



合规法律评述
2018 年 6 月

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编: 200120
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编: 100005
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2969 5300
传真: +852 2997 3385

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

企业如何落实网络安全等级保护制度？

How Should Companies Implement Graded Network Security Protection?(Summary)

作者：潘永建 | 李天航 | 朱晓阳

I. The Predecessor of GNSP.

The GNSP is an upgrade of the “graded computer information system security protection system” dated back to 1994. In promulgating the CSL, the provisions of GNSP are further confirmed, updated and upgraded in the CSL.

II. Shall Companies Implement GNSP?

Unlike the prior rules, the CSL provides that all network operators shall have the obligations to implement the GNSP. Those who fail to implement the GNSP will face administrative penalties including ordered rectification and fines.

III. How Should Companies Implement the GNSP?

The GNSP is difficult for a company to implement on its own. Companies are advised to engage professional and qualified assessment agent to assist with the implementation of the GNSP. In addition, companies themselves shall fulfill certain mandatory obligations imposed by law.

.....
如您需要了解我们的出版物,
请与下列人员联系:

郭建良: (86 21) 3135 8756
Publication@llinkslaw.com

通力律师事务所
www.llinkslaw.com

免责声明：本出版物仅代表作者个人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

企业如何落实网络安全等级保护制度？

How Should Companies Implement Graded Network Security Protection?(Summary)

IV. Reminders

1. The company is ultimately responsible for the accuracy of the grading of its network system.
2. Those network operators that are graded as level III and above shall conduct regular assessments.
3. Network operators' GNSP obligations are not fulfilled with network architectures such as SaaS. Even under such circumstances, companies are still obligated to implement the GNSP, and shall divide such obligations with the service providers based on the boundary of the relevant network.

2018 年 6 月 1 日是中国《网络安全法》正式生效实施一周年之日。为帮助企业清晰理解网安法下企业的责任与义务，通力律师事务所网络安全与数据服务团队从 6 月 1 日起陆续推出《<网络安全法>实务 30 问》系列双语指引，通过对法律规定的解读，结合典型实践案例，深度剖析企业的责任与义务，助力企业合规经营，有效防范风险。

本篇为《<网络安全法>实务 30 问》系列双语指引的第二篇，将对网络安全等级保护制度进行简要分析，以期为相关人士提供参考。

一. 网络安全等级保护制度的前身

网络安全等级保护制度不是新事物，是计算机信息系统安全等级保护制度的升级版。1994 年颁布的《中华人民共和国计算机信息系统安全保护条例》(下称《计算机安保条例》)最早明确了对计算机信息系统实行安全等级保护，由公安机关作为主管部门负责监管实施。此后，公安部会同其他相关部门逐步完善了等级保护制度和管理的具体内容，主导完善了《计算机信息系统安全保护等级划分准则》(GB-17859-1999)等一系列国家标准。随着社会的发展，网络的外延不断扩展，出现了云计算、大数据、物联网、工业控制系统等形态，计算机信息系统等级保护制度已经不能适应，因此，《网络安全法》确认并更新了等级保护(下称“等保”)制度的内容。同时，相关配套的国家标准正在制定、修订或完善中。

受侵害客体	对客体的危害程度		
	一般	严重	特别严重
用户自身利益	一级	二级	二级(拟修改为三级)
公众利益社会秩序	二级	三级	四级
国家安全	三级	四级	五级

企业如何落实网络安全等级保护制度？

How Should Companies Implement Graded Network Security Protection?(Summary)

二. 企业有义务落实等级保护制度

不少企业认为，网络安全等保制度与自己企业关系不大。在《网络安全法》正式施行前也许确实如此，《计算机安保条例》第四条规定“计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全”。但是，与《计算机等保条例》有限的适用范围不同，《网络安全法》规定网络运营者均负有实施网络安全等级保护制度的义务。并且，《网络安全法》第五十九条明确规定，未落实网络安全等级保护义务的“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。”

《网络安全法》实施后，公安机关对未履行网络安全等保义务的企业已开始实施处罚。例如，2017年7月20日汕头警方对汕头市某信息科技有限公司处以警告并责令改正；2017年7月22日，四川省宜宾市警方对未开展等保相关工作、未落实等保义务造成网站发生被黑客攻击入侵网络安全事件的翠屏区教师培训与教育研究中心处一万元罚款，其法定代表人唐某处五千元罚款。

公安机关作为网络安全的主管机关之一，在《网络安全法》配套规定和国家标准逐步完善之后，将对网络安全等级保护制度作为网络安全领域的重点工作予以推进。因此，企业不应存有侥幸心理，而应积极落实网络安全等级保护义务。

三. 网络安全等级保护制度的落实

网络安全等级保护制度包括法律和技术制度，企业仅靠自身力量实施等保义务的难度较大，宜聘请专业的律所以及有资质的评测机构协助落实。对于法律明确要求的义务，企业应当立即落实：

- (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，并按照规定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等措施；

企业如何落实网络安全等级保护制度？

How Should Companies Implement Graded Network Security Protection?(Summary)

四. 应当注意的问题

1. 定级由评测机构和专业机构说了算？

虽然聘请了专业的评测机构进行评测以帮助落实等保义务，但是对于网络信息系统定级准确性的责任由企业承担。因此，评测机构仅提出等级建议，最终的级别需要企业正确把握。对于确定为第二等级以上的，应当在等级确定后 30 日内向所在地设区的市级公安机关备案。

2. 一次等保抑或重复等保？

对定级为三级或三级以上的网络运营者而言，等保评测与定级并非一劳永逸的事情，三级网络运营者应当至少每一年进行一次评测和自查，四级网络运营者应当至少每半年进行一次评测和自查。

3. 采取 SaaS 等网络构架和租用云服务的网络运营者不承担等保义务？

当前采取 SaaS、PaaS、IaaS 等网络构架或者租用云服务或系统由他人托管的情况比较普遍，在前述情况下企业仍然负有落实等保的法律义务，应参照相关国家标准与网络服务商根据网络边界切分厘清双方责任。

企业如何落实网络安全等级保护制度？

How Should Companies Implement Graded Network Security Protection?(Summary)

《<网络安全法>实务 30 问》系列双语指引问题清单 Schedule of “30 Questions About CSL”	
1	《网络安全法》体系下企业的责任与义务概览 Summary of Companies’ Responsibilities and Liabilities under the CSL
2	企业如何落实网络安全等级保护义务 How Should Companies Implement the Graded Network Security Protection System
3	企业正确应对国家机关调取数据的实务分析 How Should Companies Properly Respond to Authorities’ Requirement for Data Access?
4	企业使用微信企业号的合规要点 Key Compliance Issues in Using Enterprise WeChat
5	浅析网络运营者的刑事责任 Criminal Liabilities of Network Operators
6	VPN 使用与跨境联网的合规要点 Key Compliance Issues in Use of VPN and Cross-border Connectivity
7	互联网信息服务提供者责任义务辨析 Analysis on The Responsibilities and Obligations of Internet Information Services Providers
8	隐私政策的合规要点与最佳实践 Key Compliance Issues and Best Practices for Privacy Policies
9	企业与第三方关于个人信息保护责任划分 Division of Responsibilities Between Companies and Third Parties Regarding Personal Information Protection
10	员工信息收集、使用合规要点 Key Compliance Issues in Collection and Use of Employee Information
11	数据出境比你想象的常见——数据出境情形分析 Data Cross-border Transfer Happens More Than You Imagine – Analysis of Data Cross-border Transfer Scenarios
12	个人信息安全事件的妥善应对 Proper Response to Personal Information Security Incidents
13	个人信息和重要数据本地化存储的实务分析 Practical Analysis on Local Storage of Personal Information and Important Data
14	网络安全事件应对-兼论网络安全应急预案的必要性 Network Security Emergency Response and Discussion on Necessity of Network Security Emergency Plans
15	网络关键设备、网络安全专用产品、网络产品及服务涉及的网络安全审查制度 Network Security Review on Key Network Equipment, Specialized Network Products and Network Products and Services

企业如何落实网络安全等级保护制度？

How Should Companies Implement Graded Network Security Protection?(Summary)

16	网络安全负责人的设立及职责辨析 Analysis on Network Security Officer and Its Duties and Responsibilities
17	个人信息使用合规分析 Compliance Analysis on Use of Personal Information
18	企业与员工关于个人信息保护的责任划分 Division of Responsibilities Between Companies and Employees Regarding Personal Information Protection
19	企业应当如何落实网络信息实名制要求 How Should Companies Implement Network Information Real-Name Requirements
20	中国法下的个人信息概念与范围辨析 Analysis on Definition and Scope of Personal Information Under PRC Law
21	客户信息收集、使用合规要点 Key Compliance Issues in Collection and Use of Customer Information
22	电商等行业使用个人信息的合规要点 Key Compliance Issues for Use of Personal Information in E-Commerce [etc.]
23	《信息安全技术 个人信息安全规范》作为推荐性国家标准（GB/T）的实践价值分析 Practical Value Analysis on <i>Information Security Technology – Personal Information Security Specification</i> as a Recommended National Standard (GB/T)
24	收购兼并中涉及数据尽职调查要点分析 Key Issues of Data Due Diligence in M&A
25	浅析企业的个人信息保护义务 Brief Analysis on Companies' Obligations of Personal Information Protection
26	关键信息基础设施的界定 Definition of Key Information Infrastructures
27	关键信息基础设施运营者的责任与义务 The Responsibilities and Obligations of Key Information Infrastructure Operators
28	重要数据的界定 Identification of Important Data
29	如何进行数据出境？——数据出境的基本流程 How to Transfer Data Abroad? – The Basic Process of Data Cross-border Transfer.
30	数据出境评估 Assessment for Data Cross-border Transfer

企业如何落实网络安全等级保护制度？

How Should Companies Implement Graded Network Security Protection?(Summary)

如需进一步信息，请联系：

作 者	
潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com	
上 海	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	刘贇春 电话: +86 21 3135 8678 bernie.liu@linkslaw.com
余 铭 电话: +86 21 3135 8770 selena.she@linkslaw.com	娄斐弘 电话: +86 21 3135 8783 nicholas.lou@linkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@linkslaw.com	孔焕志 电话: +86 21 3135 8777 kenneth.kong@linkslaw.com
吴 炜 电话: +86 21 6043 3711 david.wu@linkslaw.com	潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com
姜 琳 电话: +86 21 6043 3710 elyn.jiang@linkslaw.com	
北 京	
俞卫锋 电话: +86 10 8519 2266 david.yu@linkslaw.com	刘贇春 电话: +86 10 8519 2266 bernie.liu@linkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@linkslaw.com	
香 港(与张慧雯律师事务所有限法律责任合伙联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	吕 红 电话: +86 21 3135 8776 sandra.lu@linkslaw.com
伦 敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@linkslaw.com	

© 《<网络安全法>实务 30 问》系列双语指引独家授权威科先行网络安全与数据合规模块在线发布

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。