得伟君尚TMT行业法律研究丛书

网络安全法合规操作指引

万方　余凯　著　　顾问　蔡学恩

COMPLIANCE GUIDANCE
FOR CYBERSECURITY LAW

WUHAN UNIVERSITY PRESS
武汉大学出版社

得伟君尚TMT行业法律研究丛书

网络安全法合规操作指引

万方　余凯　著　　顾问　蔡学恩

COMPLIANCE GUIDANCE
FOR CYBERSECURITY LAW

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

网络安全法合规操作指引/万方,余凯著.—武汉:武汉大学出版社,2019.9

得伟君尚 TMT 行业法律研究丛书

ISBN 978-7-307-21073-8

Ⅰ.网… Ⅱ.①万… ②余… Ⅲ.计算机网络—科学技术管理法规—基本知识—中国 Ⅳ.D922.174

中国版本图书馆 CIP 数据核字(2019)第 155769 号

责任编辑:陈 帆 责任校对:汪欣怡 整体设计:马 佳

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮箱:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:武汉中科兴业印务有限公司

开本:720×1000 1/16 印张:14.25 字数:203 千字 插页:2

版次:2019 年 9 月第 1 版 2019 年 9 月第 1 次印刷

ISBN 978-7-307-21073-8 定价:43.00 元

作者简介

万方

湖北得伟君尚（湖北自贸区武汉片区）律师事务所执行主任、TMT事业部主任、中世律所联盟TMT行业法律研究中心主任、中国地质大学（武汉）法律硕士教育中心兼职指导导师。毕业于武汉大学，获得法律硕士学位和经济学学士（电子商务方向）学位。

曾任武汉斗鱼TV法务经理、广州荔枝FM法务总监，曾代表公司处理多起与腾讯、阿里巴巴、华多网络、优酷等公司的大型商务谈判，并作为代理人处理与上述公司的知识产权、不正当竞争、合同等纠纷，也处理过多起涉计算机网络和信息数据方面的犯罪案件。在网络安全合规、知识产权、公司治理、争议解决等方面具有丰富的经验。

邮箱：wanfang@tmt-lawyer.com

余凯

湖北得伟君尚（湖北自贸区武汉片区）律师事务所律师、TMT事业部合伙人、专利代理人。毕业于华中科技大学和中国社会科学院，拥有工学学士（热能与动力工程）学位和法律硕士（知识产权方向）学位。

曾执业于北京市金杜律师事务所，为华为、卡西欧、美国迪尔、迈图新材料、意大利比亚乔、CNTV等众多知名企业提供法律服务。在知识产权、商业秘密、不正当竞争、反垄断等各类争议解决领域有丰富的实践经验。

前　言

在“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”的背景下，《中华人民共和国网络安全法》（以下简称《网络安全法》）颁布施行。自《网络安全法》施行以来，立法机关、行政主管部门和专家学者对其都有诸多系统详尽的解读，为了能够在理论认知外帮助网络安全责任主体落实网络安全合规责任，我们编写了本操作指引。

作为法律实务工作者，在编写这本操作指引时，我们的初衷是为网络安全合规的具体落地探索一个可作为参考的操作方案。因此读者在阅读时可以发现，除了必要的法律法规解读外，这本操作指引中主要内容集中在网络安全尽职调查类目及实用表格清单上。

具体来说，本操作指引共有五个章节及附录，整体上又可以分为四个部分。

第一章到第三章主要是对《网络安全法》的解读，一方面系统解读了《网络安全法》中关键信息基础设施、个人信息保护、数据出境安全评估、网络产品和服务安全审查、网络安全等级保护制度等主要内容；另一方面为了突出重点，我们提炼出《网络安全法》合规的十大核心责任。

第四章是本操作指引的核心部分和特色内容。我们按照《网络安全法》及配套法规的要求整理了包括4大项99小项的网络安全合规尽职调查清单。除此之外，我们还整理出网络安全合规所需要的常用文件和表

格，包括 10 份制度文件和 42 份示例表格，这些文件和表格可以满足不同主体网络安全合规的基本需要。

第五章是比较典型的《网络安全法》相关案例及评析，选取的这些处罚案例涵盖了机关事业单位、高等院校、互联网企业、跨国企业、网络用户等各类主体，涉及的违法行为也涵盖了实名制、安全等级保护制度、个人信息保护、高危漏洞等各类行为，具有比较广泛的示例意义和参考价值。

附录是规范性法律文件的汇编，包括网络安全领域的相关法律、行政法规、部门规章、司法解释、规范性文件和相关国家标准及行业标准，比较全面地呈现了网络安全领域的法规现状，可以作为读者延伸阅读的索引。

综上，我们希望这本操作指引可以为各单位的网络安全负责人和广大的网络安全管理人员在网络安全合规工作上提供帮助，但由于时间和能力有限，我们的探索与尝试也存在讹误与失当之处，在此恳请各位读者不吝指正！

适用对象

《网络安全法》于2017年6月1日正式施行，是我国网络安全领域的基础性法律，是国家安全领域的一部重要性法律。它的颁布施行，对于落实总体国家安全观，维护国家网络空间主权、安全和发展利益具有十分重要的意义。

根据该法第2条及第31条之规定，所有涉网①主体都是其规制对象，尤其是政府、金融、公共通信、能源、交通、水利、教育、医疗卫生、社会保险、环境保护、公用事业、国防科工、电子商务、电子政务、食品药品等被划入关键信息基础设施(CII)行列的主体，需面对更高标准的网络安全合规要求。

本操作指引，包含了《网络安全法》的核心内容解读、十大核心法律责任梳理、典型案例评析、法律法规汇编，同时提供了网络安全合规体系架构、尽职调查清单及常用文件与表格，能够满足前述主体网络安全合规常规需求，相关单位负责人和网络安全管理人员可以参照本操作指引并结合本单位的实际情况履行网络安全法律义务。

① 《网络安全法》第76条第1款：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。

目　录

第一章 《网络安全法》的立法背景和意义

2016年11月7日，十二届全国人大常委会经表决高票通过了《网络安全法》，该法已于2017年6月1日起正式施行。作为我国的网络安全基本法，《网络安全法》是网络安全领域“依法治国”的重要体现，对保障我国网络安全有着重大意义。

（一）立法背景：网络安全已经成为关系国家安全和发展，关系广大人民群众切身利益的重大问题

在信息化时代，网络已经深刻地融入经济、社会、生活的各个方面，网络安全威胁也随之向经济社会的各个层面渗透，网络安全的重要性不断提高。

一方面，党的十八大以来，以习近平同志为核心的党中央从总体国家安全观出发，对加强国家网络安全工作作出了重要的部署，对加强网络安全法治建设提出了明确的要求，制定《网络安全法》是适应我们国家网络安全工作新形势、新任务，落实中央决策部署，保障网络安全和发展利益的重大举措，是落实国家总体安全观的重要举措。

另一方面，中国是网络大国，也是面临网络安全威胁最严重的国家之一，因此迫切需要建立和完善网络安全的法律制度，提高全社会的网络安全意识和网络安全保障水平，使我们的网络更加安全，更加开放，更加便利，也更加充满活力。

在这样的形势下，制定《网络安全法》是维护国家广大人民群众切身利益的需要，是维护网络安全的客观需要，是落实国家总体安全观的

重要举措。

(二)立法意义：肇基和里程碑

《网络安全法》的出台具有里程碑式的意义。它是全面落实党的十八大和十八届三中、四中、五中、六中全会相关决策部署的重大举措，是我国第一部网络安全的专门性综合性立法，提出了应对网络安全挑战这一全球性问题的中国方案。此次立法进程的迅速推进，显示了党和国家对网络安全问题的高度重视，是我国网络安全法治建设的一个重大战略契机。网络安全有法可依，信息安全行业将由合规性驱动过渡到合规性和强制性驱动并重。《网络安全法》对于确立国家网络安全基本管理制度的意义，具体表现为六个方面：一是服务于国家网络安全战略和网络强国战略；二是助力网络空间治理，护航“互联网+”；三是构建我国首部网络空间管辖基本法；四是提供维护国家网络主权的法律依据；五是有利于在网络空间领域贯彻落实依法治国精神；六是为网络参与者提供普遍法律准则和依据。

《网络安全法》的出台是为了保障网络安全，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，促进社会信息化的健康发展。其颁布，可谓是应时而生、因势而起，其影响也必将是深远的。

第二章 《网络安全法》重要法律制度解读

第一节 《网络安全法》下的企业责任

作为我国的网络安全基本法，《网络安全法》在“没有网络安全就没有国家安全，没有信息化就没有现代化”的强音下颁布实施，是网络安全领域“依法治国”的重要体现，对保障我国网络安全有着重大意义。

《网络安全法》全文共 7 章 79 条，包括总则、网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置、法律责任以及附则。其中第二章网络安全支持与促进和第五章监测预警与应急处置主要涉及国家机关的法定权责，而对于企业的责任和义务则集中规定在第三章和第四章，从第 21 条到第 50 条的 30 个法条中，经过梳理，可以将其分为网络运行安全保护、个人信息保护、协助和报告三类责任，下文将逐一进行解读分析。

一、网络运行安全保护责任

网络运行安全保护是企业在《网络安全法》下的核心责任，在《网络安全法》的第三章作了集中规定，并且根据主体的差异，对一般性的主体作出了一般规定，而对关键信息基础设施的运营者作出了特别规定。

(一)一般规定

对于一般性主体的网络运行安全保护责任，可以分为以下六个方面：

1. 安全等级保护制度

《网络安全法》第21条对于网络运营者应落实网络安全等级保护制度，履行具体安全保护义务作出了较详尽的规定，同时在第59条中明确了相应的法律责任，包括责令整改、警告及罚款等。具体来说，除兜底条款外，还有4项主要义务，包括：①制定内部安全管理制度和操作规程，确定网络安全负责人；②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；③采取监测、记录网络运行状态、网络安全事件的技术措施，并留存相关的网络日志不少于六个月；④采取数据分类、重要数据备份和加密。

2. 实名制

《网络安全法》第24条第1款规定了“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”。这也就是我们日常所说的实名制要求，企业违反本条规定的，主管部门可视情节不同，依照《网络安全法》第61条予以处罚，处罚方式包括责令整改、罚款、吊销营业执照等。2017年8月和9月，“BOSS直聘”和阿里云均因未落实用户实名制分别受到北京市网信办、天津市网信办和广东省通信管理局的处罚。

3. 网络安全事件应急预案及安全风险处置

对网络运营者而言，当发生网络安全事件时，如果有可供执行的应急预案，并能够积极处置安全风险，那么可能就会很大程度地降低网络安全事件造成的损害，因而《网络安全法》第25条明确了网络运营者应当制定网络安全事件应急预案，并且需要及时处置系统漏洞、计算机病

毒、网络攻击、网络侵入等安全风险。企业违反前述规定的，主管部门将依据《网络安全法》第 59 条第 1 款进行处罚，处罚方式包括责令整改、警告及罚款等。

4. 持续安全维护

网络产品和服务提供者就其提供的产品和服务进行持续安全维护，这原本属于提供者和购买者之间的合同义务，但《网络安全法》第 22 条第 2 款基于保障网络运行安全考虑，将这一义务法定化，要求网络产品、服务的提供者应当为其产品、服务持续提供安全维护，并在法律规定或者当事人约定的期限内，不得终止提供安全维护。同时还在第 60 条中设定了具体的法律责任，包括警告和罚款等。

5. 禁止设置恶意程序

鉴于网络产品和服务提供者存在一些不规范设置恶意程序的情况，为了规范市场主体的行为，《网络安全法》第 22 条第 1 款特别明确了网络产品、服务的提供者不得设置恶意程序的要求。企业违反此规定的，主管部门可以依据《网络安全法》第 60 条视违法情节予以相应处罚，具体包括警告和罚款等方式。

6. 禁止从事或协助实施危害网络安全活动

《网络安全法》第 27 条规定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。

（二）关键信息基础设施的运营者的特别责任

除一般规定外，鉴于关键信息基础设施（CII）对国家网络安全的特殊意义，《网络安全法》用专门一节对其运营者作了特别的规定，具体包括：