网络安全百问百答手册

2022 版

2022 年 9 月

要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。

要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。

要坚持促进发展和依法管理相统一，既大力培育人工智能、物联网、下一代通信网络等新技术新应用，又积极利用法律法规和标准规范引导新技术应用。

要坚持安全可控和开放创新并重，立足于开放环境维护网络安全，加强国际交流合作，提升广大人民群众在网络空间的获得感、幸福感、安全感。

2019 年 9 月 16 日，习近平总书记对国家网络安全宣传周作出重要指示，提出国家网络安全“四个坚持”的原则要求

网络安全是共同的而不是孤立的。网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上的讲话

编写人员 （按姓氏笔画排序）

任　颋　　刘　奇　　闫　东　　孙　雪

李　凯　　汪英东　　张祥体　　陈兴凯

袁洪朋　　徐　伟　　曹　明　　常　星

本手册是在中共辽宁省委网信办的指导下，由辽宁省网络安全保障工作联盟组织有关成员单位编写完成。

其中网络安全常识部分由辽宁省互联网协会网络安全工作委员会、国家计算机网络应急技术处理协调中心辽宁分中心、辽宁省信息安全与软件测评认证中心参与编写；《数据安全法》《个人信息保护法》解读部分由辽宁邮电规划设计院有限公司参与编写；《网络安全法》《等保 2.0》解读部分由北方实验室（沈阳）股份有限公司参与编写；《网络安全审查办法》《党委（党组）网络安全工作责任制实施办法》解读部分由中国科学院沈阳计算技术研究所有限公司参与编写。

在此向以上单位表示感谢。愿我们全社会携起手来，共同保障网络安全，促进行业发展！

本书编写组

2022 年 9 月

目录

第一部分 网络安全常识

第二部分 《网络安全法》解读

第三部分 《数据安全法》解读

第四部分 《个人信息保护法》解读

第五部分 《网络安全审查办法》解读

第六部分 《等保 2.0》解读

第七部分 《党委（党组）网络安全工作责任制实施办法》解读

第一部分 网络安全常识

问 1. 什么是网络安全?

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

习近平总书记在中央网络安全和信息化领导小组第一次会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济；要有高素质的网络安全和信息化人才队伍；要积极开展双边、多边的互联网国际交流合作。建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进。

网络安全是整体的而不是割裂的、网络安全是动态的而不是静态的、网络安全是开放的而不是封闭的、网络安全是相对的而不是绝对的、网络安全是共同的而不是孤立的。 网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

问 2. 我国网络安全总体态势如何? 网络空间安全形势有哪些特点?

近年来，我国持续推进网络安全法律法规体系建设，完善网络安全管理体制机制，不断加强互联网网络安全监测和治理，构建互联网发展安全基础，构筑网民安全上网环境。特别是在党政机关和重要行业方面，网络安全应急响应能力不断提升，恶意程序感染、网页篡改、网站后门等传统安全问题得到有效控制。近年来，我国基础网络运行总体平稳，未发生较大规模以上网络安全事件。但数据泄露的事件及风险、有组织的分布式拒绝服务攻击干扰我国重要网站正常运行、鱼叉钓鱼邮件攻击等事件频发，多个高危漏洞被曝出，我国网络空间仍面临诸多风险与挑战。

网络空间安全形势主要呈现出三大特点：

一是网络安全合作与竞争并存。各国在应对和预防网络犯罪、网络攻击等方面拥有巨大的共同利益，加强网络空间合作是大势所趋。但另一方面，现实世界中的双重标准、意识形态和战略竞争等问题延伸至网络空间，使得各国在网络空间领域的竞争大于合作。

二是网络军事化趋势不可逆转。近年来各国网络空间战略中的军事化因素越来越明显，战略重点从防御开始转向进攻。美国《网络空间行动战略》宣称，将以传统军事和网络进攻相结合的方式进行主动反制。北约《新战略构想》也强调将在北约框架内拟定网络战争方略。全球已经有美国等近 50 个国家组建了网络战部队，抢占网络制高点。在美国，网络空间正式与海洋、陆地、天空和太空并列成为美军的第 5 战场。

三是国家级网络攻击常态化。具有国家背景的网络攻击已经逐渐规模化、组织化和目标化，某些网络攻击甚至构成相当于大规模杀伤性武器的威力。例如，2010 年“震网”病毒；2012 年“超级火焰”病毒；2015 年的乌克兰电网事件，2017 年维基解密披露 CIA 黑客

工具等。

问 3. 国家网络空间主权的内涵是什么?

国家网络空间主权主要包含以下四方面内容:

一是各国根据本国国情，借鉴国际经验，制定本国有关网络空间的法律法规;

二是各国根据本国法律法规，管理本国网络空间;

三是采取必要措施，监测、保护、抵御来自国内外的网络空间威胁和攻击;

四是依法防范、阻止违法信息在本国网络空间的传播。

问 4. 网络安全事件管理和应急响应方面有哪些法规依据?

（一）中华人民共和国网络安全法

《中华人民共和国网络安全法》于 2017 年 6 月 1 日颁布实施，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，促进经济社会信息化健康发展，制定的法律。

（二）信息安全技术信息安全事件分类分级指南

《信息安全技术 信息安全事件分类分级指南》（GB/Z 20986—2007）主要对信息安全事件的基本概念、信息安全事件分类、信息安全事件分级进行的规范化。

《指南》将安全事件分成 7 类，分别是有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全

事件。同时将安全事件划分为 4 个等级，对信息安全事件的分级主要考虑 3 个要素：信息系统的重要程度、系统损失和社会影响。4 个等级分别是特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）和一般事件（Ⅳ级）。

（三）国家网络安全事件应急预案

2017 年 6 月，中央网信办公布了《国家网络安全事件应急预案》。制定《国家网络安全事件应急预案》是网络安全的一项基础性工作，是落实国家《突发事件应对法》的需要，更是实施《网络安全法》、加强国家网络安全保障体系建设的本质要求。

《网络安全法》第五十三条要求，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。这个预案指的便是《国家网络安全事件应急预案》，《网络安全法》授权国家网信部门牵头制定。

5. 为什么我们的网站会被篡改?

网页被篡改主要存在五个方面的原因：

第一方面，大部分网站设计更多的考虑是满足用户业务的实现，软件开发商和网站的系统运维人员对网站攻击技术不了解，日常的使用过程中没有发现可能存在的安全漏洞。黑客攻击者一般可以较好地利用这些漏洞，为自己谋取利益。

第二方面，有些攻击者通过篡改门户网站页面来传播一些非法信息，但实际上，页面在被篡改之前，黑客已经利用漏洞获得了相应的 Web 控制权限，网站虽然还能继续提供正常的服务，但实际上系统的访问者正遭受着持续的危害。

第三方面，大部分网站或系统都有相应的网络安全防护措施，采用访问控制、WAF 防火墙、入侵防御设备等各类安全设备抵制黑客攻击，对于黑客在应用层的攻击来说表现出的防御效果不佳，没有做到真正的防御。

第四方面，大部分网站或系统设计者或开发者对安全代码设计方面的知识欠缺，系统安全出现问题和漏洞时，只能停留在页面进行恢复，很难针对网站或系统具体的漏洞原理对源代码进行改造，发现问题也不能及时彻底地解决。

第五方面，由于技术人员编制有限、资金投入不足、技术能力欠缺，运维管理人员安全意识相对薄弱，有的网站或信息系统甚至使用初始用户名和密码，利用弱口令登录，或者将用户个人信息等敏感数据直接上传到网上。

问 6. 黑客攻击一般有几个阶段?

黑客的攻击步骤复杂多变，但其整个攻击过程有一定规律，一般可分为以下几个阶段：

（1）隐藏 IP

隐藏 IP，就是隐藏黑客的位置，以免被发现。典型的隐藏真实的 IP 地址的技术有两种：

其一，利用被侵入的主机作为跳板，先入侵到互联网上的一台电脑（俗称“肉鸡”或“傀儡机”），利用这台电脑在进行攻击，即使被发现，也是“肉鸡”的 IP 地址。

其二，做多级跳板“Sock 代理”，这样在入侵的电脑上留下的是代理计算机的 IP 地址。如：攻击某国的站点，一般选择远距离的

另一国家的计算机为“肉鸡”，进行跨国攻击，这类案件很难侦破。

（2）踩点扫描

踩点扫描，主要是通过各种途径对所要攻击的目标进行多方了解，确保信息准确，确定攻击时间和地点。通常黑客分两个阶段进行。踩点：黑客搜集信息，找出被信任的主机（可能是管理员使用的机器或是被认为是很安全的服务器）。扫描：利用扫描工具寻找漏洞。

（3）获得特权

获得特权，即获得管理权限。获得权限可分为 6 种方式：由系统或软件漏洞获得系统权限；由管理漏洞获取管理员权限；由监听获取敏感信息，进一步获得相应权限；以弱口令或穷举法获得远程管理员的用户密码；以攻破与目标主机有信任关系的另一台计算机，进而得到目标主机的控制权；由欺骗获得权限以及其他方法。

（4）种植后门

种植后门，黑客利用程序漏洞进入系统后安装后门程序，以便日后可不被察觉地再次进入系统。

（5）隐身退出

黑客一旦确认自己是安全的，就开始侵袭网络，为了避免被发现，黑客在入侵完毕后会及时清除登录日志以及其他相关日志，隐身退出。

7. 什么是拒绝服务攻击？当前的拒绝服务攻击有哪些特点？

拒绝服务攻击（Denial-of-Service Attack），是指向某一目标信息系统发送密集的攻击包，或执行特定的攻击操作，以期致使

目标系统停止服务的攻击行为。拒绝服务攻击是黑客常用的攻击手段之一，其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为网络协议本身的安全缺陷。

当前的拒绝服务攻击呈现以下几个特点：

一是攻击规模大。攻击流量在 10G 以上的事件日均发生次数仍高居不下，大流量的 200G、500G 的事件多有发生。2018 年 3 月，黑客利用 memcached 服务器认证和设计缺陷实施反射 DDoS 攻击的峰值流量高达 1.94T。

二是攻击来源广。既有传统的服务器和用户主机，也有新兴的联网智能设备，比如智能监控设备、智能路由器、网络摄像头、机顶盒等，联网的设备都有可能被控制发起攻击。

三是攻击追溯难。从攻击目标来看，67% 的事件与私服游戏、网络赌博等互联网地下黑色产业链有关。另一方面，攻击 IP 地址既有境内的，也有境外的，既有真实的，也有伪造的，这给追溯攻击真实来源造成了很大困难。

8. 什么是僵尸网络?

僵尸网络是指被僵尸病毒感染的计算机设备组成的网络，工信部发布的《木马和僵尸网络监测与处置机制》将僵尸网络定义为由攻击者通过控制服务器控制的受害计算机群。僵尸网络由于其庞大的主机数量，通常用于执行分布式拒绝服务攻击、发送垃圾邮件等。僵尸网络感染了新的节点后，通常新的节点既可以执行攻击命令，也可以继续进行僵尸病毒的传播，因此僵尸网络的感染十分迅速，

并且，由于僵尸网络的传播往往都是通过新感染的节点完成，僵尸网络几乎不会暴露原始传播者的指纹等信息。2019 年，在监测发现的因感染计算机恶意程序而形成的僵尸网络中，规模在 100 台主机以上的僵尸网络数量达 1，842 个，规模在 10 万台以上的僵尸网络数量达 21 个。为有效控制计算机恶意程序感染主机引发的危害，2019 年上半年，国家互联网应急中心（CNCERT）组织基础电信企业、域名服务机构等成功关闭了 714 个控制规模较大的僵尸网络。

问 9. 什么是 SQL 注入?

SQL 注入就是通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意 SQL 命令的目的。当通过 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串时，会发生 SQL 注入，而不是按照设计者意图去执行 SQL 语句。SQL 注入攻击的本质在于程序在需要执行的代码中拼接了用户输入的数据。这种攻击的发生需要两个先决条件：一是用户能够控制输入；二是应用程序未对数据和代码进行隔离。

问 10. 什么是远程代码执行漏洞? 如何进行防范?

远程命令执行漏洞是指用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定绝对路径的情况下就执行命令，可能会允许攻击者通过改变 $PATH 或程序执行环境的其他方面来执行一个恶意构造的代码。常见的远程代码执行漏洞有 weblogic 反序列化、struts2、thinkphp5 远程代码执行等。目前该漏洞主要采取以下方式进行防范：

（1）假定所有输入都是可疑的，尝试对所有输入提交可能执行命令的构造语句进行严格的检查或者控制外部输入，系统命令执行

函数的参数不允许外部传递。

（2）不仅要验证数据的类型，还要验证其格式、长度、范围和内容。

（3）不要仅仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。

（4）对输出的数据也要检查，数据库里的值有可能会在一个大网站的多处都有输出，即使在输入做了编码等操作，在各处的输出点时也要进行安全检查。

（5）在发布应用程序之前测试所有已知的威胁。

11. 什么是 APT 攻击？有哪些典型特点？

APT 攻击是以最先进的攻击方式，最高水平的手段，以窃取特定目标的核心数据为目的，长时间、高隐蔽性的网络攻击行为。相对于普通网络攻击行为，APT 窃取指定目标的核心信息。特点：

1. 是对指定目标的点对点攻击，在攻击之前会通过各种渠道、各种方式收集被攻击者的一切相关信息，如目标经常上的网站、目标使用的操作系统、目标的上网习惯等。如已知目标经常登录的网站，则可以优先对该网站进行渗透。当目标再登陆该网站时，则窃取其账户等信息。

2. 时间持续久。APT 攻击是针对某个目标的长时间渗透，APT 攻击展开实施也会有多个阶段，一般会优先攻击安全性较低的网络系统。进行目标相关的网络系统，再以此为跳板对网络安全级别更高的指定目标进行渗透。这就导致了攻击的时间持久性。

3. 攻击伪装性强。APT 攻击者为了达到对指定目标的长期攻击，

必须要在渗透成功后较好的伪装自己。伪装的方式的多种，在不同的攻击阶段也有不同的伪装方法。如在建立通道控制访问阶段，攻击者可能会通过伪造合法签名的方式，达到伪装的目的。

4. 攻击间接访问较多。APT 攻击者为了能达到隐藏自己、长时间控制的目的，会以间接的方式对入侵目标进行访问。如经常会把已入侵过的主机服务器作为媒介对指定目标访问和控制，这样以来即使攻击行为被发现，攻击者也可以快速清理入侵痕迹，切断入侵检测回溯链路，从而更好的隐藏自己。

12. 什么是网络安全风险评估和渗透性测试?

网络安全风险评估是指依据有关网络安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

渗透测试是指渗透人员在不同的位置（比如从内网、从外网等位置）利用各种手段对某个特定网络进行测试，以期发现和挖掘系统中存在的漏洞，然后输出渗透测试报告，并提交给网络所有者。网络所有者根据渗透人员提供的渗透测试报告，可以清晰知晓系统中存在的安全隐患和问题。渗透测试还具有的两个显著特点是：渗透测试是一个渐进的并且逐步深入的过程；渗透测试是选择不影响业务系统正常运行的攻击方法进行的测试。

13. 什么是勒索病毒?

勒索病毒是一种新型电脑病毒，主要以邮件、程序木马、网页挂

马的形式进行传播。勒索病毒文件一旦进入本地，就会自动运行，同时删除勒索软件样本，以躲避查杀和分析。接下来，勒索病毒利用本地的互联网访问权限连接至黑客的 C&C 服务器，进而上传本机信息并下载加密私钥与公钥，利用私钥和公钥对文件进行加密。除了病毒开发者本人，其他人是几乎不可能解密。加密完成后，还会修改壁纸，在桌面等明显位置生成勒索提示文件，指导用户去缴纳赎金。且变种类型非常快，对常规的杀毒软件都具有免疫性。攻击的样本以 exe、js、wsf、vbe 等类型为主，对常规依靠特征检测的安全产品是一个极大的挑战。该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。

问 14. 什么是网络钓鱼？

网络钓鱼是指攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，钓鱼邮件一般是攻击者伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户回复邮件、点击嵌入邮件正文的恶意链接或者打开邮件附件以植入木马或间谍程序，进而窃取用户敏感数据、个人银行账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动，因欺骗迷惑性很强，用户稍不谨慎就很容易上当。其中，对通过钓鱼邮件窃取邮箱账号密码情况进行分析，国家互联网应急中心（CNCERT）监测发现我国平均每月约数万个电子邮箱账号密码被攻击者窃取，攻击者通过控制这些电子邮件对外发起攻击。例如 2019 年初，某经济黑客组织利用我国数百个电子邮箱对其他国家的商业和金融机构发起钓鱼攻击。仅 2019 年上半年，CNCERT 监测发现恶意电子邮件数量超过 5600 万封，涉及恶意邮件附件 37 万余个，平均每个恶意电子邮件附件传播次数约 151 次。

个人用户要避免成为网络钓鱼的受害者，一定要加强安全防范意识，提高安全防范技术水平，针对性的措施可以归纳如下几点：

（1）防范垃圾邮件。

（2）安装防病毒系统和网络防火墙系统。

（3）及时给操作系统和应用系统打补丁，堵住软件漏洞。

（4）从主观意识上提高警惕性，提高自身的安全技术。

（5）妥善保管个人信息资料。

15. 什么是移动互联网恶意程序?

移动互联网恶意程序是指在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。移动互联网恶意程序一般存在以下一种或多种恶意行为，包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为。

2019 年上半年，国家互联网应急中心（CNCERT）通过自主捕获和厂商交换获得移动互联网恶意程序数量 103 万余个，通过对恶意程序的恶意行为统计发现，排名前三的分别为资费消耗类、流氓行为类和恶意扣费类。CNCERT 累计协调国内 177 家提供移动应用程序下载服务的平台，下架 1190 个移动互联网恶意程序。

2019 年上半年，我国以移动互联网为载体的虚假贷款 APP 或网站达 1.5 万个，在此类虚假贷款 APP 或网站上提交姓名、身份证照片、个人资产证明、银行账户、地址等个人隐私信息的用户数量超过 90 万。大量受害用户在诈骗平台支付了上万元的所谓“担保费”、“手续费”费用，经济利益受到实质损害。

第二部分《网络安全法》解读

问 16. 如果生活中发现有危害网络安全的行为应该如何进行举报?

任何个人和组织发现危害网络安全的八类活动、七种行为时，都有权举报。原则上讲，涉及网络犯罪的主要是向公安部门举报，其他类型的，既可以向电信部门，也可以向网信等部门举报。但是，无论是哪一类危害网络安全的行为，个人和组织都可以向网信、电信、公安等部门举报。

任何一个部门收到举报都应该及时处理，不属于本部门职责的要及时移交相关部门处理。

问 17. 为什么制定《网络安全法》?

当前，网络和信息技术迅猛发展，已经深度融入我国经济社会的各个方面，极大地改变和影响着人们的社会活动和生活方式，在促进技术创新、经济发展、文化繁荣、社会进步的同时，网络安全问题也日益凸显。一是，网络入侵、网络攻击等非法活动，严重威胁着电信、能源、交通、金融，以及国防军事、行政管理等重要领域的信息基础设施的安全，云计算、大数据、物联网等新技术、新应用面临着更为复杂的网络安全环境；二是，非法获取、泄露甚至倒卖公民个人信息，侮辱诽谤他人、侵犯知识产权等违法活动在网络上时有发生，严重损害公民、法人和其他组织的合法权益；三是，宣扬恐怖主义、极端主义，煽动颠覆国家政权、推翻社会主义制度，以及淫秽色情等违法信息，借助网络传播、扩散，严重危害国家安全和社会公共利益。

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，就网络安全问题提出了一系列新思想、新观点、新论断，对加强国家网络安全工作作出重要部署。党的十八届四中全会决定要求完善网络安全保护方面的法律法规。广大人民群众十分关注网络安全，强烈要求依法加强网络空间治理，规范网络信息传播秩序，惩治网络违法犯罪，使网络空间清朗起来。全国人大代表也提出许多议案、建议，呼吁出台网络安全相关立法。为适应国家网络安全工作的新形势新任务，落实党中央的要求，回应人民群众的期待，制定出台了《网络安全法》。

18. 如何理解国家网信部门负责统筹协调网络安全工作?

《网络安全法》明确国家网信部门统筹协调国家网络安全工作，主要是网络安全政策、信息、资源、事件处置的统筹协调，重点包括以下四方面。

一是《网络安全法》明确的统筹协调工作，包括：**第三十九条**规定的协调有关部门加强对关键信息基础设施的安全保护；**第五十一条**规定的协调有关部门加强网络安全信息收集、分析和通报工作，按照统一规定发布网络安全监测预警信息；**第五十三条**规定的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。

二是根据部门职能和中央的要求，应该承担的统筹协调工作，包括：组织拟订国家网络安全战略、规划等；统筹协调国家网络安全保障体系和可信体系建设；组织起草关键信息基础设施保护条例、数据安全保护办法等；指导组织国家网络安全标准的制定；指导督促党政军部门、重点行业网络安全保障工作；推进网络安全人才培养工作等。

三是《网络安全法》中有些工作任务未明确责任主体的，应该通过统筹协调进一步推进，如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；国务院和各地方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等。

四是《网络安全法》中多次提到了“按规定”但目前还没有规定的事项。对于没有规定的或规定不完善的，要统筹协调、抓紧制定和完善相关规定。

问 19. 如何理解国家网信部门负责网络安全相关监督管理工作?

一是《网络安全法》中明确了由国家网信部门承担的管理工作，主要包括：①受理和处置网络安全举报；②对出境数据组织安全评估；③对可能影响国家安全的产品和服务组织网络安全审查；④制定网络关键设备和网络安全专用产品目录；⑤发现法律法规禁止发布或者传输的信息时，应当要求网络运营者停止传输；⑥对来源于境外的违法信息，通知有关机构采取技术措施和其他必要措施，阻断传播。

二是根据国家有关要求，明确了由网信部门为主承担的网络安全工作，包括：①具体承担网络内容安全管理工作；②组织开展网络安全宣传教育活动等。

三是《网络安全法》中虽未明确具体部门，但有关规定在实施时实际由网信部门为主，承担工作。如第五十二条规定，负责关键信息基础设施安全保护工作的部门，应当按照规定报送网络安全监测预警信息，这里要求的信息应向网络安全应急办所在的网信部门报送。

问 20.《网络安全法》明确规定的地方政府的网络安全责任

有哪些?

一是按照第十六条要求，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。

二是按照第十九条要求，组织开展经常性的网络安全宣传教育，指导、监督有关单位做好网络安全宣传教育工作。

三是按照第五十四条要求，网络安全事件发生的风险增大时，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，采取以下措施：①要求有关部门、机构和人员及时收集、报告有关信息，加强网络安全风险的监测；②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；③向社会发布网络安全风险预警，发布避免、减轻危害的措施。

四是按照第五十五条要求，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。

五是按照第五十六条要求，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，对该网络运营者的法定代表人或者主要责任人进行约谈。

六是按照第十四条要求，建立网络安全举报受理机制。

七是按照第四十九条要求，依法对网络运营者实施监督检查。

问 21.《网络安全法》对个人和组织提出了哪些明确的行为禁则?

《网络安全法》明确禁止了八类活动、七种行为。

任何个人和组织不得利用网络从事以下八类活动：一是危害国家安全、荣誉和利益的活动；二是煽动颠覆国家政权、推翻社会主义制度的活动；三是煽动分裂国家、破坏国家统一的活动；四是宣扬恐怖主义、极端主义的活动；五是宣扬民族仇恨、民族歧视的活动；六是传播暴力、淫秽色情信息的活动；七是编造、传播虚假信息扰乱经济秩序和社会秩序的活动；八是侵害他人名誉、隐私、知识产权和其他合法权益的活动。

以下七种行为都是法律明确禁止的：一是非法侵入他人网络、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；二是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；三是明知他人从事危害网络安全的活动，仍为其提供技术支持、广告推广、支付结算等帮助；四是窃取或者以其他非法方式获取个人信息，非法出售或者非法向他人提供个人信息；五是设立用于实施诈骗，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；六是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；七是发送的电子信息、提供的应用软件，设置了恶意程序，含有法律、行政法规禁止发布或者传输的信息。

问 22. 作为关键信息基础设施运营者应该履行哪些责任、义务?

关键信息基础设施运营者除了履行网络运营者的责任、义务外，还应履行以下责任、义务。

一是第三十三条关于“三同步”的要求，即：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。

二是第三十四条提出的设置专门安全管理机构、培训等五方面要求，即：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；定期对从业人员进行网络安全教育、技术培训和技能考核；对重要系统和数据库进行容灾备份；制定网络安全事件应急预案，并定期进行演练；法律、行政法规规定的其他义务。

三是第三十五条关于国家网络安全审查要求，即：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。

四是第三十六条关于签订安全保密协议的要求，即：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。

五是第三十七条关于数据出境的要求，即：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。

六是第三十八条关于每年开展安全检测评估的要求，即：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。

问 23. 网络安全等级保护与现行的信息安全等级保护制度是否冲突?

信息安全等级保护是国家网络安全保障的重要制度，其核心是分清系统边界，明确系统责任，确保重点目标的安全。近年来，信息安全等级保护制度在国家网络安全保障中发挥了重要作用，但该制度也应随着形势的发展不断完善，如云计算、大数据、物联网、移动互联网等技术的发展，使系统边界日益模糊，迫切需要从整体上加强保护。《网络安全法》提出了“实行网络安全等级保护制度”，明确了网络安全等级保护制度的基本要求，这是在总结信息安全等级保护工作的基础上，根据网络安全的新形势、新特点提出的，标志着信息安全保护制度进入了一个新的阶段。

问 24. 什么样的设备和系统应当留存网络日志不少于六个月?

《网络安全法》第二十一条要求，网络运营者应按照规定留存相关的网络日志不少于六个月。这里的网络日志主要是指记录网络运行和安全状况、网络行为等的文件，一般不包括个人终端上的日志文件。

问 25. 网络产品、服务为什么必须符合国家标准的强制性要求？

强制性标准是在一定范围内通过法律、行政法规等强制性手段加以实施的标准，具有法律属性，强制性标准可分为全文强制和条文强制两种形式。今后，按照标准化改革方案要求，国家标准的强制

性要求，主要是指强制性国家标准。

目前，我国已经出台的国家网络安全标准，基本上为指导性标准。全国信息安全标准化技术委员会将按照《网络安全法》的要求和网络安全工作需要，从维护国家安全、用户利益出发，对网络产品、服务制定强制性国家网络安全标准。

问 26. 如果我们提供的网络产品、服务存在安全缺陷、漏洞等风险时，应如何告知用户并向有关主管部门报告？

针对近年来网络产品、服务存在缺陷、漏洞并被恶意利用，损害用户利益的情况，《网络安全法》强化了用户知情权。有关产品和服务的提供者应在避免安全缺陷与漏洞被进一步利用的前提下，选择通过电话、短信、邮件、网站公告、媒体广告等合理方式告知用户，并提供相应的风险解决或减轻措施。此外，网络产品、服务提供者应当根据产品、服务的主要使用领域、事件性质等，向网信、电信、公安等部门报告。

问 27. 网络运营者如何报告发生危害网络安全的事件？

国家网信部门已经发布了《国家网络安全事件应急预案》，网络运营者应根据国家预案，制定本单位的网络安全事件应急预案。在发生危害网络安全的事件时，网络运营者应立即启动应急预案，采取补救措施，按照《国家网络安全事件应急预案》规定的报告程序进行报告。

问 28. 企业为公安机关、国家安全机关提供技术支持和协助，是否会损害个人隐私、侵犯知识产权?

出于维护国家安全、保护公民合法权益和打击网络犯罪，特别是

打击网络恐怖活动的需要，要求企业为执法部门提供必要的支持和协助是各国的通行做法，也是企业应尽的义务。

《网络安全法》规定，相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，并明确规定相关部门及其工作人员不得泄露、出售或者非法向他人提供在履行职责中知悉的个人信息、隐私和商业秘密。在实际执行过程中，对执法部门也会有约束，执法部门要履行严格的审批程序，最大限度地降低可能对企业造成的影响。

问 29. 什么是关键信息基础设施，有哪些属于关键信息基础设施？

关键信息基础设施是指关键信息基础设施是指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、国防科技工业等重要行业和领域的，以及其他那些一旦遭到破坏、丧失功能或者数据泄露将对国家安全、国计民生、公共利益造成严重危害的网络设施和信息系统。

《关键信息基础设施安全保护条例》已经 2021 年 4 月 27 日国务院第 133 次常务会议通过，自 2021 年 9 月 1 日起施行。

问 30. 我国为什么要加强对关键信息基础设施保护?

金融、能源、通信、交通等重点行业和领域的关键信息基础设施是经济社会运行的神经中枢，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、国计民生和公共利益。当前，关键信息基础设施是网络攻击的重点目标，其安全保护是网络安全的重中之重。面对当前严峻的网络安全形势，各国普遍加强对关键信息基础设施的保护，出台了一系列政策法规。

31. 如何对关键信息基础设施进行抽查检测和应急演练?

关键信息基础设施保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。

运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。

关键信息基础设施保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练。

32. 等级保护制度与关键信息基础设施保护制度是什么关系?

《网络安全法》明确，关键信息基础设施保护要“在网络安全等级保护制度的基础上，实行重点保护”，指的是关键信息基础设施保护首先要满足网络安全等级保护的基本要求，主要是《网络安全法》第二十一条提出的要求，同时还要采取更加完善的措施来确保其安全。

今后，要按照《网络安全法》的要求，把关键信息基础设施保护作为网络安全工作的重中之重。一是要加强关键信息基础设施保护的统筹，加强顶层设计和整体防护，避免多头分散、各自为政的情况发生；二是要建立完善责任制，政府主要是加强指导监管，关键信息基础设施运营者要承担起保护的主体责任；三是要加强对从业

人员的网络安全教育、技术培训和技能考核，切实提高网络安全意识和水平；四是要做好网络安全信息共享、应急处置等基础性工作，提升关键信息基础设施保护能力；五是要加强关键信息基础设施保护中的国际合作。

问 33. 为什么要求关键信息基础设施安全保护部门编制和组织实施本行业、本领域的关键信息基础设施安全规划?

各行业、各领域关键信息基础设施形态各异，支撑的业务千差万别，具体到每一个行业，其保护工作的重点、保护的手段等不尽相同。各行业主管或监管部门对本行业的安全本身负有管理职责，且其对行业内关键信息基础设施情况最为了解，对业务网络安全需求最为明确。因此，由行业主管或监管部门编制和组织实施本行业、本领域的关键信息基础设施安全规划最为合理。

问 34. 如何对关键信息基础设施安全管理机构进行安全背景审查？

关键信息基础设施运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

问 35. 哪些从业人员需要接受网络安全教育、技术培训和技能考核?

《网络安全法》第三十四条中的“从业人员”不仅限于网络安全岗位上的专业人员，还包括其他与关键信息基础设施运营安全相关的管理人员、操作人员、使用人员、服务人员等，是全员教育、培训和考核。

第三部分《数据安全法》解读

问 36. 国家制定《数据安全法》的目的是什么？

规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

问 37. 数据安全工作的责任分工是什么？

1）中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制；

2）各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责；

3）工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责；

4）公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责；

5）国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

问 38.《数据安全法》对于数据处理的定义包括那些处理活动？

数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等。

39. 日常生活中遇到违反《数据安全法》条款的现象时如何投诉？

《数据安全法》第十二条规定：任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

40. 数据分类分级保护制度建立的依据是什么？

《数据安全法》第二十一条规定：国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

41. 数据安全保护工作的负责人和管理机构有哪些规定？

《数据安全法》第二十七条规定：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

42. 数据安全处理活动的风险监测活动有哪些规定？

《数据安全法》第二十九条规定：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

问 43. 重要数据的处理者如何展开风险评估活动？

《数据安全法》第三十条规定：重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

问 44. 关键信息基础设施的运营者的数据出境活动是如何规定的？

《数据安全法》第三十一条规定：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重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

45. 数据收集的规定有哪些？

《数据安全法》第三十二条规定：任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

问 46. 数据交易是如何规定的？

《数据安全法》第三十三条规定：从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

47. 如何处理来自境外的数据提供请求？

《数据安全法》第三十六条规定：中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

48. 国家机关委托第三方对政务数据处理时，应遵守哪些规定？

《数据安全法》第四十条规定：国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

49. 国家机关履行法定职责而进行的数据处理活动有哪些规定？

《数据安全法》第三十八条规定：国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

50. 非法窃取或获取数据的个人、组织有哪些罚则？

《数据安全法》第五十一条规定：窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第四部分《个人信息保护法》解读

问 51. 什么是法律意义上的个人信息？

《个人信息保护法》第四条规定：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

问 52. 可以随便在网上公开他人个人信息吗？

《个人信息保护法》第十条规定：任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

问 53. 哪些信息属于敏感个人信息？

根据《个人信息保护法》第二十八条第一款的规定，敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满 14 周岁未成年人的个人信息。

问 54. 信息处理者能直接处理不满 14 周岁未成年人的个人信息吗？

《个人信息保护法》第三十一条规定：个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他

监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

55. 我国境内收集和产生的个人信息存储在哪里？

《个人信息保护法》第四十条规定：关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

56. 什么情形下应当删除个人信息？

根据《个人信息保护法》第四十七条的规定，有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（三）个人撤回同意；

（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安

全保护措施之外的处理。

问 57. 发生个人信息泄露时，信息处理者应该怎么办？

《个人信息保护法》第五十七条规定：发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

问 58. 个人信息权益被侵犯了怎么办？

《个人信息保护法》第六十一条规定：履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

问 59. 违反规定处理个人信息的应当承担什么责任？

根据《个人信息保护法》第六十六条、第六十七条的规定，违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百元万元以下罚款；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。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处以五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接负责人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

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。

问 60. 履行个人信息保护职责的部门如何履行监督职能？

履行个人信息保护职责的部门在履行个人信息保护的过程当中，主动对个人信息处理活动进行信息保护，这只是其履行个人信息保护职责的部门职能的一部分，主动进行信息保护对于做好信息保护

工作是不够全面的，不足以涵盖整个履行个人信息保护职责的部门工作的全部，监督管理工作也是履行个人信息保护职责的部门的重要工作内容。根据《个人信息保护法》第六十五条的规定，任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。在履行监督管理工作的过程中，任何组织和个人都应当是个人信息保护的监督主体，都有权对违法个人信息处理活动向履行信息保护职责的部门进行投诉、举报。这样的设置能够发挥全社会的力量，能够对个人信息处理活动进行全方位的监督。履行个人信息保护职责的部门对于社会的监督也应该及时进行处理和反馈，从而形成全社会的联动机制，确保个人信息处理活动合法有效进行。

问 61. 发现个人信息不准确或者不完整时怎么办?

在个人信息被处理的过程当中，我们发现个人信息存在不准确或者不完整的情形，是有权要求个人信息处理者对存在问题的个人信息进行更正或者补充的，这是《个人信息保护法》赋予个人对个人信息处理者处理个人信息活动进行监督的一种表现形式，个人发现其个人信息存在的问题，可以及时要求改正。《个人信息保护法》也规定，对于个人提出的更正、补充的请求，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。这样的规定能够促使个人信息处理者积极有效地处理个人信息，并保证个人信息能够完整准确地被处理。

问 62. 公共场所安装图像采集设备应设置显著的提示标识吗?

根据《个人信息保护法》第二十六条的规定，在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

63. 对于侵害多人信息权益的情况，哪些主体可以提起公益诉讼?

根据《个人信息保护法》第七十条的规定，个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

64. 处理个人信息需要有明确合理的目的吗?

根据《个人信息保护法》第六条的规定，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

65. 具有公共事务职能的组织是否有权处理个人信息?

根据《个人信息保护法》第三十七条的规定，法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。法律、法规授权的具有公共事务管理职能的组织有：公安、医药、工商、税务、城管、卫生防疫、烟草、盐业等部门。上述组织基于法定职责处理个人信息是

适用《个人信息保护法》关于国家机关处理个人信息的规定的，因此具有公共事务职能的组织有权处理个人信息。

第五部分《网络安全审查办法》解读

问 66.《网络安全审查办法》的审查对象?

键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。

因此可以看出，本办法审查的对象为关键信息基础设施运营者对网络产品和服务的采购行为。

问 67. 网络安全审查应坚持什么原则?

网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。

问 68. 网络安全审查办公室设在哪个部门，主要工作内容有哪些?

网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。

问 69. 网络安全审查主要审查哪些内容?

网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：

（一）产品和服务使用后带来的关键信息基础设施被非法控制、

遭受干扰或者破坏的风险；

（二）产品和服务供应中断对关键信息基础设施业务连续性的危害；

（三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；

（四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；

（五）核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；

（六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；

（七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

问 70. 网络安全审查有无时限要求?

通常情况下，应当自向当事人发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长 15 个工作日。根据《网络安全审查办法》要求，网络安全审查办公室要求提供补充材料的，当事人、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。

问 71. 特别审查程序的主要处理流程是什么?

按照特别审查程序处理的，网络安全审查办公室应当听取相关单位和部门意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知当事人。

问 72. 审查过程中如何保证审查对象的商业秘密和知识产权?

参与网络安全审查的相关机构和人员应当严格保护知识产权，对在审查工作中知悉的商业秘密、个人信息，当事人、产品和服务提供者提交的未公开材料，以及其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或者用于审查以外的目的。当事人或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中知悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。

问 73. 违反《网络安全审查办法》中的规定应如何处理?

当事人违反本办法规定的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》的规定处理。

问 74.《网络安全审查办法》中网络产品和服务指的是什么?

《网络安全审查办法》中所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全、网络安全和数据安全有重要影响的网络产品和服务。

75.《网络安全审查办法》从什么时间开始施行?

《网络安全审查办法》自 2022 年 2 月 15 日起施行。2020 年 4 月 13 日公布的《网络安全审查办法》同时废止。

第六部分 《等保 2.0》解读

问 76. 什么是网络安全等级保护测评?

网络安全等级保护测评是指测评机构依据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》等标准，通过访谈、检查、测试等手段对安全技术和管理各层面的安全控制进行整体性验证，确保网络的安全保护措施符合相应等级的安全要求，给出第三方测评机构的网络安全等级保护测评报告。

问 77. 为什么要做网络安全等级保护测评?

《网络安全法》明确提出国家实行网络安全等级保护制度，其中第二十一条和第三十八条又进一步对网络运营者需要履行的安全保护提出了明确要求。为了满足《网络安全法》要求，网络运营者需要开展网络安全等级保护工作，履行安全保护义务，保障网络安全，最大程度的避免网络运营者承担法律责任。

《网络安全等级保护条例》的第二十二条和第二十三条明确指出第二级网络和第三级网络应当按照网络安全等级保护有关标准规范，进行安全性测试、网络安全等级测评。

问 78. 谁是网络运营者?

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。

网络运营者，是指网络的所有者、管理者和网络服务提供者。

问 79. 等级保护对象有哪些?

等级保护对象是指网络安全等级保护工作中的对象，通常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，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网(IoT)、工业控制系统和采用移动互联技术的系统等。等级保护对象根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为 1 级 ~5 级五个安全保护等级。

问 80. 等级保护对象分为几个等级?

根据等级保护相关管理文件，等级保护对象的安全保护等级分为以下五级：

1）第一级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益;

2）第二级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全;

3）第三级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害;

4）第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害;

5）第五级，等级保护对象受到破坏后，会对国家安全造成特别严重损害。

问 81. 网络安全等级保护测评关注哪些，如何做?

网络安全等级保护测评涉及安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十大安全类。网络安全等级保护测评需要基于科学的方法，利用专业的工具，辅以必要的漏扫和渗透测试手段，以规避潜在系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险为目标。

问 82. 什么系统需要做网络安全等级保护测评?

根据《网络安全法》，网络运营者在中国境内建设、运营和维护网络，应按照网络安全等级保护制度的要求，履行安全保护义务，例如：政府和企事业单位管理、办公、门户类，工业控制、云计算，基础网络、大数据平台等涉及国家安全、社会秩序、公共利益、公民、法人和其他组织合法权益的系统。

问 83. 不做网络安全等级保护测评等检测评估有什么处罚?

未按《网络安全法》要求履行网络安全等级保护义务，关键信息基础设施运营者每年未开展过检测评估，有关部门警告后拒不整改或造成危害后果的，进行罚款（单位 1 万以上 100 万以下，责任人 5000 以上 10 万以下）、拘留、暂停业务等处罚。造成严重后果的根据《刑九》处三年以下有期徒刑、拘役或者管制。

问 84. 系统托管到外单位，网络运营者还有责任吗?

本单位系统托管到外单位云平台或网络平台的，本单位作为系统的所有者或管理者，仍是责任主体，所以同样承担责任和义务。被

托管单位作为网络服务提供者，承担相应责任和义务。

85. 作为定级对象的系统有什么必备特征?

1）具有确定的主要安全责任单位。作为定级对象的信息系统应能够明确其主要安全责任单位；

2）承载相对独立的业务应用。作为定级对象的信息系统应承载相对独立的业务应用，完成不同业务目标或者支撑不同单位或不同部门职能的多个信息系统应划分为不同的定级对象；

3）具有信息系统的基本要素。作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的多资源集合，单一设备（如服务器、终端、网络设备等）不单独定级。

86. 等级保护定级和备案的时间?

网络运营者应当在规划设计阶段确定网络的安全保护等级。第二级以上网络运营者应当在网络的安全保护等级确定后 10 个工作日内，到县级以上公安机关备案。

87. 等级保护定级流程包括哪些?

定级流程包括确定定级对象、初步确定等级、专家评审、主管部门审核、公安机关备案审查、最终确定等级。

88. 等保测评流程是什么？

1）测评准备活动：等级测评项目启动、信息收集与分析、工具和表单准备；

2）方案编制活动：测评对象确定、测评指标确定、测评工具接入点确定、测评内容确定、测评指导书开发、测评方案编制；

3）现场测评活动：测评实施准备、现场测评和结果记录、结果确认和资料归还；

4）分析与报告编制活动：单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成、测评报告编制。

问 89. 测评之后哪些问题一定要立即整改?

在等保测评时会发现网络的技术措施的不足、安全管理制度不完善或缺失问题、系统漏洞、设备缺失或不足等问题；最终判定为高风险的问题，则必须立即进行整改。

问 90. 对于等保测评存在哪些误区?

误区一：系统已上云或托管，就不用做等保；

系统责任主体是属于网络运营者自己，需要承担相应的网络安全责任。

误区二：系统定级越低越好；

系统定级需要合理，安全责任没有履行到位会被处罚。

误区三：等保工作做测评就可以；

测评只是等级保护工作中的一项。

误区四：等保测评做过一次就可以了；

等保工作需要根据具体的国家标准、行业规定，安排合理的评测周期。

误区五：系统在内网，不需要做等保；

所有非涉密系统都属于等级保护范畴。

误区六：单位整体做一个等保测评就可以了；

等保测评按照网络系统开展，而不是单位。

第七部分 《党委（党组）网络安全工作责任制 实施办法》解读

问 91. 制定本办法的目的是什么？

进一步加强网络安全工作，明确和落实党委（党组）领导班子、领导干部网络安全责任。

问 92. 按照谁主管谁负责、属地管理的原则，谁承担网络安全责任？

各级党委（党组）对本地区本部门网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。

问 93. 各级党委（党组）主要承担的网络安全责任有哪些？

1）认真贯彻落实党中央和习近平总书记关于网络安全工作的重要指示精神和决策部署，贯彻落实网络安全法律法规，明确本地区本部门网络安全的主要目标、基本要求、工作任务、保护措施；

2）建立和落实网络安全责任制，把网络安全工作纳入重要议事日程，明确工作机构，加大人力、财力、物力的支持和保障力度；

3）统一组织领导本地区本部门网络安全保护和重大事件处置工作，研究解决重要问题；

4）采取有效措施，为公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动提供支持和保障；

5）组织开展经常性网络安全宣传教育，采取多种方式培养网络

安全人才，支持网络安全技术产业发展。

94. 谁对本行业本领域的网络安全负指导监管责任？

行业主管监管部门对本行业本领域的网络安全负指导监管责任。没有主管监管部门的，由所在地区负指导监管责任。

95. 各级网络安全和信息化领导小组（网信委）工作职责有哪些？

各级网络安全和信息化领导小组（注：现为网络安全和信息化委员会）应当加强和规范本地区本部门网络安全信息汇集、分析和研判工作，要求有关单位和机构及时报告网络安全信息，组织指导网络安全通报机构开展网络安全信息通报，统筹协调开展网络安全检查。

96. 网络安全先进集体和先进工作者的表彰奖励由哪个部门负责？

中央网络安全和信息化领导小组办公室（注：现为中央网络安全和信息化委员会办公室）会同有关部门按照国家有关规定对网络安全先进集体予以表彰，对网络安全先进工作者予以表彰奖励。

97. 发生哪些情形，各级党委（党组）应当逐级倒查，追究责任？

1）党政机关门户网站、重点新闻网站、大型网络平台被攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；

2）地市级以上党政机关门户网站或者重点新闻网站受到攻击后

没有及时组织处置，且瘫痪 6 个小时以上的；

3）发生国家秘密泄露、大面积个人信息泄露或者大量地理、人口、资源等国家基础数据泄露的；

4）关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；

5）封锁、瞒报网络安全事件情况，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的；

6）阻碍公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的；

7）发生其他严重危害网络安全行为的。

问 98. 对领导班子、领导干部进行问责应如何实施？

对领导班子、领导干部进行问责，应当由有管理权限的党组织依据有关规定实施。各级网络安全和信息化领导小组办公室（注：现为网络安全和信息化委员会办公室）可以向实施问责的党委（党组）、纪委（纪检组）提出问责建议。

问 99. 网络意识形态工作责任制按照什么文件执行？

网络意识形态工作责任制按照《党委（党组）网络意识形态工作责任制实施细则》执行。

问 100.《党委（党组）网络安全工作责任制实施办法》从什么时间施行？

《党委（党组）网络安全工作责任制实施办法》自 2017 年 8 月 15 日起施行。

附录一 中华人民共和国网络安全法

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。

附录二 中华人民共和国数据安全法

第一章　总则

第一条　为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条　在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条　本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条　维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条　中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条　各地区、各部门对本地区、本部门工作中收集和产生的

数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条 开展数据处理活动，应当遵守法律、法规、尊重社会公德和伦理、遵守商业道德和职业道德、诚实守信、履行数据安全保护义务、承担社会责任、不得危害国家安全、公共利益、不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法做出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条 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重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核，交易记录。

第三十四条 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批

准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，并可以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可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、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五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可

以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、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十万元以上一百万元以下罚款。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、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。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并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。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、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五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，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。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条 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。

第七章 附则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自 2021 年 9 月 1 日起施行。

附录三 中华人民共和国个人信息保护法

第一章　总则

第一条　为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

第二条　自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条　在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

（一）以向境内自然人提供产品或者服务为目的；

（二）分析、评估境内自然人的行为；

（三）法律、行政法规规定的其他情形。

第四条　个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

第五条　处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条　处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条 个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

第二章 个人信息处理规则

第一节 一般规定

第十三条 符合下列情形之一的，个人信息处理者方可处理个人信息：

（一）取得个人的同意；

（二）为订立、履行个人作为一方当事人的合同所必需，或者按

照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；

（三）为履行法定职责或者法定义务所必需；

（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

第十四条 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

第十五条 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供

产品或者服务所必需的除外。

第十七条 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

（一）个人信息处理者的名称或者姓名和联系方式；

（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）个人行使本法规定权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条 个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条 个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

第二十二条 个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十三条 个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十四条 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

通过自动化决策方式向个人进行信息推送、商业营销，应当同时

提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

第二十七条 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

第二节 敏感个人信息的处理规则

第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

第二十九条 处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第三十条 个人信息处理者处理敏感个人信息的，除本法第十七

条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节 国家机关处理个人信息的特别规定

第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章 个人信息跨境提供的规则

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 个人在个人信息处理活动中的权利

第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条 个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（三）个人撤回同意；

（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条 个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章 个人信息处理者的义务

第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）制定并组织实施个人信息安全事件应急预案；

（六）法律、行政法规规定的其他措施。

第五十二条 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者

代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条 个人信息保护影响评估应当包括下列内容：

（一）个人信息的处理目的、处理方式等是否合法、正当、必要；

（二）对个人权益的影响及安全风险；

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危

害的措施；

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

第五十八条 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：

（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；

（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；

（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；

（四）定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

第六章 履行个人信息保护职责的部门

第六十条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门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个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

第六十二条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

（一）制定个人信息保护具体规则、标准；

（二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；

（三）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设；

（四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；

（五）完善个人信息保护投诉、举报工作机制。

第六十三条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

（一）询问有关当事人，调查与个人信息处理活动有关的情况；

（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；

（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查；

（四）检查与个人信息处理活动有关的设备、物品；对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 法律责任

第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并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。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第六十七条 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。

第六十八条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；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。

履行个人信息保护职责的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。

第六十九条 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息

处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

第七十条 个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十一条 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。

第八章 附则

第七十二条 自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

第七十三条 本法下列用语的含义：

（一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

（二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第七十四条 本法自 2021 年 11 月 1 日起施行。

附录四 网络安全审查办法

第一条 为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，根据《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》，制定本办法。

第二条 关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。

前款规定的关键信息基础设施运营者、网络平台运营者统称为当事人。

第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。

第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局建立国家网络安全审查工作机制。

网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。

第五条 关键信息基础设施运营者采购网络产品和服务的，应当

预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。

关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。

第六条 对于申报网络安全审查的采购活动，关键信息基础设施运营者应当通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或者必要的技术支持服务等。

第七条 掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

第八条 当事人申报网络安全审查，应当提交以下材料：

（一）申报书；

（二）关于影响或者可能影响国家安全的分析报告；

（三）采购文件、协议、拟签订的合同或者拟提交的首次公开募股（IPO）等上市申请文件；

（四）网络安全审查工作需要的其他材料。

第九条 网络安全审查办公室应当自收到符合本办法第八条规定的审查申报材料起 10 个工作日内，确定是否需要审查并书面通知当事人。

第十条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：

（一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险；

（二）产品和服务供应中断对关键信息基础设施业务连续性的危害；

（三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；

（四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；

（五）核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；

（六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；

（七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长 15 个工作日。

第十二条 网络安全审查工作机制成员单位和相关部门应当自收到审查结论建议之日起 15 个工作日内书面回复意见。

网络安全审查工作机制成员单位、相关部门意见一致的，网络安全审查办公室以书面形式将审查结论通知当事人；意见不一致的，

按照特别审查程序处理，并通知当事人。

第十三条 按照特别审查程序处理的，网络安全审查办公室应当听取相关单位和部门意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知当事人。

第十四条 特别审查程序一般应当在 90 个工作日内完成，情况复杂的可以延长。

第十五条 网络安全审查办公室要求提供补充材料的，当事人、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。

第十六条 网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。

为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。

第十七条 参与网络安全审查的相关机构和人员应当严格保护知识产权，对在审查工作中知悉的商业秘密、个人信息，当事人、产品和服务提供者提交的未公开材料，以及其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或者用于审查以外的目的。

第十八条 当事人或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中知悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。

第十九条 当事人应当督促产品和服务提供者履行网络安全审查中作出的承诺。

网络安全审查办公室通过接受举报等形式加强事前事中事后监督。

第二十条 当事人违反本办法规定的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》的规定处理。

第二十一条 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全、网络安全和数据安全有重要影响的网络产品和服务。

第二十二条 涉及国家秘密信息的，依照国家有关保密规定执行。

国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。

第二十三条 本办法自 2022 年 2 月 15 日起施行。2020 年 4 月 13 日公布的《网络安全审查办法》（国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局令第 6 号）同时废止。

附录五 关键信息基础设施安全保护条例

第一章　总则

第一条　为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条　本条例所称关键信息基础设施，是指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等。

第三条　在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

第四条　关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者（以下简称运营者）主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

第五条　国家对关键信息基础设施实行重点保护，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，依法惩治危害关键信息基础设施安全的违法犯罪活动。

任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。

第六条 运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第七条 对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。

第二章 关键信息基础设施认定

第八条 本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。

第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

（一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）对其他行业和领域的关联性影响。

第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务

院公安部门。

第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起3个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。

第三章 运营者责任义务

第十二条 安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

第十三条 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第十四条 运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

第十五条 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：

（一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；

（二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

（三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；

（四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

（五）组织网络安全教育、培训；

（六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

（七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

（八）按照规定报告网络安全事件和重要事项。

第十六条 运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

第十七条 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

第十八条 关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

第十九条 运营者应当优先采购安全可信的网络产品和服务；采

购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第二十条 运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第二十一条 运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

第四章 保障和促进

第二十二条 保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

第二十三条 国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。

第二十四条 保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

第二十五条 保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

第二十六条 保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

第二十七条 国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。

有关部门在开展关键信息基础设施网络安全检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

第二十八条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。

第二十九条 在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。

第三十条 网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。

第三十一条 未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。

第三十二条 国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。

能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全运行提供重点保障。

第三十三条 公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动。

第三十四条 国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作。

第三十五条 国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。

第三十六条 国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。

第三十七条 国家加强网络安全服务机构建设和管理，制定管理要求并加强监督指导，不断提升服务机构能力水平，充分发挥其在关键信息基础设施安全保护中的作用。

第三十八条 国家加强网络安全军民融合，军地协同保护关键信息基础设施安全。

第五章 法律责任

第三十九条 运营者有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万

元以上 10 万元以下罚款：

（一）在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；

（二）安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的；

（三）未建立健全网络安全保护制度和责任制的；

（四）未设置专门安全管理机构的；

（五）未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；

（六）开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；

（七）专门安全管理机构未履行本条例第十五条规定的职责的；

（八）未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的；

（九）采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；

（十）发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。

第四十条 运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上

100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。

第四十一条 运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额 1 倍以上 10 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 1 万元以上 10 万元以下罚款。

第四十二条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处 5 万元以上 50 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 1 万元以上 10 万元以下罚款；情节严重的，依法追究相应法律责任。

第四十三条 实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪的，依照《中华人民共和国网络安全法》有关规定，由公安机关没收违法所得，处 5 日以下拘留，可以并处 5 万元以上 50 万元以下罚款；情节较重的，处 5 日以上 15 日以下拘留，可以并处 10 万元以上 100 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 10 万元以上 100 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。

违反本条例第五条第二款和第三十一条规定，受到治安管理处罚的人员，5 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。

第四十四条 网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十五条 公安机关、保护工作部门和其他有关部门在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十六条 网信部门、公安机关、保护工作部门等有关部门、网络安全服务机构及其工作人员将在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十七条 关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

第四十八条 电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。

第四十九条 违反本条例规定，给他人造成损害的，依法承担民事责任。

违反本条例规定，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。

第六章　附则

第五十条　存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。

第五十一条　本条例自 2021 年 9 月 1 日起施行。

附录六 党委（党组）网络安全工作责任制实施办法

第一条 为了进一步加强网络安全工作，明确和落实党委（党组）领导班子、领导干部网络安全责任，根据《中国共产党问责条例》、《中央网络安全和信息化领导小组工作规则》等有关规定，制定本办法。

第二条 网络安全工作事关国家安全、政权安全和经济社会发展。按照谁主管谁负责、属地管理的原则，各级党委（党组）对本地区本部门网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。

第三条 各级党委（党组）主要承担的网络安全责任是：

（一）认真贯彻落实党中央和习近平总书记关于网络安全工作的重要指示精神和决策部署，贯彻落实网络安全法律法规，明确本地区本部门网络安全的主要目标、基本要求、工作任务、保护措施；

（二）建立和落实网络安全责任制，把网络安全工作纳入重要议事日程，明确工作机构，加大人力、财力、物力的支持和保障力度；

（三）统一组织领导本地区本部门网络安全保护和重大事件处置工作，研究解决重要问题；

（四）采取有效措施，为公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动提供支持和保障；

（五）组织开展经常性网络安全宣传教育，采取多种方式培养网络安全人才，支持网络安全技术产业发展。

第四条 行业主管监管部门对本行业本领域的网络安全负指导监管责任。没有主管监管部门的，由所在地区负指导监管责任。

主管监管部门应当依法开展网络安全检查、处置网络安全事件，

并及时将情况通报网络和信息系统所在地区网络安全和信息化领导小组。各地区开展网络安全检查、处置网络安全事件时，涉及重要行业的，应当会同相关主管监管部门进行。

第五条 各级网络安全和信息化领导小组应当加强和规范本地区本部门网络安全信息汇集、分析和研判工作，要求有关单位和机构及时报告网络安全信息，组织指导网络安全通报机构开展网络安全信息通报，统筹协调开展网络安全检查。

第六条 各地区各部门网络安全和信息化领导小组应当向中央网络安全和信息化领导小组及时报告网络安全重大事项，包括出台涉及网络安全的重要政策和制度措施等。

各地区各部门网络安全和信息化领导小组每年向中央网络安全和信息化领导小组报告网络安全工作情况。

第七条 中央网络安全和信息化领导小组办公室会同有关部门按照国家有关规定对网络安全先进集体予以表彰，对网络安全先进工作者予以表彰奖励。

第八条 各级党委(党组)违反或者未能正确履行本办法所列职责，按照有关规定追究其相关责任。

有下列情形之一的，各级党委（党组）应当逐级倒查，追究当事人、网络安全负责人直至主要负责人责任。协调监管不力的，还应当追究综合协调或监管部门负责人责任。

（一）党政机关门户网站、重点新闻网站、大型网络平台被攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；

（二）地市级以上党政机关门户网站或者重点新闻网站受到攻击

后没有及时组织处置，且瘫痪 6 个小时以上的；

（三）发生国家秘密泄露、大面积个人信息泄露或者大量地理、人口、资源等国家基础数据泄露的；

（四）关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；

（五）封锁、瞒报网络安全事件情况，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的；

（六）阻碍公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的；

（七）发生其他严重危害网络安全行为的。

第九条 实施责任追究应当实事求是，分清集体责任和个人责任。追究集体责任时，领导班子主要负责人和主管网络安全的领导班子成员承担主要领导责任，参与相关工作决策的领导班子其他成员承担重要领导责任。

对领导班子、领导干部进行问责，应当由有管理权限的党组织依据有关规定实施。各级网络安全和信息化领导小组办公室可以向实施问责的党委（党组）、纪委（纪检组）提出问责建议。

第十条 各级党委（党组）应当建立网络安全责任制检查考核制度，完善健全考核机制，明确考核内容、方法、程序，考核结果送干部主管部门，作为对领导班子和有关领导干部综合考核评价的重要内容。

第十一条 各级审计机关在有关部门和单位的审计中，应当将网

络安全建设和绩效纳入审计范围。

第十二条 网络意识形态工作责任制按照《党委（党组）网络意识形态工作责任制实施细则》执行。涉密网络按照有关规定执行。

第十三条 本办法由中央网络安全和信息化领导小组办公室负责解释。

第十四条 本办法自 2017 年 8 月 15 日起施行。

网络安全为人民

网络安全靠人民