフラの運営者が中華人民共和国国内の運営において収集及び生成した個人情報及び重要データは、国内において保存しなければならない。業務の必要のために、国外に提供する必要が確かにある場合には、国のネット情報部門が国務院の関係部門と共同して制定する方法に従い、安全評価を行わなければならない（法律・行政法規に別段の定めがある場合には、当該定めによる。）。

第 40 条　重要な情報インフラの運営者は、自ら又はネットワーク安全サービス機構に委託して、そのネットワークの安全性及び存在する可能性のあるリスクに対し、毎年少なくとも 1 回の検査・評価を行い、かつ、検査・評価の状況及び改善措置を、重要な情報インフラの安全保護業務に責任を負う関連部門に届け出なければならない。

第 41 条　国のネット情報部門は、関係部門を統一的に調整し、重要な情報インフラの安全保護について次の各号に掲げる措置を講じなければならない。

（一）重要な情報インフラの安全リスクに対して抽出検査を行い、改善措置を打ち出す。必要である場合には、ネットワーク安全サービス機構に委託して、ネットワークに存在する安全リスクに対し検査・評価を行わせることができる。

（二）　重要な情報インフラの運営者を定期的に組織してネットワーク安全緊急時訓練を行い、ネットワーク安全インシデントへの対応水準及び協働連携能力を向上さ

せる。

（三）　関係部門、重要な情報インフラの運営者及び関係研究機構、ネットワーク安全サービス機構等の間のネットワーク安全情報の共有を促進する。

（四）　ネットワーク安全インシデントの緊急時対処及びネットワーク機能の復旧等に対し、技術サポート及び協力を与える。

第 4 章　ネットワーク情報の安全

第 42 条　ネットワーク運営者は、自身が収集したユーザー情報を厳秘として保持し、かつ、ユーザー情報保護制度を確立して健全化しなければならない。

ネットワーク運営者は、個人情報を処理する場合には、本法及び「中華人民共和国民法典」、「中華人民共和国個人情報保護法」等の法律・行政法規の規定を遵守しなければならない。

第 43 条　ネットワーク運営者は、個人情報を収集・使用する場合には、適法・正当・必要の原則に則り、収集・使用規則を公開し、情報を収集・使用する目的、方式及び範囲を明示し、かつ、被収集者の同意を経なければならない。

ネットワーク運営者は、自身が提供するサービスと関係のない個人情報を収集してはならず、法律・行政法規の規定及び双方の約定に違反して個人情報を収集・使用してはならず、かつ、法律・行政法規の規定及びユーザーとの約定により、自身が保存する個人情報を処理しなければならない。

第 44 条　ネットワーク運営者は、自身が収集した個人情報を漏洩、改ざん及び毀損してはならず、被収集者の同意を経ていない場合には、個人情報を他人に提供してはならない。但し、処理を経て特定の個人を識別できなくなっており、かつ、復元不能であるものを除く。

ネットワーク運営者は、技術的措置及びその他の必要な措置を講じて、自身が収集した個人情報の安全を確保し、情報の漏洩・毀損・紛失を防止しなければならない。個人情報の漏洩・毀損・紛失の状況が発生し、又は発生する可能性がある場合には、直ちに救済措置を講じ、規定に従って遅滞なくユーザーに告知し、かつ、関係主管部門に報告しなければならない。

第 45 条　個人は、ネットワーク運営者が法律・行政法規の規定又は双方の約定に違反してその個人情報を収集・使用していることを発見した場合には、その個人情報を削除するようネットワーク運営者に要求する権利を有し、ネットワーク運営者が収集・保存する自身の個人情報に誤りのあることを発見した場合には、これを訂正するようネットワーク運営者に要求する権利を有する。ネットワーク運営者は、措置を講じてこれを削除又は訂正しなければならない。

第 46 条　いかなる個人及び組織も、個人情報を窃取し、又はその他の不法な方式にて取得してはならず、個人情報を不法に売却し、又は不法に他人へ提供してはならない。

第 47 条　法によりネットワーク安全監督管理の職責を担う部門及びその職員は、職責履行中に知った個人情報、プライバシー及び商業秘密を厳秘として保持しなければならず、漏洩、売却又は他人への不法な提供をしてはならない。

第 48 条　いずれの個人及び組織も、自身のネットワーク使用行為に責任を負わなければな

らず、詐欺の実施、犯罪方法の伝授、禁制品・規制品の作製又は販売等の違法犯罪活動に用いられるウェブサイト及び通信グループを立ち上げてはならず、詐欺の実施、禁制品・規制品の作製又は販売及びその他の違法犯罪活動に関わる情報を、ネットワークを利用して発信してはならない。

第 49 条　ネットワーク運営者は、そのユーザーが発信する情報に対する管理を強化しなければならず、法律・行政法規により発信又は伝送が禁止されている情報を発見した場合には、直ちに当該情報の伝送を停止し、消去等の対処措置を講じて、情報の拡散を防止し、関係記録を保存し、かつ、関係主管部門に報告しなければならない。

第 50 条　いずれの個人及び組織が送信する電子情報及び提供するアプリケーションソフトウェアも、悪意のあるプログラムを組み込んではならず、法律・行政法規により発信又は伝送が禁止されている情報を含んでいてはならない。

電子情報の送信サービス提供者及びアプリケーションソフトウェアのダウンロードサービス提供者は、安全管理義務を履行しなければならず、そのユーザーに前項に定める行為があることを知った場合には、サービスの提供を停止し、消去等の対処措置を講じ、関係記録を保存し、かつ、関係主管部門に報告しなければならない。

第 51 条　ネットワーク運営者は、ネットワーク情報の安全に係る苦情申立・通報制度を確立し、苦情申立・通報の方式等の情報を公布し、ネットワーク情報の安全に関する苦情申立及び通報を遅滞なく受理し、かつ、処理しなければならない。

ネットワーク運営者は、ネット情報部門及び関係部門が法により実施する監督検査に対し、協力をしなければならない。

第 52 条　国のネット情報部門及び関係部門は、ネットワーク情報安全監督管理の職責を法により履行し、法律・行政法規により発信又は伝送が禁止されている情報を発見した場合には、伝送の停止、消去等対処措置の採用及び関係記録の保存をネットワーク運営者に要求しなければならず、中華人民共和国国外に由来する上述の情報に対しては、技術的措置及びその他の必要な措置を講じて伝播を遮断するよう関係機構に通知しなければならない。

第 5 章　モニタリング・早期警戒及び緊急時対処

第 53 条　国は、ネットワーク安全に係るモニタリング・早期警戒及び情報周知制度を確立する。国のネット情報部門は、関係部門を統一的に調整してネットワーク安全情報の収集、分析及び周知業務を強化させ、ネットワーク安全モニタリング・早期警戒情報を規定に従い統一的に発信しなければならない。

第 54 条　重要な情報インフラの安全保護業務に責任を負う部門は、当該業界・当該領域のネットワーク安全に係るモニタリング・早期警戒及び情報周知制度を確立して健全化し、かつ、規定に従い、ネットワーク安全モニタリング・早期警戒情報を届け出なければならない。

第 55 条　国のネット情報部門は、関係部門を調整して、ネットワーク安全リスクの評価及び緊急時対応業務の仕組みを確立して健全化し、ネットワーク安全インシデント緊急時対応計画を制定し、かつ、定期的に訓練を組織する。

重要な情報インフラの安全保護業務に責任を負う部門は、当該業界・当該領域のネッ

トワーク安全インシデント緊急時対応計画を制定し、かつ、定期的に訓練を組織しなければならない。

ネットワーク安全インシデント緊急時対応計画では、インシデント発生後の危害の程度、影響範囲等の要素に従いネットワーク安全インシデントに対して分級を行い、かつ、相応の緊急時対処措置を定めなければならない。

第 56 条　ネットワーク安全インシデント発生のリスクが増大した場合には、省級以上の人民政府の関係部門は、規定された権限及び手続に従って、かつ、ネットワーク安全リスクの特徴及びもたらされる可能性のある危害に基づき、次の各号に掲げる措置を講じなければならない。

（一）　関係情報を遅滞なく収集及び報告するよう関係部門、機構及び人員に要求し、ネットワーク安全リスクに対するモニタリングを強化する。

（二）　関係部門、機構及び専門家を組織して、ネットワーク安全リスク情報に対し分析評価を行わせ、インシデント発生の可能性、影響範囲及び危害の程度を予測する。

（三）　社会に対してネットワーク安全のリスクアラートを発令し、危害の回避・軽減措置を発信する。

第 57 条　ネットワーク安全インシデントが発生した場合には、直ちにネットワーク安全インシデント緊急時対応計画を始動させ、ネットワーク安全インシデントに対して調査及び評価を行って、ネットワーク運営者に対し、技術的措置及びその他の必要な措置を講じて安全上の潜在的リスクを除去し危害の拡大を防止するよう要求し、かつ、公衆と関係のある警戒情報を遅滞なく社会に対して発信しなければならない。

第 58 条　省級以上の人民政府の関係部門は、ネットワーク安全監督管理の職責履行中に、ネットワークに比較的大きい安全リスクが存在すること、又は安全インシデントが発生したことを発見した場合には、規定された権限及び手続に従って、当該ネットワークの運営者の法定代表者又は主要責任者に対して約談を行うことができる。ネットワーク運営者は、要求に従って措置を講じ、改善を行い、潜在的リスクを除去しなければならない。

第 59 条　ネットワーク安全インシデントに起因して、突発事件又は生産安全事故が発生した場合には、「中華人民共和国突発事件対応法」、「中華人民共和国安全生産法」等の関係する法律・行政法規の規定により対処しなければならない。

第 60 条　国家の安全及び社会公共の秩序を維持し、重大な突発的社会安全事件に対処する上での必要のために、国務院の決定又は承認を経た場合には、特定の区域において、ネットワーク通信に対し、制限等の暫定措置を講ずることができる。

第 6 章　法的責任

第 61 条　ネットワーク運営者が本法第 23 条又は第 27 条に定めるネットワーク安全保護義務を履行しない場合には、関係主管部門が是正を命じ、警告を行うものとし、1 万元以上 5 万元以下の過料を科すことができる。是正を拒絶し、又はネットワーク安全に危害を及ぼす等の結果を招いた場合には、5 万元以上 50 万元以下の過料を科し、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料を科す。

重要な情報インフラの運営者が本法第 35 条、第 36 条、第 38 条又は第 40 条に定める

ネットワーク安全保護義務を履行しない場合には、関係主管部門が是正を命じ、警告を行うものとし、5 万元以上 10 万元以下の過料を科すことができる。是正を拒絶し、又はネットワーク安全に危害を及ぼす等の結果を招いた場合には、10 万元以上 100 万元以下の過料を科し、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料を科す。

前二項の行為があって、大量のデータ漏洩、重要な情報インフラの部分的機能喪失等、ネットワーク安全に著しく危害を及ぼす結果をもたらした場合には、関係主管部門が 50 万元以上 200 万元以下の過料を科し、直接責任を負う主管者及びその他の直接責任者に対して 5 万元以上 20 万元以下の過料を科す。重要な情報インフラの主要機能喪失等、ネットワーク安全に特に著しく危害を及ぼす結果をもたらした場合には、200 万元以上 1000 万元以下の過料を科し、直接責任を負う主管者及びその他の直接責任者に対して 20 万元以上 100 万元以下の過料を科す。

第 62 条　本法第 24 条第 1 項、第 2 項及び第 50 条第 1 項の規定に違反し、次の各号に掲げる行為のいずれかがある場合には、関係主管部門が是正を命じ、警告を行う。是正を拒絶し、又はネットワーク安全に危害を及ぼす等の結果を招いた場合には、5 万元以上 50 万元以下の過料を科し、直接責任を負う主管者に対して 1 万元以上 10 万元以下の過料を科す。

（一）　悪意のあるプログラムを組み込んだとき。

（二）　その製品・サービスに存在する安全上の欠陥、脆弱性等のリスクに対して直ちに救済措置を講じず、又はユーザーへの告知及び関係主管部門への報告を規定どおりに遅滞なくしなかったとき。

（三）　その製品・サービス向けのセキュリティメンテナンスの提供を断りなく終了したとき。

前項第 1 号又は第 2 号の行為があって、本法第 61 条第 3 項に定める結果をもたらした場合には、当該項の規定により処罰する。

第 63 条　本法第 25 条の規定に違反して、安全認証・安全検証を経ておらず、又は安全認証で不合格若しくは安全検証で要求不適合となったネットワーク重要設備及びネットワーク安全専用製品を販売又は提供した場合には、関係主管部門が販売又は提供の停止を命じ、警告を行い、違法所得を没収する。違法所得がなく、又は違法所得が 10 万元未満である場合には、2 万元以上 10 万元以下の過料を併科し、違法所得が 10 万元以上である場合には、違法所得の相当額以上 5 倍以下の過料を併科する。情状が重大である場合には、関連業務の一時停止、営業停止・整理、関連業務許可証の取消し又は営業許可証の取消しを併せて命じることができる。法律・行政法規に別段の定めがある場合には、当該定めによる。

第 64 条　ネットワーク運営者が本法第 26 条第 1 項の規定に違反して、真実の身分情報の提供をユーザーに要求せず、又は真実の身分情報を提供していないユーザーに対して関連サービスを提供した場合には、関係主管部門が是正を命じる。是正を拒絶し、又は情状が重大である場合には、5 万元以上 50 万元以下の過料を科すものとし、関連業務の一時停止、営業停止・整理、ウェブサイト若しくはアプリケーションプログラムの閉鎖、又は関連業務許可証の取消し若しくは営業許可証の取消しを併せて命じることができ、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料

を科す。

第 65 条　本法第 28 条の規定に違反して、ネットワーク安全認証・検証、リスク評価等の活動を展開し、又はシステム脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入等のネットワーク安全情報を社会に発信した場合には、関係主管部門が是正を命じ、警告を行うものとし、1 万元以上 10 万元以下の過料を科すことができる。是正を拒絶し、又は情状が重大である場合には、10 万元以上 100 万元以下の過料を科すものとし、関連業務の一時停止、営業停止・整理、ウェブサイト若しくはアプリケーションプログラムの閉鎖、又は関連業務許可証の取消し若しくは営業許可証の取消しを併せて命じることができ、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料を科す。

前項の行為があって、本法第 61 条第 3 項に定める結果をもたらした場合には、当該項の規定により処罰する。

第 66 条　本法第 29 条の規定に違反して、ネットワーク安全に危害を及ぼす活動に従事し、若しくはネットワーク安全に危害を及ぼす活動への従事に専ら用いられるプログラム・ツールを提供し、又はネットワーク安全に危害を及ぼす活動に従事する他人のために技術サポート、広告宣伝、支払決済等の幇助をした場合で、なお犯罪を構成しないものについては、公安機関が違法所得を没収し、5 日以下の拘留に処すものとし、5 万元以上 50 万元以下の過料を併科することができる。情状が比較的重大である場合には、5 日以上 15 日以下の拘留に処すものとし、10 万元以上 100 万元以下の過料を併科することができる。

単位に前項の行為がある場合には、公安機関が違法所得を没収し、10 万元以上 100 万元以下の過料を科し、かつ、直接責任を負う主管者及びその他の直接責任者に対しては、前項の規定により処罰する。

本法第 29 条の規定に違反して、治安管理処罰を受けた人員は、ネットワーク安全管理及びネットワーク運営に係る重要部署の業務に 5 年間従事してはならず、刑事処罰を受けた人員は、ネットワーク安全管理及びネットワーク運営に係る重要部署の業務に生涯従事してはならない。

第 67 条　重要な情報インフラの運営者が本法第 37 条の規定に違反して、安全審査を経ておらず、又は安全審査を通過していないネットワーク製品又はサービスを使用した場合には、関係主管部門が、期限を定めた是正、使用の停止及び国家の安全に対する影響の除去を命じ、調達金額の相当額以上 10 倍以下の過料を科し、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料を科す。

第 68 条　本法第 48 条の規定に違反して、違法犯罪活動の実施に用いられるウェブサイト若しくは通信グループを立ち上げ、又は違法犯罪活動の実施に関わる情報をネットワークを利用して発信した場合で、なお犯罪を構成しないものについては、公安機関が 5 日以下の拘留に処すものとし、1 万元以上 10 万元以下の過料を併科することができる。情状が比較的重大である場合には、5 日以上 15 日以下の拘留に処すものとし、5 万元以上 50 万元以下の過料を併科することができる。違法犯罪活動の実施に用いられるウェブサイト及び通信グループは、閉鎖する。

単位に前項の行為がある場合には、公安機関が 10 万元以上 50 万元以下の過料を科し、かつ、直接責任を負う主管者及びその他の直接責任者に対しては、前項の規定により処

罰する。

第 69 条　ネットワーク運営者が本法第 49 条の規定に違反し、法律・行政法規により発信若しくは伝送が禁止されている情報について、伝送の停止、消去等対処措置の採用、関係記録の保存若しくは関係主管部門への報告をしなかった場合、又は本法第 52 条の規定に違反し、法律・行政法規により発信若しくは伝送が禁止されている情報について、伝送の停止、消去等対処措置の採用若しくは関係記録の保存を関係部門の要求どおりにしなかった場合には、関係主管部門が是正を命じ、警告を行い、周知をするものとし、5 万元以上 50 万元以下の過料を科すことができる。是正を拒絶し、又は情状が重大である場合には、50 万元以上 200 万元以下の過料を科すものとし、関連業務の一時停止、営業停止・整理、ウェブサイト若しくはアプリケーションプログラムの閉鎖、又は関連業務許可証の取消し若しくは営業許可証の取消しを併せて命じることができ、直接責任を負う主管者及びその他の直接責任者に対して 5 万元以上 20 万元以下の過料を科す。

前項の行為があって、特に重大な影響又は特に重大な結果をもたらした場合には、関係主管部門が 200 万元以上 1000 万元以下の過料を科し、関連業務の一時停止、営業停止・整理、ウェブサイト若しくはアプリケーションプログラムの閉鎖、又は関連業務許可証の取消し若しくは営業許可証の取消しを命じ、直接責任を負う主管者及びその他の直接責任者に対して 20 万元以上 100 万元以下の過料を科す。

電子情報の送信サービス提供者及びアプリケーションソフトウェアのダウンロードサービス提供者が、本法第 50 条第 2 項に定める安全管理義務を履行しない場合には、前二項の規定により処罰する。

第 70 条　ネットワーク運営者が本法の規定に違反し、次の各号に掲げる行為のいずれかがある場合には、関係主管部門が是正を命じる。是正を拒絶し、又は情状が重大である場合には、5 万元以上 50 万元以下の過料を科し、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料を科す。

（一）　関係部門が法により実施する監督検査を拒絶し、又は妨げたとき。

（二）　公安機関・国家安全機関に技術サポート及び協力を与えること拒絶したとき。

第 71 条　次の各号に掲げる行為のいずれかがある場合には、関係する法律・行政法規の規定により処理・処罰する。

（一）　本法第 13 条第 2 項及びその他の法律・行政法規により発信又は伝送が禁止されている情報を発信又は伝送したとき。

（二）　本法第 24 条第 3 項又は第 43 条ないし第 45 条の規定に違反して、個人情報に係る権益を侵害したとき。

（三）　本法第 39 条の規定に違反して、重要な情報インフラの運営者が個人情報及び重要データを国外において保存し、又は個人情報及び重要データを国外に提供したとき。

本法第 46 条の規定に違反して、個人情報を窃取し、若しくはその他の不法な方式にて取得し、又は不法に売却し、若しくは不法に他人へ提供した場合で、なお犯罪を構成しないものについては、関係する法律・行政法規の規定により公安機関が処罰する。

第 72 条　本法に定める違法行為があった場合には、関係する法律・行政法規の規定により信用档案に記し、かつ、これを公示する。

第 73 条　本法の規定に違反しているが、「中華人民共和国行政処罰法」に定める、軽きに従

って処罰し、処罰を減軽し、又は処罰をしない事由があるものについては、当該定めにより、軽きに従って処罰し、処罰を減軽し、又は処罰をしない。

第 74 条　国家機関政務ネットワークの運営者が本法に定めるネットワーク安全保護義務を履行しない場合には、その上級機関又は関係機関が是正を命じる。直接責任を負う主管者及びその他の直接責任者に対しては、法によりこれを処分する。

第 75 条　ネット情報部門及び関係部門が本法第 32 条の規定に違反し、ネットワーク安全保護職責の履行中に取得した情報をその他の用途に用いた場合には、直接責任を負う主管者及びその他の直接責任者に対し、法によりこれを処分する。

ネット情報部門及び関係部門の職員が職務を懈怠し、職権を濫用し、又は私利を図って不正行為をした場合で、なお犯罪を構成しないものについては、法によりこれを処分する。

第 76 条　本法の規定に違反し、他人に損害をもたらした場合には、法により民事責任を負う。

本法の規定に違反し、治安管理違反行為を構成する場合には、法により治安管理処罰をする。犯罪を構成する場合には、法により刑事責任を追及する。

第 77 条　国外の機構・組織・個人が中華人民共和国のネットワーク安全に危害を及ぼす活動に従事した場合には、法により法的責任を追及する。重大な結果がもたらされた場合には、国務院の公安部門及び関係部門は、当該機構・組織・個人に対し財産凍結又はその他の必要な制裁措置を講ずる旨を併せて決定することができる。

第 7 章　附則

第 78 条　本法において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（一）　ネットワークとは、コンピュータ又はその他の情報端末及び関連設備によって構成される、一定のルール及びプログラムに従って、情報に対し収集、保存、伝送、交換及び処理を行うシステムをいう。

（二）　ネットワーク安全とは、必要な措置を講じて、ネットワークに対する攻撃、侵入、妨害、破壊及び不法使用並びに不測の事故を予防することにより、ネットワークを安定的で信頼性の高い運行状態にさせ、及びネットワークデータの完全性・機密性・可用性を保障する能力をいう。

（三）　ネットワーク運営者とは、ネットワークの所有者、管理者及びネットワークサービス提供者をいう。

（四）　ネットワークデータとは、ネットワークを通じて収集、保存、伝送、処理及び生成される各種の電子データをいう。

（五）　個人情報とは、電子的又はその他の方式により記録された、自然人個人の身分を単独で、又はその他の情報と結合して識別することができる各種の情報をいい、自然人の氏名、生年月日、身分証番号、個人の生体識別情報、住所、電話番号等を含むが、これらに限られない。

第 79 条　国家秘密に関わる情報を保存・処理するネットワークの運行の安全の保護にあたっては、本法を遵守すべきほか、秘密保持に係る法律・行政法規の規定も遵守しなければならない。

第 80 条　軍事ネットワークの安全保護については、中央軍事委員会が別途定める。
第 81 条　本法は、2017 年 6 月 1 日から施行する。

（法令原文名称：中华人民共和国网络安全法）