

Agreements 文档



【版权声明】

版权所有©百度在线网络技术（北京）有限公司、北京百度网讯科技有限公司。 未经本公司书面许可，任何单位和个人不得擅自摘抄、复制、传播本文档内容，否则本公司有权依法追究法律责任。

【商标声明】



和其他百度系商标，均为百度在线网络技术（北京）有限公司、北京百度网讯科技有限公司的商标。 本文档涉及的第三方商标，依法由相关权利人所有。未经商标权利人书面许可，不得擅自对其商标进行使用、复制、修改、传播等行为。

【免责声明】

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导。 如您购买本文档介绍的产品、服务，您的权利与义务将依据百度智能云产品服务合同条款予以具体约定。本文档内容不作任何明示或暗示的保证。

目录

目录	2
百度智能云用户服务协议	3
百度智能云线上订购协议	13
隐私政策	20
【百度智能云】隐私政策	20
信息安全	33
信息安全规定	33
百度智能云用户行业资质收取标准	36
百度智能云信息安全处罚细则	42
法律法规	42
百度智能云账号注销协议	175
百度智能云账号实名认证相关协议	177
百度智能云主、子关联账户实名认证授权协议	177
接受账号主体变更协议	177
申请账号主体变更协议	180
百度智能云学生身份验证功能服务用户协议	183
百度智能云学生身份验证功能服务个人信息处理规则	185

百度智能云用户服务协议

🔗 声明及总则

本服务协议是百度智能云网站（包含域名为cloud.baidu.com的网站以及百度智能云客户端，如百度智能云App，以下简称为“本网站”）的经营者北京百度网讯科技有限公司（以下简称为“本公司”或“百度智能云”），与用户（以下称为“您”）就您使用百度智能云向您提供的本网站上所展示的产品与服务（下称“百度智能云服务”、“本服务”）的相关事项，而共同缔结的、对双方具有约束力的有效契约。

为使用本服务，您应当并请您务必充分审慎阅读、理解本协议，其中限制、免责条款或者其他涉及您重大权益的条款（如违约处罚、争议管辖等）会以加粗等形式提示您重点注意。如您对协议有任何疑问，可以联系客服或相关业务部门进行咨询。您通过勾选、点击确认或以其他方式表示接受本协议，或您以任何方式使用本服务的，即视为您已阅读、理解本协议并同意接受本协议的约束，并与百度智能云达成一致，本协议即在您与本公司之间产生法律效力。

本协议内容同时包括百度智能云通过本网站或其他约定的方式，已经发布、展示或可能持续增加发布、展示的关于与百度智能云具体服务相关的服务协议、服务规范/规则、服务等级协议（SLA）及服务说明、技术规范、使用流程、操作文档、计费标准、业务规则、保密协议等内容，这些内容统称为服务规则，与本协议共同构成对您和百度智能云具有约束力的文件。上述内容经本网站或其他约定的方式正式发布、展示，即为本协议不可分割的组成部分，是您接受、使用百度智能云服务需遵循的、符合公平正义原则的规则及条件，您同样应当遵守。

您同意：百度智能云基于网络服务的及时性、复杂性、高效性等特性及响应监管要求和政策规范等原因，将不断更新产品与服务范围及服务内容，最新的百度智能云服务及相关协议规则以本网站相关产品及服务介绍页面展示的以及向您实际提供的为准；百度智能云有权随时对本服务协议及相应的服务规则内容进行单方面的变更，并有权以消息推送、网页公告等方式予以公布，而无需另行单独通知您。如您使用或购买百度智能云某一具体产品和/或服务，您仍需确认具体云服务对应的服务条款。您续签或新订购某产品或服务后，应遵守当时的服务条款，百度智能云推出新的产品与服务后，将可能更新本协议中相关内容。

您同意：在本服务协议内容公告变更后，若您不同意修改后的服务协议，您有权立即停止使用本服务；若您继续使用本服务的，表示您已充分阅读、理解并接受修改后的协议内容，也将遵循修改后的协议内容使用本服务。

🔗 关于百度智能云账号

1. 账号类型

百度智能云账号分为个人账号和企业账号，通过实名认证的方式进行区分：

（1）个人账号是百度通用账号，使用手机或邮箱注册。实名认证的方式为个人认证，适用于个人开发爱好者，账号属于个人。注册时，您可根据注册页面的注册说明详细了解。

（2）企业账号是面向百度智能云商业产品的用户账号体系。实名认证的方式为企业认证，适用于企业、个体工商户、事业单位、学校、社会团体等组织，账号归属企业，相对个人账号可以享有更多产品选择权：

- 您的百度智能云商业产品账号可以访问并操作您开通的所有百度智能云商业产品，您需对用户名和密码的安全性负责，请勿向任何人透露您的用户名和密码。
- 若您忘记了账户密码，可自行通过您设置的密保手机按照自动流程找回相关信息。
- 若您公司负责管理帐户的人员已离开公司，或您在任何情况下知悉或怀疑您的用户名及密码为任何第三方所知悉，或有人未经授权而使用您的账号，请您主动向百度智能云提出申请，并按照流程要求提交相关表单。为了确认您是相关帐户的所有人，我们会要求您提供一些详细信息，如最近的付款信息或客户ID等，您应予以配合。在百度智能云根据流程处理您的账户前，您须就任何第三方使用服务或服务被用作未经授权用途负责。

2. 账号注册

（1）主体资格

您确认：在您完成注册程序或以其他方式百度智能云允许的方式实际使用本服务时，您应当是具备完全民事权利能力和完全民事行为能力的自然人、法人或其他组织（以下统称为“法律主体”）。

如果您是未成年人或限制民事行为能力人，则您不具备前述主体资格，您及您的监护人应承担因您的不当注册行为而导致的一

切后果。

您还需承诺您不是任何国家、国际组织或者地域实施的制裁、贸易管制的对象，否则您可能无法正常注册及使用百度智能云服务。

(2) 注册账号

- 在使用本服务前，您需要先注册，取得本公司提供给您的账号，您同意并保证：
 1. 您确保您已充分阅读百度智能云网站的注册指引，并正确选择了账号类型。因账号类型选择不当引发的问题，百度智能云不承担任何责任。
 2. 您所填写的用户信息是真实、准确、完整、及时的，且保证百度智能云可以通过您所填写的联系方式与您取得联系。
 3. 您设置的账号名称、头像不得违反法律法规、公序良俗以及本服务相关规则，不得与他人产生混淆或使他人产生误认。否则，您的账号可能无法注册成功，或被要求修改。若您拒绝修改的，百度智能云有权对您的账号采取账号限制措施，或拒绝向您提供产品和服务，您应当承担由此产生的后果和责任。
 4. 您应根据百度智能云对于服务的要求及时提供相应的身份证明，企业资质等资料，否则百度智能云有权拒绝向您提供相关服务。
 5. 若您提供的资料或信息包含有不正确、不真实的信息，百度智能云保留取消您账号注册资格、中止或终止为您提供服务的权利。
 6. 您应对您的百度智能云账号负责，您在本网站注册的账号是百度智能云为您提供服务的唯一服务标识，依托账号您可以获取相应的百度智能云服务。只有您本人可以使用您的百度智能云账号，未经百度智能云同意并作账号实名变更，该账号不可转让、不可赠与、不可继承。否则百度智能云有收回该账号的权利
 7. 以代理人身份代理其他自然人或者单位进行注册，您必须向百度智能云提供代理人和被代理人的详细资料和书面授权，未提供上述资料和文件的，百度智能云将视注册者为用户。
 8. 您应当准确填写并及时更新您提供的电子邮件地址、联系电话、联系地址、邮政编码等联系方式，以便百度智能云或其他用户与您进行有效联系，因通过这些联系方式无法与您取得联系，导致您在使用百度智能云服务过程中产生任何损失或增加费用的，应由您完全独自承担。您了解并同意，您有义务保持您提供的联系方式的有效性，如有变更需要更新的，您应按百度智能云的要求进行操作。

(3) 账号安全

为保障网络生态和交易秩序，您与百度智能云都需遵守国家法律法规、政策规范。百度智能云有权制定账号协议和服务规范，并设立投诉渠道。对于违反规定的账号，将采取限制和处置措施。

(4) 账号责任

百度智能云通过您的用户名和密码识别您的指示，您在本网站注册的账号是百度智能云为您提供服务的唯一服务标识，依托账号您可以获取相应的百度智能云服务。请您妥善保管您的用户名和密码，您必须对维护密码和账户的机密性承担全部责任。您需要对账户中发生的所有活动承担全部责任，对于因密码泄露或用户名遗忘所致的损失，由您自行承担。在任何时候，未经账户持有人的同意，您都不得使用其他人的账户。如百度智能云或第三方因其他人使用您的账户或因您使用其他人的账户而蒙受损失，您则应承担相应责任。

若您发现有他人冒用或盗用您的账号及密码或任何其他未经合法授权的使用或任何其他不安全的行为，您应立即以有效方式通知百度智能云，要求百度智能云暂停相关服务。同时，您理解百度智能云对您的请求采取行动需要合理期限，在此之前，百度智能云对已执行的指令及所导致的您的损失不承担任何责任。

3. 实名认证

(1) 认证资料

您了解并同意，为核验您身份的真实性以及更好地向您提供服务，并为保证您的账号和交易安全，百度智能云有权要求您完成百度智能云账号的实名认证；您知晓并同意，根据您的实名认证方式，百度智能云需要收集您的个人或企业信息，例如姓名、人脸信息、身份证件或营业执照、银行账户信息等，具体以页面提示为准。同时，百度智能云可能会就某些产品或服务的开通，依法要求您提供更多的身份资料、企业实名认证办理人身份信息或企业资质等信息，做进一步的身份认证或资格验证，您的账号只有在通过这些认证和验证之后，方可获得使用相关产品或服务的资格。

您理解并同意，在实名认证的过程中，百度智能云需要将您的信息传递给第三方权威机构进行校验，以确认您提供的信息真实、准确和有效，您同意百度智能云有权自行或委托第三方完成上述校验，百度智能云会采取必要的安全和技术措施，保障您信息的安全。如您未依照相关法律法规及百度智能云的要求完成实名认证，您将无法开通并使用百度智能云服务。

(2) 认证责任

您应对您的百度智能云账号负责，只有您本人可以使用您的百度智能云账号，**未经百度智能云同意并作账号实名变更，该账号不可转让、不可赠与、不可继承**。否则百度智能云有权收回该账号。

实名认证信息是决定百度智能云账号使用权归属的直接和主要依据。在账号使用权发生争议时，百度智能云有权依照实名认证信息判定账号使用权的归属。该账号下的权益及义务，除非有明确、直接的相反证明，应当被认定归属于百度智能云记录的当前实名认证信息的主体。

您在进行实名认证时务必谨慎对待，给予足够的重视并确保认证主体与账号使用主体保持一致，避免将企业使用的账号认证在个人名下，也不应实施将本人使用的账号认证在他人名下等任何不当认证行为。

4. 关联账号

通常情况下，您的百度智能云账号是您在本网站进行一切活动的唯一身份识别依据，每一个百度智能云账号都可以在本网站独立开展活动，但在下列情形下，百度智能云有权根据自己的判断，对同一及/或关联法律主体拥有的多个百度智能云账号进行特别约定，包括拒绝提供、限制或终止提供百度智能云的产品服务，并追究关联主体承担连带法律责任等。前述情形包括但不限于：

- 1) 多个百度智能云账号之间存在主账号与子账号、授权账号与被授权账号等关联关系，且根据法律法规、本服务协议、百度智能云各产品协议或其他百度智能云规则的规定，各账号之间互相承担连带责任的；
- 2) 多个百度智能云账号使用同一实名认证、子账号继承主账号实名认证，其中任何一个百度智能云账号存在恶意欠费及/或违反法律法规、本服务协议、百度智能云产品协议或其他百度智能云规则的行为，各账号之间应互相承担连带责任；
- 3) 多个百度智能云账号对应于同一法律实体，且该法律实体已在先被识别为恶意注册账号以获取不正当利益者；
- 4) 其他百度智能云有充足理由需要对多个百度智能云账号进行统一处理的情形。

5. 账号注销

您有权决定停止使用百度智能云服务并注销您的百度智能云账号。您可以根据 [《百度智能云账号注销协议》](#) 及操作指引发起账号注销。

6. 合法要求

您理解并同意，百度智能云有权了解您使用本网站产品及服务的真实背景及目的，有权要求您如实提供真实、全面、准确的信息；如果百度智能云有合理理由怀疑您提供的信息不真实、您进行虚假交易，或您的行为违反百度智能云的服务规则的，百度智能云有权暂时或永久限制您账号下所使用的所有产品及/或服务的全部或部分或全部功能。您理解并同意，百度智能云有权按照国家司法、行政、军事、安全等机关（包括但不限于公安机关、检察机关、法院、海关、税务机关、安全部门等）的要求对您的个人信息及在本网站的资金、交易及账号等进行查询、冻结或扣划。

🔗 用户的权利与义务

1. 您的经营许可要求 如果您利用百度智能云提供的服务进行经营或非经营的活动需要获得国家有关部门的许可或批准的，您应获得该有关的许可或批准。包括但不限于以下内容：

- 1) 如果您在云服务器服务上开办了多个网站，须保证所开办的全部网站均获得国家有关部门的许可或批准；
- 2) 如您网站提供非经营性互联网信息服务的，必须办理非经营性网站备案，并保证所提交的所有备案信息真实有效，在备案信息变化时及时在备案系统中提交更新信息；
- 3) 如您网站提供经营性互联网信息服务的，还应自行在当地通信管理部门取得经营性网站许可证；4) 如您提供BBS等电子公告服务的，也需根据相关法规政策要求备案或获得相应批准；
- 5) 如您经营互联网游戏网站的，您应依法获得网络文化经营许可证；
- 6) 如您经营互联网音、视频网站的，您应依法获得信息网络传播视听节目许可证；
- 7) 如您从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。

您理解并认可，以上列举并不能穷尽您进行经营或非经营活动需要获得国家有关部门的许可或批准的全部类型，您应获得有关的许可或批准，并应符合国家及地方不时颁布相关法律法规之要求。

2. 行为合法性保证 您保证您使用本服务时将遵从国家、地方法律法规、行业惯例和社会公共道德，不会利用本公司提供的服务进行存储、发布、传播如下信息和内容：

- 1) 违反国家法律法规政策的任何内容（信息）；
- 2) 违反国家规定的政治宣传和/或新闻信息；
- 3) 涉及国家秘密和/或安全的信息；

- 4) 封建迷信和/或淫秽、色情、下流的信息或教唆犯罪的信息；
- 5) 博彩有奖、赌博游戏；
- 6) 违反国家民族和宗教政策的信息；
- 7) 妨碍互联网运行安全的信息；
- 8) 侵害他人合法权益的信息和/或其他有损于社会秩序、治安、公共道德的信息或内容。

您同时承诺不得为他人发布上述不符合国家规定和/或服务协议约定的信息内容提供任何便利，包括但不限于设置URL、BANNER链接，发送邮件、短信等。

您同意百度智能云有权在您违反上述约定时终止向您提供服务并不予退还任何款项，因您的上述行为给百度智能云或百度智能云其他用户造成损失的，您应承担相关法律责任。

3. 禁止有害信息散布

您不应利用百度智能云提供的服务散发大量未经请求的电子邮件、电子广告或包含反动、色情等有害信息的电子邮件。“有害信息”包括但不限于：

- 1) 使用通信服务发送调查、竞赛、传销信息、连锁信、垃圾邮件或者任何复制性或主动提供的消息（商业或其他目的）；
- 2) 诽谤、辱骂、骚扰、恐吓、威胁他人或以其他方式侵犯其他人的合法权益（如隐私权和公开权）；
- 3) 发布、张贴、上载、分发或散布任何不恰当的、亵渎的、诽谤的、猥亵的、下流的或其他非法主题、名称、资料或信息；
- 4) 上传或以其他方式提供包含受知识产权法（包括但不限于著作权法或商标法）、隐私权或公开权保护的图像、照片、软件或其他资料的文件，但您自己拥有或控制这些权利或者获得所有必要许可的情况除外；
- 5) 在使用通过服务获取的任何资料或信息（包括图像、照片）时，以任何方式侵犯任何当事方的任何版权、商标、专利、商业秘密或其他专有权；
- 6) 上载含病毒、木马、蠕虫、定时炸弹、清除器、损坏的文件或者任何类似的、可能损害其他人的计算机或资产的软件或程序；
- 7) 出于任何商业目的进行广告宣传或者提出销售、购买任何商品或服务，但通信服务明确允许此类消息的情况除外；
- 8) 下载另一名通信服务用户张贴的、您明确知道或者理应知道不得以这种方式进行非法复制、展示、执行和/或分发的任何文件；
- 9) 伪造或删除任何版权管理信息，如作者归属、法律声明或其他相应的声明、专有标志、上载文件所含的软件或其他资料的来源或出处标签；
- 10) 获取或以其他方式收集其他人的信息，包括电子邮件地址；
- 11) 捏造假身份来误导其他人；
- 12) 使用、下载或以其他方式复制、或者向其他人或实体（免费或收费）提供服务用户或其他用户的任何目录、使用信息或其部分信息。

4. 通信服务资料合法性要求

百度智能云不承担监控通信服务的义务，但保留查看张贴到通信服务上的资料以及自行决定移除任何资料的权利。百度智能云保留出于合法原因随时终止您访问任何或所有通信服务的权利，并且不会另行通知。在任何通信服务中提供任何有关您自己或受您监护的人的个人身份信息时，请始终谨慎行事。百度智能云不会控制或认可任何通信服务中出现的内容、消息或信息，对通信服务以及因您加入通信服务导致的任何行为不承担任何责任。

上载到通信服务的资料可能受到有关使用、复制和/或散布的公开限制；如果您下载资料，应遵守这些限制。

5. 资源使用合法性要求

您不应大量占用，亦不得导致如程序或进程等大量占用百度智能云云计算资源（如云服务器、网络带宽、存储空间等）所组成的平台（以下简称“云平台”）中服务器内存、CPU或者网络带宽资源（如互联网挖矿等行为等），并给云平台或者平台其他用户的网络、服务器（包括但不限于本地及外地和国际的网络、服务器等）、产品/应用等带来严重的、不合理的负荷，影响百度智能云与国际互联网或其他特定网络、服务器正常通畅的联系，或者导致云平台产品与服务或者其他平台用户的服务器宕机、死机或者影响其他平台用户基于云平台的产品/应用不可访问等。一经发现，您的主机将被强制停机，您的百度智能云账号也会被立即冻结，百度智能云并保留追究您的法律责任的权利。

6. 软件使用安全要求

未经百度智能云书面许可的，您不应修改、翻译、改编、出租、转许可、在信息网络上传播或转让百度智能云提供的服务或软件，也不得逆向工程、反编译或试图以其他方式发现百度智能云提供的服务或软件的源代码。

您不应进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼，黑客，网络诈骗，网站或空间中含有或涉嫌散播：病

毒、木马、恶意代码，及对其他网站、服务器进行涉嫌攻击行为如扫描、嗅探、ARP欺骗、DDoS等）。

您不应进行任何改变或试图改变百度智能云提供的系统配置或破坏系统安全的行为。在使用服务时，不得以任何方式损坏、禁用、过载或妨碍任何百度智能云服务器或连接到任何百度智能云服务器的网络，也不得干扰任何其他用户使用和享有任何服务。您不得尝试通过入侵、密码盗取或任何其他手段擅自使用任何服务、其他账户、计算机系统或连接到任何百度智能云服务器或任何服务的网络。您不得通过任何手段获取或尝试获取服务未明确提供的任何资料或信息。

7. 用户行为限制性要求

除非您购买了专门用于此目的的服务，您不应利用本服务从事DDoS防护、DNS防护等防护售卖业务。

您不应利用百度智能云的服务从事可不经网络审查为境内获取境外非法信息的活动。

您不应在百度智能云服务或平台之上安装、使用盗版软件；您对自行安装软件和进行的操作承担相应的责任。

您应自行对因使用本服务而存储在百度服务器的各类数据等信息，在本服务之外，采取合理、安全的技术措施，确保其安全性和完整性，并对自己的行为（包括但不限于欠费，自行安装软件、采取加密措施或进行其他安全措施等）所引起的结果承担全部责任。

8. 用户行为合法性要求

您在使用本服务时须遵守本协议以及百度的相关要求，不得利用本服务从事包括但不限于以下行为，也不得为以下行为提供便利（包括但不限于为您的最终用户的行为提供便利等）：

- 1) 将本服务的云服务器用作虚拟服务器或用作磁盘空间进行出租，以及用作代理服务器（Proxy）或邮箱服务器；
- 2) 进行博彩、赌博游戏、“私服”、“外挂”等非法互联网活动；
- 3) 发布、传送、传播电子邮件广告、垃圾邮件（SPAM）；
- 4) 发布、传送、传播不受欢迎的或者未经请求的电子邮件、电子广告、短信广告或包含反动、色情等有害信息的电子邮件或短信；
- 5) 建立或利用有关设备、配置运行与所使用服务无关的程序或进程，导致大量占用本服务中的服务器内存、CPU或者网络带宽资源，给本服务的系统或者本服务中的用户所使用的其他网络、服务器（包括但不限于本地及外地和国际的网络、服务器等）、产品/应用、服务等带来严重的负荷，影响本服务与国际互联网或者本服务与特定网络、服务器及本服务内部的通畅联系，或者导致本服务或者本服务中的其他用户所使用的服务器宕机、死机或者其他百度智能云服务使用者的产品或服务不可访问等；
- 6) 进行任何破坏或试图破坏网络安全的行为，包括但不限于以病毒、木马、恶意代码、钓鱼等方式，采取对其他网站、服务器进行恶意扫描、非法侵入系统、非法获取数据等；
- 7) 进行任何改变或试图改变本服务提供的系统配置或破坏系统安全的行为；
- 8) 利用技术或其他手段破坏、扰乱本服务的运营或他人对本服务的使用；
- 9) 以任何方式干扰或企图干扰百度任何产品或任何部分、功能的正常运行，或者制作、发布、传播上述工具、方法等；
- 10) 进行任何可能违反诚实信用、公序良俗、公众道德的行为；以任何方式发布虚假信息，诱导用户分享虚假信息等行为；
- 11) 若您因从事包括但不限于“DNS解析”、“安全服务”、“域名代理”、“反向代理”等任何业务，导致百度智能云服务平台或其他用户频繁遭受攻击（包括但不限于DDoS攻击）且未及时更正您的行为或未根据百度要求消除影响，从而对本服务平台或其他平台用户产生威胁的，一经发现，您的主机将被强制停机，您的账号也会被立即冻结。

9. 数据合理处理约定

您可以指定您的内容所存储的区域。未经您的同意，我们不会从您选择的区域中迁移您的内容，除非（a）必须迁移以遵守适用的法律法规或者政府机关的约束性命令；（b）根据您的委托，您应确保您的委托已获得必要的政府许可及用户授权，有权利委托百度智能云传输相关内容至其他区域；（c）为了提供账单、管理、技术服务或者因调查安全事件或者调查违反本协议的行为。我们可能会在您使用服务的数据中心区域处理一些数据，我们也可能会在我们维护运营、支持和调查系统及团队的区域处理这些数据。

10. 非经相关主管机关许可，您及您授权使用百度智能云产品或服务主体不会通过百度智能云产品或服务向适用的出口管制及制裁法律法规禁止的目的地、实体或个人提供受管控的产品或服务。您确保不会将我们提供的产品或服务用于任何适用的出口管制及制裁法律法规禁止的用途。

11. 您同意授权百度智能云关联公司或百度智能云授权第三方合作伙伴来处理信息，为您提供客户支持服务。

12. 我们可能会与我们的关联公司、第三方（如合作的授权合作伙伴等）共享您的个人信息，我们将确保我们的关联公司、第三方受到适当的个人信息保护义务的约束。用于委托我们的关联公司或合作的授权合作伙伴来处理信息或提供技术支持服务、

客户支持服务等，以便为您提供更好的产品/服务，改善您的用户体验。对于委托处理个人信息的场景，我们会根据法律法规规定通过书面协议等方式要求受托合作方（公司、组织和个人）遵守严格的保密义务并采取有效的保密措施，要求其只能根据我们的指示在委托范围内处理您的信息，并对受托人的个人信息处理活动进行监督。相关第三方无权将共享的个人信息用于任何其他用途。我们会与第三方合作方签署数据保护协议，要求他们采取相关的保密和安全措施来处理个人信息，明确合作方对您的个人信息的保护责任和义务。

13. 如您有违反本用户服务协议的行为，百度智能云有权拒绝继续为您提供任何服务。

若您使用百度智能云产品或服务从事任何违法、违规或侵犯他人合法权益的行为，百度智能云有权依法履行网络安全管理义务，中止或终止服务，并依法保留追究您相关法律责任的权利。

14. 在以下情况之一发生时，服务期限将提前结束：

- (1) 双方同意提前结束服务；
- (2) 若您严重违反本协议（包括违反相关法律法规或未履行本协议中的任何承诺），我们有权提前终止服务并删除您的数据；
- (3) 您需理解并同意，尽管我们已采取（并将持续改进）必要的技术手段来防范网络安全威胁，如计算机病毒、网络攻击等，但由于网络安全技术的局限性和不可预测性，如果您的网站受到这些威胁，导致我们或其他网络、服务器受到影响，我们可暂停或终止服务。

🔗 百度智能云的权利与义务

1. 服务商资质承诺

北京百度网讯科技有限公司承诺是依据中国法律设立并有效存续的有限责任公司，将按照本协议约定为您提供产品和服务，并切实履行本协议项下的义务和责任。

2. 除另有约定外，我们可能委托关联公司或其他主体向您提供百度智能云的一项或多项具体服务，同时您可能会与该等公司订立相关协议，请您审慎阅读、充分理解协议内容，选择接受或不接受该协议。

3. 商业秘密保护承诺

百度智能云会严格依协议约定保护您的商业秘密和隐私，非因法定原因或您的许可，不会向任何第三方披露您的保密信息。

4. 技术架构支持

百度智能云负责操作系统以下的底层技术架构支持，以及对百度智能云提供的软件进行运营维护。您在系统上安装的第三方应用程序由您负责。

5. 按现状提供服务

百度智能云不断提升服务质量及服务水平。您理解，百度智能云无法保证所提供的产品服务毫无瑕疵，您同意，即使百度智能云提供的服务存在瑕疵，但上述瑕疵是当时行业技术水平所无法避免的，其将不被视为百度智能云违约。您同意和百度智能云一同合作解决由于行业技术水平限制造成的服务瑕疵类问题。

6. 关联账户管理

百度智能云的某些产品服务具备账户授权管理功能，您可将您对服务的全部或部分操作权限授权给您指定的一个或多个被授权账户，此种情况下，任一被授权账户下进行的所有操作行为，均将被视为您通过本人账户所进行的行为，都将由您承担相应的责任以及由此产生的服务费用。

7. 产品兼容性免责

您理解并认可，百度智能云为您提供基于某些服务的安全防护，以及云上资源管理与监控的相关功能及服务，尽管百度智能云对该等服务经过详细的测试，但并不能保证其与所有的软硬件系统完全兼容，亦不能保证其软件及服务的完全准确性。如果出现不兼容及软件错误的情况，您应立即关闭或停止使用相关功能，并及时联系百度智能云，获得技术支持。

8. 免费资源活动

您应理解并同意，百度智能云在对服务进行测试研发、新品宣传推广活动时，您免费试（使）用服务期间，或您免费使用服务的额度内，百度智能云会对服务可用性和可靠性提供最好支撑，但不做任何服务可用性、可靠性做出承诺，亦不对您使用或不能使用百度智能云服务的结果承担任何责任。百度智能云保留日后对该等免费服务收取费用的可能性，收取服务费用之前，百度智能云将另行通知您。

9. ICP备案信息真实性要求

依据《非经营性互联网信息服务备案管理办法》第二十三条规定，填报虚假备案信息的，由住所所在地省通信管理局关闭网站并注销备案。请您承诺并确认：您提交的所有备案信息真实有效，当您的备案信息发生变化时请及时到备案系统中提交更新信息，如因未及时更新而导致备案信息不准确，百度智能云有权依法依规对接入网站进行处理。您理解并同意授权百度智能云基于为您提供ICP备案服务之目的，向您收集与ICP备案工作相关的图文资料、活体信息等并自行或委托第三方可信任机构开展真实性核验，在确认您的备案信息真实性的情况下，为您提供ICP备案、备案变更、注销备案等服务。

百度智能云基于为您提供ICP备案服务之目的向您收集的信息，仅限于为该目的使用，如您对相关信息收集有异议，您有权拒绝提供，您还可以通过提交工单或电话等途径详细咨询。您理解并认可，百度智能云不会超范围收集及处理您的备案信息，如因第三方泄露您的信息或发生其他数据安全事件，由第三方承担全部法律责任。

10. 禁止滥用系统资源

百度智能云保留在您滥用系统资源的情况下，强制停机及冻结账号的权利。

11. 欠费行为制约

百度智能云保留在您资源欠费超过一定天数（具体规则参见具体产品文档）时将中止提供资源、服务的权利。对因此情形中断服务可能引发的一切后果，包括数据毁损灭失的可能后果，由您自行承担。

您名下有多个百度智能云账号的，每个百度智能云账号均是独立计费。您理解，如果您名下有的账号发生欠费，虽然百度智能云可能会给予您便利不影响您尚未欠费的账号的服务，但百度智能云始终保留对您所有百度智能云账号中的费用合并处置的权利。百度智能云有权将您账号内预缴尚未消耗的资金抵充您其他百度智能云账号欠费及您的其他应付费用，且您所有百度智能云账号内的资金不足以抵充您的欠费和其他应付费用的，对您所有百度智能云账号予以拒绝和终止服务。

并且，如果您发生欠费，我们有权向您收取违约金，并要求您赔偿损失。

12. 合规审查

百度智能云自行或根据相关部门的信息、权利人的投诉进行排查发现您可能存在违反相关法律法规或本协议的行为的，有权要求您立即删除、修改相关内容，或纠正自身行为，同时百度智能云可以向主管部门举报、报告您涉嫌违法、犯罪的行为。进一步地，为阻断、屏蔽危害行为和保护百度智能云服务的正常运营，百度智能云有权限制、暂停向您提供全部或部分百度智能云服务，以及终止向您提供百度智能云服务，对您的百度智能云账号进行限制和冻结。

百度智能云采取上述措施导致您服务不可用、业务被暂停、数据被清理等后果及损失，均由您自行承担；您的行为给百度智能云或第三方造成损失的，您应当予以赔偿。百度智能云保留依照法律、法规及本协议追究您其他责任的权利。

13. 您需理解和同意，由于技术进步、服务优化、商业策略变动或遵循国家重要技术法规调整，百度智能云无法承诺持续无限期地提供某项服务。百度智能云保留修改服务方式、规格或其他相关方面（包括服务费用和计费方式）的权利。在进行此类变更或停止服务之前，百度智能云会尽可能提前通过网站公告、内部通知、电子邮件或短信等方式通知您。

🔗 用户业务数据和公开信息

1. 用户业务数据

1. 百度智能云理解并认可，您通过百度智能云提供的服务，加工、存储、上传、下载、分发以及通过其他方式处理的数据，均为您的用户业务数据，您完全拥有您的用户业务数据。

2. 您应对您的用户业务数据的来源及内容负责，百度智能云提示您谨慎判断数据来源及内容的合法性。因您的用户业务数据内容违反法律法规、部门规章或国家政策而造成的全部结果及责任均由您自行承担。

3. 就用户业务数据，百度智能云除执行您的服务要求外，不进行任何未获授权的使用及披露；但以下情形除外：

1. 在国家有关机关依法查询或调阅用户业务数据时，百度智能云具有按照相关法律法规或政策文件要求提供配合，并向第三方或者行政、司法等机构披露的义务；

2. 您和百度智能云另行协商一致。

4. 您可自行对您的用户业务数据进行删除、更改等操作。如您自行释放服务或删除数据的，百度智能云将删除您的在线数据，按照您的指令不再保留该等数据。就数据的删除、更改等操作，您应谨慎操作。

5. 当服务期届满、服务提前终止（包括但不限于双方协商一致提前终止，其他原因导致的提前终止等）或您发生欠费时，除法律法规明确约定、主管部门要求或双方另有约定外，百度智能云仅在一定的缓冲期（以您所订购的服务适用的专有条款、产品文档、服务说明等所载明的时限为准）内继续存储您的用户业务数据（如有）。缓冲期届满，百度

智能云将删除所有用户业务数据，包括所有缓存或者备份的副本，不再保留您的任何用户业务数据

6. 用户业务数据一经删除，即不可恢复；您应自行承担数据因此被删除所引发的后果和责任，您理解并同意，百度智能云没有继续保留、导出或者返还用户业务数据的义务。
7. 根据您与百度智能云协商一致，百度智能云在您选定的数据中心存储用户业务数据。百度智能云恪守对用户的安全承诺，根据适用的法律保护用户存储在百度智能云数据中心的数据。

2. 用户账户信息

1. 您的用户账户信息，包括您在登录百度智能云账户或订购、使用百度智能云服务时：
 - (1) 所填写或提交的包括公司名称、营业执照信息、姓名、性别、出生年月日、身份证号码、护照信息、电话号码、电子邮箱、地址（含邮政编码）、支付账号
 - (2) 百度智能云对服务过程的记录，包括您的账单、历史购买信息、咨询记录、报障记录以及排障过程等。
2. 因收集您的用户账户信息是为了向您提供服务及提升服务质量的目的，为了实现这一目的，百度智能云仅把您的信息用于下列用途，除非您和百度智能云另行协商一致或在国家有关机关依法查询或调阅：
 - (1) 向您提供您使用的各项服务，并维护、改进这些服务；
 - (2) 在符合相关法律法规的要求下，向您推荐您可能感兴趣的内容，包括但不限于向您发出产品和服务信息。

3. 用户支持数据

您理解并同意，为了及时响应您的帮助请求，保障云平台的整体安全，改进百度智能云的服务，百度智能云将检测、浏览、记录您的服务使用行为、您数据的不安全特征等用户支持数据。用户支持数据不包括用户业务数据和用户账户信息。

服务的开通、付费与终止

1. 您可通过您的百度智能云账户开通、使用服务。
2. 您可以通过预充值或后付费方式开通服务，开通后您获得百度智能云向您发送的登录、使用服务的密钥、口令即可使用服务，服务期限自开通之时起算。
3. 服务期限届满前，若您无理由擅自退订相应服务，百度智能云有权采取恢复原价计费、收取违约金或收取退订/退款手续费等方式进行处理，以相应官网展示页面或相应订单中载明的方式为准；
4. 服务期间收费方式、资源使用方式、服务届满未用尽资源的处理等，以相应产品或服务订单约定为准。
5. 您理解并认可，为技术升级、服务体系升级、或因经营策略调整或配合国家重大技术、法规政策等变化，百度智能云不保证永久的提供某种服务，亦可能变更所提供服务的形式、规格或其他方面，在终止该种服务或进行此种变更前，百度智能云将尽最大努力且提前以网站公告、站内信、邮件或短信等一种或多种方式进行事先通知；如终止提供该种服务的，百度智能云的提前通知将不短于30天，并且妥善处理后续事宜（包括但不限于您已缴纳但未消费的服务费用将退还至您的百度智能云账户）。
6. 发生下列情形之一的，服务期限提前终止：
 - 1) 双方协商一致提前终止的；
 - 2) 您严重违反本协议（包括但不限于，您严重违反相关法律法规规定，或您严重违反本协议项下之任一承诺内容等），百度智能云有权提前终止服务直至清除您的全部数据；
 - 3) 您理解并充分认可，虽然百度智能云已经建立（并将根据技术的发展不断完善）必要的技术措施来防御包括计算机病毒、网络入侵和攻击破坏（包括但不限于DDoS）等危害网络安全事项或行为（以下统称该等行为），但鉴于网络安全技术的局限性、相对性以及该等行为的不可预见性，因此如因您网站遭遇该等行为而给百度智能云或百度其他网络或服务器（包括但不限于本地及外地和国际的网络、服务器等）带来危害，或影响百度智能云与国际互联网或者其他特定网络、服务器及百度智能云内部的通畅联系，百度智能云可决定暂停或终止服务或其他必要的保护措施。

免责声明

1. 百度智能云不保证（包括但不限于）：
 - (1) 百度智能云适合所有用户的使用要求；

(2) 百度智能云不受干扰，及时、安全、可靠或不出现错误；及用户经由百度智能云取得的任何产品、服务或其他材料符合用户的期望。

(3) 您使用经由百度智能云下载或取得的任何资料，其风险由您自行承担；因使用本产品导致您的电脑系统损坏或资料流失，您应负全部责任；

2. 百度智能云保留您违反国家、地方法律法规规定或违反本服务协议的情况下中止或终止为您提供服务的权利，并保留向您追究相关法律责任的权利。

3. 您同意并授权百度智能云在您使用百度智能云服务时如有欺诈、发布或销售伪劣商品、侵犯他人合法权益或其他严重违反任意百度智能云服务规则的行为，有权直接终止向您提供服务、依法追究您的法律责任，并有权在百度关联网站范围内对此进行披露，您的百度智能云账号可能被直接注销，您可能因前述行为导致不能再使用任意一款百度PC端、App端产品，不能再登录任意一家百度网站，百度所有服务同时终止向您提供。

4. 您在使用百度智能云服务过程中，本协议内容、相关产品页面上出现的关于交易操作的提示或百度智能云发送到您手机的信息（短信或电话等）内容是您使用本服务的相关指引，您使用本服务即表示您同意接受百度智能云服务的相关指引、规则。您了解并同意百度智能云有权单方改进、调整百度智能云服务的相关规则，而无须征得您的同意，服务指引、规则以您使用服务时的页面提示（或发送到该手机的短信或电话等）为准，您同意并遵照服务指引、规则是您使用百度智能云服务的前提。

5. 百度智能云可能会以电子邮件（或发送到您手机的短信或电话等）方式通知您服务进展情况以及提示您进行下一步的操作，但百度智能云不保证您能够收到或者及时收到该邮件（或发送到该手机的短信或电话等），且不承诺对此承担任何后果。因此，在服务过程中您应当及时登录到相关产品服务网站查看和进行交易操作。因您没有及时查看或/和对服务状态进行修改或确认或未能提交相关申请而导致的任何纠纷或损失，百度智能云不承担任何责任。

6. 对由于您向百度智能云提供的联络方式有误以及您用于接收百度智能云邮件的电子邮箱安全性、稳定性不佳而导致的一切后果，您应自行承担责任，包括但不限于因您未能及时收到百度智能云的相关通知而导致的后果和损失。

7. 系统中断或故障 系统可能因下列状况无法正常运作，使您无法使用各项联网服务时，百度智能云不承担损害赔偿责任，该状况包括但不限于：

(1) 百度智能云在系统停机维护期间；

(2) 任何百度智能云所属设备以外的网络、设备故障或配置调整引起的；

(3) 因台风、地震、海啸、洪水、停电、战争、恐怖袭击等不可抗力之因素，造成百度智能云系统障碍不能执行业务的；

(4) 由于黑客攻击、电信部门技术调整或故障、网站升级、银行方面的问题等原因而造成的服务中断或者延迟；

(5) 客户维护不当或保密不当致使数据、口令、密码等丢失或泄漏所引起的；

(6) 客户的疏忽或由客户授权的操作所引起的；

(7) 客户未遵循百度智能云产品使用文档或使用建议引起的，如客户在控制台、API 或者 CLI 等控制方式对BCC实例进行停机、重启、卸载云磁盘等操作引起的不可用；

(8) 本地磁盘出现宕机数据会被擦除，依赖本地磁盘及本地磁盘中数据作为启动依赖项而导致的不可用；

(9) 由于客户所安装软件或者其他非百度智能云直接运营的第三方软件或者配置引起的 BCC 实例出现错误；

(10) 由于出价低于市场价或者库存不足导致的抢占实例被释放；

(11) 其他非百度智能云原因造成的服务不可用或服务不达标的情况。

(12) 由于您或您的代理人故意或过失导致您遭受损失的情况；

8. 如您使用的服务是第三方提供，第三方所提供之服务品质由该第三方自行负责。

9. 如有链接引导您离开百度智能云站点，链接的站点不在百度智能云的控制之内，百度智能云不对任何链接站点的内容、链接站点中包含的任何链接或此类站点的任何更改或更新负责。百度智能云不对源自任何链接站点内容负责。百度智能云仅为了

提供便利的目的而向您提供这些链接，但并不暗示百度智能云认可相应的第三方站点。

10. 在法律允许的情况下，百度智能云对于与本协议有关或由本协议引起的任何间接的、惩罚性的、特殊的、派生的损失（包括业务损失、收益损失、利润损失、使用数据或其他经济利益的损失），不论是如何产生的，也不论是由对本协议的违约（包括违反保证）还是由侵权造成的，均不负有任何责任，即使事先已被告知此等损失的可能性。另外即使本协议规定的排他性救济没有达到其基本目的，也应排除百度智能云对上述损失的责任。
11. 鉴于网络服务的特殊性，您同意百度智能云在有正当理由的情况下可以随时变更、中断或终止部分或全部的服务，也无需向您承担任何责任。但是，百度智能云会尽可能事前通知您，以便您做好相关数据的转移备份以及业务调整等，以保护您的合法权益。
12. 为保证服务的安全性和稳定性，百度智能云可能对您使用的机房、服务器、宽带、数据库等产品进行不定期的检修、维护、升级、迁移等，如因此类情况造成相关服务在合理时间内中断或暂停的，百度智能云无需为此向您承担任何责任。当涉及重大变更（如机房迁移），百度智能云将尽最大努力通知您，您应予以配合，您理解并同意百度智能云可能会终止您的服务并将您已支付但未消费的款项退还至您的账户。
13. 您理解并同意：百度智能云的服务是按照现有技术和条件所能达到的现状提供的。百度智能云会尽最大努力向您提供服务，确保服务的连贯性和安全性；但百度智能云不能保证其所提供的服务毫无瑕疵，也无法随时预见和防范法律、技术以及其他风险，包括但不限于不可抗力、病毒、木马、黑客攻击、系统不稳定、第三方服务瑕疵、政府行为等原因可能导致的服务中断、数据丢失、数据泄露或被窃取以及其他的损失和风险。所以您同意：即使百度智能云提供的服务存在瑕疵，但上述瑕疵是当时行业技术水平所无法避免的，其将不被视为百度智能云违约，同时，由此给您造成的数据或信息丢失等损失百度智能云将予以免责。
14. 您理解并同意：在使用本服务的过程中，可能会遇到不可抗力等风险因素，使本服务发生中断。出现上述情况时，百度智能云将努力在第一时间与相关单位配合，及时进行修复，但是由此给您造成的损失百度智能云将予以免责。
15. 您理解并同意：您在百度智能云主机安装使用过程中，自行安装盗版软件、系统、数据资源，造成自身损失的，百度智能云不承担任何责任。您自身的行为导致百度损失的，百度保留追偿权。

🔗 知识产权

1. 百度智能云所有的产品、技术与所有程序均属于百度公司的知识产权。“百度智能云”、百度智能云其他产品服务名称及相关图形、标识等为百度智能云的注册商标。未经百度智能云及百度公司的许可，任何人不得擅自（包括但不限于：以非法的方式复制、传播、展示、镜像、上载、下载）使用。否则，百度智能云及百度公司将依法追究法律责任。
2. 在本协议项下一方向对方提供的任何资料、技术或技术支持、软件、服务等知识产权均属于提供方或其合法权利人所有；除提供方或合法权利人明示同意外，另一方无权复制、传播、转让、许可或提供他人使用上述知识成果，否则应承担相应的责任。
3. 您应保证提供至百度智能云的各项信息、上传至百度智能云服务上的全部数据、对百度智能云服务的使用，以及使用百度智能云服务所涉及的素材或产生的相应成果不会侵犯任何第三方的合法权益；如有第三方就您所提供、上传或使用的信息、数据或就您的行为及工作成果向百度智能云提起任何投诉、索赔、诉讼或其他类型的诉求，则您理解并确认，您应立即出面解决，并应赔偿百度智能云因此遭受的全部经济损失，包括但不限于各种费用、赔偿支出等。
4. 如果第三方机构或个人对百度智能云服务的知识产权归属提出质疑或投诉，您应及时告知百度智能云，百度智能云将进行处理。
5. 您向百度智能云提供的材料或者在任何百度网站上发布的材料、您向百度智能云提供的资料（包括反馈和建议），或者张贴、上传、输入或提交给任何服务或其关联服务供一般公众或任何公共、私有社区成员查看的资料（以下称您的提交资料），如果您张贴、上传、输入、提供或提交（以下简称“张贴”）您的提交资料，即表明您授予百度智能云及其关联公司、必要的分许可的被许可人使用与其互联网业务（包括但不限于所有的百度服务）运作相关的提交内容的权利，包括但不限于以下许可权利：复制、分发、传送、公开展示、公开执行、复制、编辑、翻译和重新排印您的提交资料；以及向服务的任何供应商分许可此类权利的权利。

🔗 保密条款

1. 您与百度智能云郑重承诺，除本协议约定的情形外，一方不会将在合作过程中将了解到的有关对方的保密资料，以任何形式透露给第三方，并严格限制接触保密资料的员工遵守本条之保密义务。
2. 双方同意尽最大的努力保护保密资料等不被披露。一旦发现有保密资料泄露事件，双方应合作采取一切合理措施避免或者减轻损害后果的产生。
3. 上述保密义务不因本协议的变更、解除或终止而终止。
4. 本协议项下的保密资料是指：
 - a) 与项目有关的任何协议、往来传真或邮件等纸质或电子版材料，包括本协议的内容和条款（特别是百度智能云为您提供的折扣或优惠信息）；
 - b) 价格、财务及营销规划、客户资料、未发布产品、商业计划、行销信息、投资信息、财务状况、图纸、设计思想、技术诀窍、计算机程序、源代码、研究方案及其他资料；
 - c) 在披露之时或之前，披露方以文字或标识指定为商业秘密的信息及文件；
 - d) 其它符合法定商业秘密构成要件的信息。
5. 本条款不适用于以下内容：
 - a) 已进入公众领域的信息；
 - b) 信息接收方通过正当方式取得的、非保密性的、同行业普遍了解的信息；
 - c) 信息接收方在信息披露前已知的、且无义务保密的信息；
 - d) 由第三方披露的且信息接收方经最审慎判断认为无须保密的信息；
 - e) 信息接收方独立开发的信息；
 - f) 信息披露方以书面形式同意信息接收方披露的保密信息；
 - g) 应第三方招投标要求，将本协议本身提交第三方并说明仅限投标使用的；
 - h) 为提供您所要求的服务，百度智能云在合理和必要的程度内向第三方分享您的数据；
 - i) 按法律要求需向任何机关、机构公开的内容。

🔗 其他

1. 本协议一经公布立即生效，百度智能云有权随时对协议内容进行修改，修改后的结果以消息推送、网页公告等方式公布于百度智能云网站上，而无需另行单独通知您。如果不同意百度智能云对本协议相关协议所做的修改，您有权停止使用网络服务。若您继续使用网络服务，则视为您接受百度智能云对本协议相关协议所做的修改。
2. 百度智能云拥有对本协议项下的各类优惠活动包括但不限于邀请码、代金券的合理处理权。
3. 本协议项下百度智能云对于您所有的通知均可通过工单、网页公告、站内信、电子邮件、手机短信或其他形式等方式进行；该等通知于发送之日视为已送达收件人。
4. 本协议的订立、执行和解释及争议的解决均应适用中国法律（为本协议之目的，不包括香港、澳门特别行政区和台湾地区法律，也不使用冲突法）。如双方就本协议内容或其执行发生任何争议，双方应尽量友好协商解决；协商不成时，任何一方均可向北京市海淀区有管辖权的人民法院提起诉讼。
5. 本协议构成双方对本协议之约定事项及其他有关事宜的完整协议，除本协议规定的之外，未赋予本协议各方其他权利。
6. 如本协议中的任何协议无论因何种原因完全或部分无效或不具有执行力，本协议的其余部分仍应有效并且有约束力。

百度智能云线上订购协议

🔗 1. 简介

1. 本百度智能云线上订购协议是百度智能云官网（cloud.baidu.com）的经营者北京百度网讯科技有限公司（以下简称为“百度智能云”），与您或您所代表之实体（“您”或“您的”）共同缔结的对双方具有约束力的有效合约。您通过签字、盖章、网络页面勾选、点击确认、进行下一步操作或以其他方式选择接受本协议，或事实上使用百度智能云产品服务时（以较早发生者为

准)，即表示您与百度智能云已达成协议并同意接受本协议的全部约定内容。如若双方签字、盖章文本与网络页面点击确认或以其他方式选择接受之服务条款文本有冲突，冲突之处以双方签字、盖章的协议约定为准。

2. 如本协议的内容发生重大变动，百度智能云将提前通过网站页面、站内信、邮件或其他百度智能云认为有效的方式通知您。如您不同意相关条款的修改，您有权停止使用百度智能云的服务，您应通知百度智能云终止服务，并自行负责将业务数据迁出，百度智能云与您进行服务费结算（如有）。如您继续使用服务，则视为您接受修改。
3. 在接受本服务条款之前，请您仔细阅读本服务条款的全部内容。关于本协议，提示您特别关注限制或免除责任的条款、百度智能云对您违规、违约行为的认定处理条款，以及开通或使用特定产品服务时针对该等产品服务的产品服务规则。如果您不同意本协议的任何内容或者无法准确理解本协议相关条款，您可以先行向百度智能云相关业务部门进行询问，在得到百度智能云解释说明之前，建议您不要进行后续操作。您使用本协议项下任一产品服务即视为您已阅读并同意本协议的约束。您接受本协议将视为您已经仔细阅读并理解本协议的全部内容。届时您无权以未阅读本协议的内容或者未获得服务方对您询问的解答等理由，主张本协议无效，或要求撤销本协议。

2. 定义

1. “本协议”包括本百度智能云线上订购协议正文、订单、百度智能云官网（cloud.baidu.com）所示《百度智能云用户服务协议》，以及产品服务规则。
2. “产品服务”也称为“百度智能云产品服务”或简称为“服务”，是指百度智能云根据本协议、订单向您提供的各项技术服务。具体信息请参见百度智能云官网及及相关产品服务规则。
3. “产品服务规则”是指百度智能云通过百度智能云官网\管理控制台或任何其他方式公布并可根据业务需要随时更新的，与百度智能云提供的产品服务相关的任何文档、协议、规则、条款等，包括但不限于产品表述、产品定价、操作指南、产品服务等级协议（SLA）、赔偿标准等。
4. “工作日”是指中国大陆法定工作日。
5. “订单”是指您确认向百度智能云购买产品服务的订购文件，其中含有购买的产品服务名称、服务期限、配置、计费方式、金额、对账方式等信息。
6. “协议金额”是指根据本协议、构成本协议的其它文件（如订单、补充协议等）约定，您应付给百度智能云的款项。

3. 声明陈述与保证

您与百度智能云分别向对方声明、陈述和保证：

1. 您签署本协议即表示您确认并保证您有权签署本协议并已经获得履行本协议所需要的全部资质、许可和授权；同时保证将签署或获得一切必需的文件或许可，并采取一切必要的行动以使本协议规定的条款顺利履行。
2. 您确保您签署并履行本协议符合现行有效的法律法规或对业务运作有重大影响的任何法院、管理机构或政府组织的任何判决、裁定或规定，本协议亦不损害任何第三方的合法权益。
3. 在本协议期限内，您或者百度智能云任何一方若与第三方发生合并、并购、主体变更等事件，任何一方的承继主体应继续履行本协议项下该方未完成的义务。
4. 若本协议与《百度智能云用户服务协议》存在相冲突的约定，应以本协议的约定为准。
5. 除非本协议明确授权，您或者百度智能云任何一方均无权代表对方进行抵押、做出任何声明、授权签约或以任何方式代表对方创设任何义务或责任。
6. 对于百度智能云提供的产品服务，您确认将：1) 配合、协助百度智能云提供该等产品服务，包括提供权限使百度智能云可以进入您的场所以提供相关服务等；2) 及时回应百度智能云为完成提供产品及相关服务所需的回应；3) 在百度智能云提供产品服务之前获取相应的许可、同意、批准或授权。
7. 您应在签署本协议时已明确了解百度智能云所提供服务内容并知悉[百度智能云官网](#)所示关于所提供服务的介绍、产品服务等级协议（SLA）、技术文档等全部产品服务规则。百度智能云应确保所提供的产品服务符合适用法律的要求以及官网所示文件。除此之外，百度智能云不对本协议下所提供产品服务做出超出法律法规、本协议约定以及官网所示文件的陈述和保证，

包括不保证产品服务符合特定质量或满足特定用途等。

8. 您应保障承载百度智能云产品服务的基础网络及物理环境安全。除本协议另有明确约定外，您不得进行以下行为：1) 对百度智能云提供的产品服务进行反向工程、软件破解等行为；2) 对百度智能云提供的产品服务进行完整性破坏；3) 超出授权范围的非授权使用；4) 对百度智能云提供的产品服务进行后续开发或创作衍生作品；5) 出租、出借、分销或以其他方式向他人提供百度智能云的产品服务；6) 删除百度智能云产品服务中的所有权声明；7) 不当使用百度智能云产品服务致使侵犯他人知识产权或其他权利，或者致使违反任何法律的规定。
9. 如因您实施上述上一条中列示的行为而产生任何法律责任，均应由您承担。对百度智能云造成损失的，您应予以向百度智能云赔偿。如果您违反上述约定对百度智能云提供的产品服务进行后续开发或创作衍生作品的，与之相关的知识产权等权利归百度智能云所有。
10. 您不应在百度智能云服务或平台之上安装、使用存在知识产权合规问题或瑕疵的软件；您理解并同意，百度智能云有权拒绝使用存在知识产权合规问题或瑕疵的相关应用系统在百度智能云服务或平台之上部署。您应对自己行为（如自行安装的软件和进行的操作）所引起的结果承担全部责任。如因您自行安装相关软件的合法著作权人向百度智能云提出侵权投诉、指控或其他主张，您应当采取一切合理措施以保证百度智能云免责，包括但不限于进行情况澄清、提供合规软件许可证明，以及其他足以使合法著作权人撤回其前述主张的措施。若百度智能云的服务涉及第三方软件之许可使用的，您同意遵守相关的许可协议的约束；
11. 您承诺不从事其他违法、违规或违反本服务以及百度智能云官网公布之相关管理规范及流程的行为。
12. 如百度智能云发现您违反上述条款的约定，有权根据情况采取相应的处理措施，包括但不限于立即删除相应信息、中止服务或终止服务等。如果第三方机构或个人对您提出质疑或投诉，百度智能云将通知您，您有责任在规定时间内进行说明并出具证明材料，如您未能提供相反证据或您逾期未能反馈的，百度智能云将有权采取包括但不限于立即删除相应信息、中止服务或终止服务等处理措施。因您未及时更新联系方式或联系方式不正确而致使未能联系到您的，亦视为您逾期未能反馈。

您的权利义务

1. 您可以在法律允许的范围内享受百度智能云按照现有技术以及条件标准提供的服务，并享有百度智能云的技术支持、咨询等服务。具体服务标准参见百度智能云官网公布的产品服务等级协议（SLA）及百度智能云官网公布的其他规范或本协议的约定。
2. 除非双方另有书面约定，您确认并同意百度智能云向您提供的任何资料、软件、数据等的权利属于百度智能云。您无权传播、转让、许可或提供他人使用这些资源，否则应承担相应的责任。
3. 您如更改与百度智能云产品服务相关的配置，应至少提前5（五）个工作日通知百度智能云。
4. 如您网站遇到流量异常情况，或您网站遭受到来自第三方的网络攻击等黑客行为时，您应及时与百度智能云进行沟通。上述情况导致百度智能云提供的产品服务品质受影响的，百度智能云不承担赔偿责任。
5. 如为实现本合同目的需提供相关信息、资料，您确认您提交的信息、资料真实、准确、完整、及时，否则，百度智能云有权拒绝提供相关服务，因此给百度智能云或第三方造成损失的，由您承担全部责任。
6. 您确保其提供的原始数据和资料来源合法合规，不侵犯任何第三方的合法权益，对于需要获得第三方明示同意或授权的已经取得相应证明。如果您提供的原始数据和资料存在侵犯第三方权益的情形，由此引起的一切责任由您承担。若您提供的原始数据中包含其终端用户或任何第三方的相关个人信息（包括但不限于用户或第三方的个人信息、mac地址、IMEI、idfa），您保证其收集和提供上述信息的行为已遵循合法、正当、必要的原则，已明示收集、使用信息的目的、方式和范围且已获得对应自然人的明确授权。百度智能云有权对您获得授权的情况进行核查，您应予配合。您同意百度智能云有权在为您提供本合同所述服务及优化本合同所述服务效果的范围内对数据进行处理。
7. 您理解并同意，您主动删除的数据无法复原，且当百度智能云提供产品服务的服务器整机下架或故障硬盘下架时会进行数据清除工作，相关数据将无法复原。您应对您自有数据以及基于百度智能云产品服务搭建的业务系统进行备份。如遇百度智能云在必要时对您提供服务所在的底层物理设备进行下架或迁移等工作时，您应在得到百度智能云通知后，采取相应技术措施。如您得到通知但未采取措施而造成的后果由您自行承担。
8. 您应自行对因使用百度智能云产品服务而存储在百度智能云服务器的各类数据等信息合法性负责，并采取合理、安全的技术

措施，以确保其安全性和完整性。您对自行采取的相关行为（包括但不限于违反法律法规、部门规章或国家政策、欠费、自行安装软件、采取加密措施或进行其他安全措施等）所引起的结果承担全部责任。

9. 您对自己存放在百度智能云百度智能云平台上的数据以及进入和管理该平台上各类产品与服务的口令、密码等等完整性和保密性负责，您账号下发生的行为将全部视为您行为。因您自身维护不当或保密不当所引起的一切损失和后果均由您自行承担。

10. 您应当按照本协议约定的时间支付协议金额。如未在约定时间付款，百度智能云有权要求您承担逾期付款的违约金责任，并有权单方面暂停或终止向您提供服务，同时保留向您追讨欠款及违约责任的法律权利。

11. 在您接受本服务时，若我们为您提供了付款账期（信用额度）服务，您应明确了解并同意以下条款：

11.1 您承诺在约定的付款账期内按时支付应缴费用。

11.2 若您未能按照约定期限支付费用，我们将视为您违约。在此情况下，我们有权单方面终止为您提供的相关服务，并保留追究您违约责任的权利，包括但不限于要求您立即支付未付费用、滞纳金以及由此产生的其他损失。

11.3 若因您的资信状况或其他客观情况（包括但不限于行业风险等）发生变化，导致我们认为有必要调整您的付款账期或要求您提前还款的，您同意我们有权单方面做出此类决定，并通过适当方式通知您。您确认会遵照执行，无任何异议。

12. 双方确认开具发票为附随义务，我方未开票不影响您履行付款义务。

13. 您出具合同约定的验收文件等材料，即表示您确实真实收到了我方交付的产品/服务，我方已经按照合同约定合格履行完对应合同义务，交付标的满足您及合同约定的验收要求，不存在任何未收到货/未完成验收/交付或验收存在瑕疵的情况。若有存在任何未收到货/未完成验收/交付或验收存在瑕疵下，您出具前述文件的情况，一切不利后果由您自行承担。

14. 您知悉只有加盖我方公章/合同章的协议才具备法律效力，我方员工没有权利代表我方做出任何超出加盖公章或合同专用章的合同内容的承诺或与加盖公章或合同专用章的合同内容约定不一致的承诺，如有、不具备任何法律效力。

15. 您知悉，我们为您提供产品（包括但不限于软件、硬件、技术等）可能受中国、美国、欧盟及其成员国、英国、联合国等及其他适用法域监管机构所管理、颁布或执行的出口管制与经济制裁法律法规的管辖。您同意遵守所有可适用的出口管制法律和法规，不会将本合同产品直接或间接出口、再出口、转移、销售、许可、披露或以任何形式提供给受限制的国家、地区、实体（包括但不限于下一条制裁清单中实体）或个人，亦不得用于某些受限制的用途。

16. 您承诺本协议签订时您公司从未被列入任何制裁名单（或被任何制裁名单上的一个或多个当事方直接或间接拥有 50% 或以上的股权）。制裁名单包括但不限于美国实体清单，美国未经核实清单，美国被拒绝人清单，美国军事最终用户清单，美国美国财政部海外资产控制办公室（“OFAC”）维护的各类清单，包括 SDN 清单、NS-CMIC 清单、SSI 清单等，美国《维吾尔强迫劳动预防法》实体清单，欧盟委员会“欧盟金融制裁综合清单”，欧盟理事会第 833/2014 号条例项下附件 IV 清单及附件 XIX 清单，欧盟理事会 765/2006 号条例项下附件 V 清单，英国财政部金融制裁实施办公室“英国金融制裁目标综合清单”。

17. 您确认购买产品系出于自身正常生产经营的需要以及民用/民用最终用户的需求，不涉及军事目的或恐怖主义目的，不会被用以扰乱国际和平与安全/或适用贸易管制法所禁止的任何其他最终用途。购买产品不会被您直接或最终用户以设计、研发、生产、储存或以任何方式使用大规模杀伤性武器，如核能、化学或生物武器、导弹，或任何支持此类武器或导弹技术的活动。

18. 您同意不会直接或间接出口、再出口、转移、销售、许可、披露或以任何形式向恐怖分子及组织，古巴、伊朗、朝鲜、苏丹、俄罗斯以及叙利亚等国的实体或个人提供我方交付的产品。您应根据现行法律法规持续记录、留存产品在出口、再出口和转售过程中有关目的地、最终用户、最终用途的信息，并根据我们的合理要求提供上述信息。

19. 如出现以下任一情形，则您应立即书面通知我们，并应尽最大努力采取补救措施：（1）任何与上述确认不一致、相冲突，或使得任何上述确认不完整、不准确或具有误导性的情况；（2）您方、您方关联方、任何下游客户或最终用户未履行或未完成履行任何上述承诺；或（3）您方、您方关联方、任何下游客户或最终用户受到了出口管制与经济制裁法律法规下的任何处罚、主张、索赔、诉讼、程序或调查。

20. 若因中国、美国、欧盟及其成员国、英国、联合国等及其他适用法域监管机构的出口管制等相关政策发生变化导致本合同无法履行，我们有权免责终止合同，不承担违约责任。

☞ 百度智能云的权利义务

1. 百度智能云为您提供订单或官网控制台所下订单的产品服务。
2. 百度智能云有权按照协议约定收取相应费用，百度智能云有权要求您提供开具发票所需资质。如因您原因未能提供或延迟提供发票资质，而造成发票延迟交付的，百度智能云不承担责任。
3. 在百度智能云向您提供产品服务期间，百度智能云应保障您应享受得到的服务。因您原因造成的百度智能云提供的产品服务中断，您应认同不属于百度智能云责任。除应当地法律法规、或政府监管部门的监管、审计要求或线上协议等产品文档中明确说明的产品，您的所有数据、应用及行为日志不会提供给任何第三方。
4. 百度智能云有权监督您利用百度智能云提供的产品服务从事的活动是否经过国家相关部门的认可、批准及备案。如百度智能云发现您有违反本协议或有违法、违规行为，或百度智能云接到国家机关或相关机构（包括但不限于公安机关、人民检察院、人民法院、通信管理局等）通知要求对您采取相应措施，或上述国家机关或相关机构已经对您采取法律措施，或百度智能云收到第三方权利人对于您的主张时，百度智能云有权在通知您后暂停本协议或订单项下的服务或直接采取一切百度智能云认为必要的措施（如终止提供服务）以减轻对百度智能云的不利影响。待上述机关查清问题处理完毕后再继续履行协议或者提出终止协议。百度智能云不对因此给您造成的损失负责。如因前述原因给百度智能云造成相应损失，则该损失全部由您承担。
5. 如变更、中断或终止的网络服务属于免费网络服务，百度智能云无需针对您进行单独通知。
6. 百度智能云需要定期或不定期地对提供网络服务的平台或相关的设备进行检修或者维护，可能造成收费网络服务在合理时间内的中断。百度智能云对此无需承担责任，但百度智能云应尽可能事先通知您。
7. 百度智能云仅负责操作系统以下的底层部分及百度智能云提供的软件的运营维护，例如：云服务器的相关技术架构及操作系统等。操作系统之上部分（如您在系统上安装的应用程序）由您自行负责。此外，您自行升级操作系统可能会造成宕机等不良影响，建议您谨慎操作。
8. 百度智能云提供的产品服务可能配置具有数据备份功能的工具，但除您与百度智能云另有书面约定外，该等工具并非百度智能云所提供服务的组成部分，不对您使用或不能使用该等备份工具负责。您应自行负责数据备份，并自行完成相应操作。百度智能云不对您自行进行的数据备份工作或结果承担任何责任。
9. 您理解并认可，百度智能云根据服务的特性、您所购买的规格等，向您提供相关服务功能，您应认真阅读关于相关服务的使用文档及相关说明；您进一步同意，如果您所使用的服务超过您购买的服务规格，百度智能云有权对您的服务进行适度调整或暂停。
10. 如果您使用百度智能云提供的整体安全防护服务及管理监测相关功能及服务，您理解，尽管百度智能云对该等服务经过仔细测试，但不能保证其与所有的软硬件系统完全兼容，亦不能保证其软件及服务完全没有错误。如果出现不兼容及软件错误的情况，请您关闭或停止使用相关功能，或拨打技术支持电话，获得百度智能云的技术支持。
11. 您理解并认可，百度智能云在必要时可能会将您的云服务器进行机房迁移。百度智能云在上述操作前将尽可能提前通知您，您知悉，上述操作可能需要修改您相关域名的DNS，您在接到通知后应按要求将DNS修改到百度智能云指定IP上，否则可能造成网站无法访问，这种情况下，不视为百度智能云违约。
12. 在不披露您保密信息的前提下，在本协议有效期内，百度智能云可以就您使用百度智能云服务的情况作为使用范例或成功案例用于百度智能云自身及/或业务的宣传与推广，在这类宣传推广中，百度智能云有权使用您的名称、企业标识等；除此之外，未经您书面许可，百度智能云不得擅自使用您企业名称、企业标识等。

☞ 结算方式

1. 预付费结算

- 若您购买的为先付费后使用的服务，百度智能云将在您支付全部服务费后为您提供服务；若您未及时支付，下单后7天订单自动失效；若到期后您希望继续使用该服务，需提前支付续费款项延续服务。
- 您使用百度智能云产品服务前需预充值，购买服务时百度智能云从您账户中扣除服务款项，如您账户中金额不足以支付服务款项，百度智能云保留拒绝为您提供服务的权利。

2. 后付费结算

若您购买以按量或者按次等付费形式的服务，您可先开通服务，百度智能云将根据服务类型的不同，以小时、天、周或者月等周期（具体以相关产品页面及下单时对应内容为准）自动计算上一个计费周期的使用量，并从您的百度智能云账户余额中扣除相应的服务费用，您的百度智能云账户余额不足以抵扣的，百度智能云有权从第一次扣费失败之日（即：不足以抵扣对应的结算周期结束之日的次日）起要求您支付逾期付款的违约金和/或利息，并同时有权随时终止您已经订购的相关服务。具体扣费规则以及计费项以百度智能云官网页面公布为准。

3. 百度智能云为您提供余额不足提醒服务，具体提醒服务及处理方式详见百度智能云官网，百度智能云不对该等提醒服务的及时性、准确性负责，具体余额仍以您在百度智能云平台账号内实时查询内容为准。您因百度智能云账户余额不足而服务停止，以及由此产生的相关损失，百度智能云不承担任何责任。但这并不意味着百度智能云需要为您逾期付款造成的后果承担任何责任，您作为账户的使用人及管理者仍应当及时检查您的百度智能云账户余额并按照您的运营计划补充余额。
4. 您使用百度智能云服务的情况若在我方后台有记录的，则您同意，使用情况以百度智能云后台记录为准。
5. 百度智能云官网会不定期推出优惠活动，活动内容及使用发放均以百度智能云官网公布为准。
6. 充值。您可通过支付宝、百付宝、网上银行或银行汇款等途径将服务费充值到您百度智能云的账户中，支付方式及其他具体规则以百度智能云官网展示为准。
7. 发票申请。您可向百度智能云申请开具发票，具体申请要求、发票内容、开票金额及开票流程参见百度智能云官网。

🔒 保密义务

1. 一方从另一方所接受的信息，如有标明或可以合理认知为属于披露一方的机密或专有信息(以下称“保密信息”)，该方须对该保密信息保密，且未经披露一方同意，不得披露该信息。接受方应以对待其本身机密或专有信息相同的注意程度处理。为保持本协议之机密性，双方均视为本协议中信息的接受方。披露方同意，接受方可以将保密信息提供给为进行拟定产品服务需要获知该等保密信息的接受方代表，但接受方应确保获得保密信息的接受方代表对保密信息承担与本协议下同样的保密义务。
2. 如接受方因法律程序要求或需要而披露任何信息时，接受方应立即通知披露方，以使披露方可寻求适当之保护措施，但披露方未及时答复或者根据法律要求和监管要求不得提前通知的除外。
3. 接受方为向行政管理部门、行业协会等申请某项业务资质、获得某项认定、或符合国家、行业标准/认证，需结合对方情况向前述机构提交材料或进行说明的，在该等情况下，披露方应秉持必要情况下最少披露原则及要求因此获知保密信息的机构按不低于本服务条款的标准予以保密。
4. 为管理及执行本协议及提供产品服务的目的，百度智能云可处理由您提供的信息，包括在百度智能云的数据库中储存此类信息。
5. 接受方应尽最大的努力保护上述保密信息不被披露。一旦发现有上述保密信息泄露事件，双方应合作采取一切合理措施避免或者减轻损害后果的产生。

🔒 知识产权

1. 除了本协议明确授予对方使用的权利以外，双方各自保留本协议项下各自提供的相关产品的所有权，以及其中所包含或与之相关的任何知识产权，包括但不限于著作权、专利权和商标权等。
2. 未经对方事先同意，任何一方不得擅自使用、复制对方的商标、标志、商业信息、技术及其他资料。任何一方从对方获得的知识产权授权许可均不得用于超出本协议约定的目的和范围以外的其他用途。
3. 百度智能云在为您提供服务期间所使用、取得的技术资料、统计数据及进行技术改进的方法和成果，其所有权和知识产权归百度智能云所有，事先未经百度智能云书面同意，您不得私自将其提供给任何第三方。在本协议签订前由百度智能云享有的一切权利，在本协议签订后仍归百度智能云所有。
4. 百度智能云拥有百度智能云产品和服务享有的专有权利，您不得擅自对百度智能云产品和服务相关的软件产品、程序、代码、平台等进行逆向工程、反编译、解体拆卸或任何试图发现该软件工程程序、获取源代码的行为，不得以百度智能云产品和服务相关的软件及其技术为基础或前提进行修改、升级、改造或开发其他新软件或新技术，也不得以任何其他方式进行可

能损害百度智能云专有权利的行为。

5. 如百度智能云在提供定制服务时涉及使用您的公司Logo、喷漆图案或者在软件中设置唤醒词等情形，您同意向百度智能云授予实施定制服务所需的商标许可等知识产权，并且确保所要求的定制内容不会侵犯他人合法权益以及不会违反任何法律法规的规定。如您的定制需求内容侵犯他人合法权益或违反法律法规的规定的，产生的法律责任由您承担，对百度智能云造成损失的，您应予以赔偿。

🔗 违约赔偿责任与免责

1. 如果一方未按照本协议的规定履行其在本协议下的任何义务、保证或承诺，或在有效期内明确表示（通过口头、书面或行为）其将不履行本协议下的任何义务，且经过另一方要求补救的通知后在10（十）日之内没有进行有效补救的，或者该违反行为无法补救而给对方的利益造成损害或导致合作业务无法继续进行，则构成对本协议的违约，违约方应对由于其违约所引起的另一方的损失承担违约赔偿责任。
2. 如果确因百度智能云原因造成您不能正常使用百度智能云产品服务的，百度智能云向您赔偿相应损失。具体赔偿标准参见百度智能云官网公示。
3. 如果确因百度智能云原因造成您不能正常使用百度智能云产品服务的，且百度智能云官网或百度智能云提供的其他资料未有赔偿标准约定的，百度智能云按照如下标准赔偿：每逾期1（一）日，应向您支付逾期交付产品或服务所对应金额的0.5‰（万分之五）的违约金，百度智能云逾期交付超过30（三十）日的，您有权解除协议，但因您原因导致逾期交付的除外。如您延迟付款，每逾期一日，应向百度智能云支付应付产品或服务费总金额0.5‰（万分之五）的违约金；逾期超过30（三十）日的，您应支付本协议总金额或对应订单金额10%（百分之十）的违约金，赔偿给百度智能云造成的全部损失，并应继续支付百度智能云已交付项目成果对应的协议金额，且百度智能云有权暂停服务或单方终止协议。
4. 您应遵守本协议、订单相关的规则、规范等，并对涉及的折扣优惠内容予以保密，否则，百度智能云有权单方中止/终止向您提供本协议及/或订单约定的部分或全部服务，并要求您全额赔偿因其违反本条约定给百度智能云所造成的损失。
5. 在履行本协议时，百度智能云对因第三方的作为或不作为而给您或者其他第三方造成的损失不负责任。
6. 在任何情况下，百度智能云不对任何间接性、后果性、惩戒性、偶然性、特殊性的损害，包括您使用百度智能云服务而遭受的利润损失承担责任。
7. 任何情况下，百度智能云对本协议所承担的违约赔偿责任总额不超过违约产品服务对应之协议总额。如线下协议另有约定的，则以线下协议约定为准。

🔗 不可抗力和意外事件

1. 因不可抗力或者其他意外事件，使得本服务条款的履行不可能、不必要或者无意义的，遭受不可抗力、意外事件的一方不承担责任。
2. 不可抗力、意外事件是指不能预见、不能克服并不能避免且对一方或双方当事人造成重大影响的客观事件，包括但不限于自然灾害如洪水、地震、瘟疫流行等以及社会事件如战争、动乱、政府行为、电信主干线路中断、黑客、网络堵塞、电信部门技术调整和政府管制等。
3. 在不可抗力影响消除后的合理时间内，如果您和百度智能云均存在履约能力且确有继续履行必要的，应当继续履行协议。

🔗 合同的变更与终止

1. 发生下列情形，服务期限提前终止

（1）双方协商一致提前终止的；

（2）您严重违法本服务条款,包括但不限于（a）您未按照约定履行付款义务，及/或（b）您严重违法法律规定，及/或（c）您严重违法本协议中的承诺条款等），百度智能云有权提前终止服务；

2. 您理解并充分认可，虽然百度智能云已经建立（并将根据技术的发展不断完善）必要的技术措施来防御包括计算机病毒、网络入侵和攻击破坏（包括但不限于DDoS）等危害网络安全事项或行为（以下统称该等行为），但鉴于网络安全技术的局限性、相对性以及该等行为的不可预见性，因此如因您网站遭遇该等行为而给百度智能云及其他网络或服务器（包括但不限于

本地及外地和国际的网络、服务器等)带来危害,或影响百度智能云与国际互联网或特定网络、服务器及内部的通畅联系,百度智能云可决定暂停或终止服务。如果终止服务的,百度智能云将按照实际提供服务计算您已使用的并将剩余款项(如有)返还您;

3. 您认可并同意,为技术升级、服务体系调整或经营策略调整等需要,百度智能云可提前30天通过网页公告或给您发网站内通知或邮件通知等方式,决定暂时或终止向您提供服务(或服务中的部分功能)。该情况下,百度智能云应将您已支付但未消费的款项退还给您。
4. 本协议需在法律法规规定的范围内执行,如果本协议部分条款内容与法律、政策、监管要求相抵触,该部分条款自动废止,并不影响其它条款的有效性和可执行性。您同意百度智能云将根据法律规定和业务需要,重新约定相应内容;如因法律、政策、监管原因导致本协议无法进行的,您同意百度智能云提前解除本协议,您和百度智能云互不承担违约责任。

🔗 争议解决

1. 本协议的订立、效力、解释、履行和争议的解决均适用中华人民共和国法律管辖。
2. 双方约定,因执行本协议所发生的争议或与本协议有关的一切争议,双方应通过友好协商解决。如在30(三十)日内仍协商不成时,任何一方可向北京市海淀区有管辖权的人民法院提起诉讼。本协议适用中华人民共和国法律。
3. 除争议事项外,双方应继续行使其各自在本协议项下的其他权利并继续履行其各自在本协议项下的其他义务。

🔗 其他

1. 本协议未尽事宜以百度智能云官网公布的信息为准。
2. 百度智能云对产品服务相关的各类优惠活动(包括但不限于邀请码、代金券),以对外公布的策略为准,如果您对活动策略有疑问的,您可以通过活动页面公示的联系方式进行垂询。
3. 本协议项下百度智能云对于您所有的通知均可通过网页公告、站内信、电子邮件、手机短信或其他百度智能云认为有效的方式进行;该等通知于发送之日视为已送达。
4. 除非法律另有规定,本协议任何一方未能行使或迟延履行本协议项下的权利并不构成对该等权利的放弃;单独或部分行使该等权利不应阻碍任何其他权利、权力或特权的行使。
5. 本协议中的任何条款无论因何种原因完全或部分无效或不具有执行力,本协议的其余条款仍应有效并且有约束力。
6. 未经百度智能云事先书面同意,您不得转让或让与本协议或本协议项下您的任何权利和义务。违反本条约定进行的任何转让或让与无效。
7. 如您购买特别产品或服务,例如简单消息服务(SMS)、内容分发网络CDN(CDN)、音视频直播服务、对象识别、人脸识别云服务、百度智能云千帆大模型平台服务等,双方还需遵守相关产品的专项约定,包括但不限于如下链接:
 - [分发网络类服务\(CDN、LSS、BEC\)的专项约定](#)
 - [简单消息服务\(SMS\)的专项约定](#)
 - [文字识别\(OCR\)服务的专项约定](#)
 - [人脸识别\(Face\)服务的专项约定](#)
 - [百度智能云千帆大模型平台服务的专项约定](#)
 - [百度智能云千帆AppBuilder服务的专项约定](#)

隐私政策

【百度智能云】隐私政策

欢迎您使用【百度智能云】提供的服务!北京百度网讯科技有限公司(以下简称“百度智能云”或者“我们”)非常重视您的隐私和

个人信息保护。除本隐私政策中另有说明以外，本隐私政策适用于您通过任何方式对【百度智能云】提供的各项服务的访问和使用。

您可以通过【百度智能云】获取【基础云、人工智能、智能大数据、物联网、安全、区块链、专有云等产品和服务】（以下统称“【百度智能云】产品或服务”）。我们仅会处理（如收集、存储等）您使用产品或服务所需的必要个人信息。

本隐私政策适用于您通过【百度智能云】的【网页端】来访问和使用我们的产品和服务。

本隐私政策不适用于我们作为受托人，根据委托人的委托要求处理您的个人信息、用户数据或业务数据。我们将与委托人签订协议，在确保不低于委托人要求的个人信息保护水准的前提下为委托人提供数据处理服务。

本隐私政策不适用于有单独的隐私政策且未纳入本隐私政策的第三方，通过我们向您提供产品或服务（“第三方服务”）。您使用这些第三方服务（包括您向这些第三方提供的任何含个人信息在内的信息），将受这些第三方的服务条款及隐私政策约束（而非本隐私政策），请您仔细阅读第三方的条款。例如，第三方服务商依托百度智能云平台向您提供服务时，您向服务商提供的信息不适用本隐私政策，而适用该等服务商自主的隐私政策。如果您通过激活或关联使得我们提供的服务或产品与第三方平台或社交媒体相关联（例如通过第三方网站直接登录、虚拟登录或关联登录），我们可能会根据您就此的授权将您的个人信息进行披露。请您妥善保管自己的个人信息，仅在必要的情况下向第三方提供或给予授权。

本隐私政策旨在帮助您了解我们会收集哪些个人信息、为什么收集这些个人信息，会利用这些个人信息做些什么及如何保护这些个人信息，以及您作为个人信息主体所享有的权利。我们会遵循隐私政策收集和使用您的个人信息，但不会仅因您授权同意本隐私政策而采用强制捆绑的方式收集您全部的个人信息。我们会严格按照法律法规要求，在特定情况下征求您的单独同意。除本隐私政策之外，我们还可能会通过产品页面告知、弹窗提示、信息推送等方式向您说明我们处理您个人信息的规则，具体业务功能对应的个人信息处理情况将以具体规则为准，具体规则与本隐私政策具有相同效力。

您同意本隐私政策仅代表您已了解应用提供的功能，以及功能运行所需的必要个人信息，并不代表您已同意我们可以收集拓展功能下的必要个人信息，拓展功能下的个人信息会根据您使用过程中的授权情况单独征求您的同意。

请您在使用【百度智能云】及相关产品和服务前仔细阅读并理解本隐私政策，尤其是**字体加粗、下划线**的内容，以便做出适当的选择。

本隐私政策将帮助您了解以下内容：

1. 我们收集的信息及相应的使用目的
2. 我们如何使用 Cookie 和同类技术
3. 我们如何共享、转让、公开披露您的个人信息
4. 我们如何保存及保护您的个人信息
5. 您的权利
6. 我们如何处理未成年人的个人信息
7. 您的个人信息如何进行跨境转移
8. 您的业务数据
9. 本隐私政策的更新
10. 如何联系我们

我们深知个人信息对您的重要性，也深知为您的信息提供有效保护是我们业务健康可持续发展的基石。感谢您对【百度智能云】的使用和信任！我们致力于维持您对我们的信任，恪守以下原则，保护您的个人信息：权责一致原则、目的明确原则、选择同意原则、最少够用原则、确保安全原则、主体参与原则、公开透明原则等。

我们郑重承诺，我们将按业界成熟的安全标准，采取相应的安全保护措施来保护您的个人信息。

1. 我们收集的信息及相应的使用目的

我们将遵循合法、正当、必要的原则，收集和使用您的个人信息。具体而言，我们出于为您提供相应的业务功能而收集并处理您的个人信息。相应功能中，如果您提供的是他人个人信息，请您确保已取得相关主体的授权，我们保留随时核查该等个人信息合法来源的权利。

您需要向我们提供个人信息以供我们实现【百度智能云】的基本业务功能。为实现基本业务功能所必需的信息为必要个人信息，若您拒绝提供这些必要个人信息，我们将无法向您提供该基本业务功能及相应服务。在基本业务功能之外，您可以自主选择向我们提供部分个人信息以供我们实现【百度智能云】的扩展业务功能。我们将向您告知使用的目的并基于您的授权同意或履行您选择的扩展业务功能必需的目的处理这些个人信息。您拒绝提供该等扩展业务功能信息，不会影响您使用我们的基本业务功能，但如您拒绝提供实现扩展业务功能必需的个人信息，我们将无法为您提供扩展业务功能。

为方便您的理解，我们将所提供的业务功能、处理目的及其所需个人信息如下所列：

🔗 1.1 注册、登录账号

您可以通过手机号码创建百度智能云账号或百度通用帐号，并且您可以完善您的账号信息。

- 当注册、登录百度智能云账号或百度通用帐号时，您需向我们提供您中华人民共和国境内的手机号码。您可以选择设置帐号名称、头像、登录密码、帐号绑定邮箱。
- 为了满足法律法规的强制性要求、出于提供产品或服务所必需或者基于您对增强帐号保护级别的需求，在您使用【百度智能云】有关服务时，您需提供您的真实身份信息并完成实名认证。您应根据您的身份属性选择适合的实名认证方式：

(1)如您通过企业对公账号方式进行实名认证，您需要提交您的企业名称、社会信用代码、营业执照图片，以及银行账号信息（包括开户行、银行账号和开户人），我们将以您提交信息作为百度智能云完成您的实名认证时的打款账号使用。

(2)如您通过人脸识别来进行实名认证，您需要提供真实姓名、身份证号、人脸信息，我们将以您提交信息作为百度智能云完成您的实名认证时的信息核验使用。

如您不注册帐号、登录【百度智能云】、或不进行实名认证，并不会妨碍您浏览、了解【百度智能云】的大部分业务功能，但可能会影响到您使用需要经过实名认证才能使用的业务功能（部分服务、活动仅支持实名认证用户使用或参与，若您未认证，将无法使用或参与前述服务和活动，如网络接入、域名注册、网站备案等）。

- 为了验证您提供信息的合法性、真实性和有效性，或保障您的帐号安全，我们可能会将您向百度提供的实名信息与法律法规允许的机构、政府机关授权的机构、合法留存您信息的第三方机构所保存的您的对应信息进行比对核验。

🔗 1.2 百度智能云产品功能

您可以选择【百度智能云】为您提供【ICP备案审查服务】。

- 若您使用【ICP备案审查服务】服务，我们会需要您提供【您的网站主办者证件、主体负责人及网站负责人信息、网站负责人活体核查（如人脸识别认证）及相关网站信息等】。在经您授权同意后，我们会为您提供【ICP备案审查服务】。
- 您可以随时取消授权【百度智能云】处理您的【您的网站主办者或主办单位证件信息、主体负责人及网站负责人信息、网站负责人活体核查（如人脸识别认证）及相关网站信息等】，停止我们对您上述信息的收集，之后您可能将无法获取ICP备案审查服务，但不会影响您正常使用【百度智能云】的其他不基于上述信息提供即可实现的业务功能（例如浏览、搜索百度智能云产品网页等）。
- 您可以通过【百度智能云】的【官网或APP或通过客户经理】进一步了解【ICP备案审查服务】服务。
- 【生物识别、金融账户等信息】属于敏感个人信息，您可以随时取消授权【百度智能云】对您【生物识别、金融账户等信息】的收集，之后您可能将无法使用上述基于【生物识别、金融账户等信息】提供的相关服务或功能，或者无法达到上述基于【生物识别、金融账户等信息】提供的相关服务拟达到的效果，但不会影响您正常使用【百度智能云】其他不基于【生物识别、金融账户等敏感个人信息】即可实现的业务功能。

🔗 1.3 新服务和功能运营及客服处理

- 【百度智能云】会不时针对新推出的服务和功能发起运营活动，如推出的新服务需要处理您的个人信息或申请设备系统权限，且此前未经过您的授权同意，我们会另行获得您的同意，其中，如涉及敏感个人信息的处理，我们会另行获得您的单独

同意。

- 当您使用问题上报功能时，我们将通过您的账号ID访问工单功能（包含查看工单、创建工单），用于快速创建您的服务请求以及后端技术服务人员快速响应您的服务请求。
- 为改进我们及百度智能云关联方、合作方的产品和服务，我们可能会使用收集的信息来进行必要的业务运营和分析研究，以上分析研究可能通过百度智能云千帆等人工智能程序处理，也有可能根据需要与有关合作方共享这些统计信息，但这些统计信息将不会包含您的任何身份识别信息。
- 如果您参加相关运营活动，我们可能会通过运营活动界面收集您的身份信息、联系方式、交易帐号类信息，以便与您取得联系、向您发运营奖励等，具体以运营活动界面和另行向您告知的内容为准。若您不参加相关运营活动则无需提供前述信息。
- 如您对于我们提供的产品服务有疑问或需要客服介入进行争议处理时，为了验证您的身份、定位您的问题，可能需要您提供您的身份信息进行核验。为了保障通话质量，确保纠纷得到妥善解决，我们可能会保存您与我们的沟通记录，包括通话记录、您提供的与您的争议解决相关的信息，您使用或提供的联系方式。
- 如您对于我们提供的产品服务有疑问或需要客服介入进行争议处理时，为了验证您的身份、定位您的问题，可能需要您提供您的身份信息进行核验。为了保障通话质量，确保纠纷得到妥善解决，我们可能会保存您与我们的沟通记录，包括通话记录、您提供的与您的争议解决相关的信息，您使用或提供的联系方式。

🔗 1.4 商务合作协议的履行

为实现您的交易或服务请求，例如您需要申请服务开通、测试、费用发票等，为履行合同所必需，您应提供联系人、联系方式、地址、开票信息、订单等必要信息。

🔗 1.5 商业化合作运营管理

我们还使用商务合作数据来运营管理工作，从您使用百度智能云产品服务的环境中收集或从第三方获取的数据，以便提供更加无缝、一致和个性化的体验，做出明智的业务决策，以及实现其他合法目的。

为实现这些目标而进行的个人数据处理包括自动和手动（人工）处理方法。自动方法通常与手动方法相关，并以手动方法为辅。例如，为构建、培训自动处理方法（包括人工智能 AI）并提高其准确性，我们根据预测和推断所依据的基础数据，手动检查通过自动方法产生的某些预测和推断。例如，获得你的许可并改进我们的深度合成大模型功能，我们会审查大模型调用产生的简短对话片段。这一审查工作可能由代表百度智能云员工或合作供应商进行

🔗 1.6 AI 支持的百度智能云千帆大模型技术体验

百度智能云千帆大模型平台是面向企业开发者的一站式大模型开发及服务运行平台。提供基于文心大模型（Ernie Bot）的数据管理、自动化模型定制微调以及预测服务云端部署一站式大模型定制服务，并提供可快速调用的百度智能云千帆企业级服务 API，助力各行业的生成式 AI 应用需求落地。

如本部分所述。有关千帆大模型平台技术体验的详细信息，[请访问]。

(<https://cloud.baidu.com/doc/WENXINWORKSHOP/index.html>)

🔗 1.7 消息通知

您知悉并同意，对于您在使用产品及/或服务的过程中提供的您的联系方式（例如：联系电话），我们在运营中可能会向其中的一种或多种发送多类通知，用于用户消息告知、身份验证、安全验证、用户使用体验调研等用途。此外，我们也有可能以短信、电话的方式，为您提供可能感兴趣的服务、功能或活动等商业性信息，如您不愿接受这些信息，可以通过手机短信中提供的退订方式进行退订，也可以直接与我们联系进行退订。

🔗 1.8 保证服务安全、优化和改善服务目的

当您使用【百度智能云】时，为了保障您正常使用服务，更准确定位并解决您在使用服务时遇到的问题，改进及优化服务体验，保障您的帐号安全，预防、发现、调查欺诈、危害安全、非法或违反我们的协议、政策或规则的行为，以保护您、我们或我们的关联公司、合作伙伴及社会公众的合法权益，我们会收集您的设备信息、位置信息、日志信息及其他与登录环境相关的信息。

1.9 信息的汇聚融合、个性化推荐和自动化决策

- **汇聚融合**：您同意我们将通过我们自身或受托方技术对您在本服务中主动或被动提供的个人信息进行汇聚融合、识别分析、数据画像或进一步加工，并形成多种类及不同颗粒度的能够反映您的行为习惯、兴趣爱好或者信用状况等特征的标签信息（以下简称“**标签信息**”），我们会将标签信息用于具体的场景和目的中进行**自动化决策**，向您推送个性化展示的信息和/或商业营销信息。除本服务中的信息用于汇聚融合外，对于从您的各种设备上收集到的信息，我们可能会将它们进行关联和汇聚，以便我们能在这些设备上为您提供一致的服务。例如，我们可能会将您的设备信息或电话号码与您的百度帐户相关联，但前提是您在注册、登录百度帐号时同意《百度用户协议》和《百度隐私政策总则》。在**确保个人信息均处于同一业务实体的控制之下且不改变数据安全保障能力和管理水平的情况下**，为给您提供一致化的体验，您在本服务中主动或被动提供的个人信息可能会和您在运营的其他产品服务中主动或被动提供的个人信息进行汇聚融合，并可能在进一步加工后形成标签信息一并用于我们为您提供本服务或者为您提供我们运营的其他产品服务过程中。此类汇聚融合的信息不包含可以直接识别您个人身份的信息，我们会保障信息在汇聚融合后的安全处理。
- **个性化推荐**：我们将基于标签信息以及您在百度智能云官网上的搜索、浏览等使用行为信息、设备信息和**位置信息**，以便向您推荐您可能更感兴趣、相关性更高的内容。在个性化推荐服务中，我们将同时向您提供便捷的拒绝方式，我们建立了用户对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障您调控个性化展示相关性程度的能力。
- **自动化决策**：自动化决策活动同样依赖于我们对您的使用行为信息、设备信息、**位置信息**、标签信息的处理。如果我们通过自动化决策方式作出对您的个人权益有重大影响的决定，您有权通过本政策【“10. 如何联系我们”】要求我们予以说明，并有权拒绝我们仅通过自动化决策的方式作出决定。

1.10 市场活动邀请

百度公司及其授权的合作伙伴为了邀请您参加百度智能云产品、服务、解决方案相关的市场宣传、市场推广相关活动，形式不限于论坛、会议、沙龙、展会等活动，需要收集您的包含姓名、公司、部门职位、手机、邮箱、身份证号码等个人信息，主要用途在于相关市场活动的邀约、发送相关通知以及相关场地/政府/特殊要求的身份报批，除法律法规另有强制性规定的，未经您的同意，不做任何其他用途。

1.11 间接收集信息

为共同向您提供产品/服务或改进产品服务的质量和个性化程度，或出于对产品和服务安全性的考量等合理需要，我们可能按照法律法规的规定或基于您的有效授权从百度平台、关联公司、合作伙伴及其他受信任的第三方供应商处接收您的个人信息及其他信息。我们将事先要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认，同时，我们会了解个人信息提供方已获得的个人信息处理的授权同意范围，如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的，我们将在获取个人信息后的合理期限内或处理个人信息前，征得您的明示同意，或通过个人信息提供方征得您的明示同意。

1.12 事先征得授权同意的例外

请注意：在以下情形中，收集、使用个人信息无需事先征得您的授权同意：

- 为订立、履行个人作为一方当事人的合同所必需；
- 为履行法定职责或者法定义务所必需；
- 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；
- 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；
- 依照法律法规的规定在合理的范围内处理您自行公开的个人信息，或者其他已经合法公开的个人信息（如合法的新闻报道、政府信息公开等渠道）；
- 法律、行政法规另有规定的情形。

1.13 个人信息的去标识化/匿名化处理

在不公开披露、对外提供您个人信息的前提下，百度公司有权对去标识化或者匿名化处理后的用户数据库进行挖掘、分析和利用（包括商业性使用），有权对产品/服务使用情况进行统计并与公众/第三方共享匿名化处理后的统计信息。比如，我们会对

我们服务使用情况进行统计，并可能会与公众或第三方共享这些统计信息，以展示互联网行业的发展趋势等，但这些统计信息不包含您的任何身份识别信息。

1.14 其他您另行意的目的

当我们要将信息用于本隐私政策未载明的其它用途时，会事先征求您的同意。当我们要将基于特定目的收集而来的信息用于其他目的时，会重新征求您的同意。

2. 我们如何使用 Cookie 和同类技术

Cookie和匿名标识符工具。Cookie是支持服务器端（或者脚本）在客户端上存储和检索信息的一种机制。当您使用【百度智能云】产品或服务时，我们会向您的设备发送一个或多个Cookie或匿名标识符。当您与【百度智能云】服务进行交互时，我们允许Cookie或者匿名标识符发送给百度智能云服务器。Cookie 通常包含标识符、站点名称以及一些号码和字符。运用Cookie技术，百度智能云能够了解您的使用习惯，记住您的偏好，省去您输入重复信息的步骤，为您提供更加周到的个性化服务，或帮您判断您账户的安全性。Cookie还可以帮助我们统计流量信息，分析页面设计和广告的有效性。

我们不会将 Cookie 用于本政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。有关详情，请参见 [AboutCookies.org](#)。您可以清除计算机上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要在每一次访问我们的网站时亲自更改用户设置，但您可能因为该等修改，无法登录或使用依赖于Cookie的百度智能云提供的服务或功能。

您可以通过清除您的Cookie，限制百度智能云对Cookie的使用。

3. 我们如何共享、转让、公开披露您的个人信息以及所接入的第三方

我们的某些服务将由授权合作伙伴提供，仅为实现本隐私政策中声明的目的，我们可能会与合作伙伴共享您的某些个人信息，以提供更好的客户服务和用户体验。我们仅会出于合法、正当、必要、特定、明确的目的共享您的个人信息，并且只会共享提供服务所必要的个人信息。除另行获得您的授权或法律法规另有要求，我们的合作伙伴无权将共享的个人信息用于任何其他用途。

3.1 共享

除非经过您本人事先单独同意或符合其他法律法规规定的情形，我们不会向第三方共享您的个人信息，但经过处理无法识别特定个人且不能复原的信息除外。

对我们与之共享个人信息的公司、组织和个人，我们会对其数据安全环境进行调查，与其签署严格的保密协定，要求他们按照依法采取保密和安全措施来处理个人信息。

在下列情况下，我们可能会与以下第三方共享您的个人信息：

3.1.1第三方产品或服务提供商

【百度智能云】引入丰富的第三方服务：

当您使用【百度智能云云市场】接入的第三方服务时，可能需要提交您的个人信息。我们将基于您的有效授权或在订立、履行您作为一方当事人的合同所必需的情况下，将该您的必要个人信息提供给为您提供服务的第三方。关于第三方服务具体如何收集、使用您的个人信息，建议您参考第三方服务的相关服务协议及隐私政策。

当您使用【百度智能云的销售伙伴、技术合作伙伴、服务伙伴】等第三方合作伙伴提供的服务时，可能需要向该等第三方提交您的个人信息。我们将基于您的有效授权或在订立、履行您作为一方当事人的合同所必需的情况下，将该您的个人信息提供给为您提供服务的第三方。关于第三方服务具体如何收集、使用您的个人信息，建议您参考第三方服务的相关服务协议及隐私政策。

当您使用【百度智能云与软硬件或系统供应商】等第三方合作提供的服务时，可能需要向该等第三方提交您的个人信息。我们将基于您的有效授权或在订立、履行您作为一方当事人的合同所必需的情况下，将该您的个人信息提供给为您提供服务的第三方。包括当您在服务采购协议中约定由该等第三方供应商直接向您交付产品、开具发票时，我们向第三方供应商提供您的联系方式、收货地址为向您提供产品服务所必需时，我们会将您提供的联系方式提供给为您提供产品或服务的第三方供应商；当第三方获取您的发票信息为提供产品服务所必需时，我们会将您的发票信息提供给为您提供产品或服务的第三方供应商。

当您参加第三方提供的营销活动或服务内容时，基于服务需要可能需要您提供帐号昵称、头像、姓名、联系方式等信息，我们会经过您的单独同意且在第三方为您提供营销活动或服务内容所必需时，向第三方共享您的个人信息，以保障第三方能够顺利为您提供服务或委托第三方及时向您兑现奖励。在为您提供营销活动或服务内容所必需的情况下，如您拒绝共享，第三方将无法为您提供服务或拒绝您的参与。

百度智能云接入了丰富的第三方小程序服务。第三方小程序可能收集、使用您的相关信息，调用您的设备权限，以便您使用其提供的服务。不同的第三方小程序服务收集、使用的信息以及所调用的设备权限类型可能不同。当您选择使用第三方小程序服务时，经您授权同意，我们会根据您的授权将您的信息提供给该第三方小程序服务提供方，以便其基于相关信息为您提供服务。关于第三方小程序具体调用的设备权限类型，以及如何收集、使用您的个人信息，建议您参考第三方小程序的相关服务协议及隐私政策

3.1.1 百度智能云接入的第三方软件开发工具包（SDK）

为了适配在不同手机设备上使用【百度智能云】以及第三方平台服务，实现您的【手机设备身份认证、手机设备安全、接收信息推送、登录第三方平台帐号、通过第三方平台分享信息以及支付安全】，【百度智能云】接入了第三方SDK。上述第三方SDK提供方包括手机设备厂商、社交平台、通讯运营商和第三方支付机构。部分第三方SDK可能会调用您的设备权限、获取您的相关信息，以便您在不同的手机设备或第三方平台上正常使用相应功能。不同的第三方SDK所调用的设备权限类型以及所获得的信息可能不同，可能包括获取您的【位置、读/写您的外部存储卡、读取您的手机状态和身份、查看WLAN连接、检索正在运行的应用/蓝牙信息】。关于第三方SDK具体调用的设备权限类型，以及如何收集、使用您的个人信息，建议您参考第三方SDK的相关服务协议及隐私政策。如果您希望进一步了解我们所接入的第三方SDK情况，请您阅读**第三方SDK情况说明**。

3.1.2 关联公司或同一帐号体系使用方

我们与我们的关联公司或同一帐号体系使用方之间具备高度一致的数据安全保障措施和管理水平。为了共同向您提供服务、提高您使用产品的安全性和便利性、保障一致性的服务体验，在遵循法律要求且征得您单独同意的前提下，我们会在关联公司或同一帐号体系使用方之间共享您的个人信息。在此情况下，我们只会共享必要的个人信息，如果我们共享您的敏感个人信息或接收方改变个人信息的使用及处理目的，将再次征求您的授权同意/单独同意。

对于同一帐号体系使用方，为了履行监管要求、保障帐号安全性或进行一致化的展示，基于您的有效授权，我们可能会共享您的帐号昵称、头像、绑定状态、绑定手机号信息及帐号基础信息。

3.1.3 产品或服务的受托人

为提供服务之必要，我们可能会将您的个人信息委托给支持部分服务功能的受托人处理。这些支持包括：提供仓储、物流、客服或其他服务，由受托人向您提供物流配送、订单查询、订单支付、售后服务、客户支持（如安装服务）、开票、与合作伙伴对账、支付机构调查回复、奖品发放、服务或产品内容推荐等服务。

3.1.4 以下情形请您关注：

3.1.4.1在获得您的单独同意后，我们会与其他方共享您的个人信息。

3.1.4.2在法定情形下的共享：我们可能会根据法律法规规定、诉讼、仲裁解决需要，或按行政、司法机关依法提出的要求，对外共享您的用户信息；依照法律、法规和监管规定的要求，将您提供的网站主办单位信息、主体负责人及网站负责人信息、网站负责人活体核查（刷脸实名认证）信息及相关网站信息等提供给监管机构或第三方平台用于核查比对。

如我们与上述第三方共享您的信息，我们仅会基于合法、正当、必要原则，在为提供服务所必需的范围内与其共享您的信息，并且我们将努力确保第三方在使用您的信息时遵守本声明及我们要求其遵守的其他适当的保密和安全措施。

3.2 转让

我们不会将您的个人信息转让给除百度公司外的任何公司、组织和个人，但以下情况除外：

- 事先获得您的明确授权或同意；
- 满足法律法规、法律程序的要求或强制性的政府要求或司法裁定；
- 如果我们或我们的关联公司涉及合并、分立、清算、资产或业务的收购或出售等交易，您的个人信息有可能作为此类交易的一部分而被转移，我们将确保该等信息在转移时的机密性、向您告知接收方的名称或姓名和联系方式，并通过签署协议等方

式尽最大可能确保接收方继续受此隐私政策的约束并履行个人信息处理者的义务；接收方变更本隐私政策中约定的处理目的、处理方式的，将依照法律规定重新向您征求授权同意。

3.3 公开披露

我们仅会在以下情况下，公开披露您的个人信息：

- 获得您的单独同意；
- 基于法律法规、法律程序、诉讼或政府主管部门强制性要求下。
- 对违规帐号、违规行为进行处罚公告时，我们会披露相关帐号的信息，这些信息不可避免包含帐号相关认证信息及违规情况。

3.4 共享、转让、公开披露个人信息时事先征得授权同意的例外

- 在以下情形中，共享、转让、公开披露个人信息无需事先征得个人信息主体的授权同意：
- 为订立、履行个人作为一方当事人的合同所必需；
- 为履行法定职责或者法定义务所必需；
- 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；
- 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；
- 依照法律法规的规定在合理的范围内处理您自行公开的个人信息，或者其他已经合法公开的个人信息（如合法的新闻报道、政府信息公开等渠道）；
- 法律、行政法规另有规定的情形。

3.5 委托处理

在我方作为受委托方，接受数据处理者委托处理您的数据的场景下，我们会按照法律法规要求与委托方签署符合法律法规要求的相关协议，并依法、依协议履行相关个人信息保护义务。

4. 我们如何保存及保护您的个人信息

4.1 保存期限

我们将在提供服务所需的最短期限内保存您的个人信息，您理解并认可基于不同的服务及其功能需求，必要存储期限可能会有所不同，例如，根据您的签署的产品服务合同专门约定留存个人信息的时间，或依据法律要求维护相应的日志记录，或依法、依约定履行系统和服务的安全保障，或应对可能的第三方调查取证或用户投诉、问题定位等或法律、合同等是否有保留个人信息的特殊要求等。

在您未撤回授权同意、删除或注销帐号期间，或者个人信息处理目的未实现、保存期限未届满时，我们会持续保留相关信息。

在法律法规对保存期限另有规定、您同意留存更长的期限、保证服务的安全与质量、实现争议解决目的、出现不可抗力情形等情况下，我们将依法、依约或在合理范围内延长保存期限。

在超出保存期限后，我们将删除您的个人信息或进行匿名化处理，但法律法规另有规定的除外。

4.2 保存地域

原则上，我们在中华人民共和国境内收集和产生的个人信息，将存储在中华人民共和国境内。在以下情形下，您的个人信息可能会被转移到您使用产品或服务所在国家/地区的境外管辖区，或者受到来自这些管辖区的访问：

- 1、适用的法律法规有明确规定；
- 2、获得您的单独同意；
- 3、为了履行与您订立的合同。

针对以上情形，我们会严格履行法律法规规定的义务，并按照本政策保护您的个人信息安全。

🔗 4.3 安全措施

- 我们会以“最小化”原则收集、使用、存储和传输用户信息，并通过用户协议和隐私政策告知您相关信息的使用目的和范围。
- 我们非常重视信息安全。我们成立了专责团队负责研发和应用多种安全技术和程序等，我们会对安全管理负责人和关键安全岗位的人员进行安全背景审查，我们建立了完善的信息安全管理制度和内部安全事件处置机制等。我们会采取适当的符合业界标准的安全措施和技术手段存储和保护您的个人信息，以防止您的信息丢失、遭到被未经授权的访问、公开披露、使用、毁损、丢失或泄漏。我们会采取一切合理可行的措施，保护您的个人信息。我们会使用加密技术确保数据的保密性；我们会使用受信赖的保护机制防止数据遭到恶意攻击。
- 我们会对员工进行数据安全的意识培养和安全能力的培训和考核，加强员工对于保护个人信息重要性的认识。我们会对处理个人信息的员工进行身份认证及权限控制，并会与接触您个人信息的员工、合作伙伴签署保密协议，明确岗位职责及行为准则，确保只有授权人员才可访问个人信息。若有违反保密协议的行为，会被立即终止与百度公司的合作关系，并会被追究相关法律责任，对接触个人信息人员在离岗时也提出了保密要求。
- 我们也请您理解，在互联网行业由于技术的限制和飞速发展以及可能存在的各种恶意攻击手段，即便我们竭尽所能加强安全措施，也不可能始终保证信息的百分之百安全。请您了解，您使用我们的产品和/或服务时所用的系统和通讯网络，有可能在我们控制之外的其他环节而出现安全问题。
- 根据我们的安全管理制度，个人信息泄露、毁损或丢失事件被列为最特大安全事件，一旦发生将启动公司最高级别的紧急预案，由安全部、公共事务部、法务部等多个部门组成联合应急响应小组处理。

🔗 4.4 安全事件通知

- 我们会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，我们会立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。
- 个人信息泄露、毁损、丢失属于公司级特大安全事件，我们会负责定期组织工作组成员进行安全预案演练，防止此类安全事件发生。若一旦不幸发生，我们将按照最高优先级启动应急预案，组成紧急应急小组，在最短时间内追溯原因并减少损失。
- 在不幸发生个人信息安全事件后，我们将按照法律法规的要求，及时向您告知安全事件的基本情况和可能的影响、我们已采取或将要采取的处理措施、您可自主防范和降低的风险的建议、对您的补救措施等。我们将及时将事件相关情况以站内通知、短信通知、电话、邮件等您预留的联系方式告知您，难以逐一告知时我们会采取合理、有效的方式发布公告。同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。请您理解，根据法律法规的规定，如果我们采取的措施能够有效避免信息泄露、篡改、丢失造成危害的，除非监管部门要求向您通知，我们可以选择不向您通知该个人信息安全事件。

🔗 5. 您的权利

按照中国相关的法律、法规、标准，以及其他国家、地区的通行做法，我们保障您对自己的个人信息行使以下权利，如您对权利行使有疑问或主张，您也可以通过【如何联系我们】与我们取得联系：

🔗 5.1 查阅权

您有权查阅您的个人信息，法律法规规定的例外情况除外。您可以通过以下方式自行查阅您的个人信息：

- 账户信息——如果您希望查阅或编辑您的账户的绑定信息、更改您的密码、管理安全设备信息、进行账户关联、身份认证等，您可以通过【账号与安全】执行此类操作。
- 交易信息——如果您希望查阅您在百度智能云的交易金额、您已开通的服务、订单情况等信息，您可以在您的【管理控制台】页面进行查看。

如果上述链接无法访问，您可以通过在百度智能云官网提交工单与我们联系。

🔗 5.2 更正及补充权

您发现我们处理的关于您的个人信息有错误或不完整，您有权对错误或不完整的信息自行作出更正或更新，例如：您可以随时

通过【账号与安全】修改您的绑定手机号等信息；可以通过用户中心更新您的个人信息。如您需变更通过百度智能云提交的实名认证信息的，您需到原账号注册的网站进行变更。

🔗 5.3 删除权

在以下情形中，您可以向我们提出删除个人信息的请求：

- （一）个人信息的处理目的已实现、无法实现或者为实现处理目的不再必要；
- （二）我们已停止提供产品或者服务，或者保存期限已届满；
- （三）您已撤回同意；
- （四）如果我们违反法律法规或与您的约定收集、使用、与他人共享或转让您的个人信息；
- （五）法律、行政法规规定的其他情形。

当您要求我们删除信息后，我们会依据法律规定响应您的要求，及时删除相应的信息。如果法律、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，我们将停止除存储和采取必要的安全保护措施之外的处理。

🔗 5.4 撤回同意权

您可以选择撤回您的授权，例如：您可以通过“联系我们”来提出您的诉求，包括但不限于撤回您的授权等诉求；或者您也可以

通过注销账户的方式，撤回我们继续处理您个人信息的全部授权。

请您理解，每个业务功能需要一些基本的个人信息才能得以完成，当您撤回同意或授权后，我们无法继续为您提供撤回同意或授权所对应的服务，也不再基于您此前的同意使用您相应的个人信息。但您撤回同意或授权的决定，不会影响此前基于您的授权而开展的个人信息处理的效力。

🔗 5.5 注销账号权

您随时可注销此前注册的百度智能云账户。您可以根据《百度智能云账号注销协议》的指引申请注销您的账号。您知悉并理解，注销账号的行为是不可逆的行为，当您注销账号后，我们将停止为您提供任何服务，并删除有关您账号的一切信息或对相关信息进行匿名化处理，法律另有规定的情形除外。因法律规定需要留存的用户个人信息，我们会妥善保管，并不再将其应用于业务场景。

特别提醒：您的百度智能云账号一旦注销后，我们将无法协助您找回，请您备份好账号下所有业务信息后谨慎操作。账号注销意味着账号协议及该账号下所有服务条款、协议、合同等一并解除，包括您将无法找回该账号下的个人信息、交易记录、业务数据、历史信息等。

此外，请您知悉并理解，账号注销并不代表您在该账号注销前的所有账号行为和相关责任得到豁免或减轻。

您通过第三方账号授权登录百度时，需向第三方申请注销账号。

🔗 5.6 复制权和可携带权

您有权复制我们收集的您的个人信息。在法律法规规定的条件下，同时符合国家网信部门规定指令和条件的，如果技术可行，您也可以要求我们将您的个人信息转移至您指定的其他主体。

您可以通过以下路径：通过本政策【“10. 如何联系我们”】与我们取得联系并获取您的个人信息资料副本。为保证信息安全，我们将会对您的身份进行必要的验证。

🔗 5.7 提前获知产品和服务停止运营权

若因特殊原因导致百度智能云某个产品和服务被迫停止运营，我们将提前15日或按与您签署的合作协议中约定的通知期间内，通过包括但不限于按协议约定通知方式、产品或服务的主页面或站内信或向您发送电子邮件或其他合适的能触达您的方式通知您，并将停止对您个人信息的收集，同时会按照法律规定对所持有的您的个人信息进行删除或匿名化处理等。

🔗 5.8 获得解释的权利

您有权要求我们就个人信息处理规则作出解释说明。您可以通过【“10. 如何联系我们”】与我们取得联系。

5.9 对个人信息的身前安排

根据相关法律要求，您可以提前就您的个人信息提前进行生前安排，您可以通过本政策公布的联系方式，通过书面方式告知我们您的安排；如无另行安排，您的近亲属可以基于其合法、正当利益，对您生后的相关个人信息依照相关法律规定和本政策的约定，行使查阅、复制、更正、删除等权利。

5.10 我们如何响应您的上述请求

为保障安全，您可能需要提供书面请求，或以其他方式证明您的身份。我们可能会先要求您验证自己的身份，然后再处理您的请求。

对于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情况收取一定成本费用。如果直接实现您的请求需要付出高额成本或存在其他显著困难的，我们将积极努力向您提供替代性方法。

对于那些无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际（例如，涉及备份磁带上存放的信息）的请求，我们可能会予以拒绝。

5.11 响应的例外

在以下情形中，按照法律法规要求，我们将无法响应您的上述请求：

- 与国家安全、国防安全直接相关的；
- 与公共安全、公共卫生、重大公共利益直接相关的；
- 与犯罪侦查、起诉、审判和执行判决等直接相关的；
- 我们有充分证据表明您存在主观恶意或滥用权利的（如您的请求将危害公共安全和他人合法权益，或您的请求超出了一般技术手段和商业成本可覆盖的范围）；
- 响应个人信息主体的请求将导致您或其他个人、组织的合法权益受到严重损害的；
- 涉及商业秘密的；
- 法律、行政法规另有规定的情形。

6. 我们如何处理未成年人的个人信息

百度公司非常重视对未成年人信息的保护。

我们的产品和服务主要面向成年人。我们只会在受到法律法规允许、父母或其他监护人同意的情况下处理未成年人的个人信息。

如您是未满14周岁的未成年人，在使用【百度智能云】产品和服务前，应请您的父母或其他监护人仔细阅读，或在您的父母或其他监护人的监护、指导下共同仔细阅读本隐私政策以及《百度儿童个人信息保护声明》，并在征得您的父母或其他监护人同意的前提下使用我们的产品和服务，或向我们提供信息。

如果我们发现在未事先获得可证实的父母或其他监护人同意的情况下收集了未满14周岁的未成年人的个人信息，我们将会采取措施尽快删除相关信息。如果任何时候监护人有理由相信我们在未获监护人同意的情况下收集了未成年人的个人信息，请通过本隐私政策【“10. 如何联系我们”】联系我们，我们会采取措施尽快删除相关数据。

7. 您的个人信息如何进行跨境转移

原则上，我们在中华人民共和国境内收集和产生的个人信息，将存储在中华人民共和国境内。

如您的个人信息可能会被转移到您使用产品或服务所在国家/地区的境外管辖区，或者受到来自这些管辖区的访问，我们会严格履行法律法规规定的义务并事先获得您的单独同意。

在获得您的单独同意后，您的个人信息才可能会被转移到境外管辖区，或者受到来自这些管辖区的访问；以及，因政府监管、司法协助要求等情形，需向中华人民共和国境外传输您的个人信息的，我们会向您告知所涉跨境传输的数据类型、跨境传输目的、接收方的名称或者姓名、联系方式及相关安全保障措施、您向境外接收方形式个人信息权利的方式和程序等情况，并取得您的单独同意；当我们执行此类传输时，我们会根据法律法规规定和本隐私政策，履行个人信息跨境提供的法定义务，如按照

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，以及组织开展数据出境安全自评估，在符合条件时通过国家网信部门组织的安全评估等。

我们将采取必要措施，保障境外接收方处理个人信息的活动达到与相关法律法规规定和本隐私政策规定的个人信息保护标准。例如，我们会请求您对跨境转移个人信息的单独同意，或者在跨境数据转移之前实施数据加密、去标识化等安全举措。

8. 您的业务数据

不同于您的个人信息，对于您的业务数据，我们将按如下方式处理：

您通过百度智能云提供的服务，加工、存储、上传、下载、分发以及通过其他方式处理的数据，均为您的用户业务数据，您完全拥有您的业务数据。百度智能云作为中立的技术服务提供者，会严格执行您的委托和指示，除按与您协商一致或依据特定产品规则或基于您的要求为您提供技术协助进行故障排除或解决技术问题或执行明确的法律法规要求外，我们不对您的业务数据进行任何非授权的访问、使用或披露。

您应对您的业务数据来源及内容负责，我们提示您谨慎判断数据来源及内容的合法性。您应保证您有权使用我们的产品、服务对该等业务数据进行处理，且前述处理活动均符合相关法律法规的要求，不存在任何违法违规、侵权或违反与第三方合同约定的情形，亦不会将数据用于违法违规目的。因您的用户业务数据内容违反法律法规、部门规章或国家政策而造成的全部结果及责任均由您自行承担。

当我们按本节内容处理您的业务数据时，如果涉及第三方个人信息，您应当依法提前向相关个人信息主体履行告知义务，取得相关个人信息主体的单独同意，并保证：

- (1) 根据我们要求的方式，就个人信息来源及其合法性提供书面说明和确认；
- (2) 在我们要求时，提供相关个人对信息处理的授权同意范围，包括使用目的，个人信息主体同意您使用我们的服务对其个人信息进行处理；
- (3) 如您使用我们的服务所需进行的个人信息处理活动超出该等个人信息的授权同意范围的，应在提供个人信息后的合理期限内或在我们处理个人信息前，由您负责征得个人信息主体的明示同意，并在我们要求时向我们提供书面证明。

如您违反上述义务，或未按照要求向我们提供合理满意的证明，或我们收到个人信息主体举报或投诉，我们有权单方决定拒绝处理您的业务数据，或拒绝按照您的指令处理其中所涉第三方的信息。由此产生的全部责任均由您自行承担。

您理解并同意，您应根据自身需求自行对您的业务数据进行存储，我们仅依据相关法律法规要求或特定的服务规则约定，接受您的委托为您提供数据存储服务。您理解并同意，除法律法规另有规定或依据服务规则约定，我们不会访问、存储您的业务数据，亦不对您的数据存储工作或结果承担任何责任。

9 本隐私政策的更新

我们可能适时修订本政策内容，除法律另有规定外，未经您明确同意，我们不会削减您按照本隐私政策所应享有的权利。我们会在本页面上发布对本隐私政策所做的任何变更。

对于重大变更，我们会在产品或服务的主要曝光页面或站内信或向您发送电子邮件或其他合适的能触达您的方式通知您。若您不同意该等变更，请您立即停止使用【百度智能云】产品和服务。如您不同意隐私政策的更新，系统将为您登出账号，但您仍然可以在未登录的情况下使用部分基本功能。

本政策所指的重大变更包括但不限于：

- 我们的服务模式发生重大变化。如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等；
- 我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产并购等引起的所有者变更等；
- 个人信息对外提供、转让或公开披露的主要对象发生变化；
- 您参与个人信息处理方面的权利及其行使方式发生重大变化；
- 我们负责处理个人信息安全的责任部门、联络方式及投诉渠道发生变化时；
- 个人信息安全影响评估报告表明存在高风险时。

如有本隐私政策未尽事宜，以【《百度隐私权保护声明》】为准。

10. 如何联系我们

【百度智能云】的成长离不开各方用户达人的共同努力，我们非常感谢您对【百度智能云】数据更新、使用反馈方面的贡献。

1.您可以通过个人信息保护问题反馈平台<http://help.baidu.com/personalinformation>同我们联系。

2.您也可以通过如下联络方式同我们联系：

中国北京市海淀区上地十街10号

北京百度网讯科技有限公司法务部

邮政编码：100085

为保障我们高效处理您的问题并及时向您反馈，我们可能需要您提交身份证明、有效联系方式和书面请求及相关证据，我们会在验证您的身份后于15个工作日内及时处理您的请求。

如果您对我们的回复不满意，特别是您认为我们的个人信息处理行为损害了您的合法权益，您还可以通过向有关政府部门投诉或者司法部门起诉的方式寻求解决方案，例如向北京市海淀区有管辖权的人民法院提起诉讼。

再次感谢您对【百度智能云】的信任和使用！

北京百度网讯科技有限公司

更新日期：【年月日】

生效日期：【年月日】

附：名词解释

个人信息是指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。个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

敏感个人信息是指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。

日志信息是指我们的服务器所自动记录您在使用【百度智能云】时所发出的请求，例如您的IP 地址、浏览器的类型和使用的语言、硬件设备信息、操作系统的版本、网络运营商的信息、您访问服务的日期、时间、时长等您在使用我们的产品或服务时提供、形成或留存的信息。

Cookie是指支持服务器端（或者脚本）在客户端上存储和检索信息的一种机制，通过增加简单、持续的客户端状态来扩展基于Web的客户端/服务器应用。服务器在向客户端返回HTTP对象的同时发送一条状态信息，并由客户端保存。状态信息中说明了该状态下有效的URL范围。此后，客户端发起的该范围内的HTTP请求都将把该状态信息的当前值从客户端返回给服务器，这个状态信息被称为Cookie。

设备信息是指您用于安装、运行百度智能云的终端设备的设备属性信息（例如您的硬件型号，操作系统版本，设备配置，国际移动设备身份码IMEI、国际移动用户识别码IMSI、网络设备硬件地址MAC、广告标识符IDFA、IDFV、MEID、OAID、SIM卡信息如ICCID、Android ID、硬件序列号等设备标识符）、设备连接信息（例如浏览器的类型、电信运营商、使用的语言、WIFI信息（SSID、BSSID）、蓝牙信息）以及设备状态信息（例如设备应用安装列表、传感器）、检索正在运行的应用、运行中的进程信息。

用户画像是指通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如其职业、经济、健康、教育、个人喜好、信用、行为等方面做出分析或预测，形成其个人特征模型的过程。直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

匿名化是指通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。个人信息经匿名化处理后所得的信息不属于个人信息。

百度平台是指百度公司旗下各专门频道或平台服务（包括百度搜索、百度APP及衍生版、百度百科、百度知道、百度贴吧、百度图片、百度糯米、百度手机助手及其他百度系产品<https://www.baidu.com/more/>等网站、程序、服务、工具及客户端。

关联公司是指【百度智能云】的经营者北京百度网讯科技有限公司及其他与百度公司存在关联关系的公司的单称或合称。“关联关系”是指对于任何主体（包括个人、公司、合伙企业、组织或其他任何实体）而言，即其直接或间接控制的主体，或直接或间接控制其的主体，或直接或间接与其受同一主体控制的主体。前述“控制”指，通过持有表决权、合约或其他方式，直接或间接地拥有对相关主体的管理和决策作出指示或责成他人作出指示的权力或事实上构成实际控制的其他关系。

信息安全

信息安全规定

背景

为保障百度智能云（以下简称“百度智能云”）及用户信息安全，深刻践行《互联网信息服务管理办法》、《计算机信息网络国际联网安全保护管理办法》、《文明上网自律公约》、《互联网终端安全服务自律公约》等相关法律法规，特制定本规定。作为对百度智能云用户服务协议补充。

适用对象

使用百度智能云包括但不限于BCC/BAE/BLB/CDN/BOS/SMS/BCH/VOD/LSS等产品的所有用户（包括代理商）。

综述

用户在使用百度智能云产品时，应遵守国家法律、行政法规、各部门规章等规范性文件，并自行按照相关法律法规，向相关对象提供合法的产品及服务，履行相关义务，并自行承担全部责任（包括但不限于履行信息网络安全管理义务、健全各项网络安全管理制度和落实各项安全保护技术措施），对任何涉嫌违反国家法律、行政法规、部门规章等规范性文件的行为，本规则已有规定的，适用本规则；本规则尚无规定的，百度智能云有权酌情进行处理。

说明：百度智能云对本规则拥有最终解释权，可对本规定进行更新并在百度智能云官网上予以公告。若用户不同意本规定相关变更，请立即停止使用百度智能云的相关服务及产品。百度智能云有权对用户行为及应适用的规则进行单方认定，并根据相关法律法规进行违规判定并进行处理。

一、信息安全规定细则：

1、用户在购买及使用百度智能云提供的服务或产品时，必须遵守百度智能云各类服务或产品的用户协议及其他条款。

2、用户在使用百度智能云提供的服务或产品时，除了遵守该产品的服务条款之外，还应遵守《百度智能云信息安全规定》中的如下细则。

(1) 政治类

不得发布或者存储含有反动、破坏国家统一、破坏主权及领土完整、破坏社会稳定，涉及国家机密、散布政治谣言、扰乱社会秩序，宣扬邪教迷信，宣扬宗教、种族歧视等信息，或法律法规禁止出版发行的书籍、音像制品、视频、文件资料的信息。

(2) 色情低俗类

不得发布或者存储含有色情淫秽低俗内容的音像制品、视频、音频、图片、动漫等；

不得提供色情陪聊、招嫖服务；不得提供含有可致使他人暂时失去反抗能力、意识模糊的口服或外用的催情类商品或者药品的售卖服务；

不得发布成人网站论坛等信息；

不得发布或者存储含有用于传播色情信息的软件。

(3) 侵权类

不得发布或存储侵犯个人或企业名誉权、人身攻击、侵犯个人隐私的信息；

不得发布或存储侵犯个人或企业商标、专利、图书音像制品、电视电影广播版权、网络出版物的信息。

(4) 医药、保健品、食品类

不得发布国家公示已查处、药品监督管理局认定禁止生产、使用的药品的交易信息；

不得发布未经国家药监局批准的药品的交易信息；

不得发布宣扬有明显药物治疗效果的保健品的交易信息；

不得发布未获得食品生产许可证及卫生许可证的食品的交易信息。

(5) 暴恐类

不得发布或者存储管制刀具售卖、毒品、爆炸物制作、涉恐消息、涉恐视频、涉恐音频、有暴力倾向的包括但不限于文字、图片、音视频、出版物等信息。

(6) 赌博类

不得发布或者存储含有赌博交易平台的信息；

不得发布或者存储非法赌博器具介绍或售卖的信息。

(7) 诈骗类

不得发布或者存储含有诈骗类中奖、钓鱼网站等信息；

不得发布或者存储含有伪基站相关的交易信息；

不得发布或者存储含有外挂、私服相关的网游类的信息。

(8) 违禁物品类

不得发布或者存储含有毒品、制毒原料、制毒化学品的交易信息；

不得发布或者存储含有剧毒化学品的交易信息；

不得发布或者存储含有国家名录中禁止出售的危险化学品（剧毒化学品除外）的交易信息；

不得发布或者存储含有易燃、易爆物品（烟花爆竹除外）及相关化学品类的交易信息；

不得发布或者存储介绍制作易燃易爆品方法的相关教程、书籍的交易信息；

不得发布或者存储含有枪支、弹药、军火及仿制品的交易信息；

不得发布或者存储含有枪支、弹药、军火的相关器材、配件、附属产品等的交易信息；

不得发布或者存储含有警用、军用制服、标志、设备及制品的交易信息；

不得发布或者存储含有可致使他人暂时失去反抗能力，对他人身体造成重大伤害的管制器具；

不得发布或者存储含有管制类刀具、弩配件及用于危害他人人身安全的管制器具的交易信息；

不得发布或者存储含有用于监听、窃取隐私或机密的软件及设备的交易信息；

不得发布或者存储含有用于非法摄像、录音、取证等用途的设备的交易信息；

不得发布或者存储含有烟花爆竹类的交易信息；

不得发布或者存储含有伪造/变造国家机关或特定机构颁发的文件、证书、证件、公章、防伪标签等，非法或仅限国家机关或

特定机构方可提供服务的交易信息；

不得发布或者存储含有代开尚可使用或用于报销的票据的交易信息；

不得发布或者存储含有人体器官的交易信息；

不得发布或者存储含有个人隐私信息及企业内部数据；提供个人手机定位、电话清单查询、银行账户查询等服务的交易信息；

不得发布或者存储含有作弊干扰相关的交易信息；

不得发布或者存储含有可能用于逃避交通管理的交易信息；

不得发布或者存储含有撬锁工具、开锁服务及其相关教程、书籍的交易信息；

不得发布或者存储含有违禁汽车类的交易信息；

不得发布或者存储含有烟草的交易信息；

不得发布或者存储含有濒危动植物类的交易信息。

(9) 金融类

不得发布或存储未经国家银监会、保监会等其他金融主管部门批准的金融产品（包括但不限于保险、理财、贷款、股票等）售卖或宣传的信息；

不得发布虚假捐款、非法集资等信息。

(10) 其他类

不得发布或者存储含有非法传销类信息；

不得发布或者存储含有网络雇佣（用于违法事件）的信息；

不得发布或者存储含有拐卖人口的信息；

不得发布仿冒其他网站的信息；

不得发布含有病毒、木马、带有攻击性的软件的信息；

不得发布以伤害用户体验为代价的应用，包括但不限于黑帽SEO应用。

不得利用百度智能云产品或平台以任何方式发布虚假信息，诱导用户分享虚假信息等行为，如被第三方举报或经百度智能云查证属实，百度智能云有权对违规用户做出封禁产品、账号等处罚措施。

二、违规行为等级及处罚措施

1、违规行为等级

(1) 一般违规行为

一般违规是指用户发布或者存储、指向的信息内容构成了《百度智能云信息安全规定》的相关规则中的一般违规行为。

(2) 严重违规行为

严重违规是指用户发布或者存储、指向的信息内容构成了《百度智能云信息安全规定》的相关规则中的严重违规行为。

(3) 特别严重违规行为

特别严重违规是指用户发布或者存储、指向的信息内容构成了《百度智能云信息安全规定》的相关规则中的特别严重违规行为。

2、违规处罚尺度

为维护百度智能云产品使用环境的洁净以及用户的正当权益，在用户违规处理期间按照规定的情形对用户采取以下违规处罚措

施：

- (1) 屏蔽产品中的违规内容；
- (2) 停用含有违规内容的产品；
- (3) 封禁用户账号，使其无法使用百度智能云所有的产品及服务。

3、违规处罚

用户违反本规则的相关规定，百度智能云将依照《百度智能云信息安全处罚细则》及其他相关规则对其进行处理，违规行为对应的处理分为：

- (1) 一般违规行为的处罚；
- (2) 严重违规行为的处罚；
- (3) 特别严重违规行为的处罚。

各个产品对应的处罚标准不同，详情请参照《百度智能云信息安全处罚细则》。

三、申诉解禁

用户在接到百度智能云发出的封禁通知后，需要在规定时间内按照要求清除干净违规信息，承诺加强网站信息安全管理，通过工单系统提交解禁申请，百度智能云将按照相关规定进行处理。对上级主管部门下发的封禁指令，如需解禁，需要首先得到上级主管部门的许可。

四、违规举报

网民如有发现百度智能云用户违反了《百度智能云信息安全规定》的行为，可通过[违规举报入口](#)进行举报，百度智能云将按照相关规定及时处理。

五、其他

对于上级部门要求处理的违规情况，百度智能云将会直接根据上级的处罚意见进行处理。

附则

一、本规则标准于2015年6月16日首次生效。

二、在不违反当地法律法规政策的前提下，对使用中国大陆以外地区（包括香港特别行政区和台湾、澳门及海外地区）百度智能云产品或服务用户的信息安全管理，可参照本规则执行。

三、百度智能云有权单方对本细则做出解释或更新。

附件：

[百度智能云信息安全处罚细则](#)

百度智能云用户行业资质收取标准

按照相关法律法规要求，用户在使用百度智能云服务时应提供相应的行业资质，具体标准如下：

医疗药品及相关用品

一级行业	二级行业		用户类型	所需资质文件
医疗药品及相关用品	医疗药品销售		公司类用户	营业执照副本
				《互联网药品交易服务资格证书》
	药品生产类		公司类用户	营业执照副本
				《药品生产许可证》
	医药研究、药品研发类		公司类用户	营业执照副本
				《药品生产许可证》
	药品信息类		公司类用户	营业执照副本
				《互联网药品交易服务资格证书》
				临床实验的证明文件
	医疗类衍生产品	一般化妆品类	公司类用户	营业执照副本
				化妆品生产企业卫生许可证或工业产品许可证
		特殊化妆品类	公司类用户	营业执照副本
				化妆品生产企业卫生许可证或工业产品许可证或批件
		保健品类	公司类用户	营业执照副本
				保健品批准证书或注册批件
		成人用品类	公司类用户	营业执照副本
				纸质证明材料：网站首页出现icp证或icp备案号的截图，截图上应保留浏览器整体框架及地址栏用户网址，同时在截图上加盖公章
		兽药生产销售类	公司类用户	营业执照副本
				兽药生产许可或经营许可或批准文号文件
		兽药信息平台类	公司类用户	营业执照副本
				纸质证明材料：网站首页出现icp证或icp备案号的截图，截图上应保留浏览器整体框架及地址栏用户网址，同时在截图上加盖公章
		以上医疗类衍生产品涉及代理、授权经销等性质	公司类用户	营业执照副本
				厂商对用户代理销售产品的授权
				医疗药品衍生产品的合法资质

医疗机构及相关机构

一级行业	二级行业		用户类型	所需资质文件
医疗机构及相关机构	医疗药品销售		营利性医疗机构	营业执照副本
				医疗机构执业许可证
			非营利性医疗机构	事业单位法人登记证或组织机构代码证
				医疗机构执业许可证
	计划生育服务（涉及医疗机构）		营利性医疗机构	营业执照副本
				计划生育技术服务机构执业许可证
			非营利性医疗机构	事业单位法人登记证或组织机构代码证
				计划生育技术服务机构执业许可证
	戒毒机构类		营利性医疗机构	营业执照副本
				医疗机构执业许可证（项目登记中必须包含戒毒服务）
			非营利性医疗机构	事业单位法人登记证或组织机构代码证
				医疗机构执业许可证（项目登记中必须包含戒毒服务）
	其他医疗相关机构	涉及手术方式的营利性美容医院（包括纹身、刺青等）	公司类用户	医疗机构执业许可证
				营业执照副本
		涉及手术方式的非营利性美容医院（包括纹身、刺青等）	公司类用户	医疗机构执业许可证
				事业单位法人登记证或组织机构代码证
非手术方式美容机构	公司类用户	营业执照副本		
		个人类用户	个人从业资格证（需和实名认证的身份信息相符）	

医疗器械及相关器械

一级行业	二级行业	用户类型	所需资质文件
医疗器械类	医疗器械及相关器械	公司类用户	营业执照副本
			第一类医疗器械需出具省级药品监督局的备案或市级以上药监局的器械生产注册证书、产品注册号或批准号；隐形眼镜及护理液、美瞳，若仅做展示不涉及交易，则需出具《互联网药品信息服务资格证书》，若涉及交易则需出具《互联网药品信息服务资格证书》或《互联网药品交易服务资格证书》；其他医疗器械需出具省级以上药品监督管理部门颁发的医疗器械经营许可证和（或）医疗器械生产许可证
	假肢及假肢矫形器生产装配类	营利性医疗机构	营业执照副本
			假肢和矫形器（辅助器具）生产装配企业资格认定书

医疗周边类

一级行业	二级行业	用户类型	所需资质文件
医疗周边类	从事与人体生命健康相关的医疗周边行业用户（不包含疾病治疗） 如心理疾病咨询、语言障碍矫正、产后护理、健身机构、挂号平台、无障碍器具生产等。	公司类用户	营业执照副本

版权类

一级行业	二级行业	用户类型	所需资质文件
版权类	书籍、音像制品、光盘广告销售类	公司类用户	营业执照副本、 著作权证明、版权证明或销售许可证明 互联网出版许可证、音像制品经营许可证
		个人类用户	个人身份证、 著作权证明、版权证明或销售许可证明 互联网出版许可证、音像制品经营许可证
	音视频播放类	公司类用户	营业执照副本/承诺函、 互联网视听许可证、 广播电视节目制作经营许可证、 版权方授权文件
		个人类用户	个人身份证件、视听许可证、 广播电视节目制作经营许可证
	电子公告服务(BBS)	公司类用户	营业执照副本、 电子公告服务(BBS)许可证
	新闻类	公司类用户	营业执照副本、 互联网新闻信息服务许可

金融类

一级行业	二级行业	用户类型	所需资质文件
金融类	外汇类	公司类用户	营业执照副本
			经营外汇业务许可证
	贵金属交易平台类	公司类用户	营业执照副本
			ICP备案证明
		公司类用户	贵金属交易所（中心）会员证明：出具贵金属交易所（中心）会员查询截图并加盖公章（截图上应保留浏览器整体框架及地址栏贵金属交易所（中心）网址）
	股票、基金、期货咨询类	公司类用户	营业执照副本
			证券投资咨询业务资格证书或经营证券业务许可证
	股票、基金、平台类	公司类用户	营业执照副本
			经营股票承销业务资格证书或基金代销业务资格证
	基金直销公司类	公司类用户	营业执照副本
			基金管理资格证书
	银行类	公司类用户	主体营业执照副本
			金融机构许可证
	第三方支付平台类	公司类用户	营业执照副本
			支付业务许可证
	保险	公司类用户	主体营业执照副本并核对经营范围
	贷款	公司类用户	主体营业执照副本并核对经营范围、BAE不允许创建此类应用网站
	担保类	公司类用户	主体营业执照副本并核对经营范围
	典当类	公司类用户	主体营业执照副本并核对经营范围

食品类

一级行业	二级行业	用户类型	所需资质文件
食品类	食品及食品添加剂生产类	公司类用户	营业执照副本
			全国工业产品生产许可证
	食品销售类	公司类用户	营业执照副本
			食品流通许可证

商务服务类

一级行业	二级行业	用户类型	所需资质文件
商务服务类	出国留学中介类	公司类用户	主体营业执照副本并核对经营范围，或提交《自费出国留学机构资格认定书》，或在教育涉外监管信息网《已领取资格认定的自费留学中介服务机构名单》中可查询。
	考学培训机构	公司类用户	主体营业执照副本或民办非企业单位登记证书
	旅游服务	公司类用户	主体营业执照副本并核对经营范围
		个人用户类	个人身份证复印件、旅行社业务经营许可证
	火车票销售类	公司类用户	主体营业执照副本并核对经营范围
	航空机票代理类	公司类用户	主体营业执照副本
			中国航协颁发的《资格认可证书》
			纸质证明材料：网站首页出现icp证或icp备案号的截图，截图上应保留浏览器整体框架及地址栏用户网址，同时在截图上加盖公章
	航空公司类	境内公司类用户	主体营业执照副本
			公共航空运输企业经营许可证
			中国民用航空局颁发的经营许可

生活服务类

一级行业	二级行业	用户类型	所需资质文件
生活服务类	开锁类	公司类用户	营业执照副本
			特种行业许可证（许可证经营范围注明为开锁或开锁服务）或开锁服务许可证或开锁服务卡或公安局备案证明
		个人用户类	证件及证明持有人身份证复印件
			特种行业许可证（许可证经营范围注明为开锁）或开锁服务许可证或开锁服务卡或公安局备案证明
	刻章类	公司类用户	主体营业执照副本并核对经营范围
	按摩	公司类用户	主体营业执照副本并核对经营范围
	警用装备	公司类用户	主体营业执照副本并核对经营范围
	保安安保	公司类用户	主体营业执照副本并核对经营范围
	法律服务类	律师事务所	律师事务所执业证书
		个人律师服务	个人身份证复印件、个人律师执业资格证书

其他类

一级行业	二级行业	用户类型	所需资质文件
其他类	网络游戏类	公司类用户	主体营业执照副本、网络文化经营许可证、相关游戏产品计算机著作权、游戏产品资质（游戏版号及备案）
	招聘简单劳动人员及兼职人员	公司类用户	主体营业执照副本
	充值类（不含话费充值）	公司类用户	主体营业执照副本
	招商加盟类	公司类用户	主体营业执照副本
	VPN服务	公司类用户	主体营业执照副本

注意

- 1. 用户务必保证提供相关资质的真实有效性，一旦发现虚假资质将直接进行封禁，并有权追究其法律责任；
- 2. 以上各项若有代理公司或个人，需提供原公司对应所有资质、授权代理协议、代理公司营业执照或代理个人身份证明；
- 3. 药品／食品及保健品类，除了提供上述资质外，还应严格遵守新广告法的相关规定；
- 4. 其他特殊行业资质以百度智能云公布的相关规则为准。

百度智能云信息安全处罚细则

🔗 百度智能云信息安全处罚细则

产品	违规等级	违规处罚措施
BCC	特别严重	封禁账号，不退款
	严重	封禁域名、外网IP、产品停用，不退款
	一般	封禁URL，酌情退款
BAE	特别严重	封禁账号，不退款
	严重	封禁应用、产品停用，不退款
	一般	封禁应用，酌情退款
BLB	特别严重	封禁账号，不退款
	严重	封禁域名、外网IP、产品停用，不退款
	一般	封禁URL，酌情退款
CDN	特别严重	封禁账号，不退款
	严重	封禁域名（回源）、产品停用，不退款
	一般	封禁URL，酌情退款
BOS	特别严重	封禁账号，不退款
	严重	封禁bucket、产品停用，不退款
	一般	封禁object访问，酌情退款
SMS	特别严重	封禁账号，不退款
	严重	产品停用，不退款
	一般	产品停用，不退款
SES	特别严重	封禁账号，不退款
	严重	产品停用，不退款
	一般	产品停用，不退款

说明：

- 1、 2次一般违规，处罚措施参照严重等级执行；3次及以上一般违规，处罚措施参照特别严重等级执行。
- 2、 2次及以上严重违规，处罚措施参照特别严重等级执行。

法律法规

- [《民法典》](#)
- [《个人信息保护法》](#)

- [《数据安全法》](#)
- [《关键信息基础设施安全保护条例》](#)
- [《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》](#)
- [《汽车数据安全若干规定（试行）》](#)
- [《信息安全技术 个人信息安全规范》](#)
- [《儿童个人信息网络保护规定》](#)
- [《工业和信息化部关于加强呼叫中心业务管理的通知》](#)
- [《工业和信息化部办公厅关于深入推进移动物联网全面发展的通知》](#)
- [《中华人民共和国出口管制法》](#)
- [《最高人民法院最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》](#)
- [《关于印发《App违法违规收集使用个人信息行为认定方法》的通知》](#)
- [《网络安全审查办法》](#)
- [《网络信息内容生态治理规定》](#)
- [《全国人民代表大会常务委员会关于加强网络信息保护的决定》](#)
- [《全国人民代表大会常务委员会关于维护互联网安全的决定》](#)
- [《中华人民共和国电信条例》](#)
- [《中华人民共和国计算机信息系统安全保护条例》](#)
- [《信息网络传播权保护条例（2013年1月30日修正版）》](#)
- [《最高人民法院 最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）》](#)
- [《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》](#)
- [《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》](#)
- [《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》](#)
- [《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》](#)
- [《电信服务规范》](#)
- [《互联网IP地址备案管理办法》](#)
- [《互联网域名管理办法》](#)
- [《计算机信息网络国际联网安全保护管理办法》](#)
- [《计算机信息系统安全专用产品检测和销售许可证管理办法》](#)
- [《互联网安全保护技术措施规定》](#)
- [《信息安全等级保护管理办法》](#)
- [《计算机病毒防治管理办法》](#)

- 《中国互联网络域名管理办法》
- 《关于进一步做好互联网信息服务电子公告服务审批管理工作的通知》
- 《互联网新闻信息服务管理规定》
- 《互联网医疗保健信息服务管理办法》
- 《互联网视听节目服务管理规定》
- 《教育网站和网校暂行管理办法》
- 《互联网药品信息服务管理办法》
- 《互联网文化管理暂行规定》
- 《互联网站管理工作细则》
- 《非经营性互联网信息服务备案管理办法》
- 《互联网信息服务管理办法》
- 《关于加强互联网易制毒化学品销售信息管理的公告》
- 《关于办理网络赌博犯罪案件适用法律若干问题的解释》
- 《互联网站禁止传播淫秽、色情等不良信息自律规范》
- 《互联网危险物品信息发布管理规定》
- 《互联网用户账号名称管理规定》
- 《中华人民共和国网络安全法》
- 《互联网上网服务营业场所管理条例》
- 《最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》
- 《最高人民法院、最高人民检察院关于利用网络云盘制作、复制、贩卖、传播淫秽电子信息牟利行为定罪量刑问题的批复》
- 《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的解释》
- 《最高人民法院关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释》
- 《通信短信息服务管理规定》
- 《电信业务经营许可管理办法》
- 《电信用户申诉处理办法》
- 《电信设备进网管理办法》
- 《电信和互联网用户个人信息保护规定》
- 《通信网络安全防护管理办法》
- 《工业和信息化部关于进一步规范因特网数据中心业务和因特网接入服务业务市场准入工作的通告》
- 《工业和信息化部关于清理规范互联网网络接入服务市场的通知》
- 四部门关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告

🔗 《民法典》

《民法典》：<http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml>

🔗 《个人信息保护法》

《个人信息保护法》：<https://flk.npc.gov.cn/detail2.html?ZmY4MDgxODE3YjYONzJhMzAxN2I2NTZjYzlwNDAwNDQ=>

🔗 《数据安全法》

《数据安全法》：<https://flk.npc.gov.cn/detail2.html?ZmY4MDgxODE3OWY1ZTA4MDAxNzlmODg1YzdlNzAzOTI=>

🔗 《关键信息基础设施安全保护条例》

《关键信息基础设施安全保护条例》：[https://flk.npc.gov.cn/detail2.html?](https://flk.npc.gov.cn/detail2.html?ZmY4MDgxODE3YjYkzNTAxN2I3YmNjNDk4NzdlMGI=)

[ZmY4MDgxODE3YjYkzNTAxN2I3YmNjNDk4NzdlMGI=](https://flk.npc.gov.cn/detail2.html?ZmY4MDgxODE3YjYkzNTAxN2I3YmNjNDk4NzdlMGI=)

🔗 《汽车数据安全若干规定（试行）》

《汽车数据安全若干规定（试行）》：http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm

🔗 《信息安全技术 个人信息安全规范》

《信息安全技术 个人信息安全规范》：[http://openstd.samr.gov.cn/bzgk/gb/newGbInfo?](http://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E)

[hcno=4568F276E0F8346EB0FBA097AA0CE05E](http://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E)

🔗 《儿童个人信息网络保护规定》

《儿童个人信息网络保护规定》：http://www.cac.gov.cn/2019-08/23/c_1124913903.htm

🔗 《工业和信息化部关于加强呼叫中心业务管理的通知》

《工业和信息化部关于加强呼叫中心业务管理的通

知》：https://www.miit.gov.cn/zwgk/zcwj/wjfb/txy/art/2020/art_d68d7bd0a2a148fb8f9b94547ab5397f.html

🔗 《工业和信息化部办公厅关于深入推进移动物联网全面发展的通知》

《工业和信息化部办公厅关于深入推进移动物联网全面发展的通

知》：https://www.miit.gov.cn/zwgk/zcwj/wjfb/txy/art/2020/art_8884805a987e4a4fa454cfabc3f32b2a.html

🔗 《中华人民共和国出口管制法》

《中华人民共和国出口管制

法》：<http://www.npc.gov.cn/npc/c30834/202010/cf4e0455f6424a38b5aecf8001712c43.shtml>

🔗 《最高人民法院最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》

《最高人民法院最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》

释》：http://www.cac.gov.cn/2019-10/25/c_1573534999086260.htm

🔗 关于印发《App违法违规收集使用个人信息行为认定方法》的通知

关于印发《App违法违规收集使用个人信息行为认定方法》的通知：[http://www.cac.gov.cn/2019-](http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm)

[12/27/c_1578986455686625.htm](http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm)

🔗 《网络安全审查办法》

《网络安全审查办法》：http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

🔗 《网络信息内容生态治理规定》

《网络信息内容生态治理规定》：http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm

🔗 《全国人民代表大会常务委员会关于加强网络信息保护的決定》

全国人民代表大会常务委员会关于加强网络信息保护的決定

(2012年12月28日第十一届全国人民代表大会常务委员会第三十次会议通过)

为了保护网络信息安全，保障公民、法人和其他组织的合法权益，维护国家安全和社会公共利益，特作如下决定：

一、国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。

任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。

二、网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。

网络服务提供者和其他企业事业单位收集、使用公民个人电子信息，应当公开其收集、使用规则。

三、网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

四、网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。

五、网络服务提供者应当加强对其用户发布的信息的管理，发现法律、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，保存有关记录，并向有关主管部门报告。

六、网络服务提供者为用户办理网站接入服务，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服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。

七、任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。

八、公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。

九、任何组织和个人对窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为，有权向有关主管部门举报、控告；接到举报、控告的部门应当依法及时处理。被侵权人可以依法提起诉讼。

十、有关主管部门应当在各自职权范围内依法履行职责，采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为。有关主管部门依法履行职责时，网络服务提供者应当予以配合，提供技术支持。

国家机关及其工作人员对在履行职责中知悉的公民个人电子信息应当予以保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

十一、对有违反本决定行为的，依法给予警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务等处罚，记入社会信用档案并予以公布；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。侵害他人民事权益的，依法承担民事责任。

十二、本决定自公布之日起施行。

《全国人民代表大会常务委员会关于维护互联网安全的决定》

全国人民代表大会常务委员会关于维护互联网安全的决定

(2000年12月28日第九届全国人民代表大会常务委员会第十九次会议通过)

我国的互联网，在国家大力倡导和积极推动下，在经济建设和各项事业中得到日益广泛的应用，使人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化，对于加快我国国民经济、科学技术的发展和社会服务信息化进程具有重要作用。同时，如何保障互联网的运行安全和信息安全问题已经引起全社会的普遍关注。为了兴利除弊，促进我国互联网的健康发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益，特作如下决定：

一、为了保障互联网的运行安全，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

- (一) 侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统；
- (二) 故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害；
- (三) 违反国家规定，擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行。

二、为了维护国家安全和社会稳定，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

- (一) 利用互联网造谣、诽谤或者发表、传播其他有害信息，煽动颠覆国家政权、推翻社会主义制度，或者煽动分裂国家、破坏国家统一；
- (二) 通过互联网窃取、泄露国家秘密、情报或者军事秘密；
- (三) 利用互联网煽动民族仇恨、民族歧视，破坏民族团结；
- (四) 利用互联网组织邪教组织、联络邪教组织成员，破坏国家法律、行政法规实施。

三、为了维护社会主义市场经济秩序和社会管理秩序，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

- (一) 利用互联网销售伪劣产品或者对商品、服务作虚假宣传；
- (二) 利用互联网损害他人商业信誉和商品声誉；
- (三) 利用互联网侵犯他人知识产权；
- (四) 利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息；
- (五) 在互联网上建立淫秽网站、网页，提供淫秽站点链接服务，或者传播淫秽书刊、影片、音像、图片。

四、为了保护个人、法人和其他组织的人身、财产等合法权利，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

- (一) 利用互联网侮辱他人或者捏造事实诽谤他人；
- (二) 非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密；
- (三) 利用互联网进行盗窃、诈骗、敲诈勒索。

五、利用互联网实施本决定第一条、第二条、第三条、第四条所列行为以外的其他行为，构成犯罪的，依照刑法有关规定追究刑事责任。

六、利用互联网实施违法行为，违反社会治安管理，尚不构成犯罪的，由公安机关依照《治安管理处罚条例》予以处罚；违反其他法律、行政法规，尚不构成犯罪的，由有关行政管理部门依法给予行政处罚；对直接负责的主管人员和其他直接责任人员，依法给予行政处分或者纪律处分。

利用互联网侵犯他人合法权益，构成民事侵权的，依法承担民事责任。

七、各级人民政府及有关部门要采取积极措施，在促进互联网的应用和网络技术的普及过程中，重视和支持对网络安全技术的研究和开发，增强网络的安全防护能力。有关主管部门要加强对互联网的运行安全和信息安全的宣传教育，依法实施有效的监督管理，防范和制止利用互联网进行的各种违法活动，为互联网的健康发展创造良好的社会环境。从事互联网业务的单位要依法开展活动，发现互联网上出现违法犯罪行为和有害信息时，要采取措施，停止传输有害信息，并及时向有关机关报告。任何单位和个人在利用互联网时，都要遵纪守法，抵制各种违法犯罪行为和有害信息。人民法院、人民检察院、公安机关、国家安全机关要各司其职，密切配合，依法严厉打击利用互联网实施的各种犯罪活动。要动员全社会的力量，依靠全社会的共同努力，保障互联网的运行安全与信息安全，促进社会主义精神文明和物质文明建设。

《中华人民共和国电信条例》

中华人民共和国电信条例

(中华人民共和国国务院令(第291号))

第一章 总 则

第一条 为了规范电信市场秩序，维护电信用户和电信业务经营者的合法权益，保障电信网络和信息的安全，促进电信业的健康发展，制定本条例。

第二条 在中华人民共和国境内从事电信活动或者与电信有关的活动，必须遵守本条例。

本条例所称电信，是指利用有线、无线的电磁系统或者光电系统，传送、发射或者接收语音、文字、数据、图像以及其他任何形式信息的活动。

第三条 国务院信息产业主管部门依照本条例的规定对全国电信业实施监督管理。

省、自治区、直辖市电信管理机构在国务院信息产业主管部门的领导下，依照本条例的规定对本行政区域内的电信业实施监督管理。

第四条 电信监督管理遵循政企分开、破除垄断、鼓励竞争、促进发展和公开、公平、公正的原则。

电信业务经营者应当依法经营，遵守商业道德，接受依法实施的监督检查。

第五条 电信业务经营者应当为电信用户提供迅速、准确、安全、方便和价格合理的电信服务。

第六条 电信网络和信息的安全受法律保护。任何组织或者个人不得利用电信网络从事危害国家安全、社会公共利益或者他人合法权益的活动。

第二章 电信市场

第一节 电信业务许可

第七条 国家对电信业务经营按照电信业务分类，实行许可制度。

经营电信业务，必须依照本条例的规定取得国务院信息产业主管部门或者省、自治区、直辖市电信管理机构颁发的电信业务经营许可证。

未取得电信业务经营许可证，任何组织或者个人不得从事电信业务经营活动。

第八条 电信业务分为基础电信业务和增值电信业务。

基础电信业务，是指提供公共网络基础设施、公共数据传送和基本话音通信服务的业务。增值电信业务，是指利用公共网络基础设施提供的电信与信息服务的业务。

电信业务分类的具体划分在本条例所附的《电信业务分类目录》中列出。国务院信息产业主管部门根据实际情况，可以对目录所列电信业务分类项目作局部调整，重新公布。

第九条 经营基础电信业务，须经国务院信息产业主管部门审查批准，取得《基础电信业务经营许可证》。

经营增值电信业务，业务覆盖范围在两个以上省、自治区、直辖市的，须经国务院信息产业主管部门审查批准，取得《跨地区增值电信业务经营许可证》；业务覆盖范围在一个省、自治区、直辖市行政区域内的，须经省、自治区、直辖市电信管理机构审查批准，取得《增值电信业务经营许可证》。

运用新技术试办《电信业务分类目录》未列出的新型电信业务的，应当向省、自治区、直辖市电信管理机构备案。

第十条 经营基础电信业务，应当具备下列条件：

- (一)经营者为依法设立的专门从事基础电信业务的公司，且公司中国有股权或者股份不少于51%；
- (二)有可行性研究报告和组网技术方案；
- (三)有与从事经营活动相适应的资金和专业人员；
- (四)有从事经营活动的场地及相应的资源；
- (五)有为用户提供长期服务的信誉或者能力；

(六)国家规定的其他条件。

第十一条 申请经营基础电信业务，应当向国务院信息产业主管部门提出申请，并提交本条例第十条规定的相关文件。国务院信息产业主管部门应当自受理申请之日起180日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发《基础电信业务经营许可证》；不予批准的，应当书面通知申请人并说明理由。

第十二条 国务院信息产业主管部门审查经营基础电信业务的申请时，应当考虑国家安全、电信网络安全、电信资源可持续利用、环境保护和电信市场的竞争状况等因素。

颁发《基础电信业务经营许可证》，应当按照国家有关规定采用招标方式。

第十三条 经营增值电信业务，应当具备下列条件：

(一)经营者为依法设立的公司；

(二)有与开展经营活动相适应的资金和专业人员；

(三)有为用户提供长期服务的信誉或者能力；

(四)国家规定的其他条件。

第十四条 申请经营增值电信业务，应当根据本条例第九条第二款的规定，向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构提出申请，并提交本条例第十三条规定的相关文件。申请经营的增值电信业务，按照国家有关规定须经有关主管部门审批的，还应当提交有关主管部门审核同意的文件。国务院信息产业主管部门或者省、自治区、直辖市电信管理机构应当自收到申请之日起60日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发《跨地区增值电信业务经营许可证》或者《增值电信业务经营许可证》；不予批准的，应当书面通知申请人并说明理由。

第十五条 电信业务经营者在经营过程中，变更经营主体、业务范围或者停止经营的，应当提前90日向原颁发许可证的机关提出申请，并办理相应手续；停止经营的，还应当按照国家有关规定做好善后工作。

第十六条 经批准经营电信业务的，应当持依法取得的电信业务经营许可证，向企业登记机关办理登记手续。

专用电信网运营单位在所在地区经营电信业务的，应当依照本条例规定的条件和程序提出申请，经批准，取得电信业务经营许可证，并依照前款规定办理登记手续。

第二节 电信网间互联

第十七条 电信网之间应当按照技术可行、经济合理、公平公正、相互配合的原则，实现互联互通。

主导的电信业务经营者不得拒绝其他电信业务经营者和专用网运营单位提出的互联互通要求。

前款所称主导的电信业务经营者，是指控制必要的基础电信设施并且在电信业务市场中占有较大份额，能够对其他电信业务经营者进入电信业务市场构成实质性影响的经营者。

主导的电信业务经营者由国务院信息产业主管部门确定。

第十八条 主导的电信业务经营者应当按照非歧视和透明化的原则，制定包括网间互联的程序、时限、非捆绑网络元素目录等内容的互联规程。互联规程应当报国务院信息产业主管部门审查同意。该互联规程对主导的电信业务经营者的互联互通活动具有约束力。

第十九条 公用电信网之间、公用电信网与专用电信网之间的网间互联，由网间互联双方按照国务院信息产业主管部门的网间互联管理规定进行互联协商，并订立网间互联协议。

网间互联协议应当向国务院信息产业主管部门备案。

第二十条 网间互联双方经协商未能达成网间互联协议的，自一方提出互联要求之日起60日内，任何一方均可以按照网间互联覆盖范围向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构申请协调；收到申请的机关应当依照本条例第十七条第一款规定的原则进行协调，促使网间互联双方达成协议；自网间互联一方或者双方申请协调之日起45日内经协调仍不能达成协议的，由协调机关随机邀请电信技术专家和其他有关方面专家进行公开论证并提出网间互联方案。协调机关应当根据专家论证结论和提出的网间互联方案作出决定，强制实现互联互通。

第二十一条 网间互联双方必须在协议约定或者决定规定的时限内实现互联互通。未经国务院信息产业主管部门批准，任何一方不得擅自中断互联互通。网间互联遇有通信技术障碍的，双方应当立即采取有效措施予以消除。网间互联双方在互联互通中发生争议的，依照本条例第二十条规定的程序和办法处理。

网间互联的通信质量应当符合国家有关标准。主导的电信业务经营者向其他电信业务经营者提供网间互联，服务质量不得低于本网内的同类业务及向其子公司或者分支机构提供的同类业务质量。

第二十二条 网间互联的费用结算与分摊应当执行国家有关规定，不得在规定标准之外加收费用。

网间互联的技术标准、费用结算办法和具体管理规定，由国务院信息产业主管部门制定。

第三节 电信资费

第二十三条 电信资费标准实行以成本为基础的定价原则，同时考虑国民经济与社会发展要求、电信业的发展和电信用户的承受能力等因素。

第二十四条 电信资费分为市场调节价、政府指导价和政府定价。

基础电信业务资费实行政府定价、政府指导价或者市场调节价；增值电信业务资费实行市场调节价或者政府指导价。

市场竞争充分的电信业务，电信资费实行市场调节价。

实行政府定价、政府指导价和市场调节价的电信资费分类管理目录，由国务院信息产业主管部门经征求国务院价格主管部门意见制定并公布施行。

第二十五条 政府定价的重要的电信业务资费标准，由国务院信息产业主管部门提出方案，经征求国务院价格主管部门意见，报国务院批准后公布施行。

政府指导价的电信业务资费标准幅度，由国务院信息产业主管部门经征求国务院价格主管部门意见，制定并公布施行。电信业务经营者在标准幅度内，自主确定资费标准，报省、自治区、直辖市电信管理机构备案。

第二十六条 制定政府定价和政府指导价的电信业务资费标准，应当采取举行听证会等形式，听取电信业务经营者、电信用户和其他有关方面的意见。

电信业务经营者应当根据国务院信息产业主管部门和省、自治区、直辖市电信管理机构的要求，提供准确、完备的业务成本数据及其他有关资料。

第四节 电信资源

第二十七条 国家对电信资源统一规划、集中管理、合理分配，实行有偿使用制度。

前款所称电信资源，是指无线电频率、卫星轨道位置、电信网码号等用于实现电信功能且有限的资源。

第二十八条 电信业务经营者占有、使用电信资源，应当缴纳电信资源费。具体收费办法由国务院信息产业主管部门会同国务院财政部门、价格主管部门制定，报国务院批准后公布施行。

第二十九条 电信资源的分配，应当考虑电信资源规划、用途和预期服务能力。

分配电信资源，可以采取指配的方式，也可以采用拍卖的方式。

取得电信资源使用权的，应当在规定的时限内启用所分配的资源，并达到规定的最低使用规模。未经国务院信息产业主管部门或者省、自治区、直辖市电信管理机构批准，不得擅自使用、转让、出租电信资源或者改变电信资源的用途。

第三十条 电信资源使用者依法取得电信网码号资源后，主导的电信业务经营者和其他有关单位有义务采取必要的技术措施，配合电信资源使用者实现其电信网码号资源的功能。

法律、行政法规对电信资源管理另有特别规定的，从其规定。

第三章 电信服务

第三十一条 电信业务经营者应当按照国家规定的电信服务标准向电信用户提供服务。电信业务经营者提供服务的种类、范围、

资费标准和时限，应当向社会公布，并报省、自治区、直辖市电信管理机构备案。

电信用户有权自主选择使用依法开办的各类电信业务。

第三十二条 电信用户申请安装、移装电信终端设备的，电信业务经营者应当在其公布的时限内保证装机开通；由于电信业务经营者的原因逾期未能装机开通的，应当每日按照收取的安装费、移装费或者其他费用数额百分之一的比例，向电信用户支付违约金。

第三十三条 电信用户申告电信服务障碍的，电信业务经营者应当自接到申告之日起，城镇48小时、农村72小时内修复或者调通；不能按期修复或者调通的，应当及时通知电信用户，并免收障碍期间的月租费用。但是，属于电信终端设备的原因造成电信服务障碍的除外。

第三十四条 电信业务经营者应当为电信用户交费和查询提供方便。电信用户要求提供国内长途通信、国际通信、移动通信和信息服务等收费清单的，电信业务经营者应当免费提供。

电信用户出现异常的巨额电信费用时，电信业务经营者一经发现，应当尽可能迅速告知电信用户，并采取相应的措施。

前款所称巨额电信费用，是指突然出现超过电信用户此前三个月平均电信费用5倍以上的费用。

第三十五条 电信用户应当按照约定的时间和方式及时、足额地向电信业务经营者交纳电信费用；电信用户逾期不交纳电信费用的，电信业务经营者有权要求补交电信费用，并可以按照所欠费用每日加收3‰的违约金。

对超过收费约定期限30日仍不交纳电信费用的电信用户，电信业务经营者可以暂停向其提供电信服务。电信用户在电信业务经营者暂停服务60日内仍未补交电信费用和违约金的，电信业务经营者可以终止提供服务，并可以依法追缴欠费和违约金。

经营移动电信业务的经营者可以与电信用户约定交纳电信费用的期限、方式，不受前款规定期限的限制。

电信业务经营者应当在迟延交纳电信费用的电信用户补足电信费用、违约金后的48小时内，恢复暂停的电信服务。

第三十六条 电信业务经营者因工程施工、网络建设等原因，影响或者可能影响正常电信服务的，必须按照规定的时限及时告知用户，并向省、自治区、直辖市电信管理机构报告。

因前款原因中断电信服务的，电信业务经营者应当相应减免用户在电信服务中断期间的相关费用。

出现本条第一款规定的情形，电信业务经营者未及时告知用户的，应当赔偿由此给用户造成的损失。

第三十七条 经营本地电话业务和移动电话业务的电信业务经营者，应当免费向用户提供火警、匪警、医疗急救、交通事故报警等公益性电信服务并保障通信线路畅通。

第三十八条 电信业务经营者应当及时为需要通过中继线接入其电信网的集团用户，提供平等、合理的接入服务。

未经批准，电信业务经营者不得擅自中断接入服务。

第三十九条 电信业务经营者应当建立健全内部服务质量管理制度，并可以制定并公布施行高于国家规定的电信服务标准的企业标准。

电信业务经营者应当采取各种形式广泛听取电信用户意见，接受社会监督，不断提高电信服务质量。

第四十条 电信业务经营者提供的电信服务达不到国家规定的电信服务标准或者其公布的企业标准的，或者电信用户对交纳电信费用持有异议的，电信用户有权要求电信业务经营者予以解决；电信业务经营者拒不解决或者电信用户对解决结果不满意的，电信用户有权向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构或者其他有关部门申诉。收到申诉的机关必须对申诉及时处理，并自收到申诉之日起30日内向申诉者作出答复。

电信用户对交纳本地电话费用有异议的，电信业务经营者还应当应电信用户的要求免费提供本地电话收费依据，并有义务采取必要措施协助电信用户查找原因。

第四十一条 电信业务经营者在电信服务中，不得有下列行为：

(一)以任何方式限定电信用户使用其指定的业务；

(二)限定电信用户购买其指定的电信终端设备或者拒绝电信用户使用自备的已经取得入网许可的电信终端设备；

- (三)违反国家规定，擅自改变或者变相改变资费标准，擅自增加或者变相增加收费项目；
- (四)无正当理由拒绝、拖延或者中止对电信用户的电信服务；
- (五)对电信用户不履行公开作出的承诺或者作容易引起误解的虚假宣传；
- (六)以不正当手段刁难电信用户或者对投诉的电信用户打击报复。

第四十二条 电信业务经营者在电信业务经营活动中，不得有下列行为：

- (一)以任何方式限制电信用户选择其他电信业务经营者依法开办的电信服务；
- (二)对其经营的不同业务进行不合理的交叉补贴；
- (三)以排挤竞争对手为目的，低于成本提供电信业务或者服务，进行不正当竞争。

第四十三条 国务院信息产业主管部门或者省、自治区、直辖市电信管理机构应当依据职权对电信业务经营者的电信服务质量和经营活动进行监督检查，并向社会公布监督检查结果。

第四十四条 电信业务经营者必须按照国家有关规定履行相应的电信普遍服务义务。

国务院信息产业主管部门可以采取指定的或者招标的方式确定电信业务经营者具体承担电信普遍服务的义务。

电信普遍服务成本补偿管理办法，由国务院信息产业主管部门会同国务院财政部门、价格主管部门制定，报国务院批准后公布施行。

第四章 电信建设

第一节 电信设施建设

第四十五条 公用电信网、专用电信网、广播电视传输网的建设应当接受国务院信息产业主管部门的统筹规划和行业管理。

属于全国性信息网络工程或者国家规定限额以上建设项目的公用电信网、专用电信网、广播电视传输网建设，在按照国家基本建设项目审批程序报批前，应当征得国务院信息产业主管部门同意。

基础电信建设项目应当纳入地方各级人民政府城市建设总体规划和村镇、集镇建设总体规划。

第四十六条 城市建设和村镇、集镇建设应当配套设置电信设施。建筑物内的电信管线和配线设施以及建设项目用地范围内的电信管道，应当纳入建设项目的设计文件，并随建设项目同时施工与验收。所需经费应当纳入建设项目概算。

有关单位或者部门规划、建设道路、桥梁、隧道或者地下铁道等，应当事先通知省、自治区、直辖市电信管理机构和电信业务经营者，协商预留电信管线等事宜。

第四十七条 基础电信业务经营者可以在民用建筑物上附挂电信线路或者设置小型天线、移动通信基站等公用电信设施，但是应当事先通知建筑物产权人或者使用人，并按照省、自治区、直辖市人民政府规定的标准向该建筑物的产权人或者其他权利人支付使用费。

第四十八条 建设地下、水底等隐蔽电信设施和高空电信设施，应当按照国家有关规定设置标志。

基础电信业务经营者建设海底电信缆线，应当征得国务院信息产业主管部门同意，并征求有关部门意见后，依法办理有关手续。海底电信缆线由国务院有关部门在海图上标出。

第四十九条 任何单位或者个人不得擅自改动或者迁移他人的电信线路及其他电信设施；遇有特殊情况必须改动或者迁移的，应当征得该电信设施产权人同意，由提出改动或者迁移要求的单位或者个人承担改动或者迁移所需费用，并赔偿由此造成的经济损失。

第五十条 从事施工、生产、种植树木等活动，不得危及电信线路或者其他电信设施的安全或者妨碍线路畅通；可能危及电信安全时，应当事先通知有关电信业务经营者，并由从事该活动的单位或者个人负责采取必要的安全防护措施。

违反前款规定，损害电信线路或者其他电信设施或者妨碍线路畅通的，应当恢复原状或者予以修复，并赔偿由此造成的经济损失。

第五十一条 从事电信线路建设，应当与已建的电信线路保持必要的安全距离；难以避开或者必须穿越，或者需要使用已建电信管道的，应当与已建电信线路的产权人协商，并签订协议；经协商不能达成协议的，根据不同情况，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构协调解决。

第五十二条 任何组织或者个人不得阻止或者妨碍基础电信业务经营者依法从事电信设施建设和向电信用户提供公共电信服务；但是，国家规定禁止或者限制进入的区域除外。

第五十三条 执行特殊通信、应急通信和抢险任务的电信车辆，经公安交通管理部门批准，在保障交通安全畅通的前提下可以不受各种禁止机动车通行标志的限制。

第二节 电信设备进网

第五十四条 国家对电信终端设备、无线电通信设备和涉及网间互联的设备实行进网许可制度。

接入公用电信网的电信终端设备、无线电通信设备和涉及网间互联的设备，必须符合国家规定的标准并取得进网许可证。

实行进网许可制度的电信设备目录，由国务院信息产业主管部门会同国务院产品质量监督部门制定并公布施行。

第五十五条 办理电信设备进网许可证的，应当向国务院信息产业主管部门提出申请，并附送经国务院产品质量监督部门认可的电信设备检测机构出具的检测报告或者认证机构出具的产品质量认证证书。

国务院信息产业主管部门应当自收到电信设备进网许可申请之日起60日内，对申请及电信设备检测报告或者产品质量认证证书审查完毕。经审查合格的，颁发进网许可证；经审查不合格的，应当书面答复并说明理由。

第五十六条 电信设备生产企业必须保证获得进网许可的电信设备的质量稳定、可靠，不得降低产品质量和性能。

电信设备生产企业应当在其生产的获得进网许可的电信设备上粘贴进网许可标志。

国务院产品质量监督部门应当会同国务院信息产业主管部门对获得进网许可证的电信设备进行质量跟踪和监督抽查，公布抽查结果。

第五章 电信安全

第五十七条 任何组织或者个人不得利用电信网络制作、复制、发布、传播含有下列内容的信息：

- (一)反对宪法所确定的基本原则的；
- (二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- (三)损害国家荣誉和利益的；
- (四)煽动民族仇恨、民族歧视，破坏民族团结的；
- (五)破坏国家宗教政策，宣扬邪教和封建迷信的；
- (六)散布谣言，扰乱社会秩序，破坏社会稳定的；
- (七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- (八)侮辱或者诽谤他人，侵害他人合法权益的；
- (九)含有法律、行政法规禁止的其他内容的。

第五十八条 任何组织或者个人不得有下列危害电信网络和信息安全的行为：

- (一)对电信网的功能或者存储、处理、传输的数据和应用程序进行删除或者修改；
- (二)利用电信网从事窃取或者破坏他人信息、损害他人合法权益的活动；
- (三)故意制作、复制、传播计算机病毒或者以其他方式攻击他人电信网络等电信设施；
- (四)危害电信网络和信息安全的其他行为。

第五十九条 任何组织或者个人不得有下列扰乱电信市场秩序的行为：

- (一)采取租用电信国际专线、私设转接设备或者其他方法，擅自经营国际或者香港特别行政区、澳门特别行政区和台湾地区电信业务；
- (二)盗接他人电信线路，复制他人电信码号，使用明知是盗接、复制的电信设施或者码号；
- (三)伪造、变造电话卡及其他各种电信服务有价凭证；
- (四)以虚假、冒用的身份证件办理入网手续并使用移动电话。

第六十条 电信业务经营者应当按照国家有关电信安全的规定，建立健全内部安全保障制度，实行安全保障责任制。

第六十一条 电信业务经营者在电信网络的设计、建设和运行中，应当做到与国家安全和电信网络安全的需求同步规划，同步建设，同步运行。

第六十二条 在公共信息服务中，电信业务经营者发现电信网络中传输的信息明显属于本条例第五十七条所列内容的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第六十三条 使用电信网络传输信息的内容及其后果由电信用户负责。

电信用户使用电信网络传输的信息属于国家秘密信息的，必须依照保守国家秘密法的规定采取保密措施。

第六十四条 在发生重大自然灾害等紧急情况下，经国务院批准，国务院信息产业主管部门可以调用各种电信设施，确保重要通信畅通。

第六十五条 在中华人民共和国境内从事国际通信业务，必须通过国务院信息产业主管部门批准设立的国际通信出入口局进行。

我国内地与香港特别行政区、澳门特别行政区和台湾地区之间的通信，参照前款规定办理。

第六十六条 电信用户依法使用电信的自由和通信秘密受法律保护。除因国家安全或者追查刑事犯罪的需要，由公安机关、国家安全机关或者人民检察院依照法律规定的程序对电信内容进行检查外，任何组织或者个人不得以任何理由对电信内容进行检查。

电信业务经营者及其工作人员不得擅自向他人提供电信用户使用电信网络所传输信息的内容。

第六章 罚 则

第六十七条 违反本条例第五十七条、第五十八条的规定，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照有关法律、行政法规的规定予以处罚。

第六十八条 有本条例第五十九条第(二)、(三)、(四)项所列行为之一，扰乱电信市场秩序，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正，没收违法所得，处违法所得3倍以上5倍以下罚款；没有违法所得或者违法所得不足1万元的，处1万元以上10万元以下罚款。

第六十九条 违反本条例的规定，伪造、冒用、转让电信业务经营许可证、电信设备进网许可证或者编造在电信设备上标注的进网许可证编号的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权没收违法所得，处违法所得3倍以上5倍以下罚款；没有违法所得或者违法所得不足1万元的，处1万元以上10万元以下罚款。

第七十条 违反本条例规定，有下列行为之一的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正，没收违法所得，处违法所得3倍以上5倍以下罚款；没有违法所得或者违法所得不足5万元的，处10万元以上100万元以下罚款；情节严重的，责令停业整顿：

- (一)违反本条例第七条第三款的规定或者有本条例第五十九条第(一)项所列行为，擅自经营电信业务的，或者超范围经营电信业务的；
- (二)未通过国务院信息产业主管部门批准，设立国际通信出入口进行国际通信的；
- (三)擅自使用、转让、出租电信资源或者改变电信资源用途的；
- (四)擅自中断网间互联互通或者接入服务的；

(五)拒不履行普遍服务义务的。

第七十一条 违反本条例的规定，有下列行为之一的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正，没收违法所得，处违法所得1倍以上3倍以下罚款；没有违法所得或者违法所得不足1万元的，处1万元以上10万元以下罚款；情节严重的，责令停业整顿：

(一)在电信网间互联中违反规定加收费用的；

(二)遇有网间通信技术障碍，不采取有效措施予以消除的；

(三)擅自向他人提供电信用户使用电信网络所传输信息的内容的；

(四)拒不按照规定缴纳电信资源使用费的。

第七十二条 违反本条例第四十二条的规定，在电信业务经营活动中进行不正当竞争的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正，处10万元以上100万元以下罚款；情节严重的，责令停业整顿。

第七十三条 违反本条例的规定，有下列行为之一的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正，处5万元以上50万元以下罚款；情节严重的，责令停业整顿：

(一)拒绝其他电信业务经营者提出的互联互通要求的；

(二)拒不执行国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依法作出的互联互通决定的；

(三)向其他电信业务经营者提供网间互联的服务质量低于本网及其子公司或者分支机构的。

第七十四条 违反本条例第三十四条第一款、第四十条第二款的规定，电信业务经营者拒绝免费为电信用户提供国内长途通信、国际通信、移动通信和信息服务等收费清单，或者电信用户对交纳本地电话费用有异议并提出要求时，拒绝为电信用户免费提供本地电话收费依据的，由省、自治区、直辖市电信管理机构责令改正，并向电信用户赔礼道歉；拒不改正并赔礼道歉的，处以警告，并处5000元以上5万元以下的罚款。

第七十五条 违反本条例第四十一条的规定，由省、自治区、直辖市电信管理机构责令改正，并向电信用户赔礼道歉，赔偿电信用户损失；拒不改正并赔礼道歉、赔偿损失的，处以警告，并处1万元以上10万元以下的罚款；情节严重的，责令停业整顿。

第七十六条 违反本条例的规定，有下列行为之一的，由省、自治区、直辖市电信管理机构责令改正，处1万元以上10万元以下的罚款：

(一)销售未取得进网许可的电信终端设备的；

(二)非法阻止或者妨碍电信业务经营者向电信用户提供公共电信服务的；

(三)擅自改动或者迁移他人的电信线路及其他电信设施的。

第七十七条 违反本条例的规定，获得电信设备进网许可证后降低产品质量和性能的，由产品质量监督部门依照有关法律、行政法规的规定予以处罚。

第七十八条 有本条例第五十七条、第五十八条和第五十九条所列禁止行为之一，情节严重的，由原发证机关吊销电信业务经营许可证。

国务院信息产业主管部门或者省、自治区、直辖市电信管理机构吊销电信业务经营许可证后，应当通知企业登记机关。

第七十九条 国务院信息产业主管部门或者省、自治区、直辖市电信管理机构工作人员玩忽职守、滥用职权、徇私舞弊，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，依法给予行政处分。

第七章 附 则

第八十条 外国的组织或者个人在中华人民共和国境内投资与经营电信业务和香港特别行政区、澳门特别行政区与台湾地区的组织或者个人在内地投资与经营电信业务的具体办法，由国务院另行制定。

第八十一条 本条例自公布之日起施行。

附：电信业务分类目录

一、基础电信业务

- (一)固定网络国内长途及本地电话业务；
- (二)移动网络电话和数据业务；
- (三)卫星通信及卫星移动通信业务；
- (四)互联网及其它公共数据传送业务；
- (五)带宽、波长、光纤、光缆、管道及其它网络元素出租、出售业务；
- (六)网络承载、接入及网络外包等业务；
- (七)国际通信基础设施、国际电信业务；
- (八)无线寻呼业务；
- (九)转售的基础电信业务。

第(八)、(九)项业务比照增值电信业务管理。

二、增值电信业务

- (一)电子邮件；
- (二)语音信箱；
- (三)在线信息库存储和检索；
- (四)电子数据交换；
- (五)在线数据处理与交易处理；
- (六)增值传真；
- (七)互联网接入服务；
- (八)互联网信息服务；
- (九)可视电话会议服务。

🔗 《中华人民共和国计算机信息系统安全保护条例》

《中华人民共和国计算机信息系统安全保护条例》

中华人民共和国国务院令（147号）

现发布《中华人民共和国计算机信息系统安全保护条例》，自发布之日起施行。

总理 李鹏

1994年2月18日

第一章 总则

第一条 为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定本条例。

第二条 本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，

保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第四条 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。

第五条 中华人民共和国境内的计算机信息系统的安全保护，适用本条例。未联网的微型计算机的安全保护办法，另行制定。

第六条 公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

第七条 任何组织或个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法权益的活动，不得危害计算机信息系统的安全。

第二章 安全保护制度

第八条 计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。

第九条 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。

第十条 计算机机房应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。

第十一条 进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

第十二条 运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。

第十三条 计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

第十四条 对计算机信息系统中发生的案件，有关使用单位应当在24小时内向当地县级以上人民政府公安机关报告。

第十五条 对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

第十六条 国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

第三章 安全监督

第十七条 公安机关对计算机信息系统保护工作行使下列监督职权：

- (一)监督、检查、指导计算机信息系统安全保护工作；
- (二)查处危害计算机信息系统安全的违法犯罪案件；
- (三)履行计算机信息系统安全保护工作的其他监督职责。

第十八条 公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

第十九条 公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

第四章 法律责任

第二十条 违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：

- (一)违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；
- (二)违反计算机信息系统国际联网备案制度的；
- (三)不按照规定时间报告计算机信息系统中发生的案件的；
- (四)接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；
- (五)有危害计算机信息系统安全的其他行为的。

第二十一条 计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

第二十二条 运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的，由海关依照《中华人民共和国海关法》和本条例以及其他有关法律、法规的规定处理。

第二十三条 故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以5000元以下的罚款、对单位处以15000元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得1至3倍的罚款。

第二十四条 违反本条例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚条例》的有关规定处罚；构成犯罪的，依法追究刑事责任。

第二十五条 任何组织或者个人违反本条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

第二十六条 当事人对公安机关依照本条例所作出的具体行政行为不服的，可以依法申请行政复议或者提起行政诉讼。

第二十七条 执行本条例的国家公务员利用职权，索取、收受贿赂或者有其他违法、失职行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，给予行政处分。

第五章 附则

第二十八条 本条例下列用语的含义：计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

第二十九条 军队的计算机信息系统安全保护工作，按照军队的有关法规执行。

第三十条 公安部可以根据本条例制定实施办法。

第三十一条 本条例自发布之日起施行。

《信息网络传播权保护条例（2013年1月30日修正版）》

信息网络传播权保护条例（2013年1月30日修正版）

（2006年5月18日中华人民共和国国务院令 第468号公布 根据2013年1月30日《国务院关于修改〈信息网络传播权保护条例〉的决定》修订）

第一条 为保护著作权人、表演者、录音录像制作者（以下统称权利人）的信息网络传播权，鼓励有益于社会主义精神文明、物质文明建设的作品的创作和传播，根据《中华人民共和国著作权法》（以下简称著作权法），制定本条例。

第二条 权利人享有的信息网络传播权受著作权法和本条例保护。除法律、行政法规另有规定的外，任何组织或者个人将他人的作品、表演、录音录像制品通过信息网络向公众提供，应当取得权利人许可，并支付报酬。

第三条 依法禁止提供的作品、表演、录音录像制品，不受本条例保护。

权利人行使信息网络传播权，不得违反宪法和法律、行政法规，不得损害公共利益。

第四条 为了保护信息网络传播权，权利人可以采取技术措施。

任何组织或者个人不得故意避开或者破坏技术措施，不得故意制造、进口或者向公众提供主要用于避开或者破坏技术措施的装置或者部件，不得故意为他人避开或者破坏技术措施提供技术服务。但是，法律、行政法规规定可以避开的除外。

第五条 未经权利人许可，任何组织或者个人不得进行下列行为：

（一）故意删除或者改变通过信息网络向公众提供的作品、表演、录音录像制品的权利管理电子信息，但由于技术上的原因无法避免删除或者改变的除外；

（二）通过信息网络向公众提供明知或者应知未经权利人许可被删除或者改变权利管理电子信息的作品、表演、录音录像制品。

第六条 通过信息网络提供他人作品，属于下列情形的，可以不经著作权人许可，不向其支付报酬：

- （一）为介绍、评论某一作品或者说明某一问题，在向公众提供的作品中适当引用已经发表的作品；
- （二）为报道时事新闻，在向公众提供的作品中不可避免地再现或者引用已经发表的作品；
- （三）为学校课堂教学或者科学研究，向少数教学、科研人员提供少量已经发表的作品；
- （四）国家机关为执行公务，在合理范围内向公众提供已经发表的作品；
- （五）将中国公民、法人或者其他组织已经发表的、以汉语言文字创作的作品翻译成少数民族语言文字作品，向中国境内少数民族提供；
- （六）不以营利为目的，以盲人能够感知的独特方式向盲人提供已经发表的文字作品；
- （七）向公众提供在信息网络上已经发表的关于政治、经济问题的时事性文章；
- （八）向公众提供在公众集会上发表的讲话。

第七条 图书馆、档案馆、纪念馆、博物馆、美术馆等可以不经著作权人许可，通过信息网络向本馆馆舍内服务对象提供本馆收藏的合法出版的数字作品和依法为陈列或者保存版本的需要以数字化形式复制的作品，不向其支付报酬，但不得直接或者间接获得经济利益。当事人另有约定的除外。前款规定的为陈列或者保存版本需要以数字化形式复制的作品，应当是已经损毁或者濒临损毁、丢失或者失窃，或者其存储格式已经过时，并且在市场上无法购买或者只能以明显高于标定的价格购买的作品。

第八条 为通过信息网络实施九年制义务教育或者国家教育规划，可以不经著作权人许可，使用其已经发表作品的片断或者短小的文字作品、音乐作品或者单幅的美术作品、摄影作品制作课件，由制作课件或者依法取得课件的远程教育机构通过信息网络向注册学生提供，但应当向著作权人支付报酬。

第九条 为扶助贫困，通过信息网络向农村地区的公众免费提供中国公民、法人或者其他组织已经发表的种植养殖、防病治病、防灾减灾等与扶助贫困有关的作品和适应基本文化需求的作品，网络服务提供者应当在提供前公告拟提供的作品及其作者、拟支付报酬的标准。自公告之日起30日内，著作权人不同意提供的，网络服务提供者不得提供其作品；自公告之日起满30日，著作权人没有异议的，网络服务提供者可以提供其作品，并按照公告的标准向著作权人支付报酬。网络服务提供者提供著作权人的作品后，著作权人不同意提供的，网络服务提供者应当立即删除著作权人的作品，并按照公告的标准向著作权人支付提供作品期间的报酬。

依照前款规定提供作品的，不得直接或者间接获得经济利益。

第十条 依照本条例规定不经著作权人许可、通过信息网络向公众提供其作品的，还应当遵守下列规定：

- （一）除本条例第六条第（一）项至第（六）项、第七条规定的情形外，不得提供作者事先声明不许提供的作品；
- （二）指明作品的名称和作者的姓名（名称）；
- （三）依照本条例规定支付报酬；
- （四）采取技术措施，防止本条例第七条、第八条、第九条规定的服务对象以外的其他人获得著作权人的作品，并防止本条例第七条规定的服务对象的复制行为对著作权人利益造成实质性损害；
- （五）不得侵犯著作权人依法享有的其他权利。

第十一条 通过信息网络提供他人表演、录音录像制品的，应当遵守本条例第六条至第十条的规定。

第十二条 属于下列情形的，可以避开技术措施，但不得向他人提供避开技术措施的技术、装置或者部件，不得侵犯权利人依法享有的其他权利：

- （一）为学校课堂教学或者科学研究，通过信息网络向少数教学、科研人员提供已经发表的作品、表演、录音录像制品，而该作品、表演、录音录像制品只能通过信息网络获取；
- （二）不以营利为目的，通过信息网络以盲人能够感知的独特方式向盲人提供已经发表的文字作品，而该作品只能通过信息网络获取；

(三) 国家机关依照行政、司法程序执行公务；

(四) 在信息网络上对计算机及其系统或者网络的安全性能进行测试。

第十三条 著作权行政管理部门为了查处侵犯信息网络传播权的行为，可以要求网络服务提供者提供涉嫌侵权的服务对象的姓名（名称）、联系方式、网络地址等资料。

第十四条 对提供信息存储空间或者提供搜索、链接服务的网络服务提供者，权利人认为其服务所涉及的作品、表演、录音录像制品，侵犯自己的信息网络传播权或者被删除、改变了自己的权利管理电子信息的，可以向该网络服务提供者提交书面通知，要求网络服务提供者删除该作品、表演、录音录像制品，或者断开与该作品、表演、录音录像制品的链接。通知书应当包含下列内容：

(一) 权利人的姓名（名称）、联系方式和地址；

(二) 要求删除或者断开链接的侵权作品、表演、录音录像制品的名称和网络地址；

(三) 构成侵权的初步证明材料。

权利人应当对通知书的真实性负责。

第十五条 网络服务提供者接到权利人的通知书后，应当立即删除涉嫌侵权的作品、表演、录音录像制品，或者断开与涉嫌侵权的作品、表演、录音录像制品的链接，并同时将通知书转送提供作品、表演、录音录像制品的服务对象；服务对象网络地址不明、无法转送的，应当将通知书的内容同时在信息网络上公告。

第十六条 服务对象接到网络服务提供者转送的通知书后，认为其提供的作品、表演、录音录像制品未侵犯他人权利的，可以向网络服务提供者提交书面说明，要求恢复被删除的作品、表演、录音录像制品，或者恢复与被断开的作品、表演、录音录像制品的链接。书面说明应当包含下列内容：

(一) 服务对象的姓名（名称）、联系方式和地址；

(二) 要求恢复的作品、表演、录音录像制品的名称和网络地址；

(三) 不构成侵权的初步证明材料。

服务对象应当对书面说明的真实性负责。

第十七条 网络服务提供者接到服务对象的书面说明后，应当立即恢复被删除的作品、表演、录音录像制品，或者可以恢复与被断开的作品、表演、录音录像制品的链接，同时将服务对象的书面说明转送权利人。权利人不得再通知网络服务提供者删除该作品、表演、录音录像制品，或者断开与该作品、表演、录音录像制品的链接。

第十八条 违反本条例规定，有下列侵权行为之一的，根据情况承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任；同时损害公共利益的，可以由著作权行政管理部门责令停止侵权行为，没收违法所得，非法经营额5万元以上的，可处非法经营额1倍以上5倍以下的罚款；没有非法经营额或者非法经营额5万元以下的，根据情节轻重，可处25万元以下的罚款；情节严重的，著作权行政管理部门可以没收主要用于提供网络服务的计算机等设备；构成犯罪的，依法追究刑事责任：

(一) 通过信息网络擅自向公众提供他人的作品、表演、录音录像制品的；

(二) 故意避开或者破坏技术措施的；

(三) 故意删除或者改变通过信息网络向公众提供的作品、表演、录音录像制品的权利管理电子信息，或者通过信息网络向公众提供明知或者应知未经权利人许可而被删除或者改变权利管理电子信息的作品、表演、录音录像制品的；

(四) 为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品超过规定范围，或者未按照公告的标准支付报酬，或者在权利人不同意提供其作品、表演、录音录像制品后未立即删除的；

(五) 通过信息网络提供他人的作品、表演、录音录像制品，未指明作品、表演、录音录像制品的名称或者作者、表演者、录音录像制作者的姓名（名称），或者未支付报酬，或者未依照本条例规定采取技术措施防止服务对象以外的其他人获得他人的作品、表演、录音录像制品，或者未防止服务对象的复制行为对权利人利益造成实质性损害的。

第十九条 违反本条例规定，有下列行为之一的，由著作权行政管理部门予以警告，没收违法所得，没收主要用于避开、破坏技术措施的装置或者部件；情节严重的，可以没收主要用于提供网络服务的计算机等设备，非法经营额5万元以上的，可处非法经营额1倍以上5倍以下的罚款；没有非法经营额或者非法经营额5万元以下的，根据情节轻重，可处25万元以下的罚款；构成犯罪的，依法追究刑事责任：

（一）故意制造、进口或者向他人提供主要用于避开、破坏技术措施的装置或者部件，或者故意为他人避开或者破坏技术措施提供技术服务的；

（二）通过信息网络提供他人的作品、表演、录音录像制品，获得经济利益的；

（三）为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品，未在提供前公告作品、表演、录音录像制品的名称和作者、表演者、录音录像制作者的姓名（名称）以及报酬标准的。

第二十条 网络服务提供者根据服务对象的指令提供网络自动接入服务，或者对服务对象提供的作品、表演、录音录像制品提供自动传输服务，并具备下列条件的，不承担赔偿责任：

（一）未选择并且未改变所传输的作品、表演、录音录像制品；

（二）向指定的服务对象提供该作品、表演、录音录像制品，并防止指定的服务对象以外的其他人获得。

第二十一条 网络服务提供者为提高网络传输效率，自动存储从其他网络服务提供者获得的作品、表演、录音录像制品，根据技术安排自动向服务对象提供，并具备下列条件的，不承担赔偿责任：

（一）未改变自动存储的作品、表演、录音录像制品；

（二）不影响提供作品、表演、录音录像制品的原网络服务提供者掌握服务对象获取该作品、表演、录音录像制品的情况；

（三）在原网络服务提供者修改、删除或者屏蔽该作品、表演、录音录像制品时，根据技术安排自动予以修改、删除或者屏蔽。

第二十二条 网络服务提供者服务对象提供信息存储空间，供服务对象通过信息网络向公众提供作品、表演、录音录像制品，并具备下列条件的，不承担赔偿责任：

（一）明确标示该信息存储空间是为服务对象所提供，并公开网络服务提供者的名称、联系人、网络地址；

（二）未改变服务对象所提供的作品、表演、录音录像制品；

（三）不知道也没有合理的理由应当知道服务对象提供的作品、表演、录音录像制品侵权；

（四）未从服务对象提供作品、表演、录音录像制品中直接获得经济利益；

（五）在接到权利人的通知书后，根据本条例规定删除权利人认为侵权的作品、表演、录音录像制品。

第二十三条 网络服务提供者服务对象提供搜索或者链接服务，在接到权利人的通知书后，根据本条例规定断开与侵权的作品、表演、录音录像制品的链接的，不承担赔偿责任；但是，明知或者应知所链接的作品、表演、录音录像制品侵权的，应当承担共同侵权责任。

第二十四条 因权利人的通知导致网络服务提供者错误删除作品、表演、录音录像制品，或者错误断开与作品、表演、录音录像制品的链接，给服务对象造成损失的，权利人应当承担赔偿责任。

第二十五条 网络服务提供者无正当理由拒绝提供或者拖延提供涉嫌侵权的服务对象的姓名（名称）、联系方式、网络地址等资料的，由著作权行政管理部门予以警告；情节严重的，没收主要用于提供网络服务的计算机等设备。

第二十六条 本条例下列用语的含义：

信息网络传播权，是指以有线或者无线方式向公众提供作品、表演或者录音录像制品，使公众可以在其个人选定的时间和地点获得作品、表演或者录音录像制品的权利。

技术措施，是指用于防止、限制未经权利人许可浏览、欣赏作品、表演、录音录像制品的或者通过信息网络向公众提供作品、表演、录音录像制品的有效技术、装置或者部件。

权利管理电子信息，是指说明作品及其作者、表演及其表演者、录音录像制品及其制作者的信息，作品、表演、录音录像制品权利人的信息和使用条件的信息，以及表示上述信息的数字或者代码。

《最高人民法院 最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）》

最高人民法院 最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二） 法释〔2010〕3号（2010年1月18日最高人民法院审判委员会第1483次会议、2010年1月14日最高人民检察院第十一届检察委员会第28次会议通过）

为依法惩治利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息，通过声讯台传播淫秽语音信息等犯罪行为，维护社会秩序，保障公民权益，根据《中华人民共和国刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》的规定，现对办理该类刑事案件具体应用法律的若干问题解释如下：

第一条 以牟利为目的，利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息的，依照《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》第一条、第二条的规定定罪处罚。

以牟利为目的，利用互联网、移动通讯终端制作、复制、出版、贩卖、传播内容含有不满十四周岁未成年人的淫秽电子信息，具有下列情形之一的，依照刑法第三百六十三条第一款的规定，以制作、复制、出版、贩卖、传播淫秽物品牟利罪定罪处罚：

- （一）制作、复制、出版、贩卖、传播淫秽电影、表演、动画等视频文件十个以上的；
- （二）制作、复制、出版、贩卖、传播淫秽音频文件五十个以上的；
- （三）制作、复制、出版、贩卖、传播淫秽电子刊物、图片、文章等一百件以上的；
- （四）制作、复制、出版、贩卖、传播的淫秽电子信息，实际被点击数达到五千次以上的；
- （五）以会员制方式出版、贩卖、传播淫秽电子信息，注册会员达一百人以上的；
- （六）利用淫秽电子信息收取广告费、会员注册费或者其他费用，违法所得五千元以上的；
- （七）数量或者数额虽未达到第（一）项至第（六）项规定标准，但分别达到其中两项以上标准一半以上的；
- （八）造成严重后果的。

实施第二款规定的行为，数量或者数额达到第二款第（一）项至第（七）项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。

第二条 利用互联网、移动通讯终端传播淫秽电子信息的，依照《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》第三条的规定定罪处罚。

利用互联网、移动通讯终端传播内容含有不满十四周岁未成年人的淫秽电子信息，具有下列情形之一的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚：

- （一）数量达到第一条第二款第（一）项至第（五）项规定标准二倍以上的；
- （二）数量分别达到第一条第二款第（一）项至第（五）项两项以上标准的；
- （三）造成严重后果的。

第三条 利用互联网建立主要用于传播淫秽电子信息的群组，成员达三十人以上或者造成严重后果的，对建立者、管理者和主要传播者，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚。

第四条 以牟利为目的，网站建立者、直接负责的管理者明知他人制作、复制、出版、贩卖、传播的是淫秽电子信息，允许或者放任他人在自己所有、管理的网站或者网页上发布，具有下列情形之一的，依照刑法第三百六十三条第一款的规定，以传播淫秽物品牟利罪定罪处罚：

- (一) 数量或者数额达到第一条第二款第(一)项至第(六)项规定标准五倍以上的；
- (二) 数量或者数额分别达到第一条第二款第(一)项至第(六)项两项以上标准二倍以上的；
- (三) 造成严重后果的。

实施前款规定的行为，数量或者数额达到第一条第二款第(一)项至第(七)项规定标准二十五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准一百倍以上的，应当认定为“情节特别严重”。

第五条 网站建立者、直接负责的管理者明知他人制作、复制、出版、贩卖、传播的是淫秽电子信息，允许或者放任他人在自己所有、管理的网站或者网页上发布，具有下列情形之一的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚：

- (一) 数量达到第一条第二款第(一)项至第(五)项规定标准十倍以上的；
- (二) 数量分别达到第一条第二款第(一)项至第(五)项两项以上标准五倍以上的；
- (三) 造成严重后果的。

第六条 电信业务经营者、互联网信息服务提供者明知是淫秽网站，为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、代收等服务，并收取服务费，具有下列情形之一的，对直接负责的主管人员和其他直接责任人员，依照刑法第三百六十三条第一款的规定，以传播淫秽物品牟利罪定罪处罚：

- (一) 为五个以上淫秽网站提供上述服务的；
- (二) 为淫秽网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道等服务，收取服务费数额在二万元以上的；
- (三) 为淫秽网站提供代收服务，收取服务费数额在五万元以上的；
- (四) 造成严重后果的。

实施前款规定的行为，数量或者数额达到前款第(一)项至第(三)项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。

第七条 明知是淫秽网站，以牟利为目的，通过投放广告等方式向其直接或者间接提供资金，或者提供费用结算服务，具有下列情形之一的，对直接负责的主管人员和其他直接责任人员，依照刑法第三百六十三条第一款的规定，以制作、复制、出版、贩卖、传播淫秽物品牟利罪的共同犯罪处罚：

- (一) 向十个以上淫秽网站投放广告或者以其他方式提供资金的；
- (二) 向淫秽网站投放广告二十条以上的；
- (三) 向十个以上淫秽网站提供费用结算服务的；
- (四) 以投放广告或者其他方式向淫秽网站提供资金数额在五万元以上的；
- (五) 为淫秽网站提供费用结算服务，收取服务费数额在二万元以上的；
- (六) 造成严重后果的。

实施前款规定的行为，数量或者数额达到前款第(一)项至第(五)项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。

第八条 实施第四条至第七条规定的行为，具有下列情形之一的，应当认定行为人“明知”，但是有证据证明确实不知道的除外：

- (一) 行政主管机关书面告知后仍然实施上述行为的；
- (二) 接到举报后不履行法定管理职责的；
- (三) 为淫秽网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道、代收服务、费用结算等服务，收取服务费明显高于市场价格的；

(四) 向淫秽网站投放广告, 广告点击率明显异常的;

(五) 其他能够认定行为人明知的情形。

第九条 一年内多次实施制作、复制、出版、贩卖、传播淫秽电子信息行为未经处理, 数量或者数额累计计算构成犯罪的, 应当依法定罪处罚。

第十条 单位实施制作、复制、出版、贩卖、传播淫秽电子信息犯罪的, 依照《中华人民共和国刑法》、《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》和本解释规定的相应个人犯罪的定罪量刑标准, 对直接负责的主管人员和其他直接责任人员定罪处罚, 并对单位判处罚金。

第十一条 对于以牟利为目的, 实施制作、复制、出版、贩卖、传播淫秽电子信息犯罪的, 人民法院应当综合考虑犯罪的违法所得、社会危害性等情节, 依法判处罚金或者没收财产。罚金数额一般在违法所得的一倍以上五倍以下。

第十二条 《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》和本解释所称网站, 是指可以通过互联网域名、IP 地址等方式访问的内容提供站点。

以制作、复制、出版、贩卖、传播淫秽电子信息为目的建立或者建立后主要从事制作、复制、出版、贩卖、传播淫秽电子信息活动的网站, 为淫秽网站。

第十三条 以前发布的司法解释与本解释不一致的, 以本解释为准。

《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》

最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释

(2004年9月1日最高人民法院审判委员会第1323次会议、2004年9月2日最高人民检察院第十届检察委员会第26次会议通过)

(法释〔2004〕11号)

中华人民共和国最高人民法院公告

《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》已于2004年9月1日由最高人民法院审判委员会第1323次会议、2004年9月2日由最高人民检察院第十届检察委员会第26次会议通过, 现予公布, 自2004年9月6日起施行。

二〇〇四年九月三日

为依法惩治利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息、通过声讯台传播淫秽语音信息等犯罪活动, 维护公共网络、通讯的正常秩序, 保障公众的合法权益, 根据《中华人民共和国刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》的规定, 现对办理该类刑事案件具体应用法律的若干问题解释如下:

第一条 以牟利为目的, 利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息, 具有下列情形之一的, 依照刑法第三百六十三条第一款的规定, 以制作、复制、出版、贩卖、传播淫秽物品牟利罪定罪处罚:

- (一) 制作、复制、出版、贩卖、传播淫秽电影、表演、动画等视频文件二十个以上的;
- (二) 制作、复制、出版、贩卖、传播淫秽音频文件一百个以上的;
- (三) 制作、复制、出版、贩卖、传播淫秽电子刊物、图片、文章、短信息等二百件以上的;
- (四) 制作、复制、出版、贩卖、传播的淫秽电子信息, 实际被点击数达到一万次以上的;
- (五) 以会员制方式出版、贩卖、传播淫秽电子信息, 注册会员达二百人以上的;

(六) 利用淫秽电子信息收取广告费、会员注册费或者其他费用，违法所得一万元以上的；

(七) 数量或者数额虽未达到第（一）项至第（六）项规定标准，但分别达到其中两项以上标准一半以上的；

(八) 造成严重后果的。

利用聊天室、论坛、即时通信软件、电子邮件等方式，实施第一款规定行为的，依照刑法第三百六十三条第一款的规定，以制作、复制、出版、贩卖、传播淫秽物品牟利罪定罪处罚。

第二条 实施第一条规定的行为，数量或者数额达到第一条第一款第（一）项至第（六）项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。

第三条 不以牟利为目的，利用互联网或者移动通讯终端传播淫秽电子信息，具有下列情形之一的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚：

(一) 数量达到第一条第一款第（一）项至第（五）项规定标准二倍以上的；

(二) 数量分别达到第一条第一款第（一）项至第（五）项两项以上标准的；

(三) 造成严重后果的。

利用聊天室、论坛、即时通信软件、电子邮件等方式，实施第一款规定行为的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚。

第四条 明知是淫秽电子信息而在自己所有、管理或者使用的网站或者网页上提供直接链接的，其数量标准根据所链接的淫秽电子信息的种类计算。

第五条 以牟利为目的，通过声讯台传播淫秽语音信息，具有下列情形之一的，依照刑法第三百六十三条第一款的规定，对直接负责的主管人员和其他直接责任人员以传播淫秽物品牟利罪定罪处罚：

(一) 向一百人次以上传播的；

(二) 违法所得一万元以上的；

(三) 造成严重后果的。

实施前款规定行为，数量或者数额达到前款第（一）项至第（二）项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。

第六条 实施本解释前五条规定的犯罪，具有下列情形之一的，依照刑法第三百六十三条第一款、第三百六十四条第一款的规定从重处罚：

(一) 制作、复制、出版、贩卖、传播具体描绘不满十八周岁未成年人性行为的淫秽电子信息的；

(二) 明知是具体描绘不满十八周岁的未成年人性行为的淫秽电子信息而在自己所有、管理或者使用的网站或者网页上提供直接链接的；

(三) 向不满十八周岁的未成年人贩卖、传播淫秽电子信息和语音信息的；

(四) 通过使用破坏性程序、恶意代码修改用户计算机设置等方法，强制用户访问、下载淫秽电子信息的。

第七条 明知他人实施制作、复制、出版、贩卖、传播淫秽电子信息犯罪，为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、费用结算等帮助的，对直接负责的主管人员和其他直接责任人员，以共同犯罪论处。

第八条 利用互联网、移动通讯终端、声讯台贩卖、传播淫秽书刊、影片、录像带、录音带等以实物为载体的淫秽物品的，依照《最高人民法院关于审理非法出版物刑事案件具体应用法律若干问题的解释》的有关规定定罪处罚。

第九条 刑法第三百六十七条第一款规定的“其他淫秽物品”，包括具体描绘性行为或者露骨宣扬色情的诲淫性的视频文件、音频文件、电子刊物、图片、文章、短信息等互联网、移动通讯终端电子信息和声讯台语音信息。

有关人体生理、医学知识的电子信息和声讯台语音信息不是淫秽物品。包含色情内容的有艺术价值的电子文学、艺术作品

不视为淫秽物品。

《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》

《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》

最高人民法院公告

《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》已于2012年11月26日由最高人民法院审判委员会第1561次会议通过，现予公布，自2013年1月1日起施行。

最高人民法院

2012年12月17日

最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定

(法释〔2012〕20号)

为正确审理侵害信息网络传播权民事纠纷案件，依法保护信息网络传播权，促进信息网络产业健康发展，维护公共利益，根据《中华人民共和国民事诉讼法》、《中华人民共和国侵权责任法》、《中华人民共和国著作权法》、《中华人民共和国民事诉讼法》等有关法律规定，结合审判实际，制定本规定。

第一条 人民法院审理侵害信息网络传播权民事纠纷案件，在依法行使裁量权时，应当兼顾权利人、网络服务提供者和社会公众的利益。

第二条 本规定所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

第三条 网络用户、网络服务提供者未经许可，通过信息网络提供权利人享有信息网络传播权的作品、表演、录音录像制品，除法律、行政法规另有规定外，人民法院应当认定其构成侵害信息网络传播权行为。

通过上传到网络服务器、设置共享文件或者利用文件分享软件等方式，将作品、表演、录音录像制品置于信息网络中，使公众能够在个人选定的时间和地点以下载、浏览或者其他方式获得的，人民法院应当认定其实施了前款规定的提供行为。

第四条 有证据证明网络服务提供者与他人以分工合作等方式共同提供作品、表演、录音录像制品，构成共同侵权行为的，人民法院应当判令其承担连带责任。网络服务提供者能够证明其仅提供自动接入、自动传输、信息存储空间、搜索、链接、文件分享技术等网络服务，主张其不构成共同侵权行为的，人民法院应予支持。

第五条 网络服务提供者以提供网页快照、缩略图等方式实质替代其他网络服务提供者向公众提供相关作品的，人民法院应当认定其构成提供行为。

前款规定的提供行为不影响相关作品的正常使用，且未不合理损害权利人对该作品的合法权益，网络服务提供者主张其未侵害信息网络传播权的，人民法院应予支持。

第六条 原告有初步证据证明网络服务提供者提供了相关作品、表演、录音录像制品，但网络服务提供者能够证明其仅提供网络服务，且无过错的，人民法院不应认定为构成侵权。

第七条 网络服务提供者在提供网络服务时教唆或者帮助网络用户实施侵害信息网络传播权行为的，人民法院应当判令其承担侵权责任。

网络服务提供者以言语、推介技术支持、奖励积分等方式诱导、鼓励网络用户实施侵害信息网络传播权行为的，人民法院应当认定其构成教唆侵权行为。

网络服务提供者明知或者应知网络用户利用网络服务侵害信息网络传播权，未采取删除、屏蔽、断开链接等必要措施，或者提供技术支持等帮助行为的，人民法院应当认定其构成帮助侵权行为。

第八条 人民法院应当根据网络服务提供者的过错，确定其是否承担教唆、帮助侵权责任。网络服务提供者的过错包括对于网络用户侵害信息网络传播权行为的明知或者应知。

网络服务提供者未对网络用户侵害信息网络传播权的行为主动进行审查的，人民法院不应据此认定其具有过错。

网络服务提供者能够证明已采取合理、有效的技术措施，仍难以发现网络用户侵害信息网络传播权行为的，人民法院应当认定其不具有过错。

第九条 人民法院应当根据网络用户侵害信息网络传播权的具体事实是否明显，综合考虑以下因素，认定网络服务提供者是否构成应知：

- （一）基于网络服务提供者提供服务的性质、方式及其引发侵权的可能性大小，应当具备的管理信息的能力；
- （二）传播的作品、表演、录音录像制品的类型、知名度及侵权信息的明显程度；
- （三）网络服务提供者是否主动对作品、表演、录音录像制品进行了选择、编辑、修改、推荐等；
- （四）网络服务提供者是否积极采取了预防侵权的合理措施；
- （五）网络服务提供者是否设置便捷程序接收侵权通知并及时对侵权通知作出合理的反应；
- （六）网络服务提供者是否针对同一网络用户的重复侵权行为采取了相应的合理措施；
- （七）其他相关因素。

第十条 网络服务提供者在提供网络服务时，对热播影视作品等以设置榜单、目录、索引、描述性段落、内容简介等方式进行推荐，且公众可以在其网页上直接以下载、浏览或者其他方式获得的，人民法院可以认定其应知网络用户侵害信息网络传播权。

第十一条 网络服务提供者从网络用户提供的作品、表演、录音录像制品中直接获得经济利益的，人民法院应当认定其对该网络用户侵害信息网络传播权的行为负有较高的注意义务。

网络服务提供者针对特定作品、表演、录音录像制品投放广告获取收益，或者获取与其传播的作品、表演、录音录像制品存在其他特定联系的经济利益，应当认定为前款规定的直接获得经济利益。网络服务提供者因提供网络服务而收取一般性广告费、服务费等，不属于本款规定的情形。

第十二条 有下列情形之一的，人民法院可以根据案件具体情况，认定提供信息存储空间服务的网络服务提供者应知网络用户侵害信息网络传播权：

- （一）将热播影视作品等置于首页或者其他主要页面等能够为网络服务提供者明显感知的位置的；
- （二）对热播影视作品等的主题、内容主动进行选择、编辑、整理、推荐，或者为其设立专门的排行榜的；
- （三）其他可以明显感知相关作品、表演、录音录像制品为未经许可提供，仍未采取合理措施的情形。

第十三条 网络服务提供者接到权利人以书信、传真、电子邮件等方式提交的通知，未及时采取删除、屏蔽、断开链接等必要措施的，人民法院应当认定其明知相关侵害信息网络传播权行为。

第十四条 人民法院认定网络服务提供者采取的删除、屏蔽、断开链接等必要措施是否及时，应当根据权利人提交通知的形式，通知的准确程度，采取措施的难易程度，网络服务的性质，所涉作品、表演、录音录像制品的类型、知名度、数量等因素综合判断。

第十五条 侵害信息网络传播权民事纠纷案件由侵权行为地或者被告住所地人民法院管辖。侵权行为地包括实施被诉侵权行为的网络服务器、计算机终端等设备所在地。侵权行为地和被告住所地均难以确定或者在境外的，原告发现侵权内容的计算机终端等设备所在地可以视为侵权行为地。

第十六条 本规定施行之日起，《最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》（法释〔2006〕11号）同时废止。

本规定施行之后尚未终审的侵害信息网络传播权民事纠纷案件，适用本规定。本规定施行前已经终审，当事人申请再审或者按照审判监督程序决定再审的，不适用本规定。

《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》

为了保护公民、法人和其他组织的合法权益，维护社会秩序，根据《中华人民共和国刑法》《全国人民代表大会常务委员会关于维护互联网安全的决定》等规定，对办理利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等刑事案件适用法律的若干问题解释如下：

第一条 具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“捏造事实诽谤他人”：

- （一）捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；
- （二）将信息网络上涉及他人的原始信息内容篡改改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏造事实诽谤他人”论。

第二条 利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“情节严重”：

- （一）同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的；
- （二）造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；
- （三）二年内曾因诽谤受过行政处罚，又诽谤他人的；
- （四）其他情节严重的情形。

第三条 利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第二款规定的“严重危害社会秩序和国家利益”：

- （一）引发群体性事件的；
- （二）引发公共秩序混乱的；
- （三）引发民族、宗教冲突的；
- （四）诽谤多人，造成恶劣社会影响的；
- （五）损害国家形象，严重危害国家利益的；
- （六）造成恶劣国际影响的；
- （七）其他严重危害社会秩序和国家利益的情形。

第四条 一年内多次实施利用信息网络诽谤他人行为未经处理，诽谤信息实际被点击、浏览、转发次数累计计算构成犯罪的，应当依法定罪处罚。

第五条 利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的，依照刑法第二百九十三条第一款第（二）项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第（四）项的规定，以寻衅滋事罪定罪处罚。

第六条 以在信息网络上发布、删除等方式处理网络信息为由，威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

第七条 违反国家规定，以营利为目的，通过信息网络有偿提供删除信息服务，或者明知是虚假信息，通过信息网络有偿提供发布信息等服务，扰乱市场秩序，具有下列情形之一的，属于非法经营行为“情节严重”，依照刑法第二百二十五条第（四）项的规定，以非法经营罪定罪处罚：

- （一）个人非法经营数额在五万元以上，或者违法所得数额在二万元以上的；
- （二）单位非法经营数额在十五万元以上，或者违法所得数额在五万元以上的。

实施前款规定的行为，数额达到前款规定的数额五倍以上的，应当认定为刑法第二百二十五条规定的“情节特别严重”。

第八条 明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，以共同犯罪论处。

第九条 利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营犯罪，同时又构成刑法第二百二十一条规定的损害商业信誉、商品声誉罪，第二百七十八条规定的煽动暴力抗拒法律实施罪，第二百九十一条之一规定的编造、故意传播虚假恐怖信息罪等犯罪的，依照处罚较重的规定定罪处罚。

第十条 本解释所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》

《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》

《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》已于2014年6月23日由最高人民法院审判委员会第1621次会议通过，现予公布，自2014年10月10日起施行。

最高人民法院

2014年8月21日

为正确审理利用信息网络侵害人身权益民事纠纷案件，根据《中华人民共和国民事诉讼法》《中华人民共和国侵权责任法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国民事诉讼法》等法律的规定，结合审判实践，制定本规定。

第一条 本规定所称的利用信息网络侵害人身权益民事纠纷案件，是指利用信息网络侵害他人姓名权、名称权、名誉权、荣誉权、肖像权、隐私权等人身权益引起的纠纷案件。

第二条 利用信息网络侵害人身权益提起的诉讼，由侵权行为地或者被告住所地人民法院管辖。

侵权行为实施地包括实施被诉侵权行为的计算机等终端设备所在地，侵权结果发生地包括被侵权人住所地。

第三条 原告依据侵权责任法第三十六条第二款、第三款的规定起诉网络用户或者网络服务提供者的，人民法院应予受理。

原告仅起诉网络用户，网络用户请求追加涉嫌侵权的网络服务提供者作为共同被告或者第三人的，人民法院应予准许。

原告仅起诉网络服务提供者，网络服务提供者请求追加可以确定的网络用户为共同被告或者第三人的，人民法院应予准许。

第四条 原告起诉网络服务提供者，网络服务提供者以涉嫌侵权的信息系网络用户发布为由抗辩的，人民法院可以根据原告的请求及案件的具体情况，责令网络服务提供者向人民法院提供能够确定涉嫌侵权的网络用户的姓名（名称）、联系方式、网络地址等信息。

网络服务提供者无正当理由拒不提供的，人民法院可以依据民事诉讼法第一百一十四条的规定对网络服务提供者采取处罚等措施。

原告根据网络服务提供者提供的信息请求追加网络用户为被告的，人民法院应予准许。

第五条 依据侵权责任法第三十六条第二款的规定，被侵权人以书面形式或者网络服务提供者公示的方式向网络服务提供者发出的通知，包含下列内容的，人民法院应当认定有效：

- （一）通知人的姓名（名称）和联系方式；
- （二）要求采取必要措施的网络地址或者足以准确定位侵权内容的相关信息；
- （三）通知人要求删除相关信息的理由。

被侵权人发送的通知未满足上述条件，网络服务提供者主张免除责任的，人民法院不予支持。 第六条 人民法院适用侵权责任法第三十六条第二款的规定，认定网络服务提供者采取的删除、屏蔽、断开链接等必要措施是否及时，应当根据网络

服务的性质、有效通知的形式和准确程度，网络信息侵害权益的类型和程度等因素综合判断。

第七条 其发布的信息被采取删除、屏蔽、断开链接等措施的网络用户，主张网络服务提供者承担违约责任或者侵权责任，网络服务提供者以收到通知为由抗辩的，人民法院应予支持。

被采取删除、屏蔽、断开链接等措施的网络用户，请求网络服务提供者提供通知内容的，人民法院应予支持。

第八条 因通知人的通知导致网络服务提供者错误采取删除、屏蔽、断开链接等措施，被采取措施的网路用户请求通知人承担侵权责任的，人民法院应予支持。

被错误采取措施的网路用户请求网络服务提供者采取相应恢复措施的，人民法院应予支持，但受技术条件限制无法恢复的除外。

第九条 人民法院依据侵权责任法第三十六条第三款认定网络服务提供者是否“知道”，应当综合考虑下列因素：

- （一）网络服务提供者是否以人工或者自动方式对侵权网络信息以推荐、排名、选择、编辑、整理、修改等方式作出处理；
- （二）网络服务提供者应当具备的管理信息的能力，以及所提供服务的性质、方式及其引发侵权的可能性大小；
- （三）该网络信息侵害人身权益的类型及明显程度；
- （四）该网络信息的社会影响程度或者一定时间内的浏览量；
- （五）网络服务提供者采取预防侵权措施的技术可能性及其是否采取了相应的合理措施；
- （六）网络服务提供者是否针对同一网络用户的重复侵权行为或者同一侵权信息采取了相应的合理措施；
- （七）与本案相关的其他因素。

第十条 人民法院认定网络用户或者网络服务提供者转载网络信息行为的过错及其程度，应当综合以下因素：

- （一）转载主体所承担的与其性质、影响范围相适应的注意义务；
- （二）所转载信息侵害他人人身权益的明显程度；
- （三）对所转载信息是否作出实质性修改，是否添加或者修改文章标题，导致其与内容严重不符以及误导公众的可能性。

第十一条 网络用户或者网络服务提供者采取诽谤、诋毁等手段，损害公众对经营主体的信赖，降低其产品或者服务的社会评价，经营主体请求网络用户或者网络服务提供者承担侵权责任的，人民法院应依法予以支持。

第十二条 网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，造成他人损害，被侵权人请求其承担侵权责任的，人民法院应予支持。但下列情形除外：

- （一）经自然人书面同意且在约定范围内公开；
- （二）为促进社会公共利益且在必要范围内；
- （三）学校、科研机构等基于公共利益为学术研究或者统计的目的，经自然人书面同意，且公开的方式不足以识别特定自然人；
- （四）自然人自行在网络上公开的信息或者其他已合法公开的个人信息；
- （五）以合法渠道获取的个人信息；
- （六）法律或者行政法规另有规定。

网络用户或者网络服务提供者以违反社会公共利益、社会公德的方式公开前款第四项、第五项规定的个人信息，或者公开该信息侵害权利人值得保护的重大利益，权利人请求网络用户或者网络服务提供者承担侵权责任的，人民法院应予支持。

国家机关行使职权公开个人信息的，不适用本条规定。

第十三条 网络用户或者网络服务提供者，根据国家机关依职权制作的文书和公开实施的职权行为等信息来源所发布的信息，有下列情形之一的，侵害他人人身权益，被侵权人请求侵权人承担侵权责任的，人民法院应予支持：

- （一）网络用户或者网络服务提供者发布的信息与前述信息来源内容不符；
- （二）网络用户或者网络服务提供者以添加侮辱性内容、诽谤性信息、不当标题或者通过增删信息、调整结构、改变顺序等方式致人误解；
- （三）前述信息来源已被公开更正，但网络用户拒绝更正或者网络服务提供者不予更正；
- （四）前述信息来源已被公开更正，网络用户或者网络服务提供者仍然发布更正之前的信息。

第十四条 被侵权人与构成侵权的网络用户或者网络服务提供者达成一方支付报酬，另一方提供删除、屏蔽、断开链接等服务的协议，人民法院应认定为无效。

擅自篡改、删除、屏蔽特定网络信息或者以断开链接的方式阻止他人获取网络信息，发布该信息的网络用户或者网络服务提供者请求侵权人承担侵权责任的，人民法院应予支持。接受他人委托实施该行为的，委托人与受托人承担连带责任。

第十五条 雇佣、组织、教唆或者帮助他人发布、转发网络信息侵害他人人身权益，被侵权人请求行为人承担连带责任的，人民法院应予支持。

第十六条 人民法院判决侵权人承担赔礼道歉、消除影响或者恢复名誉等责任形式的，应当与侵权的具体方式和所造成的影响范围相当。侵权人拒不履行的，人民法院可以采取在网络上发布公告或者公布裁判文书等合理的方式执行，由此产生的费用由侵权人承担。

第十七条 网络用户或者网络服务提供者侵害他人人身权益，造成财产损失或者严重精神损害，被侵权人依据侵权责任法第二十条和第二十二条的规定请求其承担赔偿责任的，人民法院应予支持。

第十八条 被侵权人为制止侵权行为所支付的合理开支，可以认定为侵权责任法第二十条规定的财产损失。合理开支包括被侵权人或者委托代理人对侵权行为进行调查、取证的合理费用。人民法院根据当事人的请求和具体案情，可以将符合国家有关部门规定的律师费用计算在赔偿范围内。

被侵权人因人身权益受侵害造成的财产损失或者侵权人因此获得的利益无法确定的，人民法院可以根据具体案情在50万元以下的范围内确定赔偿数额。

精神损害的赔偿数额，依据《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》第十条的规定予以确定。

第十九条 本规定施行后人民法院正在审理的一审、二审案件适用本规定。

本规定施行前已经终审，本规定施行后当事人申请再审或者按照审判监督程序决定再审的案件，不适用本规定。

🔗 《电信服务规范》

《电信服务规范》

电信服务规范

🔗 《互联网IP地址备案管理办法》

《互联网IP地址备案管理办法》

中华人民共和国信息产业部令（第34号）

《互联网IP地址备案管理办法》已经2005年1月28日中华人民共和国信息产业部第十二次部务会议审议通过，现予发布，自2005年3月20日起施行。

部长：王旭东

二〇〇五年二月八日

第一条 为加强对互联网IP地址资源使用的管理，保障互联网络的安全，维护广大互联网用户的根本利益，促进互联网业的健康发展，制定本办法。

第二条 在中华人民共和国境内直接从亚太互联网信息中心等具有IP地址管理权的国际机构获得IP地址的单位和具有分配IP地址供其他单位或者个人使用的单位，适用本办法。

第三条 直接从亚太互联网信息中心等具有IP地址管理权的国际机构获得IP地址自用或分配给其他用户使用的单位统称为第一级IP地址分配机构。

直接从第一级IP地址分配机构获得IP地址除自用外还分配给本单位互联网用户以外的其他用户使用的单位为第二级IP地址分配机构（以下各级IP地址分配机构的级别依此类推）。

第四条 国家对IP地址的分配使用实行备案管理。

第五条 中华人民共和国信息产业部（以下简称“信息产业部”）对基础电信业务经营者、公益性互联网络单位和中国互联网络信息中心的IP地址备案实施监督管理。

各省、自治区、直辖市通信管理局（以下简称“省通信管理局”）对本行政区域内其他各级IP地址分配机构的IP地址备案活动实施监督管理。

第六条 信息产业部统一建设并管理全国的互联网IP地址数据库，制定和调整IP地址分配机构需报备的IP地址信息；各省通信管理局通过使用全国互联网IP地址数据库管理本行政区域内各级IP地址分配机构报备的IP地址信息。

第七条 各级IP地址分配机构应当通过信息产业部指定的网站，按照IP地址备案的要求以电子形式报备IP地址信息。

第八条 各级IP地址分配机构在进行IP地址备案时，应当如实、完整地报备IP地址信息（需报备的IP地址信息参见本办法附录）。

第九条 各级IP地址分配机构应自取得IP地址之日起二十个工作日内完成IP地址信息的第一次报备。

第十条 各级IP地址分配机构申请和分配使用的IP地址信息发生变化的，IP地址分配机构应自变化之日起五个工作日内通过信息产业部指定的网站，按照IP地址备案的要求以电子形式提交变更后的IP地址信息。

各级IP地址分配机构的联系人或联系方式发生变更的，应自变更之日起十个工作日内报备变更后的信息。

第十一条 基础电信业务经营者IP地址信息的报备，由各基础电信业务经营者集团公司（总公司）和基础电信业务经营者的省级公司（省级分支机构）共同完成。

各基础电信业务经营者集团公司（总公司）按照本办法的规定完成由其申请、使用和分配到省级公司（省级分支机构）的IP地址信息的报备。各基础电信业务经营者的省级公司（省级分支机构）按照本办法的规定统一完成该省级公司（省级分支机构）及其所属公司（分支机构）申请、使用和分配的IP地址信息的报备。

第十二条 中国教育和科研计算机网、中国科学技术网、中国国际经济贸易互联网、中国长城互联网等公益性互联网的网路管理单位应当按照本办法的规定，统一完成其申请、使用和分配的IP地址信息的报备。

第十三条 IP地址分配机构同时是互联网接入服务提供者的，应当如实记录和保存由其提供接入服务的使用自带IP地址的用户的IP地址信息，并自提供接入服务之日起五日内，填报IP地址备案信息，进行备案。

第十四条 各级IP地址分配机构应当建立健全本单位的IP地址管理制度。

第十五条 各级IP地址分配机构分配IP地址时，应当通知其下一级IP地址分配机构报备IP地址信息。

第十六条 信息产业部和省通信管理局及其工作人员对IP地址分配机构报备的IP地址信息，有保密的义务。

信息产业部和省通信管理局及其工作人员不得向他人提供IP地址分配机构报备的IP地址信息，但法律、行政法规另有规定的除外。

第十七条 违反本办法第八条、第九条、第十条、第十三条的规定的，由信息产业部或者省通信管理局依据职权责令限期改正；逾期不改的，给予警告或者处人民币一万元罚款，或者同时处以上两种处罚。

第十八条 违反本办法第十四条规定，未建立IP地址管理制度的，由信息产业部或者省通信管理局依据职权责令限期改正；逾期不改的，给予警告或者处人民币五千元以上一万元以下罚款，或者同时处以上两种处罚。

第十九条 本办法实施前直接从亚太互联网信息中心等具有IP地址管理权的国际机构获得IP地址供本单位使用或者分配IP地址供其他单位或个人使用的，应自本办法施行之日起四十五个工作日内，按照本办法的规定完成备案手续。

第二十条 本办法自2005年3月20日起实施。

附录：

需报备的IP地址信息

一、备案单位基本情况，包括备案单位名称、备案单位地址、备案单位性质、电信业务经营许可证编号、联系人姓名、联系人电话、联系人电子邮件等。

二、备案单位的IP地址来源信息，包括IP地址来源机构名称、IP地址总量、各IP地址段起止地址码等。

三、备案单位的IP地址分配使用信息，包括：

（一）本单位自用的IP地址信息，包括IP地址总量、各IP地址段起止IP地址码、IP地址使用方式、网关IP地址、网关所在地；

（二）尚未分配的IP地址信息，包括IP地址总量、各IP地址段起止地址码；

（三）向其他用户分配的IP地址信息，包括所分配的用户基本信息（包括用户名称、单位类别、单位所属行业、单位详细地址、联系人姓名、联系人电话、联系人电子邮件）、所分配的IP地址总量、各IP地址段起止地址码、网关IP地址、网关所在地、IP地址使用方式。

四、自带IP地址的互联网接入用户信息，包括用户基本信息（含用户名称、单位类别、单位所属行业、单位详细地址、联系人姓名、联系人电话、联系人电子邮件）、自带IP地址总量、IP地址段起止地址码、自带IP地址的来源、网关IP地址、网关所在地、IP地址使用方式等。

《互联网域名管理办法》

《互联网域名管理办法》

（工业和信息化部令（第43号））

第一章 总 则

第一条 为了规范互联网域名服务，保护用户合法权益，保障互联网域名系统安全、可靠运行，推动中文域名和国家顶级域名发展和应用，促进中国互联网健康发展，根据《中华人民共和国行政许可法》《国务院对确需保留的行政审批项目设定行政许可的决定》等规定，参照国际上互联网域名管理准则，制定本办法。

第二条 在中华人民共和国境内从事互联网域名服务及其运行维护、监督管理等相关活动，应当遵守本办法。

本办法所称互联网域名服务（以下简称域名服务），是指从事域名根服务器运行和管理、顶级域名运行和管理、域名注册、域名解析等活动。

第三条 工业和信息化部对全国的域名服务实施监督管理，主要职责是：

- （一）制定互联网域名管理规章及政策；
- （二）制定中国互联网域名体系、域名资源发展规划；
- （三）管理境内的域名根服务器运行机构和域名注册管理机构；
- （四）负责域名体系的网络与信息安全管理；
- （五）依法保护用户个人信息和合法权益；
- （六）负责与域名有关的国际协调；

(七) 管理境内的域名解析服务；

(八) 管理其他与域名服务相关的活动。

第四条 各省、自治区、直辖市通信管理局对本行政区域内的域名服务实施监督管理，主要职责是：

(一) 贯彻执行域名管理法律、行政法规、规章和政策；

(二) 管理本行政区域内的域名注册服务机构；

(三) 协助工业和信息化部对本行政区域内的域名根服务器运行机构和域名注册管理机构进行管理；

(四) 负责本行政区域内域名系统的网络与信息安全管理；

(五) 依法保护用户个人信息和合法权益；

(六) 管理本行政区域内的域名解析服务；

(七) 管理本行政区域内其他与域名服务相关的活动。

第五条 中国互联网域名体系由工业和信息化部予以公告。根据域名发展的实际情况，工业和信息化部可以对中国互联网域名体系进行调整。

第六条 “.CN”和“.中国”是中国的国家顶级域名。

中文域名是中国互联网域名体系的重要组成部分。国家鼓励和支持中文域名系统的技术研究和推广应用。

第七条 提供域名服务，应当遵守国家相关法律法规，符合相关技术规范 and 标准。

第八条 任何组织和个人不得妨碍互联网域名系统的安全和稳定运行。

第二章 域名管理

第九条 在境内设立域名根服务器及域名根服务器运行机构、域名注册管理机构和域名注册服务机构的，应当依据本办法取得工业和信息化部或者省、自治区、直辖市通信管理局（以下统称电信管理机构）的相应许可。

第十条 申请设立域名根服务器及域名根服务器运行机构的，应当具备以下条件：

(一) 域名根服务器设置在境内，并且符合互联网发展相关规划及域名系统安全稳定运行要求；

(二) 是依法设立的法人，该法人及其主要出资者、主要经营管理人员具有良好的信用记录；

(三) 具有保障域名根服务器安全可靠运行的场地、资金、环境、专业人员和技术能力以及符合电信管理机构要求的信息管理系统；

(四) 具有健全的网络与信息安全保障措施，包括管理人员、网络与信息安全管理制度、应急处置预案和相关技术、管理措施等；

(五) 具有用户个人信息保护能力、提供长期服务的能力及健全的服务退出机制；

(六) 法律、行政法规规定的其他条件。

第十一条 申请设立域名注册管理机构的，应当具备以下条件：

(一) 域名管理系统设置在境内，并且持有的顶级域名符合相关法律法规及域名系统安全稳定运行要求；

(二) 是依法设立的法人，该法人及其主要出资者、主要经营管理人员具有良好的信用记录；

(三) 具有完善的业务发展计划和技术方案以及与从事顶级域名运行管理相适应的场地、资金、专业人员以及符合电信管理机构要求的信息管理系统；

(四) 具有健全的网络与信息安全保障措施，包括管理人员、网络与信息安全管理制度、应急处置预案和相关技术、管理措施

等；

(五) 具有进行真实身份信息核验和用户个人信息保护的能力、提供长期服务的能力及健全的服务退出机制；

(六) 具有健全的域名注册服务管理制度和对域名注册服务机构的监督机制；

(七) 法律、行政法规规定的其他条件。

第十二条 申请设立域名注册服务机构的，应当具备以下条件：

(一) 在境内设置域名注册服务系统、注册数据库和相应的域名解析系统；

(二) 是依法设立的法人，该法人及其主要出资者、主要经营管理人员具有良好的信用记录；

(三) 具有与从事域名注册服务相适应的场地、资金和专业人员以及符合电信管理机构要求的信息管理系统；

(四) 具有进行真实身份信息核验和用户个人信息保护的能力、提供长期服务的能力及健全的服务退出机制；

(五) 具有健全的域名注册服务管理制度和对域名注册代理机构的监督机制；

(六) 具有健全的网络与信息安全保障措施，包括管理人员、网络与信息安全管理、应急处置预案和相关技术、管理措施等；

(七) 法律、行政法规规定的其他条件。

第十三条 申请设立域名根服务器及域名根服务器运行机构、域名注册管理机构的，应当向工业和信息化部提交申请材料。申请设立域名注册服务机构的，应当向住所地省、自治区、直辖市通信管理局提交申请材料。

申请材料应当包括：

(一) 申请单位的基本情况及其法定代表人签署的依法诚信经营承诺书；

(二) 对域名服务实施有效管理的证明材料，包括相关系统及场所、服务能力的证明材料、管理制度、与其他机构签订的协议等；

(三) 网络与信息安全保障制度及措施；

(四) 证明申请单位信誉的材料。

第十四条 申请材料齐全、符合法定形式的，电信管理机构应当向申请单位出具受理申请通知书；申请材料不齐全或者不符合法定形式的，电信管理机构应当场或者在5个工作日内一次性书面告知申请单位需要补正的全部内容；不予受理的，应当出具不予受理通知书并说明理由。

第十五条 电信管理机构应当自受理之日起20个工作日内完成审查，作出予以许可或者不予许可的决定。20个工作日内不能作出决定的，经电信管理机构负责人批准，可以延长10个工作日，并将延长期限的理由告知申请单位。需要组织专家论证的，论证时间不计入审查期限。

予以许可的，应当颁发相应的许可文件；不予许可的，应当书面通知申请单位并说明理由。

第十六条 域名根服务器运行机构、域名注册管理机构和域名注册服务机构的许可有效期为5年。

第十七条 域名根服务器运行机构、域名注册管理机构和域名注册服务机构的名称、住所、法定代表人等信息发生变更的，应当自变更之日起20日内向原发证机关办理变更手续。

第十八条 在许可有效期内，域名根服务器运行机构、域名注册管理机构、域名注册服务机构拟终止相关服务的，应当提前30日书面通知用户，提出可行的善后处理方案，并向原发证机关提交书面申请。

原发证机关收到申请后，应当向社会公示30日。公示期结束60日内，原发证机关应当完成审查并做出决定。

第十九条 许可有效期届满需要继续从事域名服务的，应当提前90日向原发证机关申请延续；不再继续从事域名服务的，应当提前90日向原发证机关报告并做好善后工作。

第二十条 域名注册服务机构委托域名注册代理机构开展市场销售等工作的，应当对域名注册代理机构的工作进行监督和管理。

域名注册代理机构受委托开展市场销售等工作的过程中，应当主动表明代理关系，并在域名注册服务合同中明示相关域名注册服务机构名称及代理关系。

第二十一条 域名注册管理机构、域名注册服务机构应当在境内设立相应的应急备份系统并定期备份域名注册数据。

第二十二条 域名根服务器运行机构、域名注册管理机构、域名注册服务机构应当在其网站首页和经营场所显著位置标明其许可相关信息。域名注册管理机构还应当标明与其合作的域名注册服务机构名单。

域名注册代理机构应当在其网站首页和经营场所显著位置标明其代理的域名注册服务机构名称。

第三章 域名注册

第二十三条 域名根服务器运行机构、域名注册管理机构和域名注册服务机构应当向用户提供安全、方便、稳定的服务。

第二十四条 域名注册管理机构应当根据本办法制定域名注册实施细则并向社会公开。

第二十五条 域名注册管理机构应当通过电信管理机构许可的域名注册服务机构开展域名注册服务。

域名注册服务机构应当按照电信管理机构许可的域名注册服务项目提供服务，不得为未经电信管理机构许可的域名注册管理机构提供域名注册服务。

第二十六条 域名注册服务原则上实行“先申请先注册”，相应域名注册实施细则另有规定的，从其规定。

第二十七条 为维护国家利益和社会公众利益，域名注册管理机构应当建立域名注册保留字制度。

第二十八条 任何组织或者个人注册、使用的域名中，不得含有下列内容：

- （一）反对宪法所确定的基本原则的；
- （二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- （三）损害国家荣誉和利益的；
- （四）煽动民族仇恨、民族歧视，破坏民族团结的；
- （五）破坏国家宗教政策，宣扬邪教和封建迷信的；
- （六）散布谣言，扰乱社会秩序，破坏社会稳定的；
- （七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- （八）侮辱或者诽谤他人，侵害他人合法权益的；
- （九）含有法律、行政法规禁止的其他内容的。

域名注册管理机构、域名注册服务机构不得为含有前款所列内容的域名提供服务。

第二十九条 域名注册服务机构不得采用欺诈、胁迫等不正当手段要求他人注册域名。

第三十条 域名注册服务机构提供域名注册服务，应当要求域名注册申请者提供域名持有者真实、准确、完整的身份信息等领域注册信息。

域名注册管理机构和域名注册服务机构应当对域名注册信息的真实性、完整性进行核验。

域名注册申请者提供的域名注册信息不准确、不完整的，域名注册服务机构应当要求其予以补正。申请者不补正或者提供不真实的域名注册信息的，域名注册服务机构不得为其提供域名注册服务。

第三十一条 域名注册服务机构应当公布域名注册服务的内容、时限、费用，保证服务质量，提供域名注册信息的公共查询服务。

第三十二条 域名注册管理机构、域名注册服务机构应当依法存储、保护用户个人信息。未经用户同意不得将用户个人信息提供

给他 人，但法律、行政法规另有规定的除外。

第三十三条 域名持有者的联系方式等信息发生变更的，应当在变更后30日内向域名注册服务机构办理域名注册信息变更手续。

域名所有者将域名转让给他人的，受让人应当遵守域名注册的相关要求。

第三十四条 域名所有者有权选择、变更域名注册服务机构。变更域名注册服务机构的，原域名注册服务机构应当配合域名所有者转移其域名注册相关信息。

无正当理由的，域名注册服务机构不得阻止域名所有者变更域名注册服务机构。

电信管理机构依法要求停止解析的域名，不得变更域名注册服务机构。

第三十五条 域名注册管理机构和域名注册服务机构应当设立投诉受理机制，并在其网站首页和经营场所显著位置公布投诉受理方式。

域名注册管理机构和域名注册服务机构应当及时处理投诉；不能及时处理的，应当说明理由和处理时限。

第三十六条 提供域名解析服务，应当遵守有关法律、法规、标准，具备相应的技术、服务和网络安全保障能力，落实网络与信息安全保障措施，依法记录并留存域名解析日志、维护日志和变更记录，保障解析服务质量和解析系统安全。涉及经营电信业务的，应当依法取得电信业务经营许可。

第三十七条 提供域名解析服务，不得擅自篡改解析信息。

任何组织或者个人不得恶意将域名解析指向他人的IP地址。

第三十八条 提供域名解析服务，不得为含有本办法第二十八条第一款所列内容的域名提供域名跳转。

第三十九条 从事互联网信息服务的，其使用域名应当符合法律法规和电信管理机构的有关规定，不得将域名用于实施违法行为。

第四十条 域名注册管理机构、域名注册服务机构应当配合国家有关部门依法开展的检查工作，并按照电信管理机构的要求对存在违法行为的域名采取停止解析等处置措施。

域名注册管理机构、域名注册服务机构发现其提供服务的域名发布、传输法律和行政法规禁止发布或者传输的信息的，应当立即采取消除、停止解析等处置措施，防止信息扩散，保存有关记录，并向有关部门报告。

第四十一条 域名根服务器运行机构、域名注册管理机构和域名注册服务机构应当遵守国家相关法律、法规和标准，落实网络与信息安全保障措施，配置必要的网络通信应急设备，建立健全网络与信息安全监测技术手段和应急制度。域名系统出现网络与信息安全事件时，应当在24小时内向电信管理机构报告。

因国家安全和处置紧急事件的需要，域名根服务器运行机构、域名注册管理机构和域名注册服务机构应当服从电信管理机构的统一指挥与协调，遵守电信管理机构的管理要求。

第四十二条 任何组织或者个人认为他人注册或者使用的域名侵害其合法权益的，可以向域名争议解决机构申请裁决或者依法向人民法院提起诉讼。

第四十三条 已注册的域名有下列情形之一的，域名注册服务机构应当予以注销，并通知域名所有者：

- （一）域名所有者申请注销域名的；
- （二）域名所有者提交虚假域名注册信息的；
- （三）依据人民法院的判决、域名争议解决机构的裁决，应当注销的；
- （四）法律、行政法规规定予以注销的其他情形。

第四章 监督检查

第四十四条 电信管理机构应当加强对域名服务的监督检查。域名根服务器运行机构、域名注册管理机构、域名注册服务机构应

当接受、配合电信管理机构的监督检查。

鼓励域名服务行业自律管理，鼓励公众监督域名服务。

第四十五条 域名根服务器运行机构、域名注册管理机构、域名注册服务机构应当按照电信管理机构的要求，定期报送业务开展情况、安全运行情况、网络与信息安全责任落实情况、投诉和争议处理情况等信息。

第四十六条 电信管理机构实施监督检查时，应当对域名根服务器运行机构、域名注册管理机构和域名注册服务机构报送的材料进行审核，并对其执行法律法规和电信管理机构有关规定的情况进行检查。

电信管理机构可以委托第三方专业机构开展有关监督检查活动。

第四十七条 电信管理机构应当建立域名根服务器运行机构、域名注册管理机构和域名注册服务机构的信用记录制度，将其违反本办法并受到行政处罚的行为记入信用档案。

第四十八条 电信管理机构开展监督检查，不得妨碍域名根服务器运行机构、域名注册管理机构和域名注册服务机构正常的经营和服务活动，不得收取任何费用，不得泄露所知悉的域名注册信息。

第五章 罚则

第四十九条 违反本办法第九条规定，未经许可擅自设立域名根服务器及域名根服务器运行机构、域名注册管理机构、域名注册服务机构的，电信管理机构应当根据《中华人民共和国行政许可法》第八十一条的规定，采取措施予以制止，并视情节轻重，予以警告或者处一万元以上三万元以下罚款。

第五十条 违反本办法规定，域名注册管理机构或者域名注册服务机构有下列行为之一的，由电信管理机构依据职权责令限期改正，并视情节轻重，处一万元以上三万元以下罚款，向社会公告：

- （一）为未经许可的域名注册管理机构提供域名注册服务，或者通过未经许可的域名注册服务机构开展域名注册服务的；
- （二）未按照许可的域名注册服务项目提供服务的；
- （三）未对域名注册信息的真实性、完整性进行核验的；
- （四）无正当理由阻止域名持有人变更域名注册服务机构的。

第五十一条 违反本办法规定，提供域名解析服务，有下列行为之一的，由电信管理机构责令限期改正，可以视情节轻重处一万元以上三万元以下罚款，向社会公告：

- （一）擅自篡改域名解析信息或者恶意将域名解析指向他人IP地址的；
- （二）为含有本办法第二十八条第一款所列内容的域名提供域名跳转的；
- （三）未落实网络与信息安全保障措施的；
- （四）未依法记录并留存域名解析日志、维护日志和变更记录的；
- （五）未按照要求对存在违法行为的域名进行处置的。

第五十二条 违反本办法第十七条、第十八条第一款、第二十一条、第二十二条、第二十八条第二款、第二十九条、第三十一条、第三十二条、第三十五条第一款、第四十条第二款、第四十一条规定的，由电信管理机构依据职权责令限期改正，可以并处一万元以上三万元以下罚款，向社会公告。

第五十三条 法律、行政法规对有关违法行为的处罚另有规定的，依照有关法律、行政法规的规定执行。

第五十四条 任何组织或者个人违反本办法第二十八条第一款规定注册、使用域名，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由有关部门依法予以处罚。

第六章 附则

第五十五条 本办法下列用语的含义是：

- （一）域名：指互联网上识别和定位计算机的层次结构式的字符标识，与该计算机的IP地址相对应。

(二) 中文域名：指含有中文文字的域名。

(三) 顶级域名：指域名体系中根节点下的第一级域的名称。

(四) 域名根服务器：指承担域名体系中根节点功能的服务器（含镜像服务器）。

(五) 域名根服务器运行机构：指依法获得许可并承担域名根服务器运行、维护和管理工作的机构。

(六) 域名注册管理机构：指依法获得许可并承担顶级域名运行和管理工作的机构。

(七) 域名注册服务机构：指依法获得许可、受理域名注册申请并完成域名在顶级域名数据库中注册的机构。

(八) 域名注册代理机构：指受域名注册服务机构的委托，受理域名注册申请，间接完成域名在顶级域名数据库中注册的机构。

(九) 域名管理系统：指域名注册管理机构在境内开展顶级域名运行和管理所需的主要信息系统，包括注册管理系统、注册数据库、域名解析系统、域名信息查询系统、身份信息核验系统等。

(十) 域名跳转：指对某一域名的访问跳转至该域名绑定或者指向的其他域名、IP地址或者网络信息服务等。

第五十六条 本办法中规定的日期，除明确为工作日的以外，均为自然日。

第五十七条 在本办法施行前未取得相应许可开展域名服务的，应当自本办法施行之日起十二个月内，按照本办法规定办理许可手续。

在本办法施行前已取得许可的域名根服务器运行机构、域名注册管理机构和域名注册服务机构，其许可有效期适用本办法第十六条的规定，有效期自本办法施行之日起计算。

第五十八条 本办法自2017年11月1日起施行。2004年11月5日公布的《中国互联网络域名管理办法》（原信息产业部令第30号）同时废止。本办法施行前公布的有关规定与本办法不一致的，按照本办法执行。

《计算机信息网络国际联网安全保护管理办法》

《计算机信息网络国际联网安全保护管理办法》

中华人民共和国公安部令（第33号）

《计算机信息网络国际联网安全保护管理办法》，已于1997年12月11日经国务院批准，现予发布，自1997年12月30日起施行。

公安部部长 陶驷驹 一九九七年十二月十六日

第一章 总则

第一条 为了加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和其他法律、行政法规的规定，制定本办法。

第二条 中华人民共和国境内的计算机信息网络国际联网安全保护管理，适用本办法。

第三条 公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。

公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第四条 任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

第五条 任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

- (二) 煽动颠覆国家政权、推翻社会主义制度的；
- (三) 煽动分裂国家、破坏国家统一的；
- (四) 煽动民族仇恨、民族歧视，破坏民族团结的；
- (五) 捏造或者歪曲事实，散布谣言，扰乱社会秩序的；
- (六) 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；
- (七) 公然侮辱他人或者捏造事实诽谤他人的；
- (八) 损害国家机关信誉的；
- (九) 其他违反宪法和法律、行政法规的。

第六条 任何单位和个人不得从事下列危害计算机信息网络安全的活动：

- (一) 未经允许，进入计算机信息网络或者使用计算机信息网络资源的；
- (二) 未经允许，对计算机信息网络功能进行删除、修改或者增加的；
- (三) 未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；
- (四) 故意制作、传播计算机病毒等破坏性程序的；
- (五) 其他危害计算机信息安全的。

第七条 用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

第二章 安全保护责任

第八条 从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

第九条 国际出入口信道提供单位、互联单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

第十条 互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责：

- (一) 负责本网络的安全保护管理工作，建立健全安全保护管理制度；
- (二) 落实安全保护技术措施，保障本网络的运行安全和信息安全；
- (三) 负责对本网络用户的安全教育和培训；
- (四) 对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；
- (五) 建立计算机信息网络电子公告系统的用户登记和信息管理制度；
- (六) 发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告；
- (七) 按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十一条 用户在接入单位办理入网手续时，应当填写用户备案表。备案表由公安部监制。

第十二条 互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织（包括跨省、自治区、直辖市联网的单位和所属的分支机构），应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及时报告本网络中接入单位和用户的

变更情况。

第十三条 使用公用账号的注册者应当加强对公用账号的管理，建立账号使用登记制度。用户账号不得转借、转让。

第十四条 涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。

前款所列单位的计算机信息网络与国际联网，应当采取相应的安全保护措施。

第三章 安全监督

第十五条 省、自治区、直辖市公安厅（局），地（市）、县（市）公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十六条 公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国家有关规定逐级上报。

第十七条 公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

第十八条 公安机关计算机管理监察机构发现含有本办法第五条所列内容的地址、目录或者服务器时，应当通知有关单位关闭或者删除。

第十九条 公安机关计算机管理监察机构应当负责追踪和查处通过计算机信息网络的违法行为和针对计算机信息网络的犯罪案件，对违反本办法第四条、第七条规定的违法犯罪行为，应当按照国家有关规定移送有关部门或者司法机关处理。

第四章 法律责任

第二十条 违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

第二十一条 有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的期限内未改正的，对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

- （一）未建立安全保护管理制度的；
- （二）未采取安全技术保护措施的；
- （三）未对网络用户进行安全教育和培训的；
- （四）未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的；
- （五）对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的；
- （六）未建立电子公告系统的用户登记和信息管理制度的；
- （七）未按照国家有关规定，删除网络地址、目录或者关闭服务器的；
- （八）未建立公用账号使用登记制度的；
- （九）转借、转让用户账号的。

第二十二条 违反本办法第四条、第七条规定的，依照有关法律、法规予以处罚。 第二十三条 违反本办法第十一条、第十二条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过六个月的处罚。

第五章 附则

第二十四条 与香港特别行政区和台湾、澳门地区联网的计算机信息网络的安全保护管理，参照本办法执行。

第二十五条 本办法自发布之日起施行。

《计算机信息系统安全专用产品检测和销售许可证管理办法》

《计算机信息系统安全专用产品检测和销售许可证管理办法》

(公安部第 32 号令)

第一章 总则

第一条 为了加强计算机信息系统安全专用产品（以下简称安全专用产品）的管理，保证安全专用产品的安全功能，维护计算机信息系统的安全，根据《中华人民共和国计算机信息系统安全保护条例》第十六条的规定，制定本办法。

第二条 本办法所称计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

第三条 中华人民共和国境内的安全专用产品进入市场销售，实行销售许可证制度。安全专用产品的生产者在其产品进入市场销售之前，必须申领《计算机信息系统安全专用产品销售许可证》（以下简称销售许可证）。

第四条 安全专用产品的生产者申领销售许可证，必须对其产品进行安全功能检测和认定。

第五条 公安部计算机管理监察部门负责销售许可证的审批颁发工作和安全专用产品安全功能检测机构（以下简称检测机构）的审批工作。

地（市）级以上人民政府公安机关负责销售许可证的监督检查工作。

第二章 检测机构的申请与批准

第六条 经省级以上技术监督行政主管部门或者其授权的部门考核合格的检测机构，可以向公安部计算机管理监察部门提出承担安全专用产品检测任务的申请。

第七条 公安部计算机管理监察部门对提出申请的检测机构的检测条件和能力进行审查，经审查合格的，批准其承担安全专用产品检测任务。

第八条 检测机构应当履行下列职责：

- （一）严格执行公安部计算机管理监察部门下达的检测任务；
- （二）按照标准格式填写安全专用产品检测报告；
- （三）出具检测结果报告；
- （四）接受公安部计算机管理监察部门对检测过程的监

督及查阅检测机构内部验证和审核试验的原始测试记录；

- （五）保守检测产品的技术秘密，并不得非法占有他人科技成果；

- （六）不得从事与检测产品有关的开发和对外咨询业务。

第九条 公安部计算机管理监察部门对承担检测任务的检测机构每年至少进行一次监督检查。

第十条 被取消检测资格的检测机构，两年后方准许重新申请承担安全专用产品的检测任务。第三章 安全专用产品的检测

第十一条 安全专用产品的生产者应当向经公安部计算机管理监察部门批准的检测机构申请安全功能检测。

对在国内生产的安全专用产品，由其生产者负责送交检测；对境外生产在国内销售的安全专用产品，由国外生产者指定的国内具有法人资格的企业或单位负责送交检测。

当安全专用产品的安全功能发生改变时，安全专用产品应当进行重新检测。

第十二条 送交安全专用产品检测时，应当向检测机构提交以下材料：

- (一) 安全专用产品的安全功能检测申请；
- (二) 营业执照（复印件）；
- (三) 样品；
- (四) 产品功能及性能的中文说明；
- (五) 证明产品功能及性能的有关材料；
- (六) 采用密码技术的安全专用产品必须提交国家密码管理部门的审批文件；
- (七) 根据有关规定需要提交的其他材料。

第十三条 检测机构收到检测申请、样品及其他有关材料后，应当按照安全专用产品的功能说明，检测其是否具有计算机信息系统安全保护功能。

第十四条 检测机构应当及时检测，并将检测报告报送公安部计算机管理监察部门备案。

第四章 销售许可证的审批与颁发

第十五条 安全专用产品的生产者申领销售许可证，应当向公安部计算机管理监察部门提交以下材料：

- (一) 营业执照（复印件）；
- (二) 安全专用产品检测结果报告；
- (三) 防治计算机病毒的安全专用产品须提交公安机关颁发的计算机病毒防治研究的备案证明。

第十六条 公安部计算机管理监察部门自接到申请之日起，应当在十五日内对安全专用产品作出审核结果，特殊情况可延至三十日；经审核合格的，颁发销售许可证和安全专用产品“销售许可”标记；不合格的，书面通知申领者，并说明理由。

第十七条 已取得销售许可证的安全专用产品，生产者应当在固定位置标明“销售许可”标记。

任何单位和个人不得销售无“销售许可”标记的安全专用产品。

第十八条 销售许可证只对所申请销售的安全专用产品有效。当安全专用产品的功能发生改变时，必须重新申领销售许可证。

第十九条 销售许可证自批准之日起两年内有效。期满需要延期的，应当于期满前三十日内向公安部计算机管理监察部门申请办理延期手续。

第五章 罚则

第二十条 生产企业违反本办法的规定，有下列情形之一的，视为未经许可出售安全专用产品，由公安机关根据《中华人民共和国计算机信息系统安全保护条例》的规定予以处罚：

- (一) 没有申领销售许可证而将生产的安全专用产品进入市场销售的；
- (二) 安全专用产品的功能发生改变，而没有重新申领销售许可证进行销售的；
- (三) 销售许可证有效期满，未办理延期申领手续而继续销售的；
- (四) 提供虚假的安全专用产品检测报告或者虚假的计算机病毒防治研究的备案证明，骗取销售许可证的；
- (五) 销售的安全专用产品与送检样品安全功能不一致的；
- (六) 未在安全专用产品上标明“销售许可”标记而销售的；

(七) 伪造、变造销售许可证和“销售许可”标记的。

第二十一条 检测机构违反本办法的规定，情节严重的，取消检测资格

第二十二条 安全专用产品中含有有害数据危害计算机信息系统安全的，依据《中华人民共和国计算机信息系统安全保护条例》第二十三条的规定处罚；构成犯罪的，依法追究刑事责任。

第二十三条 依照本办法作出的行政处罚，应当由县级以上（含县级）公安机关决定，并填写行政处罚决定书，向被处罚人宣布。

第六章 附则

第二十四条 安全专用产品的检测通告和经安全功能检测确认的安全专用产品目录，由公安部计算机管理监察部门发布。

第二十五条 检测机构申请书、检测机构批准书、《计算机信息系统安全专用产品销售许可证》、“销售许可”标记，由公安部制定式样，统一监制。

第二十六条 本办法自一九九七年十二月十二日起施行。

《互联网安全保护技术措施规定》

《互联网安全保护技术措施规定》

(公安部令第 82 号)

《互联网安全保护技术措施规定》已经2005年11月23日公安部部长办公会议通过，现予发布，自2006年3月1日起施行。

公安部部长：周永康

2005年12月13日

第一条 为加强和规范互联网安全技术防范工作，保障互联网网络安全和信息安全，促进互联网健康、有序发展，维护国家安全、社会秩序和公共利益，根据《计算机信息网络国际联网安全保护管理办法》，制定本规定。

第二条 本规定所称互联网安全保护技术措施，是指保障互联网网络安全和信息安全、防范违法犯罪的技术设施和技术方法。

第三条 互联网服务提供者、联网使用单位负责落实互联网安全保护技术措施，并保障互联网安全保护技术措施功能的正常发挥。

第四条 互联网服务提供者、联网使用单位应当建立相应的管理制度。未经用户同意不得公开、泄露用户注册信息，但法律、法规另有规定的除外。

互联网服务提供者、联网使用单位应当依法使用互联网安全保护技术措施，不得利用互联网安全保护技术措施侵犯用户的通信自由和通信秘密。

第五条 公安机关公共信息网络安全监察部门负责对互联网安全保护技术措施的落实情况依法实施监督管理。

第六条 互联网安全保护技术措施应当符合国家标准。没有国家标准的，应当符合公共安全行业标准。

第七条 互联网服务提供者和联网使用单位应当落实以下互联网安全保护技术措施：

- (一) 防范计算机病毒、网络入侵和攻击破坏等危害网络安全事项或者行为的技术措施；
- (二) 重要数据库和系统主要设备的冗余备份措施；
- (三) 记录并留存用户登录和退出时间、主叫号码、账号、互联网地址或域名、系统维护日志的技术措施；
- (四) 法律、法规和规章规定应当落实的其他安全保护技术措施。

第八条 提供互联网接入服务的单位除落实本规定第七条规定的互联网安全保护技术措施外，还应当落实具有以下功能的安全保护技术措施：

- (一) 记录并留存用户注册信息；

(二) 使用内部网络地址与互联网网络地址转换方式为用户提供接入服务的，能够记录并留存用户使用的互联网网络地址和内部网络地址对应关系；

(三) 记录、跟踪网络运行状态，监测、记录网络安全事件等安全审计功能。

第九条 提供互联网信息服务的单位除落实本规定第七条规定的互联网安全保护技术措施外，还应当落实具有以下功能的安全保护技术措施：

(一) 在公共信息服务中发现、停止传输违法信息，并保留相关记录；

(二) 提供新闻、出版以及电子公告等服务的，能够记录并留存发布的信息内容及发布时间；

(三) 开办门户网站、新闻网站、电子商务网站的，能够防范网站、网页被篡改，被篡改后能够自动恢复；

(四) 开办电子公告服务的，具有用户注册信息和发布信息审计功能；

(五) 开办电子邮件和网上短信息服务的，能够防范、清除以群发方式发送伪造、隐匿信息发送者真实标记的电子邮件或者短信息。

第十条 提供互联网数据中心服务的单位和联网使用单位除落实本规定第七条规定的互联网安全保护技术措施外，还应当落实具有以下功能的安全保护技术措施：

(一) 记录并留存用户注册信息；

(二) 在公共信息服务中发现、停止传输违法信息，并保留相关记录；

(三) 联网使用单位使用内部网络地址与互联网网络地址转换方式向用户提供接入服务的，能够记录并留存用户使用的互联网网络地址和内部网络地址对应关系。

第十一条 提供互联网上网服务的单位，除落实本规定第七条规定的互联网安全保护技术措施外，还应当安装并运行互联网公共上网服务场所安全管理系统。

第十二条 互联网服务提供者依照本规定采取的互联网安全保护技术措施应当具有符合公共安全行业技术标准的联网接口。

第十三条 互联网服务提供者和联网使用单位依照本规定落实的记录留存技术措施，应当具有至少保存六十天记录备份的功能。

第十四条 互联网服务提供者和联网使用单位不得实施下列破坏互联网安全保护技术措施的行为：

(一) 擅自停止或者部分停止安全保护技术设施、技术手段运行；

(二) 故意破坏安全保护技术设施；

(三) 擅自删除、篡改安全保护技术设施、技术手段运行程序和记录；

(四) 擅自改变安全保护技术措施的用途和范围；

(五) 其他故意破坏安全保护技术措施或者妨碍其功能正常发挥的行为。

第十五条 违反本规定第七条至第十四条规定的，由公安机关依照《计算机信息网络国际联网安全保护管理办法》第二十一条的规定予以处罚。

第十六条 公安机关应当依法对辖区内互联网服务提供者和联网使用单位安全保护技术措施的落实情况进行指导、监督和检查。

公安机关在依法监督检查时，互联网服务提供者、联网使用单位应当派人参加。公安机关对监督检查发现的问题，应当提出改进意见，通知互联网服务提供者、联网使用单位及时整改。 公安机关在监督检查时，监督检查人员不得少于二人，并应当出示执法身份证件。

第十七条 公安机关及其工作人员违反本规定，有滥用职权，徇私舞弊行为的，对直接负责的主管人员和其他直接责任人员依法给予行政处分；构成犯罪的，依法追究刑事责任。

第十八条 本规定所称互联网服务提供者，是指向用户提供互联网接入服务、互联网数据中心服务、互联网信息服务和互联网上网服务的单位。

本规定所称联网使用单位，是指为本单位应用需要连接并使用互联网的单位。

本规定所称提供互联网数据中心服务的单位，是指提供主机托管、租赁和虚拟空间租用等服务的单位。

第十九条 本规定自2006年3月1日起施行。

《信息安全等级保护管理办法》

《信息安全等级保护管理办法》

(公安部、国家保密局、国家密码管理局、国务院信息工作办公室联合印发)

公安部、国家保密局、国家密码管理局、国务院信息工作办公室关于印发《信息安全等级保护管理办法》的通知

(公通字[2007]43号)

各省、自治区、直辖市公安厅(局)、保密局、国家密码管理局(国家密码管理委员会办公室)、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理局、信息化领导小组办公室，中央和国家机关各部委保密委员会办公室、密码工作领导小组办公室、信息化领导小组办公室，各人民团体保密委员会办公室：

为加快推进信息安全等级保护，规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定了《信息安全等级保护管理办法》。现印发给你们，请认真贯彻执行。

公安部

国家保密局

国家密码管理局

国务院信息工作办公室

二〇〇七年六月二十二日

第一章 总则

第一条 为规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规，制定本办法。

第二条 国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

第三条 公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。国务院信息化工作办公室及地方信息化领导小组办公室负责等级保护工作的部门间协调。

第四条 信息系统主管部门应当依照本办法及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

第五条 信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。

第二章 等级划分与保护

第六条 国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统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因素确定。

第七条 信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，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。

第二级，信息系统受到破坏后，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。

第三级，信息系统受到破坏后，会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。

第四级，信息系统受到破坏后，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。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第八条 信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

第三章 等级保护的实施与管理

第九条 信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。

第十条 信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。有主管部门的，应当经主管部门审核批准。

跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。

对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。

第十一条 信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

第十二条 在信息系统建设过程中，运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）、《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）、《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）、《信息安全技术 服务器技术要求》、《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671-2006）等技术标准同步建设符合该等级要求的信息安全设施。

第十三条 运营、使用单位应当参照《信息安全技术 信息系统安全管理要求》（GB/T20269-2006）、《信息安全技术 信息系统安全工程管理要求》（GB/T20282-2006）、《信息系统安全等级保护基本要求》等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。

第十四条 信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。

信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据特殊安全需求进行自查。

经测评或者自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

第十五条 已运营（运行）的第二级以上信息系统，应当在安全保护等级确定后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

新建第二级以上信息系统，应当在投入运行后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。

第十六条 办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料：

- （一）系统拓扑结构及说明；
- （二）系统安全组织机构和管理制度；
- （三）系统安全保护设施设计实施方案或者改建实施方案；
- （四）系统使用的信息安全产品清单及其认证、销售许可证明；
- （五）测评后符合系统安全保护等级的技术检测评估报告；
- （六）信息系统安全保护等级专家评审意见；
- （七）主管部门审核批准信息系统安全保护等级的意见。

第十七条 信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，应当在收到备案材料之日起的10个工作日内颁发信息系统安全等级保护备案证明；发现不符合本办法及有关标准的，应当在收到备案材料之日起的10个工作日内通知备案单位予以纠正；发现定级不准的，应当在收到备案材料之日起的10个工作日内通知备案单位重新审核确定。

运营、使用单位或者主管部门重新确定信息系统等级后，应当按照本办法向公安机关重新备案。

第十八条 受理备案的公安机关应当对第三级、第四级信息系统的运营、使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次，对第四级信息系统每半年至少检查一次。对跨省或者全国统一联网运行的信息系统的检查，应当会同其主管部门进行。对第五级信息系统，应当由国家指定的专门部门进行检查。

公安机关、国家指定的专门部门应当对下列事项进行检查：

- （一）信息系统安全需求是否发生变化，原定保护等级是否准确；
- （二）运营、使用单位安全管理制度、措施的落实情况；
- （三）运营、使用单位及其主管部门对信息系统安全状况的检查情况；
- （四）系统安全等级测评是否符合要求；
- （五）信息安全产品使用是否符合要求；
- （六）信息系统安全整改情况；
- （七）备案材料与运营、使用单位、信息系统的符合情况；
- （八）其他应当进行监督检查的事项。

第十九条 信息系统运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导，如实向公安机

关、国家指定的专门部门提供下列有关信息安全保护的信息资料及数据文件：

- (一) 信息系统备案事项变更情况；
- (二) 安全组织、人员的变动情况；
- (三) 信息安全管理制度、措施变更情况；
- (四) 信息系统运行状况记录；
- (五) 运营、使用单位及主管部门定期对信息系统安全状况的检查记录；
- (六) 对信息系统开展等级测评的技术测评报告；
- (七) 信息安全产品使用的变更情况；
- (八) 信息安全事件应急预案，信息安全事件应急处置结果报告；
- (九) 信息系统安全建设、整改结果报告。

第二十条 公安机关检查发现信息系统安全保护状况不符合信息安全等级保护有关管理规范和技术标准的，应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求，按照管理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案。必要时，公安机关可以对整改情况组织检查。

第二十一条 第三级以上信息系统应当选择使用符合以下条件的信息安全产品：

- (一) 产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；
- (二) 产品的核心技术、关键部件具有我国自主知识产权；
- (三) 产品研制、生产单位及其主要业务、技术人员无犯罪记录；
- (四) 产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；
- (五) 对国家安全、社会秩序、公共利益不构成危害；
- (六) 对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

第二十二条 第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：

- (一) 在中华人民共和国境内注册成立（港澳台地区除外）；
- (二) 由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；
- (三) 从事相关检测评估工作两年以上，无违法记录；
- (四) 工作人员仅限于中国公民；
- (五) 法人及主要业务、技术人员无犯罪记录；
- (六) 使用的技术装备、设施应当符合本办法对信息安全产品的要求；
- (七) 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；
- (八) 对国家安全、社会秩序、公共利益不构成威胁。

第二十三条 从事信息系统安全等级测评的机构，应当履行下列义务：

- (一) 遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；
- (二) 保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险；
- (三) 对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律义务，并负

责检查落实。

第四章 涉及国家秘密信息系统的分级保护管理

第二十四条 涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。

非涉密信息系统不得处理国家秘密信息。

第二十五条 涉密信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密三个等级。

涉密信息系统建设使用单位应当在信息规范定密的基础上，依据涉密信息系统分级保护管理办法和国家保密标准BMB17-2006《涉及国家秘密的计算机信息系统分级保护技术要求》确定系统等级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定保护等级。

保密工作部门和机构应当监督指导涉密信息系统建设使用单位准确、合理地进行系统定级。

第二十六条 涉密信息系统建设使用单位应当将涉密信息系统定级和建设使用情况，及时上报业务主管部门的保密工作机构和负责系统审批的保密工作部门备案，并接受保密部门的监督、检查、指导。

第二十七条 涉密信息系统建设使用单位应当选择具有涉密集成资质的单位承担或者参与涉密信息系统的设计与实施。

涉密信息系统建设使用单位应当依据涉密信息系统分级保护管理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。

第二十八条 涉密信息系统使用的信息安全保密产品原则上应当选用国产品，并应当通过国家保密局授权的检测机构依据有关国家保密标准进行的检测，通过检测的产品由国家保密局审核发布目录。

第二十九条 涉密信息系统建设使用单位在系统工程实施结束后，应当向保密工作部门提出申请，由国家保密局授权的系统测评机构依据国家保密标准BMB22-2007《涉及国家秘密的计算机信息系统分级保护测评指南》，对涉密信息系统进行安全保密测评。

涉密信息系统建设使用单位在系统投入使用前，应当按照《涉及国家秘密的信息系统审批管理规定》，向设区的市级以上保密工作部门申请进行系统审批，涉密信息系统通过审批后方可投入使用。已投入使用的涉密信息系统，其建设使用单位在按照分级保护要求完成系统整改后，应当向保密工作部门备案。

第三十条 涉密信息系统建设使用单位在申请系统审批或者备案时，应当提交以下材料：

- (一) 系统设计、实施方案及审查论证意见；
- (二) 系统承建单位资质证明材料；
- (三) 系统建设和工程监理情况报告；
- (四) 系统安全保密检测评估报告；
- (五) 系统安全保密组织机构和管理制度情况；
- (六) 其他有关材料。

第三十一条 涉密信息系统发生涉密等级、连接范围、环境设施、主要应用、安全保密管理责任单位变更时，其建设使用单位应当及时向负责审批的保密工作部门报告。保密工作部门应当根据实际情况，决定是否对其重新进行测评和审批。

第三十二条 涉密信息系统建设使用单位应当依据国家保密标准BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》，加强涉密信息系统运行中的保密管理，定期进行风险评估，消除泄密隐患和漏洞。

第三十三条 国家和地方各级保密工作部门依法对各地区、各部门涉密信息系统分级保护工作实施监督管理，并做好以下工作：

- (一) 指导、监督和检查分级保护工作的开展；

(二) 指导涉密信息系统建设使用单位规范信息定密, 合理确定系统保护等级;

(三) 参与涉密信息系统分级保护方案论证, 指导建设使用单位做好保密设施的同步规划设计; (四) 依法对涉密信息系统集成资质单位进行监督管理;

(五) 严格进行系统测评和审批工作, 监督检查涉密信息系统建设使用单位分级保护管理制度和技术措施的落实情况;

(六) 加强涉密信息系统运行中的保密监督检查。对秘密级、机密级信息系统每两年至少进行一次保密检查或者系统测评, 对绝密级信息系统每年至少进行一次保密检查或者系统测评;

(七) 了解掌握各级各类涉密信息系统的管理使用情况, 及时发现和查处各种违规违法行为和泄密事件。

第五章 信息安全等级保护的密码管理

第三十四条 国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度, 被保护对象的安全防护要求和涉密程度, 被保护对象被破坏后的危害程度以及密码使用部门的性质等, 确定密码的等级保护准则。

信息系统运营、使用单位采用密码进行等级保护的, 应当遵照《信息安全等级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

第三十五条 信息系统安全等级保护中密码的配备、使用和管理等, 应当严格执行国家密码管理的有关规定。

第三十六条 信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的, 应报经国家密码管理局审批, 密码的设计、实施、使用、运行维护和日常管理等, 应当按照国家密码管理有关规定和相关标准执行; 采用密码对不涉及国家秘密的信息和信息系统进行保护的, 须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准, 其密码的配备使用情况应当向国家密码管理机构备案。

第三十七条 运用密码技术对信息系统进行系统等级保护建设和整改的, 必须采用经国家密码管理部门批准使用或者准予销售的密码产品进行安全保护, 不得采用国外引进或者擅自研制的密码产品; 未经批准不得采用含有加密功能的进口信息技术产品。

第三十八条 信息系统中的密码及密码设备的测评工作由国家密码管理局认可的测评机构承担, 其他任何部门、单位和个人不得对密码进行评测和监控。

第三十九条 各级密码管理部门可以定期或者不定期对信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评, 对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和测评。在监督检查过程中, 发现存在安全隐患或者违反密码管理相关规定或者未达到密码相关标准要求的, 应当按照国家密码管理的相关规定进行处置。

第六章 法律责任

第四十条 第三级以上信息系统运营、使用单位违反本办法规定, 有下列行为之一的, 由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正; 逾期不改正的, 给予警告, 并向其上级主管部门通报情况, 建议对其直接负责的主管人员和其他直接责任人员予以处理, 并及时反馈处理结果:

(一) 未按本办法规定备案、审批的;

(二) 未按本办法规定落实安全管理制度、措施的;

(三) 未按本办法规定开展系统安全状况检查的;

(四) 未按本办法规定开展系统安全技术测评的;

(五) 接到整改通知后, 拒不整改的;

(六) 未按本办法规定选择使用信息安全产品和测评机构的;

(七) 未按本办法规定如实提供有关文件和证明材料的;

(八) 违反保密管理规定的;

(九) 违反密码管理规定的；

(十) 违反本办法其他规定的。

违反前款规定，造成严重损害的，由相关部门依照有关法律、法规予以处理。

第四十一条 信息安全监管部门及其工作人员在履行监督管理职责中，玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第七章 附则

第四十二条 已运行信息系统的运营、使用单位自本办法施行之日起180日内确定信息系统的安全保护等级；新建信息系统在设计、规划阶段确定安全保护等级。

第四十三条 本办法所称“以上”包含本数（级）。

第四十四条 本办法自发布之日起施行，《信息安全等级保护管理办法（试行）》（公通字[2006]7号）同时废止。

《计算机病毒防治管理办法》

《计算机病毒防治管理办法》

(中华人民共和国公安部令 第51号)

《计算机病毒防治管理办法》已经2000年3月30日公安部部长办公会议通过，现予发布施行。

公安部部长 贾春旺

二〇〇〇年四月二十六日

第一条 为了加强对计算机病毒的预防和治理，保护计算机信息系统安全，保障计算机的应用与发展，根据《中华人民共和国计算机信息系统安全保护条例》的规定，制定本办法。

第二条 本办法所称的计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

第三条 中华人民共和国境内的计算机信息系统以及未联网计算机的计算机病毒防治管理工作，适用本办法。

第四条 公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作。

地方各级公安机关具体负责本行政区域内的计算机病毒防治管理工作。

第五条 任何单位和个人不得制作计算机病毒。

第六条 任何单位和个人不得有下列传播计算机病毒的行为：

(一)故意输入计算机病毒，危害计算机信息系统安全；

(二)向他人提供含有计算机病毒的文件、软件、媒体；

(三)销售、出租、附赠含有计算机病毒的媒体；

(四)其他传播计算机病毒的行为。

第七条 任何单位和个人不得向社会发布虚假的计算机病毒疫情。

第八条 从事计算机病毒防治产品生产的单位，应当及时向公安部公共信息网络安全监察部门批准的计算机病毒防治产品检测机构提交病毒样本。

第九条 计算机病毒防治产品检测机构应当对提交的病毒样本及时进行分析、确认，并将确认结果上报公安部公共信息网络安全监察部门。

第十条 对计算机病毒的认定工作，由公安部公共信息网络安全监察部门批准的机构承担。

第十一条 计算机信息系统的使用单位在计算机病毒防治工作中应当履行下列职责：

- (一)建立本单位的计算机病毒防治管理制度；
- (二)采取计算机病毒安全技术防治措施；
- (三)对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训；
- (四)及时检测、清除计算机信息系统中的计算机病毒，并备有检测、清除的记录；
- (五)使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品；
- (六)对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向公安机关报告，并保护现场。

第十二条 任何单位和个人在从计算机信息网络上下载程序、数据或者购置、维修、借入计算机设备时，应当进行计算机病毒检测。

第十三条 任何单位和个人销售、附赠的计算机病毒防治产品，应当具有计算机信息系统安全专用产品销售许可证，并贴有“销售许可”标记。

第十四条 从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人，应当对计算机设备或者媒体进行计算机病毒检测、清除工作，并备有检测、清除的记录。

第十五条 任何单位和个人应当接受公安机关对计算机病毒防治工作的监督、检查和指导。

第十六条 在非经营活动中有违反本办法第五条、第六条第二、三、四项规定行为之一的，由公安机关处以一千元以下罚款。

在经营活动中有违反本办法第五条、第六条第二、三、四项规定行为之一，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。

违反本办法第六条第一项规定的，依照《中华人民共和国计算机信息系统安全保护条例》第二十三条的规定处罚。

第十七条 违反本办法第七条、第八条规定行为之一的，由公安机关对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款；对个人处以五百元以下罚款。

第十八条 违反本办法第九条规定的，由公安机关处以警告，并责令其限期改正；逾期不改正的，取消其计算机病毒防治产品检测机构的检测资格。

第十九条 计算机信息系统的使用单位有下列行为之一的，由公安机关处以警告，并根据情况责令其限期改正；逾期不改正的，对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款：

- (一)未建立本单位计算机病毒防治管理制度的；
- (二)未采取计算机病毒安全技术防治措施的；
- (三)未对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训的；
- (四)未及时检测、清除计算机信息系统中的计算机病毒，对计算机信息系统造成危害的；
- (五)未使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品，对计算机信息系统造成危害的。

第二十条 违反本办法第十四条规定，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。

第二十一条 本办法所称计算机病毒疫情，是指某种计算机病毒爆发、流行的时间、范围、破坏特点、破坏后果等情况的报告或者预报。

本办法所称媒体，是指计算机软盘、硬盘、磁带、光盘等。

第二十二条 本办法自发布之日起施行。

🔗 《中国互联网络域名管理办法》

《中国互联网络域名管理办法》

(中华人民共和国信息产业部令第 30 号公布)

《中国互联网络域名管理办法》已经2004年9月28日信息产业部第8次部务会议审议通过，现予公布，自2004年12月20日起施行。

部长 王旭东 二〇〇四年十一月五日

第一章 总则

第一条 为促进中国互联网络的健康发展，保障中国互联网络域名系统安全、可靠地运行，规范中国互联网络域名系统管理和域名注册服务，根据国家有关规定，参照国际上互联网络域名管理准则，制定本办法。

第二条 在中华人民共和国境内从事域名注册服务及相关活动，应当遵守本办法。

第三条 本办法下列用语的含义是：

- (一) 域名：是互联网络上识别和定位计算机的层次结构式的字符标识，与该计算机的互联网协议（IP）地址相对应。
- (二) 中文域名：是指含有中文文字的域名。
- (三) 域名根服务器：是指承担域名体系中根节点功能的服务器。
- (四) 域名根服务器运行机构：是指承担运行、维护和管理域名根服务器的机构。
- (五) 顶级域名：是指域名体系中根节点下的第一级域的名称。
- (六) 域名注册管理机构：是指承担顶级域名系统的运行、维护和管理工作的机构。
- (七) 域名注册服务机构：是指受理域名注册申请，直接完成域名在国内顶级域名数据库中注册、直接或间接完成域名在国外顶级域名数据库中注册的机构。

第四条 信息产业部负责中国互联网络域名的管理工作，主要职责是：

- (一) 制定互联网络域名管理的规章及政策；
- (二) 制定国家（或地区）顶级域名CN和中文域名体系；
- (三) 管理在中华人民共和国境内设置并运行域名根服务器（含镜像服务器）的域名根服务器运行机构；
- (四) 管理在中华人民共和国境内设立的域名注册管理机构和域名注册服务机构；
- (五) 监督管理域名注册活动；
- (六) 负责与域名有关的国际协调。

第五条 任何组织或者个人不得采取任何手段妨碍中华人民共和国境内互联网域名系统的正常运行。

第二章 域名管理

第六条 我国互联网的域名体系由信息产业部以公告形式予以公布。根据域名发展的实际情况，信息产业部可以对互联网的域名体系进行调整，并发布更新公告。

第七条 中文域名是我国域名体系的重要组成部分。信息产业部鼓励和支持中文域名系统的技术研究和逐步推广应用。

第八条 在中华人民共和国境内设置域名根服务器及设立域名根服务器运行机构，应当经信息产业部批准。

第九条 申请设置互联网域名根服务器及设立域名根服务器运行机构，应当具备以下条件：

- (一) 具有相应的资金和专门人员；
- (二) 具有保障域名根服务器安全可靠运行的环境条件和技术能力；

- (三) 具有健全的网络与信息安全保障措施；
- (四) 符合互联网络发展以及域名系统稳定运行的需要；
- (五) 符合国家其他有关规定。

第十条 申请设置域名根服务器及设立域名根服务器运行机构，应向信息产业部提交以下书面申请材料：

- (一) 申请单位的基本情况；
- (二) 拟运行维护的域名根服务器情况；
- (三) 网络技术方案；
- (四) 网络与信息安全技术保障措施的证明。

第十一条 在中华人民共和国境内设立域名注册管理机构和域名注册服务机构，应当经信息产业部批准。

第十二条 申请成为域名注册管理机构，应当具备以下条件：

(一) 在中华人民共和国境内设置顶级域名服务器（不含镜像服务器），且相应的顶级域名符合国际互联网域名体系和中国互联网域名体系；

- (二) 有与从事域名注册有关活动相适应的资金和专业人员；
- (三) 有从事互联网域名等相关服务的良好业绩和运营经验；
- (四) 有为用户提供长期服务的信誉或者能力；
- (五) 有业务发展计划和相关技术方案；
- (六) 有健全的域名注册服务监督机制和网络与信息安全保障措施；
- (七) 符合国家其他有关规定。

第十三条 申请成为域名注册管理机构的，应当向信息产业部提交下列材料：

- (一) 有关资金和人员的说明材料；
- (二) 对境内的顶级域名服务器实施有效管理的证明材料；
- (三) 证明申请人信誉的材料；
- (四) 业务发展计划及相关技术方案；
- (五) 域名注册服务监督机制和网络与信息安全技术保障措施；
- (六) 拟与域名注册服务机构签署的协议范本；
- (七) 法定代表人签署的遵守国家有关法律、政策和我国域名体系的承诺书。

第十四条 从事域名注册服务活动，应当具备下列条件：

- (一) 是依法设立的企业法人或事业法人；
- (二) 注册资金不得少于人民币100万元，在中华人民共和国境内设置有域名注册服务系统，且有专门从事域名注册服务的技术人员和客户服务人员；
- (三) 有为用户提供长期服务的信誉或者能力；
- (四) 有业务发展计划及相关技术方案；
- (五) 有健全的网络与信息安全保障措施；

(六) 有健全的域名注册服务退出机制；

(七) 符合国家其他有关规定。

第十五条 申请成为域名注册服务机构，应当向信息产业部提交以下书面材料：

(一) 法人资格证明；

(二) 拟提供注册服务的域名项目及技术人员、客户服务人员的情况说明；

(三) 与相关域名注册管理机构或境外的域名注册服务机构签订的合作意向书或协议；

(四) 用户服务协议范本；

(五) 业务发展计划及相关技术方案；

(六) 网络与信息安全技术保障措施的证明；

(七) 证明申请人信誉的有关材料；

(八) 法定代表人签署的遵守国家有关法律、政策的承诺书。

第十六条 对申请材料齐全、符合法定形式的，信息产业部应当向申请人发出受理申请通知书；对申请材料不齐全或者不符合法定形式的，应当当场或在五日内一次性书面告知申请人需要补齐的全部内容；对不予受理的，应当向申请人出具不予受理通知书，并说明理由。

第十七条 信息产业部应当自发出受理申请通知书之日起二十个工作日内完成审查工作，作出批准或者不予批准的决定。二十个工作日内不能作出决定的，经信息产业部负责人批准，可以延长十个工作日，并将延长期限的理由告知申请人。

予以批准的，出具批准意见书；不予以批准的，书面通知申请人并说明理由。

第十八条 域名注册管理机构应当自觉遵守国家相关的法律、行政法规和规章，保证域名系统安全、可靠地运行，公平、合理地为用户注册服务机构提供安全、方便的域名服务。

无正当理由，域名注册管理机构不得擅自中断域名注册服务机构的域名注册服务。

第十九条 域名注册服务机构应当自觉遵守国家相关法律、行政法规和规章，公平、合理地为用户提供域名注册服务。

域名注册服务机构不得采用欺诈、胁迫等不正当的手段要求用户注册域名。

第二十条 域名注册服务机构的名称、地址、法定代表人等登记信息发生变更或者域名注册服务机构与其域名注册管理机构的合作关系发生变更或终止时，域名注册服务机构应当在变更或终止后三十日内报信息产业部备案。

第二十一条 域名注册管理机构应当配置必要的网络和通信应急设备，制定切实有效的网络通信保障应急预案，健全网络与信息安全应急制度。

因国家安全和处置紧急事件的需要，域名注册管理机构和域名注册服务机构应当服从信息产业部的统一指挥与协调，遵守并执行信息产业部的管理要求。

第二十二条 信息产业部应当加强对域名注册管理机构和域名注册服务机构的监督检查，纠正监督检查过程中发现的违法行为。

第三章 域名注册

第二十三条 域名注册管理机构应当根据本办法制定相应的域名注册实施细则，报信息产业部备案后施行。

第二十四条 域名注册服务遵循“先申请先注册”原则。

第二十五条 为维护国家利益和社会公众利益，域名注册管理机构可以对部分保留字进行必要保护，报信息产业部备案后施行。

除前款规定外，域名注册管理机构和注册服务机构不得预留或变相预留域名。域名注册管理机构和注册服务机构在提供域

名注册服务过程中不得代表任何实际或潜在的域名持有者。

第二十六条 域名注册管理机构和域名注册服务机构应当公布域名注册服务的内容、时限、费用，提供域名注册信息的公共查询服务，保证域名注册服务的质量，并有义务向信息产业部提供域名注册信息。

未经用户同意，域名注册管理机构和域名注册服务机构不得将域名注册信息用于前款规定以外的其他用途，但国家法律、行政法规另有规定的除外。

第二十七条 任何组织或个人注册和使用的域名，不得含有下列内容：

- （一）反对宪法所确定的基本原则的；
- （二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- （三）损害国家荣誉和利益的；
- （四）煽动民族仇恨、民族歧视，破坏民族团结的；
- （五）破坏国家宗教政策，宣扬邪教和封建迷信的；
- （六）散布谣言，扰乱社会秩序，破坏社会稳定的；
- （七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- （八）侮辱或者诽谤他人，侵害他人合法权益的；
- （九）含有法律、行政法规禁止的其他内容的。

第二十八条 域名注册申请者应当提交真实、准确、完整的域名注册信息，并与域名注册服务机构签订用户注册协议。

域名注册完成后，域名注册申请者即成为其注册域名的持有者。

第二十九条 域名持有者应当遵守国家有关互联网络的法律、行政法规和规章。

因持有或使用域名而侵害他人合法权益的责任，由域名持有者承担。

第三十条 注册域名应当按期缴纳域名运行费用。域名注册管理机构应当制定具体的域名运行费用收费办法，并报信息产业部备案。

第三十一条 域名注册信息发生变更的，域名持有者应当在变更后三十日内向域名注册服务机构申请变更注册信息。

第三十二条 域名持有者可以选择和变更域名注册服务机构。域名持有者变更域名注册服务机构的，原域名注册服务机构应当承担转移域名持有者注册信息的义务。

无正当理由，域名注册服务机构不得阻止域名持有者变更域名注册服务机构。

第三十三条 域名注册管理机构应当设立用户投诉受理热线或采取其他必要措施，及时处理用户对域名注册服务机构提出的意见；难以及时处理的，必须向用户说明理由和相关处理时限。

对于向域名注册管理机构投诉没有处理结果或对处理结果不满意，或者对域名注册管理机构的服务不满意的，用户或域名注册服务机构可以向信息产业部提出申诉。

第三十四条 已注册的域名出现下外情形之一时，原域名注册服务机构应当予以注销，并以书面形式通知域名持有者：

- （一）域名持有者或其代理人申请注销域名的；
- （二）域名持有者提交的域名注册信息不真实、不准确、不完整的；
- （三）域名持有者未按照规定缴纳相应费用的；
- （四）依据人民法院、仲裁机构或域名争议解决机构作出的裁判，应当注销的；
- （五）违反相关法律、行政法规及本办法规定的。

第三十五条 域名注册管理机构和域名注册服务机构有义务配合国家主管部门开展网站检查工作，必要时按要求暂停或停止相关的域名解析服务。

第四章 域名争议

第三十六条 域名注册管理机构可以指定中立的域名争议解决机构解决域名争议。

第三十七条 任何人就已经注册或使用的域名向域名争议解决机构提出投诉，并且符合域名争议解决办法规定的条件的，域名持有者应当参与域名争议解决程序。

第三十八条 域名争议解决机构作出的裁决只涉及争议域名持有者信息的变更。

域名争议解决机构作出的裁决与人民法院或者仲裁机构已经发生法律效力的裁判不一致的，域名争议解决机构的裁决服从于人民法院或者仲裁机构发生法律效力的裁判。

第三十九条 域名争议在人民法院、仲裁机构或域名争议解决机构处理期间域名持有者不得转让有争议的域名，但域名受让方以书面形式同意接受人民法院裁判、仲裁裁决或争议解决机构裁决约束的除外。

第五章 罚则

第四十条 违反本办法第八条、第十一条的规定，未经行政许可擅自设置域名根服务器或者设立域名根服务器运行机构、擅自设立域名注册管理机构和域名注册服务机构的，信息产业部应当根据《中华人民共和国行政许可法》第八十一条的规定，采取措施制止其开展业务或者提供服务，并视情节轻重，予以警告或处三万元以下罚款。

第四十一条 域名注册服务机构超出批准的项目范围提供域名注册服务的，由信息产业部责令限期改正；逾期不改正的，信息产业部应当根据《中华人民共和国行政许可法》第八十一条的规定，采取措施制止其提供超范围的服务，并视情节轻重，予以警告或处三万元以下罚款。

第四十二条 违反本办法第五条、第十八条、第十九条、第二十条、第二十五条、第二十六条、第三十二条、第三十五条规定的，由信息产业部责令限期改正，并视情节轻重，予以警告或处三万元以下罚款。

第四十三条 违反本办法第二十七条的规定，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由国家有关机关依照有关法律、行政法规的规定予以处罚。

第六章 附则

第四十四条 在本办法施行前已经开展互联网域名注册服务的域名注册管理机构和域名注册服务机构，应当自本办法施行之日起六十日内，到信息产业部办理登记手续。

第四十五条 本办法自2004年12月20日起施行。2002年8月1日公布的《中国互联网络域名管理办法》（信息产业部令第24号）同时废止。

《关于进一步做好互联网信息服务电子公告服务审批管理工作的通知》

关于进一步做好互联网信息服务电子公告服务审批管理工作的通知

信息产业部关于进一步做好互联网信息服务电子公告服务审批管理工作的通知

（2001年3月7日发布）

各省、自治区、直辖市通信管理局：

根据《互联网信息服务管理办法》，按照《互联网电子公告服务管理规定》以及《关于<互联网信息服务管理办法有关问题的通知>（信电〔2000〕208号）的有关规定，各地通信管理局正在认真贯彻落实对互联网信息服务业务（以下简称ICP）核发经营许可证和备案工作，同时对其中电子公告服务（以下简称BBS）实行专项审批。随着此项工作的深入开展，各地均遇到了一些新情况、新问题。为了进一步做好发证备案和BBS专项审批工作，促进上述业务健康有序地发展，现将有关事项进一步明确如下：

一、严格审批管理BBS

B B S 的专项审批是整个审批工作的重点。申请开办 B B S 除应符合《互联网信息服务管理办法》有关规定外，还要具备《互联网电子公告服务管理规定》第六条各项条件，同时应建立下述各项制度，未建立如下制度或未严格执行的不予批准 B B S，已开展 B B S 的勒令取缔。

（一）栏目明确制度。网站在提出 B B S 专项申请时，应明确列出拟开办的 B B S 的各具体栏目和类别，如时事论坛、网民聊天室、文化艺术类留言板、I T 行业布告板、新闻跟贴等，所有申请开办的项目应逐项列出。各局审批时按上报栏目逐项审查，批准的栏目予以载明。网站开办 B B S 时应严格按批准的栏目进行，不得超越范围随意开放，对已开设 B B S 的应进行清理和规范。

（二）版主负责制度。网站开办 B B S 时应有相应人员对 B B S 实施有效管理。获准开展 B B S 的网站必须对获得批准的各个 B B S 栏目指定专职人员充当版主，每个栏目不得少于一个专职版主，并实行版主责任制。版主负责监管该栏目的信息内容，除采取必要的技术手段外，应对登载的信息负有人工过滤、筛选和监控的责任。一旦发现 B B S 的栏目中有违规内容，有关主管部门将追究网站和该栏目版主的责任并予以处理。

版主的有关个人资料应报受理其专项审批的通信管理局备案。

（三）用户登记制度。提供 B B S 的网站应要求上网用户使用 B B S 前预先履行用户登记程序，填写网站提供的注册表格，提供真实、准确、最新的个人信息（包括姓名、电话、身份证号）。注册表格由网站妥善保存并不得随意泄漏，用户注册后则可使用该网站提供的所有 B B S 栏目和相关服务。一旦发现用户违反规定或提供虚假信息，网站有权暂停或中止该用户使用本网站包括 B B S 在内的所有或部分服务。

网站应采用相应技术手段保证本制度的有效实施。

（四）规则张贴制度

1．严格要求开办 B B S 的网站在留言板、论坛、聊天室、跟贴等 B B S 网页的显著位置张贴 I C P 经营许可证号或备案号。点击经营许可证号或备案号，应弹出该许可证或备案表的清晰可认的扫描图片。

2．上网使用者点击 B B S 某一栏目时，应首先弹出载有电子公告服务规则的页面，该页面内容旨在对使用者的行为作出符合法律规章和政府要求的警示和限定，其中包括 2 0 0 0 年 1 2 月 2 8 日第九届全国人大常委会第十九次会议通过的《全国人民代表大会常务委员会关于维护互联网安全的决定》有关条款。

（五）安全保障制度。开展 B B S 的网点，对 B B S 用户发出的信息应预先进行软件自动过滤和人工过滤，然后供人浏览，不得未经审查直接上网公开。

（六）网站从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，需经有关主管部门审核同意。对未提供有关主管部门的前置审批批准材料的网站，各通信管理局不批准其开办涉及上述内容的 B B S 栏目。

二、建立对所批准 B B S 的监督管理制度

（一）工作责任制。各通信管理局应指定专人着重加强对信息内容多、浏览量大、影响广的重点网站上经营行为和 B B S 信息内容的监管，可采取定期或不定期抽样浏览或轮流浏览的方式加强审查。

（二）工作联系制度。各通信管理局应与重点网站建立定期例会制度，有针对性地对较突出的问题进行通气，对网上尤其是 B B S 上出现的违规现象进行通报，加强对网站的监管，发现重大问题及时向部报告。同时要求重点网站加强自律，指定专人负责网上信息内容的监管，并成立联络小组，以确保管理部门随时能与网站取得联系并及时处理网上出现的违法行为。

（三）建立处罚制度。各通信管理局对发现 B B S 内容违反规定的网站，应按有关规定给予处罚，并以适当形式向社会披露。

三、妥善处理审批工作中的具体问题

（一）关于外资参股经营 I C P 问题

根据我国现行政策，目前外资不允许经营包括 I C P 在内的电信业务。涉及外资的网站申办经营许可证时，应要求该网站先进行外资股份的剥离，待完成外资剥离后，方可受理。对未进行外资剥离的，各通信管理局可按实际情况规定完成外资剥离工作的期限，逾期按有关规定进行处理。

外资股份的剥离符合以下两种情况可视为完成剥离：

1、网站所有外资股撤资或全部转让给中资；

2、另成立一个纯中资公司，与网站的 I C P 业务有关的资产、人员、域名、商标、经营权、用户关系等均通过协议有偿或无偿转让给纯中资公司，由中资公司独立自主经营 I C P。有外资的原公司不再经营网站，但可以将中资公司视为用户与其进行技术服务等商业合作。

（二）相关前置审批工作问题

鉴于《互联网信息服务管理办法》规定的前置审批涉及到的部分相关主管部门有关规定出台滞后，目前部分前置审批工作尚未启动。因此可先对网站的已通过前置审批的业务和非前置审批业务办理发证和备案；对需前置审批而暂未办理前置审批的信息内容暂停网上发布，待相关主管部门前置审批工作启动后及时补办前置审批手续。对这部分暂停业务经过补办前置审批手续后，获批准的信息内容可予以发证或备案并恢复上网发布，未获批准的信息内容将予以取缔。相关前置审批的管理办法由对应的国务院主管部门负责制度实施，其前置审批的程序、受理机构等有关问题的解释以及信息内容的界定均由对应的主管部门负责。

（三）经营性 I C P 和非经营性 I C P 的区别

经营性 I C P，是指通过互联网，向上网用户提供信息内容或者利用网站向用户提供某种在线应用，从而获得收入的活动。经营性 I C P 目前提供的网上信息大都是免费游览的，收费项目主要是网上广告、代制作网页、服务器内存空间出租、有偿提供特定信息内容、电子商务及其它网上应用服务，经营性 I C P 是以盈利为目的的商务活动。

非经营性 I C P，是指通过互联网向用户无偿提供具有公开性、共享性信息服务的活动。非经营性网站主要是各级政府部门的网站、新闻机构的电子版报刊，企业、事业单位、教育科研机构的各类公益性网站和对本单位产品或业务作自我宣传的网站，不向上网用户收费，也不利用互联网站直接进行以盈利为目的的商业活动，但对一些特定服务可能收取一些成本费或象征性收费。

（四）现有网站补办手续的申报时限问题

网站补办审批手续的最后申报期限由各通信管理局视当地实际情况而定，最迟不得超过 2001 年 7 月 1 日清理完毕。

（五）跨地区经营 I C P 的公司分支机构发证问题

各通信管理局在对跨地区、多设置网站经营 I C P 的公司发证时，若该公司在各地网站所在地设立了具有独立法人资格的分支机构，则应对分支机构分别审核发证；若没有分支机构或分支机构没有独立法人资格则不单独发证，要求使用与其上级机构同样的 I C P 许可证和编号，并通过其上级机构对其进行管理，同时该公司在办证时应对其各地此类网站作详细说明（包括各地镜像网站）。

（六）公司注册地和网站服务器所在地不一致问题

在网站办证和备案过程中，若公司注册地和网站服务器所在地不在同一个省级行政区域内，可主要以公司注册地为准办理发证或备案手续，同时到服务器所在地通信管理局进行备案；若服务器所在地设有具有法人资格的分支机构，则可以服务器所在地办理。服务器设在境外的境内网站，应办理备案手续，以便管理。

对此类网站的监管，应以注册所在地通信管理局为主，服务器所在地通信管理局应大力协助、主动合作。各相关通信管理局应加强沟通。

（七）代理网站、个人网站和个人主页问题

代理网站是指有独立的域名、网址和网页、自己不建立实际网站、由他人（I C P 运营商）代为制作网页并租用 I C P 运营商的服务器空间的单位；个人网站是指使用自己独有的域名、通过购买或租用服务器、以个人名义建立的网站；个人主页是指在他人网站页面上生成的个人专项或专栏，个人不拥有单独的域名和服务器。各通信管理局应对代理网站、个人网站实行备案制度，对个人主页无需办证或备案，而是作为 I C P 运营商的用户、通过 I C P 运营商对其进行管理。

（八）I S P 运营商同时经营 I C P 的问题

对 I S P 运营商同时从事 I C P，可根据其网站内容，分为经营性 I C P 和非经营性 I C P，分别予以办证和备案。

《互联网新闻信息服务管理规定》

《互联网新闻信息服务管理规定》

(国务院新闻办公室、信息产业部令第37号)

《互联网新闻信息服务管理规定》现予公布，自公布之日起施行。

新闻办主任 蔡武

信息产业部部长 王旭东

2005年9月25日

第一章 总则

第一条 为了规范互联网新闻信息服务，满足公众对互联网新闻信息的需求，维护国家安全和公共利益，保护互联网新闻信息服务单位的合法权益，促进互联网新闻信息服务健康、有序发展，制定本规定。

第二条 在中华人民共和国境内从事互联网新闻信息服务，应当遵守本规定。

本规定所称新闻信息，是指时政类新闻信息，包括有关政治、经济、军事、外交等社会公共事务的报道、评论，以及有关社会突发事件的报道、评论。

本规定所称互联网新闻信息服务，包括通过互联网登载新闻信息、提供时政类电子公告服务和向公众发送时政类通讯信息。

第三条 互联网新闻信息服务单位从事互联网新闻信息服务，应当遵守宪法、法律和法规，坚持为人民服务、为社会主义服务的方向，坚持正确的舆论导向，维护国家利益和公共利益。国家鼓励互联网新闻信息服务单位传播有益于提高民族素质、推动经济发展、促进社会进步的健康、文明的新闻信息。

第四条 国务院新闻办公室主管全国的互联网新闻信息服务监督管理工作。省、自治区、直辖市人民政府新闻办公室负责本行政区域内的互联网新闻信息服务监督管理工作。

第二章 互联网新闻信息服务单位的设立

第五条 互联网新闻信息服务单位分为以下三类：

(一) 新闻单位设立的登载超出本单位已刊登播发的新闻信息、提供时政类电子公告服务、向公众发送时政类通讯信息的互联网新闻信息服务单位；

(二) 非新闻单位设立的转载新闻信息、提供时政类电子公告服务、向公众发送时政类通讯信息的互联网新闻信息服务单位；

(三) 新闻单位设立的登载本单位已刊登播发的新闻信息的互联网新闻信息服务单位。

根据《国务院对确需保留的行政审批项目设定行政许可的决定》和有关行政法规，设立前款第(一)项、第(二)项规定的互联网新闻信息服务单位，应当经国务院新闻办公室审批。设立本条第一款第(三)项规定的互联网新闻信息服务单位，应当向国务院新闻办公室或者省、自治区、直辖市人民政府新闻办公室备案。

第六条 新闻单位与非新闻单位合作设立互联网新闻信息服务单位，新闻单位拥有的股权不低于51%的，视为新闻单位设立互联网新闻信息服务单位；新闻单位拥有的股权低于51%的，视为非新闻单位设立互联网新闻信息服务单位。

第七条 设立本规定第五条第一款第(一)项规定的互联网新闻信息服务单位，应当具备下列条件：

- (一) 有健全的互联网新闻信息服务管理规章制度；
- (二) 有5名以上在新闻单位从事新闻工作3年以上的专职新闻编辑人员；
- (三) 有必要的场所、设备和资金，资金来源应当合法。

可以申请设立前款规定的互联网新闻信息服务单位的机构，应当是中央新闻单位，省、自治区、直辖市直属新闻单位，以

及省、自治区人民政府所在地的市直属新闻单位。

审批设立本条第一款规定的互联网新闻信息服务单位，除应当依照本条规定条件外，还应当符合国务院新闻办公室关于互联网新闻信息服务行业发展的总量、结构、布局的要求。

第八条 设立本规定第五条第一款第（二）项规定的互联网新闻信息服务单位，除应当具备本规定第七条第一款第（一）项、第（三）项规定条件外，还应当有10名以上专职新闻编辑人员；其中，在新闻单位从事新闻工作3年以上的新闻编辑人员不少于5名。

可以申请设立前款规定的互联网新闻信息服务单位的组织，应当是依法设立2年以上的从事互联网信息服务的法人，并在最近2年内没有因违反有关互联网信息服务管理的法律、法规、规章的规定受到行政处罚；申请组织为企业法人的，注册资本应当不低于1000万元人民币。

审批设立本条第一款规定的互联网新闻信息服务单位，除应当依照本条规定条件外，还应当符合国务院新闻办公室关于互联网新闻信息服务行业发展的总量、结构、布局的要求。

第九条 任何组织不得设立中外合资经营、中外合作经营和外资经营的互联网新闻信息服务单位。

互联网新闻信息服务单位与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及互联网新闻信息服务业务的合作，应当报经国务院新闻办公室进行安全评估。

第十条 申请设立本规定第五条第一款第（一）项、第（二）项规定的互联网新闻信息服务单位，应当填写申请登记表，并提交下列材料：

- （一）互联网新闻信息服务管理规章制度；
- （二）场所的产权证明或者使用权证明和资金的来源、数额证明；
- （三）新闻编辑人员的从业资格证明。

申请设立本规定第五条第一款第（一）项规定的互联网新闻信息服务单位的机构，还应当提交新闻单位资质证明；申请设立本规定第五条第一款第（二）项规定的互联网新闻信息服务单位的组织，还应当提交法人资格证明。

第十一条 申请设立本规定第五条第一款第（一）项、第（二）项规定的互联网新闻信息服务单位，中央新闻单位应当向国务院新闻办公室提出申请；省、自治区、直辖市直属新闻单位和省、自治区人民政府所在地的市直属新闻单位以及非新闻单位应当通过所在地省、自治区、直辖市人民政府新闻办公室向国务院新闻办公室提出申请。

通过省、自治区、直辖市人民政府新闻办公室提出申请的，省、自治区、直辖市人民政府新闻办公室应当自收到申请之日起20日内进行实地检查，提出初审意见报国务院新闻办公室；国务院新闻办公室应当自收到初审意见之日起40日内作出决定。向国务院新闻办公室提出申请的，国务院新闻办公室应当自收到申请之日起40日内进行实地检查，作出决定。批准的，发给互联网新闻信息服务许可证；不批准的，应当书面通知申请人并说明理由。

第十二条 本规定第五条第一款第（三）项规定的互联网新闻信息服务单位，属于中央新闻单位设立的，应当自从事互联网新闻信息服务之日起1个月内向国务院新闻办公室备案；属于其他新闻单位设立的，应当自从事互联网新闻信息服务之日起1个月内向所在地省、自治区、直辖市人民政府新闻办公室备案。

办理备案时，应当填写备案登记表，并提交互联网新闻信息服务管理规章制度和新闻单位资质证明。

第十三条 互联网新闻信息服务单位依照本规定设立后，应当依照有关互联网信息服务管理的行政法规向电信主管部门办理有关手续。

第十四条 本规定第五条第一款第（一）项、第（二）项规定的互联网新闻信息服务单位变更名称、住所、法定代表人或者主要负责人、股权构成、服务项目、网站网址等事项的，应当向国务院新闻办公室申请换发互联网新闻信息服务许可证。根据电信管理的有关规定，需报电信主管部门批准或者需要电信主管部门办理许可证或者备案变更手续的，依照有关规定办理。

本规定第五条第一款第（三）项规定的互联网新闻信息服务单位变更名称、住所、法定代表人或者主要负责人、股权构成、网站网址等事项的，应当向原备案机关重新备案；但是，股权构成变更后，新闻单位拥有的股权低于51%的，应当依照本规定办理许可手续。根据电信管理的有关规定，需报电信主管部门批准或者需要电信主管部门办理许可证或者备案变更手续的，依照有关规定办理。

第三章 互联网新闻信息服务规范

第十五条 互联网新闻信息服务单位应当按照核定的服务项目提供互联网新闻信息服务。

第十六条 本规定第五条第一款第（一）项、第（二）项规定的互联网新闻信息服务单位，转载新闻信息或者向公众发送时政类通讯信息，应当转载、发送中央新闻单位或者省、自治区、直辖市直属新闻单位发布的新闻信息，并应当注明新闻信息来源，不得歪曲原新闻信息的内容。

本规定第五条第一款第（二）项规定的互联网新闻信息服务单位，不得登载自行采编的新闻信息。

第十七条 本规定第五条第一款第（一）项、第（二）项规定的互联网新闻信息服务单位转载新闻信息，应当与中央新闻单位或者省、自治区、直辖市直属新闻单位签订书面协议。中央新闻单位设立的互联网新闻信息服务单位，应当将协议副本报国务院新闻办公室备案；其他互联网新闻信息服务单位，应当将协议副本报所在地省、自治区、直辖市人民政府新闻办公室备案。

中央新闻单位或者省、自治区、直辖市直属新闻单位签订前款规定的协议，应当核验对方的互联网新闻信息服务许可证，不得向没有互联网新闻信息服务许可证的单位提供新闻信息。

第十八条 中央新闻单位与本规定第五条第一款第（二）项规定的互联网新闻信息服务单位开展除供稿之外的互联网新闻业务合作，应当在开展合作业务10日前向国务院新闻办公室报告；其他新闻单位与本规定第五条第一款第（二）项规定的互联网新闻信息服务单位开展除供稿之外的互联网新闻业务合作，应当在开展合作业务10日前向所在地省、自治区、直辖市人民政府新闻办公室报告。

第十九条 互联网新闻信息服务单位登载、发送的新闻信息或者提供的时政类电子公告服务，不得含有下列内容：

- （一）违反宪法确定的基本原则的；
- （二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- （三）损害国家荣誉和利益的；
- （四）煽动民族仇恨、民族歧视，破坏民族团结的；
- （五）破坏国家宗教政策，宣扬邪教和封建迷信的；
- （六）散布谣言，扰乱社会秩序，破坏社会稳定的；
- （七）散布淫秽、色情、赌博、暴力、恐怖或者教唆犯罪的；
- （八）侮辱或者诽谤他人，侵害他人合法权益的；
- （九）煽动非法集会、结社、游行、示威、聚众扰乱社会秩序的；
- （十）以非法民间组织名义活动的；
- （十一）含有法律、行政法规禁止的其他内容的。

第二十条 互联网新闻信息服务单位应当建立新闻信息内容管理责任制度。不得登载、发送含有违反本规定第三条第一款、第十九条规定内容的新闻信息；发现提供的时政类电子公告服务中含有违反本规定第三条第一款、第十九条规定内容的，应当立即删除，保存有关记录，并在有关部门依法查询时予以提供。

第二十一条 互联网新闻信息服务单位应当记录所登载、发送的新闻信息内容及其时间、互联网地址，记录备份应当至少保存60日，并在有关部门依法查询时予以提供。

第四章 监督管理

第二十二条 国务院新闻办公室和省、自治区、直辖市人民政府新闻办公室，依法对互联网新闻信息服务单位进行监督检查，有关单位、个人应当予以配合。

国务院新闻办公室和省、自治区、直辖市人民政府新闻办公室的工作人员依法进行实地检查时，应当出示执法证件。

第二十三条 国务院新闻办公室和省、自治区、直辖市人民政府新闻办公室，应当对互联网新闻信息服务进行监督；发现互联网新闻信息服务单位登载、发送的新闻信息或者提供的时政类电子公告服务中含有违反本规定第三条第一款、第十九条规

定内容的，应当通知其删除。互联网新闻信息服务单位应当立即删除，保存有关记录，并在有关部门依法查询时予以提供。

第二十四条 本规定第五条第一款第（一）项、第（二）项规定的互联网新闻信息服务单位，属于中央新闻单位设立的，应当每年在规定期限内向国务院新闻办公室提交年度业务报告；属于其他新闻单位或者非新闻单位设立的，应当每年在规定期限内通过所在地省、自治区、直辖市人民政府新闻办公室向国务院新闻办公室提交年度业务报告。国务院新闻办公室根据报告情况，可以对互联网新闻信息服务单位的管理制度、人员资质、服务内容等进行检查。

第二十五条 互联网新闻信息服务单位应当接受公众监督。

国务院新闻办公室应当公布举报网站网址、电话，接受公众举报并依法处理；属于其他部门职责范围的举报，应当移交有关部门处理。

第五章 法律责任

第二十六条 违反本规定第五条第二款规定，擅自从事互联网新闻信息服务，或者违反本规定第十五条规定，超出核定的服务项目从事互联网新闻信息服务的，由国务院新闻办公室或者省、自治区、直辖市人民政府新闻办公室依据各自职权责令停止违法活动，并处1万元以上3万元以下的罚款；情节严重的，由电信主管部门根据国务院新闻办公室或者省、自治区、直辖市人民政府新闻办公室的书面认定意见，按照有关互联网信息服务管理的行政法规的规定停止其互联网信息服务或者责令互联网接入服务者停止接入服务。

第二十七条 互联网新闻信息服务单位登载、发送的新闻信息含有本规定第十九条禁止内容，或者拒不履行删除义务的，由国务院新闻办公室或者省、自治区、直辖市人民政府新闻办公室给予警告，可以并处1万元以上3万元以下的罚款；情节严重的，由电信主管部门根据有关主管部门的书面认定意见，按照有关互联网信息服务管理的行政法规的规定停止其互联网信息服务或者责令互联网接入服务者停止接入服务。

互联网新闻信息服务单位登载、发送的新闻信息含有违反本规定第三条第一款规定内容的，由国务院新闻办公室或者省、自治区、直辖市人民政府新闻办公室依据各自职权依照前款规定的处罚种类、幅度予以处罚。

第二十八条 违反本规定第十六条规定，转载来源不合法的新闻信息、登载自行采编的新闻信息或者歪曲原新闻信息内容的，由国务院新闻办公室或者省、自治区、直辖市人民政府新闻办公室依据各自职权责令改正，给予警告，并处5000元以上3万元以下的罚款。违反本规定第十六条规定，未注明新闻信息来源的，由国务院新闻办公室或者省、自治区、直辖市人民政府新闻办公室依据各自职权责令改正，给予警告，可以并处5000元以上2万元以下的罚款。

第二十九条 违反本规定有下列行为之一的，由国务院新闻办公室或者省、自治区、直辖市人民政府新闻办公室依据各自职权责令改正，给予警告，可以并处3万元以下的罚款：

- （一）未履行备案义务的；
- （二）未履行报告义务的；
- （三）未履行记录、记录备份保存或者提供义务的。

第三十条 违反本规定第十七条第二款规定，向没有互联网新闻信息服务许可证的单位提供新闻信息的，对负有责任的主管人员和其他直接责任人员依法给予行政处分。

第三十一条 国务院新闻办公室和省、自治区、直辖市人民政府新闻办公室以及电信主管部门的工作人员，玩忽职守、滥用职权、徇私舞弊，造成严重后果，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，对负有责任的主管人员和其他直接责任人员依法给予行政处分。

第六章 附则

第三十二条 本规定所称新闻单位是指依法设立的报社、广播电台、电视台和通讯社；其中，中央新闻单位包括中央国家机关各部门设立的新闻单位。

第三十三条 本规定自公布之日起施行。

🔗 《互联网医疗保健信息服务管理办法》

《互联网医疗保健信息服务管理办法》

(中华人民共和国卫生部令第66号)

《互联网医疗保健信息服务管理办法》已于2009年3月25日经卫生部部务会议审议通过，现予以发布，自2009年7月1日起施行。

部 长 陈 竺

二〇〇九年五月一日

第一章 总则

第一条 为规范互联网医疗保健信息服务活动，保证互联网医疗保健信息科学、准确，促进互联网医疗保健信息服务健康发展，根据《互联网信息服务管理办法》，制定本办法。

第二条 在中华人民共和国境内从事互联网医疗保健信息服务活动，适用本办法。

本办法所称互联网医疗保健信息服务是指通过开办医疗卫生机构网站、预防保健知识网站或者在综合网站设立预防保健类频道向上网用户提供医疗保健信息的服务活动。

开展远程医疗会诊咨询、视频医学教育等互联网信息服务的，按照卫生部相关规定执行。

第三条 互联网医疗保健信息服务分为经营性和非经营性两类。

经营性互联网医疗保健信息服务，是指向上网用户有偿提供医疗保健信息等服务的活动。

非经营性互联网医疗保健信息服务，是指向上网用户无偿提供公开、共享性医疗保健信息等服务的活动。

第四条 从事互联网医疗保健信息服务，在向通信管理部门申请经营许可或者履行备案手续前，应当经省、自治区、直辖市人民政府卫生行政部门、中医药管理部门审核同意。

第二章 设立

第五条 申请提供互联网医疗保健信息服务，应当具备下列条件：

- (一) 主办单位为依法设立的医疗卫生机构、从事预防保健服务的企事业单位或者其他社会组织；
- (二) 具有与提供的互联网医疗保健信息服务活动相适应的专业人员、设施及相关制度；
- (三) 网站或者频道有2名以上熟悉医疗卫生管理法律、法规和医疗卫生专业知识的技术人员；提供性知识宣传的，应当有1名副高级以上卫生专业技术职务任职资格的医师。

第六条 申请提供的互联网医疗保健信息服务中含有性心理、性伦理、性医学、性治疗等性科学研究内容的，除具备第五条规定条件外，还应当同时具备下列条件：

- (一) 主办单位必须是医疗卫生机构；
- (二) 具有仅向从事相关临床和科研工作的专业人员开放的相关网络技术措施。

第七条 申请提供互联网医疗保健信息服务的，应当按照属地管理原则，向主办单位所在地省、自治区、直辖市人民政府卫生行政部门、中医药管理部门提出申请，并提交下列材料：

- (一) 申请书和申请表。申请表内容主要包括：网站类别、服务性质（经营性或者非经营性）、内容分类（普通、性知识、性科研）、网站设置地点、预定开始提供服务日期、主办单位名称、机构性质、通信地址、邮政编码、负责人及其身份证号码、联系人、联系电话等；
- (二) 主办单位基本情况，包括机构法人证书或者企业法人营业执照；
- (三) 医疗卫生专业人员学历证明及资格证书、执业证书复印件，网站负责人身份证及简历；
- (四) 网站域名注册的相关证书证明文件；
- (五) 网站栏目设置说明；

- (六) 网站对历史发布信息进行备份和查阅的相关管理制度及执行情况说明；
- (七) 卫生行政部门、中医药管理部门在线浏览网站上所有栏目、内容的方法及操作说明；
- (八) 健全的网络与信息安全保障措施，包括网站安全保障措施、信息安全保密管理制度、用户信息安全管理；
- (九) 保证医疗保健信息来源科学、准确的管理措施、情况说明及相关证明。

第八条 从事互联网医疗卫生信息服务网站的中文名称，除与主办单位名称相同的以外，不得以“中国”、“中华”、“全国”等冠名。

第九条 省、自治区、直辖市人民政府卫生行政部门、中医药管理部门自受理之日起20日内，对申请提供互联网医疗保健信息服务的材料进行审核，并作出予以同意或不同意的审核意见。予以同意的，核发《互联网医疗保健信息服务审核同意书》，发布公告，并向卫生部、国家中医药管理局备案；不同意的，应当书面通知申请人并说明理由。

《互联网医疗保健信息服务审核同意书》格式由卫生部统一制定。

第十条 互联网医疗保健信息服务提供者变更下列事项之一的，应当向原发证机关申请办理变更手续，填写《互联网医疗保健信息服务项目变更申请表》，同时提供相关证明文件：

- (一) 《互联网医疗保健信息服务审核同意书》中审核同意的项目；
- (二) 互联网医疗保健信息服务主办单位的基本项目；
- (三) 提供互联网医疗保健信息服务的基本情况。

第十一条 《互联网医疗保健信息服务审核同意书》有效期2年。需要继续提供互联网医疗保健信息服务的，应当在有效届满前2个月内，向原审核机关申请复核。通过复核的，核发《互联网医疗保健信息服务复核同意书》。

第三章 医疗保健信息服务

第十二条 互联网医疗保健信息服务内容必须科学、准确，必须符合国家有关法律、法规和医疗保健信息管理的相关规定。

提供互联网医疗保健信息服务的网站应当对发布的全部信息包括所链接的信息负全部责任。

不得发布含有封建迷信、淫秽内容的信息；不得发布虚假信息；不得发布未经审批的医疗广告；不得从事网上诊断和治疗活动。

非医疗机构不得在互联网上储存和处理电子病历和健康档案信息。

第十三条 发布医疗广告，必须符合《医疗广告管理办法》的有关规定。应当注明医疗广告审查证明文号，并按照核准的广告成品样件内容登载。

不得夸大宣传，严禁刊登违法广告。

第十四条 开展性知识宣传，必须提供信息内容的来源，并在明显位置标明。信息内容要由医疗卫生专业人员审核把关，确保其科学、准确。

不得转载、摘编非法出版物的内容；不得以宣传性知识为名渲染性心理、性伦理、性医学、性治疗等性科学研究的内容；严禁传播淫秽内容。

第十五条 开展性科学研究的医疗保健网站，只能向从事相关临床和科研工作的专业人员开放。

严禁以开展性科学研究为名传播淫秽内容。综合性网站的预防保健类频道不得开展性科学研究内容服务。

第十六条 提供医疗保健信息服务的网站登载的新闻信息，应当符合《互联网新闻信息服务管理办法》的相关规定；登载的药品信息应当符合《互联网药品信息服务管理办法》的相关规定。

第十七条 提供互联网医疗保健信息服务，应当在其网站主页底部的显著位置标明卫生行政部门、中医药管理部门《互联网医疗保健信息服务审核同意书》或者《互联网医疗保健信息服务复核同意书》的编号。

第四章 监督管理

第十八条 卫生部、国家中医药管理局对各省、自治区、直辖市人民政府卫生行政部门、中医药管理部门的审核和日常监管工作进行指导和管理。

省、自治区、直辖市人民政府卫生行政部门、中医药管理部门依法负责对本行政区域内主办单位提供的医疗保健信息服务开展审核工作，对本行政区域的互联网医疗保健信息服务活动进行监督管理。

第十九条 各级卫生行政部门、中医药管理部门对下列内容进行日常监管：

- (一) 开办医疗机构类网站的，其医疗机构的真实性和合法性；
- (二) 提供性知识宣传和普通医疗保健信息服务的，是否取得互联网医疗保健信息服务资格，是否超范围提供服务；
- (三) 提供性科学研究信息服务的，其主办单位是否具备相应资质，是否违规向非专业人士开放；
- (四) 是否利用性知识宣传和性科学研究的名义传播淫秽内容，是否刊载违法广告和禁载广告。

第二十条 卫生行政部门、中医药管理部门设立投诉举报电话和电子信箱，接受上网用户对互联网医疗保健信息服务的投诉举报。

第二十一条 卫生行政部门、中医药管理部门对上网用户投诉举报和日常监督管理中发现的问题，要及时通知互联网医疗保健信息服务提供者予以改正；对超范围提供互联网医疗保健信息服务的，应责令其停止提供。

第二十二条 互联网医疗保健信息服务审核和监督管理情况应当向社会公告。

第五章 法律责任

第二十三条 未经过卫生行政部门、中医药管理部门审核同意从事互联网医疗保健信息服务的，由省级以上人民政府卫生行政部门、中医药管理部门通报同级通信管理部门，依法予以查处；情节严重的，依照有关法律法规给予处罚。

第二十四条 已通过卫生行政部门、中医药管理部门审核或者复核同意从事互联网医疗保健信息服务的，违反本办法，有下列情形之一的，由省、自治区、直辖市人民政府卫生行政部门、中医药管理部门给予警告，责令其限期改正；情节严重的，对非经营性互联网医疗保健信息服务提供者处以3000元以上1万元以下罚款，对经营性互联网医疗保健信息服务提供者处以1万元以上3万元以下罚款；拒不改正的，提出监管处理意见，并移交通信管理部门依法处理；构成犯罪的，移交司法部门追究刑事责任：

- (一) 超出审核同意范围提供互联网医疗保健信息服务的；
- (二) 超出有效期使用《互联网医疗保健信息服务审核同意书》的；
- (三) 未在网站首页规定位置标明卫生行政部门、中医药管理部门审核或者复核同意书编号的；
- (四) 提供不科学、不准确医疗保健信息服务，并造成不良社会影响的；
- (五) 借开展性知识宣传和性科学研究为名传播淫秽内容的。

第二十五条 省、自治区、直辖市人民政府卫生行政部门、中医药管理部门违规对互联网医疗保健信息服务申请作出审核意见的，原审核机关应当撤销原批准的《互联网医疗保健信息服务审核同意书》；对主管人员和其他直接责任人员，由其所在单位上级机关依法给予处分。

第六章 附则

第二十六条 本办法自2009年7月1日起施行。2001年1月3日卫生部发布的《卫生部关于印发〈互联网医疗卫生信息服务办法〉的通知》（卫办发〔2001〕3号）同时废止。

🔗 《互联网视听节目服务管理规定》

《互联网视听节目服务管理规定》

(国家广播电影电视总局、信息产业部令第56号)

《互联网视听节目服务管理规定》经国家广播电影电视总局、中华人民共和国信息产业部审议通过，现予发布，自2008年1月31日起施行。

国家广播电影电视总局局长：王太华

中华人民共和国信息产业部部长：王旭东

二〇〇七年十二月二十日

第一条 为维护国家利益和公共利益，保护公众和互联网视听节目服务单位的合法权益，规范互联网视听节目服务秩序，促进健康有序发展，根据国家有关规定，制定本规定。

第二条 在中华人民共和国境内向公众提供互联网（含移动互联网，以下简称互联网）视听节目服务活动，适用本规定。

本规定所称互联网视听节目服务，是指制作、编辑、集成并通过互联网向公众提供视音频节目，以及为他人提供上载传播视听节目服务的活动。

第三条 国务院广播电影电视主管部门作为互联网视听节目服务的行业主管部门，负责对互联网视听节目服务实施监督管理，统筹互联网视听节目服务的产业发展、行业管理、内容建设和安全监管。国务院信息产业主管部门作为互联网行业主管部门，依据电信行业管理职责对互联网视听节目服务实施相应的监督管理。

地方人民政府广播电影电视主管部门和地方电信管理机构依据各自职责对本行政区域内的互联网视听节目服务单位及接入服务实施相应的监督管理。

第四条 互联网视听节目服务单位及其相关网络运营单位，是重要的网络文化建设力量，承担建设中国特色网络文化和维护网络文化信息安全的责任，应自觉遵守宪法、法律和行政法规，接受互联网视听节目服务行业主管部门和互联网行业主管部门的管理。

第五条 互联网视听节目服务单位组成的全国性社会团体，负责制定行业自律规范，倡导文明上网、文明办网，营造文明健康的网络环境，传播健康有益视听节目，抵制腐朽落后思想文化传播，并在国务院广播电影电视主管部门指导下开展活动。

第六条 发展互联网视听节目服务要有益于传播社会主义先进文化，推动社会全面进步和人的全面发展、促进社会和谐。从事互联网视听节目服务，应当坚持为人民服务、为社会主义服务，坚持正确导向，把社会效益放在首位，建设社会主义核心价值观体系，遵守社会主义道德规范，大力弘扬体现时代发展和社会进步的思想文化，大力弘扬民族优秀传统文化传统，提供更多更好的互联网视听节目服务，满足人民群众日益增长的需求，不断丰富人民群众的精神文化生活，充分发挥文化滋润心灵、陶冶情操、愉悦身心的作用，为青少年成长创造良好的网上空间，形成共建共享的精神家园。

第七条 从事互联网视听节目服务，应当依照本规定取得广播电影电视主管部门颁发的《信息网络传播视听节目许可证》（以下简称《许可证》）或履行备案手续。

未按照本规定取得广播电影电视主管部门颁发的《许可证》或履行备案手续，任何单位和个人不得从事互联网视听节目服务。

互联网视听节目服务业务指导目录由国务院广播电影电视主管部门商国务院信息产业主管部门制定。

第八条 申请从事互联网视听节目服务的，应当同时具备以下条件：

- （一）具备法人资格，为国有独资或国有控股单位，且在申请之日前三年内无违法违规记录；
- （二）有健全的节目安全传播管理制度和安全保护技术措施；
- （三）有与其业务相适应并符合国家规定的视听节目资源；
- （四）有与其业务相适应的技术能力、网络资源和资金，且资金来源合法；
- （五）有与其业务相适应的专业人员，且主要出资者和经营者在申请之日前三年内无违法违规记录；
- （六）技术方案符合国家标准、行业标准和技术规范；
- （七）符合国务院广播电影电视主管部门确定的互联网视听节目服务总体规划、布局和业务指导目录；

(八) 符合法律、行政法规和国家有关规定的条件。

第九条 从事广播电台、电视台形态服务和时政类视听新闻服务的，除符合本规定第八条规定外，还应当持有广播电视播出机构许可证或互联网新闻信息服务许可证。其中，以自办频道方式播放视听节目的，由地（市）级以上广播电台、电视台、中央新闻单位提出申请。

从事主持、访谈、报道类视听服务的，除符合本规定第八条规定外，还应当持有广播电视节目制作经营许可证和互联网新闻信息服务许可证；从事自办网络剧（片）类服务的，还应当持有广播电视节目制作经营许可证。

未经批准，任何组织和个人不得在互联网上使用广播电视专有名称开展业务。

第十条 申请《许可证》，应当通过省、自治区、直辖市人民政府广播电影电视主管部门向国务院广播电影电视主管部门提出申请，中央直属单位可以直接向国务院广播电影电视主管部门提出申请。

省、自治区、直辖市人民政府广播电影电视主管部门应当提供便捷的服务，自收到申请之日起20日内提出初审意见，报国务院广播电影电视主管部门审批；国务院广播电影电视主管部门应当自收到申请或者初审意见之日起40日内作出许可或者不予许可的决定，其中专家评审时间为20日。予以许可的，向申请人颁发《许可证》，并向社会公告；不予许可的，应当书面通知申请人并说明理由。《许可证》应当载明互联网视听节目服务的播出标识、名称、服务类别等事项。

《许可证》有效期为3年。有效期届满，需继续从事互联网视听节目服务的，应于有效期届满前30日内，持符合本办法第八条规定条件的相关材料，向原发证机关申请办理续办手续。

地（市）级以上广播电台、电视台从事互联网视听节目转播类服务的，到省级以上广播电影电视主管部门履行备案手续。中央新闻单位从事互联网视听节目转播类服务的，到国务院广播电影电视主管部门履行备案手续。备案单位应在节目开播30日前，提交网址、网站名、拟转播的广播电视频道、栏目名称等有关备案材料，广播电影电视主管部门应将备案情况向社会公告。

第十一条 取得《许可证》的单位，应当依据《互联网信息服务管理办法》，向省（自治区、直辖市）电信管理机构或国务院信息产业主管部门（以下简称电信主管部门）申请办理电信业务经营许可或者履行相关备案手续，并依法到工商行政管理部门办理注册登记或变更登记手续。电信主管部门应根据广播电影电视主管部门许可，严格互联网视听节目服务单位的域名和IP地址管理。

第十二条 互联网视听节目服务单位变更注册资本、股东、股权结构，有重大资产变动或有上市等重大融资行为的，以及业务项目超出《许可证》载明范围的，应按本规定办理审批手续。互联网视听节目服务单位的办公场所、法定代表人以及互联网信息服务单位的网址、网站名依法变更的，应当在变更后15日内向省级以上广播电影电视主管部门和电信主管部门备案，变更事项涉及工商登记的，应当依法到工商行政管理部门办理变更登记手续。

第十三条 互联网视听节目服务单位应当在取得《许可证》90日内提供互联网视听节目服务。未按期提供服务的，其《许可证》由原发证机关予以注销。如因特殊原因，应经发证机关同意。申请终止服务的，应提前60日向原发证机关申报，其《许可证》由原发证机关予以注销。连续停止业务超过60日的，由原发证机关按终止业务处理，其《许可证》由原发证机关予以注销。

第十四条 互联网视听节目服务单位应当按照《许可证》载明或备案的事项开展互联网视听节目服务，并在播出界面显著位置标注国务院广播电影电视主管部门批准的播出标识、名称、《许可证》或备案编号。

任何单位不得向未持有《许可证》或备案的单位提供与互联网视听节目服务有关的代收费及信号传输、服务器托管等金融和技术服务。

第十五条 鼓励国有战略投资者投资互联网视听节目服务企业；鼓励互联网视听节目服务单位积极开发适应新一代互联网和移动通信特点的新业务，为移动多媒体、多媒体网站生产积极健康的视听节目，努力提高互联网视听节目的供给能力；鼓励影视生产基地、电视节目制作单位多生产适合在网上传播的影视剧（片）、娱乐节目，积极发展民族网络影视产业；鼓励互联网视听节目服务单位传播公益性视听节目。

互联网视听节目服务单位应当遵守著作权法律、行政法规的规定，采取版权保护措施，保护著作权人的合法权益。

第十六条 互联网视听节目服务单位提供的、网络运营单位接入的视听节目应当符合法律、行政法规、部门规章的规定。已播出的视听节目应至少完整保留60日。视听节目不得含有以下内容：

- (一) 反对宪法确定的基本原则的；
- (二) 危害国家统一、主权和领土完整的；
- (三) 泄露国家秘密、危害国家安全或者损害国家荣誉和利益的；
- (四) 煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的；
- (五) 宣扬邪教、迷信的；
- (六) 扰乱社会秩序，破坏社会稳定的；
- (七) 诱导未成年人违法犯罪和渲染暴力、色情、赌博、恐怖活动的；
- (八) 侮辱或者诽谤他人，侵害公民个人隐私等他人合法权益的；
- (九) 危害社会公德，损害民族优秀文化传统的；
- (十) 有关法律、行政法规和国家规定禁止的其他内容。

第十七条 用于互联网视听节目服务的电影电视剧类节目和其它节目，应当符合国家有关广播电影电视节目的管理规定。互联网视听节目服务单位播出时政类视听新闻节目，应当是地（市）级以上广播电台、电视台制作、播出的节目和中央新闻单位网站登载的时政类视听新闻节目。

未持有《许可证》的单位不得为个人提供上载传播视听节目服务。互联网视听节目服务单位不得允许个人上载时政类视听新闻节目，在提供播客、视频分享等上载传播视听节目服务时，应当提示上载者不得上载违反本规定的视听节目。任何单位和个人不得转播、链接、聚合、集成非法的广播电视频道、视听节目网站的节目。

第十八条 广播电影电视主管部门发现互联网视听节目服务单位传播违反本规定的视听节目，应当采取必要措施予以制止。互联网视听节目服务单位对含有违反本规定内容的视听节目，应当立即删除，并保存有关记录，履行报告义务，落实有关主管部门的管理要求。

互联网视听节目服务单位主要出资者和经营者应对播出和上载的视听节目内容负责。

第十九条 互联网视听节目服务单位应当选择依法取得互联网接入服务电信业务经营许可证或广播电视节目传送业务经营许可证的网络运营单位提供服务；应当依法维护用户权利，履行对用户的承诺，对用户信息保密，不得进行虚假宣传或误导用户、做出对用户不公平不合理的规定、损害用户的合法权益；提供有偿服务时，应当以显著方式公布所提供服务的视听节目种类、范围、资费标准和时限，并告知用户中止或者取消互联网视听节目服务的条件和方式。

第二十条 网络运营单位提供互联网视听节目信号传输服务时，应当保障视听节目服务单位的合法权益，保证传输安全，不得擅自插播、截留视听节目信号；在提供服务前应当查验视听节目服务单位的《许可证》或备案证明材料，按照《许可证》载明事项或备案范围提供接入服务。

第二十一条 广播电影电视和电信主管部门应建立公众监督举报制度。公众有权举报视听节目服务单位的违法违规行为，有关主管部门应当及时处理，不得推诿。广播电影电视、电信等监督管理部门发现违反本规定的行为，不属于本部门职责的，应当移交有权处理的部门处理。

电信主管部门应当依照国家有关规定向广播电影电视主管部门提供必要的技术系统接口和网站数据查询资料。

第二十二条 广播电影电视主管部门依法对互联网视听节目服务单位进行实地检查，有关单位和个人应当予以配合。广播电影电视主管部门工作人员依法进行实地检查时应当主动出示有关证件。

第二十三条 违反本规定有下列行为之一的，由县级以上广播电影电视主管部门予以警告、责令改正，可并处3万元以下罚款；同时，可对其主要出资者和经营者予以警告，可并处2万元以下罚款：

- (一) 擅自在互联网上使用广播电视专有名称开展业务的；
- (二) 变更注册资本、股东、股权结构，或上市融资，或重大资产变动时，未办理审批手续的；
- (三) 未建立健全节目运营规范，未采取版权保护措施，或对传播有害内容未履行提示、删除、报告义务的；

- (四) 未在播出界面显著位置标注播出标识、名称、《许可证》和备案编号的；
- (五) 未履行保留节目记录、向主管部门如实提供查询义务的；
- (六) 向未持有《许可证》或备案的单位提供代收费及信号传输、服务器托管等与互联网视听节目服务有关的服务的；
- (七) 未履行查验义务，或向互联网视听节目服务单位提供其《许可证》或备案载明事项范围以外的接入服务的；
- (八) 进行虚假宣传或者误导用户的；
- (九) 未经用户同意，擅自泄露用户信息秘密的；
- (十) 互联网视听服务单位在同一年度内三次出现违规行为的；
- (十一) 拒绝、阻挠、拖延广播电影电视主管部门依法进行监督检查或者在监督检查过程中弄虚作假的；
- (十二) 以虚假证明、文件等手段骗取《许可证》的。

有本条第十二项行为的，发证机关应撤销其许可证。

第二十四条 擅自从事互联网视听节目服务的，由县级以上广播电影电视主管部门予以警告、责令改正，可并处3万元以下罚款；情节严重的，根据《广播电视管理条例》第四十七条的规定予以处罚。

传播的视听节目内容违反本规定的，由县级以上广播电影电视主管部门予以警告、责令改正，可并处3万元以下罚款；情节严重的，根据《广播电视管理条例》第四十九条的规定予以处罚。

未按照许可证载明或备案的事项从事互联网视听节目服务的或违规播出时政类视听新闻节目的，由县级以上广播电影电视主管部门予以警告、责令改正，可并处3万元以下罚款；情节严重的，根据《广播电视管理条例》第五十条之规定予以处罚。

转播、链接、聚合、集成非法的广播电视频道和视听节目网站内容的，擅自插播、截留视听节目信号的，由县级以上广播电影电视主管部门予以警告、责令改正，可并处3万元以下罚款；情节严重的，根据《广播电视管理条例》第五十一条之规定予以处罚。

第二十五条 对违反本规定的互联网视听节目服务单位，电信主管部门应根据广播电影电视主管部门的书面意见，按照电信管理和互联网管理的法律、行政法规的规定，关闭其网站，吊销其相应许可证或撤销备案，责令为其提供信号接入服务的网络运营单位停止接入；拒不执行停止接入服务决定，违反《电信条例》第五十七条规定的，由电信主管部门依据《电信条例》第七十八条的规定吊销其许可证。

违反治安管理规定，由公安机关依法予以处罚；构成犯罪的，由司法机关依法追究刑事责任。

第二十六条 广播电影电视、电信等主管部门不履行规定的职责，或滥用职权的，要依法给予有关责任人处分，构成犯罪的，由司法机关依法追究刑事责任。

第二十七条 互联网视听节目服务单位出现重大违法违规行为的，除按有关规定予以处罚外，其主要出资者和经营者自互联网视听节目服务单位受到处罚之日起5年内不得投资和从事互联网视听节目服务。

第二十八条 通过互联网提供音视频即时通讯服务，由国务院信息产业主管部门按照国家有关规定进行监督管理。

利用局域网络及利用互联网架设虚拟专网向公众提供网络视听节目服务，须向行业主管部门提出申请，由国务院信息产业主管部门前置审批，国务院广播电影电视主管部门审核批准，按照国家有关规定进行监督管理。

第二十九条 本规定自2008年1月31日起施行。此前发布的规定与本规定不一致之处，依本规定执行。

《教育网站和网校暂行管理办法》

《教育网站和网校暂行管理办法》

教育部关于印发《教育网站和网校暂行管理办法》的通知

(2000年7月5日 教技〔2000〕5号)

为进一步促进互联网上教育信息服务和现代远程教育健康、有序的发展，教育部制订了《教育网站和网校暂行管理办

法》，现印发你们，并自即日起施行。

第一条 为了促进互联网上教育信息服务和现代远程教育健康、有序的发展，规范从事现代远程教育和通过互联网进行教育信息服务的行为，根据国家有关法律法规，制定本暂行管理办法。

第二条 现代远程教育和教育信息服务是我国社会主义教育事业的重要组成部分，开展现代远程教育和教育信息服务必须遵循国家的教育方针。

第三条 教育网站是指通过收集、加工、存储教育信息等方式建立信息库或者同时建立网上教育平台与信息获取及搜索等工具，通过互联网服务提供单位（ISP）接入互联网或者教育电视台，向上网用户提供教学和其他有关教育公共信息服务的机构。

第四条 教育网校是指进行各级各类学历学位教育或者通过培训颁发各种证书的教育网站。

第五条 教育网站和网校凡利用卫星网络进行教育教学活动的，必须经由中国教育电视台上星。

第六条 教育网站和网校可涉及高等教育、基础教育、幼儿教育、师范教育、职业教育、成人教育、继续教育及其他种类教育和教育公共信息服务。

第七条 主管的教育行政部门按与面授教育管理对口的原则负责对教育网站和网校进行审批和管理，并报教育部信息化工作领导小组备案。

第八条 凡在中华人民共和国境内申报开办教育网站和网校，必须向主管教育行政部门申请，经审查批准后方可开办。已开办的教育网站和网校，如未经主管教育行政部门批准的，应及时补办申请、批准手续。未经主管教育行政部门批准，不得擅自开办教育网站和网校。

第九条 开办各类教育网站，必须具备下列基本条件：

- （一）具有必要的资金及资金来源的有效证明。
- （二）符合国家法律、法规及国家主管教育行政部门规定的其他条件。

第十条 开办教育网校，除符合本办法第九条规定的条件外，还必须是主管教育行政部门认可的、具有在中华人民共和国境内从事与所办网校相同类型教育活动资格的事业法人，或者是与该机构合作并由其提供质量保证的事业法人或者企业法人组织。

第十一条 申请开办教育网站和网校的机构（以下简称申办机构）应向主管教育行政部门提供下列材料：

- （一）开办（或确认）教育网站和网校的书面申请。包括：教育网站和网校的类别、网站和网校设置地点、辅导站设置地点（如果设置）、预定开始提供服务日期和申办机构性质、通信地址、邮政编码、负责人及其身份证号码、联系人、联系电话等。
- （二）本办法第十条所述基本条件证明。
- （三）申办机构概况。
- （四）由学校与企业合资开办教育网站和网校的，应该提供会计师事务所或者审计师事务所出具的资信证明或者验资报告。
- （五）由学校与企业合资开办教育网站和网校的，应提供申办机构的公司章程、股东协议书等文件。
- （六）信息安全保障措施。

第十二条 申请开办教育网校，还应提供开办教育网校的办学条件，包括教学大纲、教学管理手段、师资力量、招生对象和资信担保证明等资料。

第十三条 主管教育行政部门每年两次受理申办机构的申请材料。如发现申请材料不符合要求，应在10个工作日内文字通知申办机构限期补齐，逾期不补齐或者所补材料仍不符合要求者，视为放弃申请。主管教育行政部门经初步审查合格后正式受理申请，在正式受理之日起20个工作日内，做出是否批准的决定，并书面通知申办机构。

第十四条 已获准开办的教育网站和网校，如果开办者主体或者名称、地点等需要变更的，应在变更前20个工作日内向负责批准的原主管教育行政部门提出申请，由主管教育行政部门对新的承办主体进行资格审查，审查合格后方可办理变更报批手续。

第十五条 已获准开办的教育网站和网校应在其网络主页上标明已获主管教育行政部门批准的信息，包括批准的日期、文号等。

第十六条 凡获得批准开办的教育网站以企业形式申请境内外上市的，应事先征得教育部同意。

第十七条 已获准开办的教育网站和网校，由教育部信息化工作领导小组负责定期向社会公布。

第十八条 教育网站和网校应遵循国家有关法律、法规，不得在网络上制作、发布、传播下列信息内容：

- (一) 泄露国家秘密危害国家安全的；
- (二) 违反国家民族、宗教与教育政策的；
- (三) 宣扬封建迷信、邪教、黄色淫秽制品、违反社会公德以及赌博和教唆犯罪等；
- (四) 煽动暴力；
- (五) 散布谣言、扰乱社会秩序、鼓动聚众滋事；
- (六) 暴露个人隐私和攻击他人与损害他人合法权益；
- (七) 损害社会公共利益；
- (八) 计算机病毒；
- (九) 法律和法规禁止的其他有害信息。

如发现上述有害信息内容，应及时向有关主管部门报告，并采取有效措施制止其扩散。

第十九条 凡国家法律、法规规定面向社会公开的公益信息，任何教育网站和网校不得进行有偿服务。

第二十条 未经教育部批准，教育网站和网校不得冠以“中国”字样。凡冠以政府职能部门名称的教育网站，均不得从事经营活动。

第二十一条 违反本办法第八条、第十八条、第十九条、第二十条，主管教育行政部门应根据有关行政法规的规定，视情节轻重予以警告、通报批评、取消教育网站和网校开办资格等处罚，情节严重的，依法追究法律责任。

第二十二条 境外机构在中华人民共和国境内参与教育网校建设的，根据中外合作办学的有关规定并参照本办法执行。

第二十三条 有关教育网站和网校收费标准与办法，由开办机构提出申请，所在地的教育行政部门商物价管理部门确定；对跨省区办学单位的收费，由开办机构商所服务区域的物价主管部门确定。

第二十四条 凡现有规定与本办法不符的，以本办法为准。

第二十五条 本办法由教育部负责解释。

第二十六条 本办法自发布之日起执行。

《互联网药品信息服务管理办法》

《互联网药品信息服务管理办法》

(国家食品药品监督管理局局令第9号)

《互联网药品信息服务管理办法》于2004年5月28日经国家食品药品监督管理局局务会议审议通过，现予公布。本规定自公布之日起施行。

局长：郑筱萸

二〇〇四年七月八日

第一条 为加强药品监督管理，规范互联网药品信息服务活动，保证互联网药品信息的真实、准确，根据《中华人民共和国药品管理法》、《互联网信息服务管理办法》，制定本办法。

第二条 在中华人民共和国境内提供互联网药品信息服务活动，适用本办法。

本办法所称互联网药品信息服务，是指通过互联网上网用户提供药品（含医疗器械）信息的服务活动。

第三条 互联网药品信息服务分为经营性和非经营性两类。

经营性互联网药品信息服务是指通过互联网上网用户有偿提供药品信息等服务的活动。

非经营性互联网药品信息服务是指通过互联网上网用户无偿提供公开的、共享性药品信息等服务的活动。

第四条 国家食品药品监督管理局对全国提供互联网药品信息服务活动的网站实施监督管理。

省、自治区、直辖市（食品）药品监督管理局对本行政区域内提供互联网药品信息服务活动的网站实施监督管理。

第五条 拟提供互联网药品信息服务的网站，应当在向国务院信息产业主管部门或者省级电信管理机构申请办理经营许可证或者办理备案手续之前，按照属地监督管理的原则，向该网站主办单位所在地省、自治区、直辖市（食品）药品监督管理部门提出申请，经审核同意后取得提供互联网药品信息服务的资格。

第六条 各省、自治区、直辖市（食品）药品监督管理局对本辖区内申请提供互联网药品信息服务的互联网站进行审核，符合条件的核发《互联网药品信息服务资格证书》。

第七条 《互联网药品信息服务资格证书》的格式由国家食品药品监督管理局统一制定。

第八条 提供互联网药品信息服务的网站，应当在其网站主页显著位置标注《互联网药品信息服务资格证书》的证书编号。

第九条 提供互联网药品信息服务网站所登载的药品信息必须科学、准确，必须符合国家的法律、法规和国家有关药品、医疗器械管理的相关规定。

提供互联网药品信息服务的网站不得发布麻醉药品、精神药品、医疗用毒性药品、放射性药品、戒毒药品和医疗机构制剂的产品信息。

第十条 提供互联网药品信息服务的网站发布的药品（含医疗器械）广告，必须经过（食品）药品监督管理部门审查批准。

提供互联网药品信息服务的网站发布的药品（含医疗器械）广告要注明广告审查批准文号。

第十一条 申请提供互联网药品信息服务，除应当符合《互联网信息服务管理办法》规定的要求外，还应当具备下列条件：

（一）互联网药品信息服务的提供者应当为依法设立的企事业单位或者其它组织；

（二）具有与开展互联网药品信息服务活动相适应的专业人员、设施及相关制度；

（三）有两名以上熟悉药品、医疗器械管理法律、法规和药品、医疗器械专业知识，或者依法经资格认定的药学、医疗器械技术人员。

第十二条 提供互联网药品信息服务的申请应当以一个网站为基本单元。

第十三条 申请提供互联网药品信息服务，应当填写国家食品药品监督管理局统一制发的《互联网药品信息服务申请表》，向网站主办单位所在地省、自治区、直辖市（食品）药品监督管理部门提出申请，同时提交以下材料：

（一）企业营业执照复印件（新办企业提供工商行政管理部门出具的名义核准通知书及相关材料）；

（二）网站域名注册的相关证书或者证明文件。从事互联网药品信息服务网站的中文名称，除与主办单位名称相同的以外，不得以“中国”、“中华”、“全国”等冠名；除取得药品招标代理机构资格证书的单位开办的互联网站外，其它提供互联网药品信息服务的网站名称中不得出现“电子商务”、“药品招商”、“药品招标”等内容；

（三）网站栏目设置说明（申请经营性互联网药品信息服务的网站需提供收费栏目及收费方式的说明）；

- (四) 网站对历史发布信息进行备份和查阅的相关管理制度及执行情况说明；
- (五) (食品) 药品监督管理部门在线浏览网站上所有栏目、内容的方法及操作说明；
- (六) 药品及医疗器械相关专业技术人员学历证明或者其专业技术资格证书复印件、网站负责人身份证复印件及简历；
- (七) 健全的网络与信息安全保障措施，包括网站安全保障措施、信息安全保密管理制度、用户信息安全管理措施；
- (八) 保证药品信息来源合法、真实、安全的管理措施、情况说明及相关证明。

第十四条 省、自治区、直辖市(食品)药品监督管理部门在收到申请材料之日起5日内做出受理与否的决定，受理的，发给受理通知书；不受理的，书面通知申请人并说明理由，同时告知申请人享有依法申请行政复议或者提起行政诉讼的权利。

第十五条 对于申请材料不规范、不完整的，省、自治区、直辖市(食品)药品监督管理部门自申请之日起5日内一次告知申请人需要补正的全部内容；逾期不告知的，自收到材料之日起即为受理。

第十六条 省、自治区、直辖市(食品)药品监督管理部门自受理之日起20日内对申请提供互联网药品信息服务的材料进行审核，并作出同意或者不同意的决定。同意的，由省、自治区、直辖市(食品)药品监督管理部门核发《互联网药品信息服务资格证书》，同时报国家食品药品监督管理局备案并发布公告；不同意的，应当书面通知申请人并说明理由，同时告知申请人享有依法申请行政复议或者提起行政诉讼的权利。

国家食品药品监督管理局对各省、自治区、直辖市(食品)药品监督管理部门的审核工作进行监督。

第十七条 《互联网药品信息服务资格证书》有效期为5年。有效期届满，需要继续提供互联网药品信息服务的，持证单位应当在有效期届满前6个月向原发证机关申请换发《互联网药品信息服务资格证书》。原发证机关审核后，认为符合条件的，予以换发新证；认为不符合条件的，发给不予换发新证的通知并说明理由，原《互联网药品信息服务资格证书》由原发证机关收回并公告注销。

省、自治区、直辖市(食品)药品监督管理部门根据申请人的申请，应当在《互联网药品信息服务资格证书》有效期届满前作出是否准予其换证的决定。逾期未作出决定的，视为准予换证。

第十八条 《互联网药品信息服务资格证书》可以根据互联网药品信息服务提供者的书面申请，由原发证机关收回，原发证机关应当报国家食品药品监督管理局备案并发布公告。被收回《互联网药品信息服务资格证书》的网站不得从事互联网药品信息服务。

第十九条 互联网药品信息服务提供者变更下列事项之一的，应当向原发证机关申请办理变更手续，填写《互联网药品信息服务项目变更申请表》，同时提供下列相关证明文件：

- (一) 《互联网药品信息服务资格证书》中审核批准的项目(互联网药品信息服务提供者单位名称、网站名称、IP地址等)；
- (二) 互联网药品信息服务提供者的基本项目(地址、法定代表人、企业负责人等)；
- (三) 网站提供互联网药品信息服务的基本情况(服务方式、服务项目等)。

第二十条 省、自治区、直辖市(食品)药品监督管理部门自受理变更申请之日起20个工作日内作出是否同意变更的审核决定。同意变更的，将变更结果予以公告并报国家食品药品监督管理局备案；不同意变更的，以书面形式通知申请人并说明理由。

省、自治区、直辖市(食品)药品监督管理部门对申请人的申请进行审查时，应当公示审批过程和审批结果。申请人和利害关系人可以对直接关系其重大利益的事项提交书面意见进行陈述和申辩。依法应当听证的，按照法定程序举行听证。

第二十二条 未取得或者超出有效期使用《互联网药品信息服务资格证书》从事互联网药品信息服务的，由国家食品药品监督管理局或者省、自治区、直辖市(食品)药品监督管理部门给予警告，并责令其停止从事互联网药品信息服务；情节严重的，移送相关部门，依照有关法律、法规给予处罚。

第二十三条 提供互联网药品信息服务的网站不在其网站主页的显著位置标注《互联网药品信息服务资格证书》的证书编号的，国家食品药品监督管理局或者省、自治区、直辖市(食品)药品监督管理部门给予警告，责令限期改正；在限定期限内拒不改正的，对提供非经营性互联网药品信息服务的网站处以500元以下罚款，对提供经营性互联网药品信息服务的网站处以

5000元以上1万元以下罚款。

第二十四条 互联网药品信息服务提供者违反本办法，有下列情形之一的，由国家食品药品监督管理局或者省、自治区、直辖市（食品）药品监督管理部门给予警告，责令限期改正；情节严重的，对提供非经营性互联网药品信息服务的网站处以1000元以下罚款，对提供经营性互联网药品信息服务的网站处以1万元以上3万元以下罚款；构成犯罪的，移送司法部门追究刑事责任：

- （一）已经获得《互联网药品信息服务资格证书》，但提供的药品信息直接撮合药品网上交易的；
- （二）已经获得《互联网药品信息服务资格证书》，但超出审核同意的范围提供互联网药品信息服务的；
- （三）提供不真实互联网药品信息服务并造成不良社会影响的；
- （四）擅自变更互联网药品信息服务项目的。

第二十五条 互联网药品信息服务提供者在其业务活动中，违法使用《互联网药品信息服务资格证书》的，由国家食品药品监督管理局或者省、自治区、直辖市（食品）药品监督管理部门依照有关法律、法规的规定处罚。

第二十六条 省、自治区、直辖市（食品）药品监督管理部门违法对互联网药品信息服务申请作出审核批准的，原发证机关应当撤销原批准的《互联网药品信息服务资格证书》，由此给申请人的合法权益造成损害的，由原发证机关依照国家赔偿法的规定给予赔偿；对直接负责的主管人员和其他直接责任人员，由其所在单位或者上级机关依法给予行政处分。

第二十七条 省、自治区、直辖市（食品）药品监督管理部门应当对提供互联网药品信息服务的网站进行监督检查，并将检查情况向社会公告。

第二十八条 本办法由国家食品药品监督管理局负责解释。

第二十九条 本办法自公布之日起施行。国家药品监督管理局令第26号《互联网药品信息服务管理暂行规定》同时废止。

🔗 《互联网文化管理暂行规定》

《互联网文化管理暂行规定》

（文化部令第27号）

《互联网文化管理暂行规定》已经2011年2月11日文化部部务会议审议通过，现予发布，自2011年4月1日起施行。

部长 蔡 武

二〇一一年二月十七日

第一条 为了加强对互联网文化的管理，保障互联网文化单位的合法权益，促进我国互联网文化健康、有序地发展，根据《全国人民代表大会常务委员会关于维护互联网安全的决定》和《互联网信息服务管理办法》以及国家法律法规有关规定，制定本规定。

第二条 本规定所称互联网文化产品是指通过互联网生产、传播和流通的文化产品，主要包括：

（一）专门为互联网而生产的网络音乐娱乐、网络游戏、网络演出剧（节）目、网络表演、网络艺术品、网络动漫等互联网文化产品；

（二）将音乐娱乐、游戏、演出剧（节）目、表演、艺术品、动漫等文化产品以一定的技术手段制作、复制到互联网上传播的互联网文化产品。

第三条 本规定所称互联网文化活动是指提供互联网文化产品及其服务的活动，主要包括：

- （一）互联网文化产品的制作、复制、进口、发行、播放等活动；
- （二）将文化产品登载在互联网上，或者通过互联网、移动通信网等信息网络发送到计算机、固定电话机、移动电话机、电视机、游戏机等用户端以及网吧等互联网上网服务营业场所，供用户浏览、欣赏、使用或者下载的在线传播行为；
- （三）互联网文化产品的展览、比赛等活动。

互联网文化活动分为经营性和非经营性两类。经营性互联网文化活动是指以营利为目的，通过向上网用户收费或者以电子商务、广告、赞助等方式获取利益，提供互联网文化产品及其服务的活动。非经营性互联网文化活动是指不以营利为目的向上网用户提供互联网文化产品及其服务的活动。

第四条 本规定所称互联网文化单位，是指经文化行政部门和电信管理机构批准或者备案，从事互联网文化活动的互联网信息服务提供者。

在中华人民共和国境内从事互联网文化活动，适用本规定。

第五条 从事互联网文化活动应当遵守宪法和有关法律、法规，坚持为人民服务、为社会主义服务的方向，弘扬民族优秀文化，传播有益于提高公众文化素质、推动经济发展、促进社会进步的思想道德、科学技术和文化知识，丰富人民的精神生活。

第六条 文化部负责制定互联网文化发展与管理的方针、政策和规划，监督管理全国互联网文化活动。

省、自治区、直辖市人民政府文化行政部门对申请从事经营性互联网文化活动的单位进行审批，对从事非经营性互联网文化活动的单位进行备案。

县级以上人民政府文化行政部门负责本行政区域内互联网文化活动的监督管理工作。县级以上人民政府文化行政部门或者文化市场综合执法机构对从事互联网文化活动违反国家有关法规的行为实施处罚。

第七条 申请设立经营性互联网文化单位，应当符合《互联网信息服务管理办法》的有关规定，并具备以下条件：

- (一) 单位的名称、住所、组织机构和章程；
- (二) 确定的互联网文化活动范围；
- (三) 适应互联网文化活动需要并取得相应从业资格的8名以上业务管理人员和专业技术人员；
- (四) 适应互联网文化活动需要的设备、工作场所以及相应的经营管理技术措施；
- (五) 不低于100万元的注册资金，其中申请从事网络游戏经营活动的应当具备不低于1000万元的注册资金；
- (六) 符合法律、行政法规和国家有关规定的条件。

审批设立经营性互联网文化单位，除依照前款所列条件外，还应当符合互联网文化单位总量、结构和布局的规划。

第八条 申请设立经营性互联网文化单位，应当向所在地省、自治区、直辖市人民政府文化行政部门提出申请，由省、自治区、直辖市人民政府文化行政部门审核批准。

第九条 申请设立经营性互联网文化单位，应当提交下列文件：

- (一) 申请书；
- (二) 企业名称预先核准通知书或者营业执照和章程；
- (三) 资金来源、数额及其信用证明文件；
- (四) 法定代表人、主要负责人及主要经营管理人员、专业技术人员的资格证明和身份证明文件；
- (五) 工作场所使用权证明文件；
- (六) 业务发展报告；
- (七) 依法需要提交的其他文件。

对申请设立经营性互联网文化单位的，省、自治区、直辖市人民政府文化行政部门应当自受理申请之日起20日内做出批准或者不批准的决定。批准的，核发《网络文化经营许可证》，并向社会公告；不批准的，应当书面通知申请人并说明理由。

《网络文化经营许可证》有效期为3年。有效期届满，需继续从事经营的，应当于有效期届满30日前申请续办。

第十条 非经营性互联网文化单位，应当自设立之日起60日内向所在地省、自治区、直辖市人民政府文化行政部门备案，并提交下列文件：

- (一) 备案报告书；
- (二) 章程；
- (三) 资金来源、数额及其信用证明文件；
- (四) 法定代表人或者主要负责人、主要经营管理人员、专业技术人员的资格证明和身份证明文件；
- (五) 工作场所使用权证明文件；
- (六) 需要提交的其他文件。

第十一条 申请设立经营性互联网文化单位经批准后，应当持《网络文化经营许可证》，按照《互联网信息服务管理办法》的有关规定，到所在地电信管理机构或者国务院信息产业主管部门办理相关手续。

第十二条 互联网文化单位应当在其网站主页的显著位置标明文化行政部门颁发的《网络文化经营许可证》编号或者备案编号，标明国务院信息产业主管部门或者省、自治区、直辖市电信管理机构颁发的经营许可证编号或者备案编号。

第十三条 经营性互联网文化单位变更单位名称、网站名称、网站域名、法定代表人、注册地址、经营地址、注册资金、股权结构以及许可经营范围的，应当自变更之日起20日内到所在地省、自治区、直辖市人民政府文化行政部门办理变更手续。

非经营性互联网文化单位变更名称、地址、法定代表人或者主要负责人、业务范围的，应当自变更之日起60日内到所在地省、自治区、直辖市人民政府文化行政部门办理备案手续。

第十四条 经营性互联网文化单位终止互联网文化活动的，应当自终止之日起30日内到所在地省、自治区、直辖市人民政府文化行政部门办理注销手续。

经营性互联网文化单位自取得《网络文化经营许可证》并依法办理企业登记之日起满180日未开展互联网文化活动的，由原审核的省、自治区、直辖市人民政府文化行政部门注销《网络文化经营许可证》，同时通知相关省、自治区、直辖市电信管理机构。

非经营性互联网文化单位停止互联网文化活动的，由原备案的省、自治区、直辖市人民政府文化行政部门注销备案，同时通知相关省、自治区、直辖市电信管理机构。

第十五条 经营进口互联网文化产品的活动应当由取得文化行政部门核发的《网络文化经营许可证》的经营性互联网文化单位实施，进口互联网文化产品应当报文化部进行内容审查。

文化部应当自受理内容审查申请之日起20日内（不包括专家评审所需时间）做出批准或者不批准的决定。批准的，发给批准文件；不批准的，应当说明理由。

经批准的进口互联网文化产品应当在其显著位置标明文化部的批准文号，不得擅自变更产品名称或者增删内容。自批准之日起一年内未在国内经营的，进口单位应当报文化部备案并说明原因；决定终止进口的，文化部撤销其批准文号。

经营性互联网文化单位经营的国产互联网文化产品应当自正式经营起30日内报省级以上文化行政部门备案，并在其显著位置标明文化部备案编号，具体办法另行规定。

第十六条 互联网文化单位不得提供载有以下内容的文化产品：

- (一) 反对宪法确定的基本原则的；
- (二) 危害国家统一、主权和领土完整的；
- (三) 泄露国家秘密、危害国家安全或者损害国家荣誉和利益的；
- (四) 煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的；
- (五) 宣扬邪教、迷信的；
- (六) 散布谣言，扰乱社会秩序，破坏社会稳定的；
- (七) 宣扬淫秽、赌博、暴力或者教唆犯罪的；

(八) 侮辱或者诽谤他人，侵害他人合法权益的；

(九) 危害社会公德或者民族优秀传统文化的；

(十) 有法律、行政法规和国家规定禁止的其他内容的。

第十七条 互联网文化单位提供的文化产品，使公民、法人或者其他组织的合法权益受到侵害的，互联网文化单位应当依法承担民事责任。

第十八条 互联网文化单位应当建立自审制度，明确专门部门，配备专业人员负责互联网文化产品内容和活动的自查与管理，保障互联网文化产品内容和活动的合法性。

第十九条 互联网文化单位发现所提供的互联网文化产品含有本规定第十六条所列内容之一的，应当立即停止提供，保存有关记录，向所在地省、自治区、直辖市人民政府文化行政部门报告并抄报文化部。

第二十条 互联网文化单位应当记录备份所提供的文化产品内容及其时间、互联网地址或者域名；记录备份应当保存60日，并在国家有关部门依法查询时予以提供。

第二十一条 未经批准，擅自从事经营性互联网文化活动的，由县级以上人民政府文化行政部门或者文化市场综合执法机构依据《无照经营查处取缔办法》的规定予以查处。

第二十二条 非经营性互联网文化单位违反本规定第十条，逾期未办理备案手续的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令限期改正；拒不改正的，责令停止互联网文化活动，并处1000元以下罚款。

第二十三条 经营性互联网文化单位违反本规定第十二条的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令限期改正，并可根据情节轻重处10000元以下罚款。

非经营性互联网文化单位违反本规定第十二条的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令限期改正；拒不改正的，责令停止互联网文化活动，并处500元以下罚款。

第二十四条 经营性互联网文化单位违反本规定第十三条的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令改正，没收违法所得，并处10000元以上30000元以下罚款；情节严重的，责令停业整顿直至吊销《网络文化经营许可证》；构成犯罪的，依法追究刑事责任。

非经营性互联网文化单位违反本规定第十三条的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令限期改正；拒不改正的，责令停止互联网文化活动，并处1000元以下罚款。

第二十五条 经营性互联网文化单位违反本规定第十五条，经营进口互联网文化产品未在其显著位置标明文化部批准文号、经营国产互联网文化产品未在其显著位置标明文化部备案编号的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令改正，并可根据情节轻重处10000元以下罚款。

第二十六条 经营性互联网文化单位违反本规定第十五条，擅自变更进口互联网文化产品的名称或者增删内容的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令停止提供，没收违法所得，并处10000元以上30000元以下罚款；情节严重的，责令停业整顿直至吊销《网络文化经营许可证》；构成犯罪的，依法追究刑事责任。

第二十七条 经营性互联网文化单位违反本规定第十五条，经营国产互联网文化产品逾期未报文化行政部门备案的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令改正，并可根据情节轻重处20000元以下罚款。

第二十八条 经营性互联网文化单位提供含有本规定第十六条禁止内容的互联网文化产品，或者提供未经文化部批准进口的互联网文化产品的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令停止提供，没收违法所得，并处10000元以上30000元以下罚款；情节严重的，责令停业整顿直至吊销《网络文化经营许可证》；构成犯罪的，依法追究刑事责任。

非经营性互联网文化单位，提供含有本规定第十六条禁止内容的互联网文化产品，或者提供未经文化部批准进口的互联网文化产品的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令停止提供，处1000元以下罚款；构成犯罪的，依法追究刑事责任。

第二十九条 经营性互联网文化单位违反本规定第十八条的，由县级以上人民政府文化行政部门或者文化市场综合执法机构责令改正，并可根据情节轻重处20000元以下罚款。

第三十条 经营性互联网文化单位违反本规定第十九条的，由县级以上人民政府文化行政部门或者文化市场综合执法机构予以警告，责令限期改正，并处10000元以下罚款。

第三十一条 违反本规定第二十条的，由省、自治区、直辖市电信管理机构责令改正；情节严重的，由省、自治区、直辖市电信管理机构责令停业整顿或者责令暂时关闭网站。

第三十二条 本规定所称文化市场综合执法机构是指依照国家有关法律、法规和规章的规定，相对集中地行使文化领域行政处罚权以及相关监督检查权、行政强制权的行政执法机构。

第三十三条 文化行政部门或者文化市场综合执法机构查处违法经营活动，依照实施违法经营行为的企业注册地或者企业实际经营地进行管辖；企业注册地和实际经营地无法确定的，由从事违法经营活动网站的信息服务许可地或者备案地进行管辖；没有许可或者备案的，由该网站服务器所在地管辖；网站服务器设置在境外的，由违法行为发生地进行管辖。

第三十四条 本规定自2011年4月1日起施行。2003年5月10日发布、2004年7月1日修订的《互联网文化管理暂行规定》同时废止。

《互联网站管理工作细则》

《互联网站管理工作细则》

(信部电[2005]501号)

信息产业部关于发布《互联网站管理工作细则》的通告

(信部电[2005]501号)

各省、自治区、直辖市通信管理局，各互联网接入服务提供者、各互联网信息服务提供者、各IP地址备案单位、各域名注册服务机构：

为切实加强互联网站管理工作，规范、细化互联网行业管理流程，促进我国互联网全面、协调、可持续发展，根据国家有关法规，我部制定了《互联网站管理工作细则》，现予发布，请遵照执行。在执行中遇到问题，请及时反馈我部电信管理局。

中华人民共和国信息产业部

二〇〇五年十月二十五日

第一章 总则

第一条 为切实加强互联网站管理工作，建立互联网站管理工作长效机制，规范、细化互联网行业内部管理流程，不断提高互联网信息服务提供者（ICP）、互联网IP地址、互联网络域名等网站管理基础信息数据库的完整性、准确性，根据《互联网信息服务管理办法》、《中国互联网络域名管理办法》、《非经营性互联网信息服务管理办法》、《互联网IP地址备案管理办法》等有关规定，制定本细则。

第二条 互联网站管理工作坚持属地管理原则。按照“谁运营谁负责”、“谁接入谁负责”的要求，辅以相应的技术手段，做到政府管理、行业自律和社会监督相结合。

第三条 互联网站管理有关数据使用和发布应严格遵守国家和信息产业部有关保密规定。

第四条 本细则涉及的主体有：信息产业部、省（自治区、直辖市）通信管理局（以下简称“省通信管理局”）、互联网接入服务提供者（以下简称“接入提供者”）、互联网信息服务提供者（以下简称“网站主办者”）、IP地址备案单位、域名注册管理机构、域名注册服务机构等。

接入服务提供者是因特网接入服务业务经营者、因特网数据中心业务经营者以及以其他方式为网站提供接入服务的电信业务经营者的统称。

IP地址备案单位是指直接从亚太互联网络信息中心等具有IP地址管理权的国际机构获得IP地址的单位和具有分配IP地址供其它单位或个人使用行为的单位。

第二章 相关主体职责与义务

第五条 信息产业部对全国ICP、IP地址及域名信息备案管理工作及相关工作进行监督、指导及协调。

- (一) 根据互联网站管理工作的需要制定相关管理规定。
- (二) 指导、检查、督促省通信管理局开展互联网站管理工作。
- (三) 了解掌握备案管理工作中存在的问题和情况，组织研究解决。
- (四) 组织开展“信息产业部ICP、IP地址、域名信息备案管理系统”（以下简称“备案管理系统”）的优化、完善等工作。
- (五) 负责对跨地区经营性互联网信息服务提供者ICP备案信息进行录入、审核。
- (六) 对域名注册服务机构和相关IP地址备案单位的备案工作进行业务指导和监督检查。
- (七) 定期通报备案工作进展情况和及时通报未备案网站、备案信息真实性等备案信息的相关情况。
- (八) 协调部级前置审批部门、专项内容主管部门、公益性互联网站主管部门等相关部门开展互联网站管理工作。

第六条 省通信管理局具体负责本行政区ICP、IP地址信息备案管理，查处违法违规网站、监管互联网接入服务市场、对网站进行年度审核等工作。

- (一) 依法对ICP备案信息进行日常审核工作。
- (二) 指导监督本行政区接入提供者、网站主办者、IP地址备案单位的ICP和IP地址信息备案工作；加强对其制度建立、机构设置、数据库系统建设等日常工作的监督检查。
- (三) 依法采用多种手段切实加强对互联网接入服务市场的监管，将接入提供者对互联网站的管理情况纳入其经营许可证年检、行风评议等考核工作中。
- (四) 依法做好接入提供者、IP地址备案单位、网站主办者等违法违规行为的查处工作。
- (五) 负责本行政区互联网站年度审核工作。
- (六) 负责对本行政区经营性互联网信息服务提供者ICP备案信息进行录入、审核。
- (七) 协同本行政区前置审批部门、专项内容主管部门等相关部门开展互联网站管理工作。
- (八) 积极支持引导互联网协会、通信企业协会等社团组织配合做好网站管理工作。
- (九) 建立健全社会监督渠道，公布举报电话（传真）、电子信箱等举报方式，广泛听取并认真查处社会各界对网站未经备案擅自提供互联网信息服务、备案信息不真实、接入提供者违规提供接入服务等违法违规行为的举报。

第七条 接入提供者是为网站主办者提供互联网接入服务的主体。接入提供者应当按照“谁运营谁负责”、“谁接入谁负责”的要求，切实加强内部管理和对所接入互联网站的管理。

- (一) 设立专岗专职，负责网站备案、规范网站行为及相关管理工作，专岗专职名单报省通信管理局备案。人员发生变动时要做好工作交接，变化后人员名单及时报省通信管理局备案。
- (二) 按照“先备案后接入”的要求制定完善接入服务流程，建立健全为用户代为备案信息的事前核验制度、对用户行为的事中监督制度、配合对违法违规网站的事后查处制度、网络与信息安全责任制等工作制度。
- (三) 应记录网站主办者的备案信息，对所接入网站主办者的备案信息进行动态核实，保证备案信息的真实、准确。
- (四) 接入提供者要杜绝为未备案的网站主办者提供接入服务，实时搜索已接入的未备案网站信息，及时停止并督促网站主办者履行备案手续。
- (五) 受网站主办者的委托应依法为网站主办单位履行备案、备案变更、备案注销等手续。代为备案时，用户名、密码和系统提示信息要及时移交网站主办者，并指导、督促网站主办者下载安装电子证书。不得在已知或应知互联网站主办者备案信息不真实或不准确的情况下，为其代为履行备案、备案变更、备案注销手续。
- (六) 对直接接入及间接接入的网站客户负有管理责任。

(七) 应建设必要的业务管理系统，满足行业主管部门对网站管理的要求。

(八) 做好用户记录留存、有害信息报告等网络信息安全管理工作的。

(九) 配合省通信管理局开展互联网站年度审核工作。

(十) 配合省通信管理局对违法违规网站依法进行查处。

(十一) 自觉接受省通信管理局的监督管理。

第八条 网站主办者应依法开展互联网信息服务业务。

(一) 应当自行或委托接入提供者履行备案、备案变更、备案注销手续。

(二) 应当保证备案信息内容的真实准确。

(三) 在通过备案审核后，应当在网站开通时在主页底部中央位置标明备案编号，在备案编号下方链接信息产业部“备案管理系统”网址，按要求将电子验证标识放置在其网站指定目录下。

(四) 备案信息发生变化时应及时进行变更，同时再次安装电子证书。

(五) 涉及前置审批及电子公告服务的，应在取得前置审批部门和专项审批部门批准并办理相关备案手续后方可提供相关内容信息。

(六) 网站主办者应妥善保管用户名和密码，用户名和密码丢失的，应提交书面申请，省通信管理局经确认后予以补发。

(七) 按照省通信管理局和相关内容主管部门的要求做好年度审核工作。

(八) 应当自觉接受互联网行业主管部门的监督管理。

第九条 IP地址备案单位具体承担IP地址信息报备工作。

(一) IP地址备案单位应当按要求通过“备案管理系统”报备IP地址信息。其中，基础电信运营公司IP地址信息的报备由总部和省级公司共同完成，基础电信运营公司总部应对其省级公司的IP地址信息报备工作进行指导和监督。公益性互联网络的管理单位负责统一完成其网络上使用的所有IP地址信息的报备。跨省经营因特网接入服务业务提供者IP地址信息的报备由其开展业务所在地的所有分支机构共同完成。

(二) IP地址备案单位应当确保其所报备的IP地址信息完整、准确。

(三) IP地址备案信息发生变化时，IP地址备案单位应按规定要求自变化之日起五个工作日内向“备案管理系统”提交变更后的IP地址信息。

(四) IP地址备案单位应当建立健全本单位的IP地址管理制度。

(五) 应当自觉接受互联网行业主管部门的监督管理。

第十条 中国互联网络信息中心和相关域名注册服务机构具体承担域名信息的报备工作。

(一) 中国互联网络信息中心和相关域名注册服务机构应当按要求通过“备案管理系统”报备域名信息。其中，中国互联网络信息中心负责报备所有CN和中文域名注册信息；相关域名注册服务机构负责报备所有境外域名注册信息。

(二) 中国互联网络信息中心和相关域名注册服务机构应当确保所报备的域名注册信息完整、准确。

(三) 域名注册信息、域名备案联系人等信息发生变化时，中国互联网络信息中心和相关域名注册服务机构应当自变化之日起五个工作日内向“备案管理系统”提交变更后的域名报备信息。

第三章 相关处理流程

第十一条 接入提供者为用户网站提供接入互联网络服务流程：

(一) 网站主办者向接入提供者提出接入申请。

(二) 接入提供者向网站主办者预分配IP地址。

(三) 网站主办者获得接入提供者预分配的IP地址后履行备案手续(网站主办者可自行备案也可由接入提供者代为备案)。

1、网站主办者自行备案的,网站主办者在收到“备案管理系统”反馈的备案编号后告知接入提供者备案成功,并将备案编号和备案信息一并提供给接入提供者,接入提供者登录“备案管理系统”核实该备案信息,在确认备案信息真实、准确的前提下为网站开通接入服务。如果发现备案信息不真实、不准确,不得开通接入服务,应当督促网站主办者核实相关信息,经备案后方可为其提供接入服务。

2、接入提供者代为履行备案的,接入提供者收到“备案管理系统”反馈的备案编号后即可为网站提供接入服务。

第十二条 网站主办者委托接入提供者代为履行ICP备案、备案变更的处理流程(见图一):

(一) 网站主办者将相关ICP备案信息提交给其接入提供者。

(二) 接入提供者对网站主办者提交的信息进行核实,在确认信息真实、准确的前提下将ICP备案信息导入“备案管理系统”;如存在不真实、不准确的信息,接入提供者要求网站主办者重新填报或补充相关信息。

(三) “备案管理系统”对接入提供者导入的信息进行自动核查,经识别没有发现问题的转相关省通信管理局;存在问题的,将相关意见反馈接入提供者。

(四) 相关省通信管理局对备案信息进行审核,符合备案条件的予以备案;不符合备案条件的不予备案,并说明理由。

(五) “备案管理系统”对予以备案的,核配备案编号,生成备案电子验证标识(简称电子证书),同时将审核意见反馈接入提供者;对不予以备案的,“备案管理系统”将不予备案理由反馈相关接入提供者。并通知相关接入提供者对相关信息进行修改,重新填报。

(六) 对予以备案的,接入提供者将审核意见、用户名和密码及时反馈给网站主办者,并指导网站主办者下载、安装电子证书。网站主办者在接入提供者的指导下及时完成电子证书下载、安装等后续工作,并保管好用户名和密码。

(七) 对不予备案的,接入提供者及时通知网站主办者对相关信息进行修改,重新填报或补报信息。

第十三条 网站主办者自行履行ICP备案、备案变更处理流程(见图二):

(一) 网站主办者向“备案管理系统”输入相关备案信息。

(二) “备案管理系统”收到网站主办者提交的信息后,对信息进行自动核查,没有发现问题的转相关省通信管理局;存在问题的,将相关意见反馈网站主办者。

(三) 相关省通信管理局对备案信息进行审核,符合备案条件的予以备案;不符合备案条件的不予备案,并说明理由。

(四) “备案管理系统”对予以备案的,核配备案编号,生成电子证书,同时将审核意见反馈网站主办者;对不予以备案的,“备案管理系统”将不予备案理由反馈相关网站主办者,并通知网站主办者对相关信息进行修改,重新填报或补报信息。

(五) 网站主办者收到备案编号和电子证书后,及时完成证书下载、安装等工作。

第十四条 涉及前置审批的ICP备案流程:

(一) 拟从事新闻、出版、教育、医疗保健、药品和医疗器械、视听节目、网络文化等互联网信息服务的,在履行ICP备案手续前应获得相关前置审批部门的批准。

(二) 网站主办者获得前置审批部门批准后,按本细则第十二条或者第十三条相关流程履行备案手续,同时需向住所(身份证住所/注册住所)所在地省通信管理局书面提交相关前置审批部门的审批文件。

(三) 网站主办者提交备案信息后五个工作日内尚未提交审批文件的,不予备案。

(四) 备案完成后,省通信管理局向相关省级前置审批部门通报网站备案信息。

第十五条 ICP备案注销处理流程:

(一) 网站主办者停止互联网信息服务时应注销其备案信息。网站主办者可以直接履行备案注销手续,也可以由接入提供者代为履行备案注销手续。

(二) 网站主办者直接履行备案注销手续的,由网站主办者直接将备案注销申请提交“备案管理系统”;接入提供者代为履行备案注销手续的,接入提供者向“备案管理系统”提交网站注销申请,同时提交该网站主办者相应的书面委托书。

(三) “备案管理系统”收到网站备案注销申请信息后,将注销申请转相关省通信管理局。

(四) 相关省通信管理局进行审核,符合注销条件的予以注销,并将相关意见反馈注销申请者。

(五) 对注销的网站,接入提供者应及时停止接入服务。

第十六条 查处违法违规网站流程(见图三):

(一) 省通信管理局根据涉嫌违法违规网站线索(包括举报材料、省通信管理局例行检查、信息产业部的通报、相关部门要求协助查处意见等),对确属违法违规网站进行依法处理。

(二) 涉嫌违法违规网站主办者住所所在地不在本行政区的,省通信管理局应及时将违法违规网站基本资料转送至网站主办者住所所在地省通信管理局,由该省通信管理局依法处理。

(三) 网站主办者住所所在地在本行政区的,省通信管理局应依法处理。

(四) 对依法应当关闭网站的,省通信管理局应向书面通知相关接入提供者停止接入,相关接入提供者应及时将执行情况上报省通信管理局。

(五) 网站接入地不在本行政区的,省通信管理局可以直接发函要求接入地省通信管理局配合关闭网站,接入地省通信管理局应积极予以配合,及时书面通知相关接入提供者停止接入,并将执行情况反馈网站主办者住所所在地省通信管理局。

第十七条 查处接入提供者违规行为的流程:

省通信管理局应加强对接入提供者的管理,监督检查接入提供者对用户代为备案信息的事前核验、用户行为的事中监督、违法违规网站的事后查处配合等责任的落实情况。

对违法违规的接入提供者,违法违规行为发生地通信管理局要立案调查,接入提供者主体所在地不在本行政区的,可以请相关省通信管理局配合。

第十八条 互联网站年度审核工作流程:

(一) 每年第一季度开始对互联网站进行年度审核工作。

(二) 对“备案管理系统”搜索出IP地址、域名等信息与ICP备案信息不一致的,要求相关网站主办者及时更新备案信息。

(三) 对于相关内容主管部门年度审核意见是“取消业务资格”、“关闭网站”的,属于年度审核不合格意见,根据相关内容主管部门提供的书面年度审核意见,实行一票否决制。

第十九条 IP地址备案工作流程:

(一) IP地址备案单位向“备案管理系统”导入IP地址备案信息。

(二) “备案管理系统”对导入的IP地址信息进行自动核查,输出核查报告,并分送给信息产业部或相关通信管理局。

(三) 信息产业部或相关通信管理局对核查报告进行分析处理。

第二十条 域名备案工作流程:

(一) 中国互联网络信息中心和相关域名注册服务机构(以下简称域名备案单位)向“备案管理系统”导入域名备案信息。

(二) “备案管理系统”自动进行数据处理定期输出统计报告。

(三) 信息产业部对统计报告进行分析,发现未备案的,依法处理。

第四章 附则

第二十一条 本细则由信息产业部电信管理局解释。

第二十二条 本细则自2005年12月1日起施行。

图一：接入提供者代为备案、备案变更的处理流程（略）

图二：网站主办者直接履斜赴浮 1. 赴副涓的处理流程（略）

图三：违规网站查处流程（略）

《非经营性互联网信息服务备案管理办法》

《非经营性互联网信息服务备案管理办法》

(信息产业部令第33号)

《非经营性互联网信息服务备案管理办法》已经2005年1月28日中华人民共和国信息产业部第十二次部务会议审议通过，现予发布，自2005年3月20日起施行。

部长：王旭东

二00五年二月八日

第一条 为规范非经营性互联网信息服务备案及备案管理，促进互联网信息服务业的健康发展，根据《互联网信息服务管理办法》、《中华人民共和国电信条例》及其他相关法律、行政法规的规定，制定本办法。

第二条 在中华人民共和国境内提供非经营性互联网信息服务，履行备案手续，实施备案管理，适用本办法。

第三条 中华人民共和国信息产业部（以下简称“信息产业部”）对全国非经营性互联网信息服务备案管理工作进行监督指导，省、自治区、直辖市通信管理局（以下简称“省通信管理局”）具体实施非经营性互联网信息服务的备案管理工作。

拟从事非经营性互联网信息服务的，应当向其住所所在地省通信管理局履行备案手续。

第四条 省通信管理局在备案管理中应当遵循公开、公平、公正的原则，提供便民、优质、高效的服务。

非经营性互联网信息服务提供者从事非经营性互联网信息服务时，应当遵守国家的有关规定，接受有关部门依法实施的监督管理。

第五条 在中华人民共和国境内提供非经营性互联网信息服务，应当依法履行备案手续。

未经备案，不得在中华人民共和国境内从事非经营性互联网信息服务。

本办法所称在中华人民共和国境内提供非经营性互联网信息服务，是指在中华人民共和国境内的组织或个人利用通过互联网域名访问的网站或者利用仅能通过互联网IP地址访问的网站，提供非经营性互联网信息服务。

第六条 省通信管理局通过信息产业部备案管理系统，采用网上备案方式进行备案管理。

第七条 拟从事非经营性互联网信息服务的，应当通过信息产业部备案管理系统如实填报《非经营性互联网信息服务备案登记表》（以下简称“《备案登记表》”，格式见本办法附录），履行备案手续。

信息产业部根据实际情况，对《备案登记表》进行调整和公布。

第八条 拟通过接入经营性互联网络从事非经营性互联网信息服务的，可以委托因特网接入服务业务经营者、因特网数据中心业务经营者和以其他方式为其网站提供接入服务的电信业务经营者代为履行备案、备案变更、备案注销等手续。

第九条 拟通过接入中国教育和科研计算机网、中国科学技术网、中国国际经济贸易互联网、中国长城互联网等公益性互联网络从事非经营性互联网信息服务的，可以由为其网站提供互联网接入服务的公益性互联网络单位代为履行备案、备案变更、备案注销等手续。

第十条 因特网接入服务业务经营者、因特网数据中心业务经营者以及以其他方式为网站提供接入服务的电信业务经营者和公益性互联网络单位（以下统称“互联网接入服务提供者”）不得在已知或应知拟从事非经营性互联网信息服务的组织或者个人的备案信息不真实的情况下，为其代为履行备案、备案变更、备案注销等手续。

第十一条 拟从事新闻、出版、教育、医疗保健、药品和医疗器械、文化、广播电影电视节目等互联网信息服务，根据法律、行政法规以及国家有关规定应经有关主管部门审核同意的，在履行备案手续时，还应向其住所所在地省通信管理局提交相关主管部门审核同意的文件。拟从事电子公告服务的，在履行备案手续时，还应当向其住所所在地省通信管理局提交电子公告服务专项备案材料。

第十二条 省通信管理局在收到备案人提交的备案材料后，材料齐全的，应在二十个工作日内予以备案，向其发放备案电子验证标识和备案编号，并通过信息产业部备案管理系统向社会公布有关备案信息；材料不齐全的，不予备案，在二十个工作日内通知备案人并说明理由。

第十三条 非经营性互联网信息服务提供者应当在其网站开通时在主页底部的中央位置标明其备案编号，并在备案编号下方按要求链接信息产业部备案管理系统网址，供公众查询核对。

非经营性互联网信息服务提供者应当在其网站开通时，按照信息产业部备案管理系统的要求，将备案电子验证标识放置在其网站的指定目录下。

第十四条 非经营性互联网信息服务提供者在备案有效期内需要变更其《备案登记表》中填报的信息的，应当提前三十日登录信息产业部备案系统向原备案机关履行备案变更手续。

第十五条 非经营性互联网信息服务提供者在备案有效期内需要终止提供服务的，应当在服务终止之日登录信息产业部备案系统向原备案机关履行备案注销手续。

第十六条 非经营性互联网信息服务提供者应当保证所提供的信息内容合法。

本办法所称非经营性互联网信息服务提供者提供的信息内容，是指互联网信息服务提供者的网站的互联网域名或IP地址下所包括的信息内容。

第十七条 省通信管理局应当建立信誉管理、社会监督、情况调查等管理机制，对非经营性互联网信息服务活动实施监督管理。

第十八条 互联网接入服务提供者不得为未经备案的组织或者个人从事非经营性互联网信息服务提供互联网接入服务。

对被省通信管理局处以暂时关闭网站或关闭网站处罚的非经营性互联网信息服务提供者或者非法从事非经营性互联网信息服务的组织或者个人，互联网接入服务提供者应立即暂停或终止向其提供互联网接入服务。

第十九条 互联网接入服务提供者应当记录其接入的非经营性互联网信息服务提供者的备案信息。

互联网接入服务提供者应当依照国家有关规定做好用户信息动态管理、记录留存、有害信息报告等网络信息安全工作，根据信息产业部和省通信管理局的要求对所接入用户进行监督。（相关资料：地方法规1篇）

第二十条 省通信管理局依法对非经营性互联网信息服务备案实行年度审核。

省通信管理局通过信息产业部备案管理系统，采用网上方式进行年度审核。

第二十一条 非经营性互联网信息服务提供者应当在每年规定时间登录信息产业部备案管理系统，履行年度审核手续。

第二十二条 违反本办法第五条的规定，未履行备案手续提供非经营性互联网信息服务的，由住所所在地省通信管理局责令限期改正，并处一万元罚款；拒不改正的，关闭网站。

超出备案的项目提供服务的，由住所所在地省通信管理局责令限期改正，并处五千元以上一万元以下罚款；拒不改正的，关闭网站并注销备案。

第二十三条 违反本办法第七条第一款的规定，填报虚假备案信息的，由住所所在地省通信管理局关闭网站并注销备案。

第二十四条 违反本办法第十条、第十八条、第十九条的规定的，由违法行为发生地省通信管理局责令改正，并处一万元罚款。

第二十五条 违反本办法第十三条的规定，未在其备案编号下方链接信息产业部备案管理系统网址的，或未将备案电子验证标识放置在其网站指定目录下的，由住所所在地省通信管理局责令改正，并处五千元以上一万元以下罚款。

第二十六条 违反本办法第十四条、第十五条的规定，未在规定时间内履行备案变更手续，或未依法履行备案注销手续的，由住所所在地省通信管理局责令限期改正，并处一万元罚款。

第二十七条 非经营性信息服务提供者违反国家有关法律规定，依法应暂停或终止服务的，省通信管理局可根据法律、行政法规授权的同级机关的书面认定意见，暂时关闭网站，或关闭网站并注销备案。

第二十八条 在年度审核时，非经营性互联网信息服务提供者有下列情况之一的，由其住所所在地的省通信管理局通过信息产业部备案系统等媒体通告责令其限期改正；拒不改正的，关闭网站并注销备案：

（一）未在规定时间内登录备案网站提交年度审核信息的；

（二）新闻、教育、公安、安全、文化、广播电影电视、出版、保密等国家部门依法对各自主管的专项内容提出年度审核否决意见的。

第二十九条 本办法自2005年3月20日起施行。

《互联网信息服务管理办法》

《互联网信息服务管理办法》

（国务院第31次常务会议通过）

中华人民共和国国务院令

（第292号）

《互联网信息服务管理办法》已经2000年9月20日国务院第31次常务会议通过，现予公布施行。

总理 朱镕基

二〇〇〇年九月二十五日

第一条 为了规范互联网信息服务活动，促进互联网信息服务健康有序发展，制定本办法。

第二条 在中华人民共和国境内从事互联网信息服务活动，必须遵守本办法。

本办法所称互联网信息服务，是指通过互联网向上网用户提供信息的服务活动。

第三条 互联网信息服务分为经营性和非经营性两类。

经营性互联网信息服务，是指通过互联网向上网用户有偿提供信息或者网页制作等服务活动。非经营性互联网信息服务，是指通过互联网向上网用户无偿提供具有公开性、共享性信息的服务活动。

第四条 国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度。

未取得许可或者未履行备案手续的，不得从事互联网信息服务。

第五条 从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意的，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。

第六条 从事经营性互联网信息服务，除应当符合《中华人民共和国电信条例》规定的要求外，还应当具备下列条件：

（一）有业务发展计划及相关技术方案；

（二）有健全的网络与信息安全保障措施，包括网站安全保障措施、信息安全保密管理制度、用户信息安全管理；

（三）服务项目属于本办法第五条规定范围的，已取得有关主管部门同意的文件。

第七条 从事经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门申请办理互联网信息服务增值电信业务经营许可证（以下简称经营许可证）。

省、自治区、直辖市电信管理机构或者国务院信息产业主管部门应当自收到申请之日起60日内审查完毕，作出批准或者

不予批准的决定。予以批准的，颁发经营许可证；不予批准的，应当书面通知申请人并说明理由。

申请人取得经营许可证后，应当持经营许可证向企业登记机关办理登记手续。

第八条 从事非经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门办理备案手续。办理备案时，应当提交下列材料：

- (一) 主办单位和网站负责人的基本情况；
- (二) 网站网址和服务项目；
- (三) 服务项目属于本办法第五条规定范围的，已取得有关主管部门的同意文件。

省、自治区、直辖市电信管理机构对备案材料齐全的，应当予以备案并编号。

第九条 从事互联网信息服务，拟开办电子公告服务的，应当在申请经营性互联网信息服务许可或者办理非经营性互联网信息服务备案时，按照国家有关规定提出专项申请或者专项备案。

第十条 省、自治区、直辖市电信管理机构和国务院信息产业主管部门应当公布取得经营许可证或者已履行备案手续的互联网信息服务提供者名单。

第十一条 互联网信息服务提供者应当按照经许可或者备案的项目提供服务，不得超出经许可或者备案的项目提供服务。

非经营性互联网信息服务提供者不得从事有偿服务。

互联网信息服务提供者变更服务项目、网站网址等事项的，应当提前30日向原审核、发证或者备案机关办理变更手续。

第十二条 互联网信息服务提供者应当在其网站主页的显著位置标明其经营许可证编号或者备案编号。

第十三条 互联网信息服务提供者应当向上网用户提供良好的服务，并保证所提供的信息内容合法。

第十四条 从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者，应当记录提供的信息内容及其发布时间、互联网地址或者域名；互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。

互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存60日，并在国家有关机关依法查询时，予以提供。

第十五条 互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

- (一) 反对宪法所确定的基本原则的；
- (二) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- (三) 损害国家荣誉和利益的；
- (四) 煽动民族仇恨、民族歧视，破坏民族团结的；
- (五) 破坏国家宗教政策，宣扬邪教和封建迷信的；
- (六) 散布谣言，扰乱社会秩序，破坏社会稳定的；
- (七) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- (八) 侮辱或者诽谤他人，侵害他人合法权益的；
- (九) 含有法律、行政法规禁止的其他内容的。

第十六条 互联网信息服务提供者发现其网站传输的信息明显属于本办法第十五条所列内容之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第十七条 经营性互联网信息服务提供者申请在境内境外上市或者同外商合资、合作，应当事先经国务院信息产业主管部门审查同意；其中，外商投资的比例应当符合有关法律、行政法规的规定。

第十八条 国务院信息产业主管部门和省、自治区、直辖市电信管理机构，依法对互联网信息服务实施监督管理。

新闻、出版、教育、卫生、药品监督管理、工商行政管理和公安、国家安全等有关主管部门，在各自职责范围内依法对互联网信息内容实施监督管理。

第十九条 违反本办法的规定，未取得经营许可证，擅自从事经营性互联网信息服务，或者超出许可的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正，有违法所得的，没收违法所得，处违法所得3倍以上5倍以下的罚款；没有违法所得或者违法所得不足5万元的，处10万元以上100万元以下的罚款；情节严重的，责令关闭网站。

违反本办法的规定，未履行备案手续，擅自从事非经营性互联网信息服务，或者超出备案的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正；拒不改正的，责令关闭网站。

第二十条 制作、复制、发布、传播本办法第十五条所列内容之一的信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照《中华人民共和国治安管理处罚条例》、《计算机信息网络国际联网安全保护管理办法》等有关法律、行政法规的规定予以处罚；对经营性互联网信息服务提供者，并由发证机关责令停业整顿直至吊销经营许可证，通知企业登记机关；对非经营性互联网信息服务提供者，并由备案机关责令暂时关闭网站直至关闭网站。

第二十一条 未履行本办法第十四条规定的义务的，由省、自治区、直辖市电信管理机构责令改正；情节严重的，责令停业整顿或者暂时关闭网站。

第二十二条 违反本办法的规定，未在其网站主页上标明其经营许可证编号或者备案编号的，由省、自治区、直辖市电信管理机构责令改正，处5000元以上5万元以下的罚款。

第二十三条 违反本办法第十六条规定的义务的，由省、自治区、直辖市电信管理机构责令改正；情节严重的，对经营性互联网信息服务提供者，并由发证机关吊销经营许可证，对非经营性互联网信息服务提供者，并由备案机关责令关闭网站。

第二十四条 互联网信息服务提供者在其业务活动中，违反其他法律、法规的，由新闻、出版、教育、卫生、药品监督管理局和工商行政管理等有关主管部门依照有关法律、法规的规定处罚。

第二十五条 电信管理机构和其他有关主管部门及其工作人员，玩忽职守、滥用职权、徇私舞弊，疏于对互联网信息服务的监督管理，造成严重后果，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，对直接负责的主管人员和其他直接责任人员依法给予降级、撤职直至开除的行政处分。

第二十六条 在本办法公布前从事互联网信息服务的，应当自本办法公布之日起60日内依照本办法的有关规定补办有关手续。

第二十七条 本办法自公布之日起施行。

《关于加强互联网易制毒化学品销售信息管理的公告》

《关于加强互联网易制毒化学品销售信息管理的公告》

(公安部、工信部、工商总局、安监总局、食品药品监督管理局近日联合发布)

公安部、工业和信息化部、国家工商行政管理总局、国家安全监管总局、国家食品药品监督管理局关于加强互联网易制毒化学品销售信息管理的公告

为进一步加强互联网易制毒化学品销售信息的监管，有效防范不法分子利用互联网非法销售易制毒化学品，净化网络环境，根据《中华人民共和国禁毒法》、《中华人民共和国广告法》、《易制毒化学品管理条例》、《互联网信息服务管理办法》等规定，现将有关事项公告如下：

一、严格互联网易制毒化学品销售信息发布的准入制度。任何单位在互联网上发布非药品类易制毒化学品销售信息，应当具有工商营业执照、非药品类易制毒化学品生产、经营许可证或备案证明等资质材料；禁止个人在互联网上发布非药品类易制毒化学品销售信息；禁止任何单位和个人在互联网上发布药品类易制毒化学品销售信息。

二、认真审查拟接入互联网的非药品类易制毒化学品销售信息。拟在互联网上发布非药品类易制毒化学品销售信息的网站主办者，应当向网站接入服务商提交销售单位的非药品类易制毒化学品生产、经营许可证或备案证明副本复印件，并在网站上公布销售单位名称及其许可证或备案证明编号。对发现无许可证或备案证明擅自在互联网上发布非药品类易制毒化学品销售信息的网站，网站接入服务商应当暂停接入，并向当地公安机关和工商行政管理、安全监管等部门报告。

三、认真清理互联网上的易制毒化学品销售信息。公安机关将会同有关部门及时依法清理互联网上的易制毒化学品违法销售信息；网站接入服务商如发现网站含有属明显违规的易制毒化学品销售信息，应当及时向当地公安机关和工商行政管理、安全监管、食品药品监管等部门报告，并配合有关部门做好删除清理、调查取证等相关工作。网站主办者应当加强对网上虚拟社区、论坛的管理，认真审查发帖内容，如发现信息含有属明显违规的易制毒化学品销售信息，应当及时删除，并向当地公安机关和工商行政管理、安全监管、食品药品监管等部门报告。

四、加强对互联网上易制毒化学品销售信息服务的监督检查。工商行政管理、安全监管、食品药品监管、通信管理等部门将进一步加强对互联网上易制毒化学品销售信息的监督检查，在各自的职责范围内，对在互联网上发布违法易制毒化学品销售信息的生产经营单位、网站主办者，将依法予以行政处罚。公安机关将进一步加大对网上非法买卖易制毒化学品案件的打击力度，严厉打击利用互联网从事走私贩卖易制毒化学品的违法犯罪活动。

公安 部

工业和信息化部

国家工商行政管理总局

国家安全监管总局

国家食品药品监管局

二〇一〇年九月二十一日

《关于办理网络赌博犯罪案件适用法律若干问题的意见》

《关于办理网络赌博犯罪案件适用法律若干问题的意见》

（最高人民法院、最高人民检察院、公安部联合印发）

最高人民法院、最高人民检察院、公安部关于办理网络赌博犯罪案件适用法律若干问题的意见（公通字[2010]40号）

各省、自治区、直辖市高级人民法院、人民检察院、公安厅、局，新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局：

为依法惩治网络赌博犯罪活动，根据《中华人民共和国刑法》、《中华人民共和国刑事诉讼法》和最高人民法院、最高人民检察院《关于办理赌博刑事案件具体应用法律若干问题的解释》等有关规定，结合司法实践，现就办理网络赌博犯罪案件适用法律的若干问题，提出如下意见：

一、关于网上开设赌场犯罪的定罪量刑标准

利用互联网、移动通讯终端等传输赌博视频、数据，组织赌博活动，具有下列情形之一的，属于刑法第三百零三条第二款规定的“开设赌场”行为：

- （一）建立赌博网站并接受投注的；
- （二）建立赌博网站并提供给他人组织赌博的；
- （三）为赌博网站担任代理并接受投注的；
- （四）参与赌博网站利润分成的。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第三百零三条第二款规定的“情节严重”：

- （一）抽头渔利数额累计达到3万元以上的；
- （二）赌资数额累计达到30万元以上的；
- （三）参赌人数累计达到120人以上的；
- （四）建立赌博网站后通过提供给他人组织赌博，违法所得数额在3万元以上的；
- （五）参与赌博网站利润分成，违法所得数额在3万元以上的；

(六) 为赌博网站招募下级代理，由下级代理接受投注的；

(七) 招揽未成年人参与网络赌博的；

(八) 其他情节严重的情形。

二、关于网上开设赌场共同犯罪的认定和处罚

明知是赌博网站，而为其提供下列服务或者帮助的，属于开设赌场罪的共同犯罪，依照刑法第三百零三条第二款的规定处罚：

(一) 为赌博网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道、投放广告、发展会员、软件开发、技术支持等服务，收取服务费数额在2万元以上的；

(二) 为赌博网站提供资金支付结算服务，收取服务费数额在1万元以上或者帮助收取赌资20万元以上的；

(三) 为10个以上赌博网站投放与网址、赔率等信息有关的广告或者为赌博网站投放广告累计100条以上的。

实施前款规定的行为，数量或者数额达到前款规定标准5倍以上的，应当认定为刑法第三百零三条第二款规定的“情节严重”。

实施本条第一款规定的行为，具有下列情形之一的，应当认定行为人“明知”，但是有证据证明确实不知道的除外：

(一) 收到行政主管部门书面等方式的告知后，仍然实施上述行为的；

(二) 为赌博网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道、投放广告、软件开发、技术支持、资金支付结算等服务，收取服务费明显异常的；

(三) 在执法人员调查时，通过销毁、修改数据、账本等方式故意规避调查或者向犯罪嫌疑人通风报信的；

(四) 其他有证据证明行为人明知的。

如果有开设赌场的犯罪嫌疑人尚未到案，但是不影响对已到案共同犯罪嫌疑人、被告人的犯罪事实认定的，可以依法对已到案者定罪处罚。

三、关于网络赌博犯罪的参赌人数、赌资数额和网站代理的认定

赌博网站的会员账号数可以认定为参赌人数，如果查实一个账号多人使用或者多个账号一人使用的，应当按照实际使用的人数计算参赌人数。

赌资数额可以按照在网上投注或者赢取的点数乘以每一点实际代表的金额认定。

对于将资金直接或间接兑换为虚拟货币、游戏道具等虚拟物品，并用其作为筹码投注的，赌资数额按照购买该虚拟物品所需资金数额或者实际支付资金数额认定。

对于开设赌场犯罪中用于接收、流转赌资的银行账户内的资金，犯罪嫌疑人、被告人不能说明合法来源的，可以认定为赌资。向该银行账户转入、转出资金的银行账户数量可以认定为参赌人数。如果查实一个账户多人使用或多个账户一人使用的，应当按照实际使用的人数计算参赌人数。

有证据证明犯罪嫌疑人在赌博网站上的账号设置下级账号的，应当认定其为赌博网站的代理。

四、关于网络赌博犯罪案件的管辖

网络赌博犯罪案件的地域管辖，应当坚持以犯罪地管辖为主、被告人居住地管辖为辅的原则。

“犯罪地”包括赌博网站服务器所在地、网络接入地，赌博网站建立者、管理者所在地，以及赌博网站代理人、参赌人实施网络赌博行为地等。

公安机关对侦办跨区域网络赌博犯罪案件的管辖权有争议的，应本着有利于查清犯罪事实、有利于诉讼的原则，认真协商解决。经协商无法达成一致的，报共同的上级公安机关指定管辖。对即将侦查终结的跨省（自治区、直辖市）重大网络赌博案

件，必要时可由公安部商最高人民法院和最高人民检察院指定管辖。

为保证及时结案，避免超期羁押，人民检察院对于公安机关提请审查逮捕、移送审查起诉的案件，人民法院对于已进入审判程序的案件，犯罪嫌疑人、被告人及其辩护人提出管辖异议或者办案单位发现没有管辖权的，受案人民检察院、人民法院经审查可以依法报请上级人民检察院、人民法院指定管辖，不再自行移送有管辖权的人民检察院、人民法院。

五、关于电子证据的收集与保全

侦查机关对于能够证明赌博犯罪案件真实情况的网页、上网记录、电子邮件、电子合同、电子交易记录、电子账册等电子数据，应当作为刑事证据予以提取、复制、固定。

侦查人员应当对提取、复制、固定电子数据的过程制作相关文字说明，记录案由、对象、内容以及提取、复制、固定的时间、地点、方法，电子数据的规格、类别、文件格式等，并由提取、复制、固定电子数据的制作人、电子数据的持有人签名或者盖章，附所提取、复制、固定的电子数据一并随案移送。

对于电子数据存储在境外的计算机上的，或者侦查机关从赌博网站提取电子数据时犯罪嫌疑人未到案的，或者电子数据的持有人无法签字或者拒绝签字的，应当由能够证明提取、复制、固定过程的见证人签名或者盖章，记明有关情况。必要时，可对提取、复制、固定有关电子数据的过程拍照或者录像。

《互联网站禁止传播淫秽、色情等不良信息自律规范》

《互联网站禁止传播淫秽、色情等不良信息自律规范》

(中国互联网协会互联网新闻信息服务工作委员会)

互联网站禁止传播淫秽、色情等不良信息自律规范

第一条 为促进互联网信息服务提供商加强自律，遏制淫秽、色情等不良信息通过互联网传播，推动互联网行业的持续健康发展，特制定本规范。

第二条 互联网站不得登载和传播淫秽、色情等中华人民共和国法律、法规禁止的不良信息内容。

第三条 淫秽信息是指在整体上宣扬淫秽行为，具有下列内容之一，挑动人们性欲，导致普通人腐化、堕落，而又没有艺术或科学价值的文字、图片、音频、视频等信息内容，包括：

- 1、淫褻性地具体描写性行为、性交及其心理感受；
- 2、宣扬色情淫荡形象；
- 3、淫褻性地描述或者传授性技巧；
- 4、具体描写乱伦、强奸及其他性犯罪的手段、过程或者细节，可能诱发犯罪的；
- 5、具体描写少年儿童的性行为；
- 6、淫褻性地具体描写同性恋的性行为或者其他性变态行为，以及具体描写与性变态有关的暴力、虐待、侮辱行为；
- 7、其他令普通人不能容忍的对性行为淫褻性描写。

第四条 色情信息是指在整体上不是淫秽的，但其中一部分有第三条中1至7的内容，对普通人特别是未成年人的身心健康有毒害，缺乏艺术价值或者科学价值的文字、图片、音频、视频等信息内容。

第五条 互联网站从事登载新闻信息、电子公告服务以及移动通信增值服务等业务，应当依照有关法律法规的规定，履行审批或备案手续，取得合法资格；新闻信息应来源于具有向互联网站提供新闻信息资质的媒体或其他合法的内容提供商。

第六条 不渲染、不集中展现关于性暴力、性犯罪、性绯闻等新闻信息；此类内容须严格控制数量，并不得在多个频道或栏目同时登载。登载这类新闻信息，应有利于弘扬社会正气和维护社会公德，确保导向正确。

第七条 登载有关医学医疗、生理卫生、婚姻家庭、人体艺术和与此相关的自然、社会科学信息内容，应建立信息内容的审核制度，做到内容健康、科学，来源合法、可靠。

第八条 不开设或变相开设为不道德性行为 and 性交易提供便利的频道或专栏；开设交友类专题频道或栏目，应明确说明该栏目的目的、网友行为规范和公布有关法律警示；非注册用户不得在该类频道或栏目张贴信息，对注册用户上传的信息实行先审后发。

第九条 对利用互联网电子公告服务系统，短信息服务系统传播淫秽、色情等不良信息的用户，应将其IP地址列入“黑名单”，对涉嫌犯罪的，应主动向公安机关举报。

第十条 不与非法网站建立任何性质的合作关系；不与其他网站或企业建立违背政府有关部门规定的联盟或协作关系。

第十一条 不以任何形式登载和传播含有淫秽、色情等不良信息内容的广告；不为含有淫秽、色情等不良信息内容的网站或网页提供任何形式的宣传和链接。

第十二条 违反本自律规范的互联网站，应及时纠正违规行为；经劝说、警告无效的，互联网新闻信息服务工作委员会有义务向政府有关部门建议，取消其提供相关信息服务的资质。

第十三条 互联网信息服务提供商和从业人员均有自觉维护中华人民共和国法律法规、社会主义道德规范的责任和义务，自觉接受政府的管理。

第十四条 加入《互联网站信息服务自律公约》的成员单位应遵守本自律规范。

第十五条 《互联网站禁止传播淫秽、色情等不良信息自律规范》由互联网新闻信息服务工作委员会负责监督执行。

第十六条 本规范从发布之日起执行。

中国互联网协会互联网

新闻信息服务工作委员会

二00四年六月十日

《互联网危险物品信息发布管理规定》

《互联网危险物品信息发布管理规定》

公安部、国家互联网信息办公室、工业和信息化部、环境保护部、国家工商行政管理总局、国家安全生产监督管理总局关于印发《互联网危险物品信息发布管理规定》的通知

（公通字〔2015〕5号）

各省、自治区、直辖市公安厅（局）、互联网信息办、工业和信息化部、通信管理局、环境保护厅（局）、工商行政管理局、安全生产监督管理局，新疆生产建设兵团公安局、互联网信息办、工业和信息化部、环境保护局、工商行政管理局、安全生产监督管理局：

为进一步加强互联网危险物品信息的管理，规范危险物品从业单位信息发布行为，依法查处、打击涉及危险物品违法犯罪活动，净化网络环境，保障公共安全，公安部、国家互联网信息办公室、工业和信息化部、环境保护部、国家工商行政管理总局、国家安全生产监督管理总局联合制定了《互联网危险物品信息发布管理规定》，现印发给你们，请结合本地实际，认真贯彻执行。

公安部

国家互联网信息办公室

工业和信息化部

环境保护部

国家工商行政管理总局

国家安全生产监督管理总局

2015年2月5日

第一条 为进一步加强互联网危险物品信息的管理，规范危险物品从业单位信息发布行为，依法查处、打击涉及危险物品的违法犯罪活动，净化网络环境，保障公共安全，根据《全国人大常委会关于加强网络信息保护的决定》、《全国人大常委会关于维护互联网安全的决定》、《广告法》、《枪支管理法》、《放射性污染防治法》和《民用爆炸物品安全管理条例》、《烟花爆竹安全管理条例》、《危险化学品安全管理条例》、《放射性同位素与射线装置安全和防护条例》、《核材料管制条例》、《互联网信息服务管理办法》等法律、法规和规章，制定本规定。

第二条 本规定所称危险物品，是指枪支弹药、爆炸物品、剧毒化学品、易制爆危险化学品和其他危险化学品、放射性物品、核材料、管制器具等能够危及人身安全和财产安全的物品。

第三条 本规定所称危险物品从业单位，是指依法取得危险物品生产、经营、使用资质的单位以及从事危险物品相关工作的教学、科研、社会团体、中介机构等单位。具体包括：

（一）经公安机关核发《民用枪支（弹药）制造许可证》、《民用枪支（弹药）配售许可证》的民用枪支、弹药制造、配售企业；

（二）经民用爆炸物品行业主管部门核发《民用爆炸物品生产许可证》、《民用爆炸物品销售许可证》的民用爆炸物品生产、销售企业，经公安机关核发《爆破作业单位许可证》的爆破作业单位；

（三）经安全生产监督管理部门核发《烟花爆竹安全生产许可证》、《烟花爆竹经营（批发）许可证》、《烟花爆竹经营（零售）许可证》的烟花爆竹生产、经营单位；

（四）经安全生产监督管理部门核发《危险化学品安全生产许可证》、《危险化学品经营许可证》、《危险化学品安全使用许可证》的危险化学品生产、经营、使用单位；

（五）经环境保护主管部门核发《辐射安全许可证》的生产、销售、使用放射性同位素和射线装置单位；

（六）经国务院核材料管理部门核发《核材料许可证》的核材料持有、使用、生产、储存、运输和处置单位；

（七）经公安机关批准的弩制造企业、营业性射击场，经公安机关登记备案的管制刀具制造、销售单位；

（八）从事危险物品教学、科研、服务的高等院校、科研院所、社会团体、中介机构和技术服务企业；

（九）法律、法规规定的其他危险物品从业单位。

第四条 本规定所称危险物品信息，是指在互联网上发布的危险物品生产、经营、储存、使用信息，包括危险物品种类、性能、用途和危险物品专业服务等相关信息。

第五条 危险物品从业单位从事互联网信息服务的，应当按照《互联网信息服务管理办法》规定，向电信主管部门申请办理互联网信息服务增值电信业务经营许可证或者办理非经营性互联网信息服务备案手续，并按照《计算机信息网络国际联网安全保护管理办法》规定，持从事危险物品活动的合法资质材料到所在地县级以上人民政府公安机关接受网站安全检查。

第六条 危险物品从业单位依法取得互联网信息服务增值电信业务经营许可证或者办理非经营性互联网信息服务备案手续后，可以在本单位网站发布危险物品信息。

禁止个人在互联网上发布危险物品信息。

第七条 接入服务提供者应当与危险物品从业单位签订协议或者确认提供服务，不得为未取得增值电信业务经营许可证或者未办理非经营性互联网信息服务备案手续的危险物品从业单位提供接入服务。

接入服务提供者不得为危险物品从业单位以外的任何单位或者个人提供危险物品信息发布网站接入服务。

第八条 危险物品从业单位应当在本单位网站主页显著位置标明可供查询的互联网信息服务经营许可证编号或者备案编号、从事危险物品活动的合法资质和营业执照等材料。

第九条 危险物品从业单位应当在本单位网站网页显著位置标明单位、个人购买相关危险物品应当具备的资质、资格条件：

（一）购买民用枪支、弹药应当持有省级或者设区的市级人民政府公安机关核发的《民用枪支（弹药）配购证》。

（二）购买民用爆炸物品应当持有国务院民用爆炸物品行业主管部门核发的《民用爆炸物品生产许可证》，或者省级人民

政府民用爆炸物品行业主管部门核发的《民用爆炸物品销售许可证》，或者所在地县级人民政府公安机关核发的《民用爆炸物品购买许可证》。

（三）购买烟花爆竹的，批发企业应当持有安全生产监督管理部门核发的《烟花爆竹经营（批发）许可证》；零售单位应当持有安全生产监督管理部门核发的《烟花爆竹经营（零售）许可证》；举办焰火晚会以及其他大型焰火燃放活动的应当持有公安机关核发的《焰火燃放许可证》；个人消费者应当向持有安全生产监督管理部门核发的《烟花爆竹经营（零售）许可证》的零售单位购买。批发企业向烟花爆竹生产企业采购烟花爆竹；零售经营者向烟花爆竹批发企业采购烟花爆竹。严禁零售单位和个人购买专业燃放类烟花爆竹。

（四）购买剧毒化学品应当持有安全生产监督管理部门核发的《危险化学品安全生产许可证》，或者设区的市级人民政府安全生产监督管理部门核发的《危险化学品经营许可证》或者《危险化学品安全使用许可证》，或者县级人民政府公安机关核发的《剧毒化学品购买许可证》。

购买易制爆危险化学品应当持有安全生产监督管理部门核发的《危险化学品安全生产许可证》，或者工业和信息化部核发的《民用爆炸物品生产许可证》，或者设区的市级人民政府安全生产监督管理部门核发的《危险化学品经营许可证》或者《危险化学品安全使用许可证》，或者本单位出具的合法用途证明。

（五）购买放射性同位素的单位应当持有环境保护主管部门核发的《辐射安全许可证》。

（六）购买核材料的单位应当持有国务院核材料管理部门核发的《核材料许可证》。

（七）购买弩应当持有省级人民政府公安机关批准使用的许可文件。

（八）购买匕首、三棱刮刀应当持有所在单位的批准文件或者证明，且匕首仅限于军人、警察、专业狩猎人员和地质、勘探等野外作业人员购买，三棱刮刀仅限于机械加工单位购买。

（九）法律、法规和相关管理部门的其他规定。

第十条 禁止危险物品从业单位在本单位网站以外的互联网应用服务中发布危险物品信息及建立相关链接。

危险物品从业单位发布的危险物品信息不得包含诱导非法购销危险物品行为的内容。

第十一条 禁止任何单位和个人在互联网上发布危险物品制造方法的信息。

第十二条 网络服务提供者应当加强对接入网站及用户发布信息的管理，定期对发布信息进行巡查，对法律、法规和本规定禁止发布或者传输的危险物品信息，应当立即停止传输，采取删除等处置措施，保存有关记录，并向公安机关等主管部门报告。

第十三条 各级公安、网信、工业和信息化、电信主管、环境保护、工商行政管理、安全监管等部门在各自的职责范围内依法履行职责，完善危险物品从业单位许可、登记备案、信息情况通报和信息发布机制，加强协作配合，共同防范危险物品信息发布的违法犯罪行为。

第十四条 违反规定制作、复制、发布、传播含有危险物品内容的信息，或者故意为制作、复制、发布、传播违法违规危险物品信息提供服务的，依法给予停止联网、停机整顿、吊销许可证或者取消备案、暂时关闭网站直至关闭网站等处罚；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。

第十五条 任何组织和个人对在互联网上违法违规发布危险物品信息和利用互联网从事走私、贩卖危险物品的违法犯罪行为，有权向有关主管部门举报。接到举报的部门应当依法及时处理，并对举报有功人员予以奖励。

第十六条 本规定自2015年3月1日起执行。

🔗 《互联网用户账号名称管理规定》

互联网用户账号名称管理规定

（国家互联网信息办公室 2015年2月4日）

第一条 为加强对互联网用户账号名称的管理，保护公民、法人和其他组织的合法权益，根据《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》和有关法律、行政法规，制定本规定。

第二条 在中华人民共和国境内注册、使用和管理互联网用户账号名称，适用本规定。

本规定所称互联网用户账号名称，是指机构或个人在博客、微博客、即时通信工具、论坛、贴吧、跟帖评论等互联网信息服务中注册或使用的账号名称。

第三条 国家互联网信息办公室负责对全国互联网用户账号名称的注册、使用实施监督管理，各省、自治区、直辖市互联网信息内容主管部门负责对本行政区域内互联网用户账号名称的注册、使用实施监督管理。

第四条 互联网信息服务提供者应当落实安全管理责任，完善用户服务协议，明示互联网信息服务使用者在账号名称、头像和简介等注册信息中不得出现违法和不良信息，配备与服务规模相适应的专业人员，对互联网用户提交的账号名称、头像和简介等注册信息进行审核，对含有违法和不良信息的，不予注册；保护用户信息及公民个人隐私，自觉接受社会监督，及时处理公众举报的账号名称、头像和简介等注册信息中的违法和不良信息。

第五条 互联网信息服务提供者应当按照“后台实名、前台自愿”的原则，要求互联网信息服务使用者通过真实身份信息认证后注册账号。

互联网信息服务使用者注册账号时，应当与互联网信息服务提供者签订协议，承诺遵守法律法规、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等七条底线。

第六条 任何机构或个人注册和使用的互联网用户账号名称，不得有下列情形：

- （一）违反宪法或法律法规规定的；
- （二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- （三）损害国家荣誉和利益的，损害公共利益的；
- （四）煽动民族仇恨、民族歧视，破坏民族团结的；
- （五）破坏国家宗教政策，宣扬邪教和封建迷信的；
- （六）散布谣言，扰乱社会秩序，破坏社会稳定的；
- （七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- （八）侮辱或者诽谤他人，侵害他人合法权益的；
- （九）含有法律、行政法规禁止的其他内容的。

第七条 互联网信息服务使用者以虚假信息骗取账号名称注册，或其账号头像、简介等注册信息存在违法和不良信息的，互联网信息服务提供者应当采取通知限期改正、暂停使用、注销登记等措施。

第八条 对冒用、关联机构或社会名人注册账号名称的，互联网信息服务提供者应当注销其账号，并向互联网信息内容主管部门报告。

第九条 对违反本规定的行为，由有关部门依照相关法律规定处理。

第十条 本规定自2015年3月1日起施行。

🔗 《中华人民共和国网络安全法》

中华人民共和国网络安全法

（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）

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、维护和使用的网络，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与互联互通，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、行政法规规定的其它义务。

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

《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、采取删除等处置措施、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、删除等处置措施的；
- （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。

🔗 《互联网上网服务营业场所管理条例》

互联网上网服务营业场所管理条例

(2002年9月29日中华人民共和国国务院令 第363号公布根据2011年1月8日《国务院关于废止和修改部分行政法规的决定》(国务院令 第588号)第一次修订根据2016年2月6日《国务院关于修改部分行政法规的决定》(国务院令 第666号)第二次修订)

第一章 总则

第一条 为了加强对互联网上网服务营业场所的管理，规范经营者的经营行为，维护公众和经营者的合法权益，保障互联网上网服务经营活动健康发展，促进社会主义精神文明建设，制定本条例。

第二条 本条例所称互联网上网服务营业场所，是指通过计算机等装置向公众提供互联网上网服务的网吧、电脑休闲室等营业性场所。

学校、图书馆等单位内部附设的为特定对象获取资料、信息提供上网服务的场所，应当遵守有关法律、法规，不适用本条例。

第三条 互联网上网服务营业场所经营单位应当遵守有关法律、法规的规定，加强行业自律，自觉接受政府有关部门依法实施的监督管理，为上网消费者提供良好的服务。

互联网上网服务营业场所的上网消费者，应当遵守有关法律、法规的规定，遵守社会公德，开展文明、健康的上网活动。

第四条 县级以上人民政府文化行政部门负责互联网上网服务营业场所经营单位的设立审批，并负责对依法设立的互联网上网服务营业场所经营单位经营活动的监督管理；公安机关负责对互联网上网服务营业场所经营单位的信息网络安全、治安及消防安全的监督管理；工商行政管理部门负责对互联网上网服务营业场所经营单位登记注册和营业执照的管理，并依法查处无照经营活动；电信管理等其他有关部门在各自职责范围内，依照本条例和有关法律、行政法规的规定，对互联网上网服务营业场所经营单位分别实施有关监督管理。

第五条 文化行政部门、公安机关、工商行政管理部门和其他有关部门及其工作人员不得从事或者变相从事互联网上网服务经营活动，也不得参与或者变相参与互联网上网服务营业场所经营单位的经营活动。

第六条 国家鼓励公民、法人和其他组织对互联网上网服务营业场所经营单位的经营活动进行监督，并对有突出贡献的给予奖励。

第二章 设立

第七条 国家对互联网上网服务营业场所经营单位的经营活动实行许可制度。未经许可，任何组织和个人不得从事互联网上网服务经营活动。

第八条 互联网上网服务营业场所经营单位从事互联网上网服务经营活动，应当具备下列条件：

- (一)有企业的名称、住所、组织机构和章程；
- (二)有与其经营活动相适应的资金；
- (三)有与其经营活动相适应并符合国家规定的消防安全条件的营业场所；
- (四)有健全、完善的信息网络安全管理制度和安全技术措施；
- (五)有固定的网络地址和与其经营活动相适应的计算机等装置及附属设备；
- (六)有与其经营活动相适应并取得从业资格的安全管理人员、经营管理人员、专业技术人员；
- (七)法律、行政法规和国务院有关部门规定的其他条件。

互联网上网服务营业场所的最低营业面积、计算机等装置及附属设备数量、单机面积的标准，由国务院文化行政部门规定。审批从事互联网上网服务经营活动，除依照本条第一款、第二款规定的条件外，还应当符合国务院文化行政部门和省、自治区、直辖市人民政府文化行政部门规定的互联网上网服务营业场所经营单位的总量和布局要求。

第九条 中学、小学校园周围200米范围内和居民住宅楼(院)内不得设立互联网上网服务营业场所。

第十条 互联网上网服务营业场所经营单位申请从事互联网上网服务经营活动，应当向县级以上地方人民政府文化行政部门提出申请，并提交下列文件：

- (一) 企业营业执照和章程；
- (二) 法定代表人或者主要负责人的身份证明材料；
- (三) 资金信用证明；
- (四) 营业场所产权证明或者租赁意向书；
- (五) 依法需要提交的其他文件。

第十一条 文化行政部门应当自收到申请之日起20个工作日内作出决定；经审查，符合条件的，发给同意筹建的批准文件。

申请人完成筹建后，持同意筹建的批准文件到同级公安机关申请信息网络安全和消防安全审核。公安机关应当自收到申请之日起20个工作日内作出决定；经实地检查并审核合格的，发给批准文件。

申请人持公安机关批准文件向文化行政部门申请最终审核。文化行政部门应当自收到申请之日起15个工作日内依据本条例第八条的规定作出决定；经实地检查并审核合格的，发给《网络文化经营许可证》。

对申请人的申请，文化行政部门经审查不符合条件的，或者公安机关经审核不合格的，应当分别向申请人书面说明理由。

第十二条 互联网上网服务营业场所经营单位不得涂改、出租、出借或者以其他方式转让《网络文化经营许可证》。

第十三条 互联网上网服务营业场所经营单位变更营业场所地址或者对营业场所进行改建、扩建，变更计算机数量或者其他重要事项的，应当经原审核机关同意。

互联网上网服务营业场所经营单位变更名称、住所、法定代表人或者主要负责人、注册资本、网络地址或者终止经营活动的，应当依法到工商行政管理部门办理变更登记或者注销登记，并到文化行政部门、公安机关办理有关手续或者备案。

第三章 经营

第十四条 互联网上网服务营业场所经营单位和上网消费者不得利用互联网上网服务营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用含有下列内容的信息：

- (一) 反对宪法确定的基本原则的；
- (二) 危害国家统一、主权和领土完整的；
- (三) 泄露国家秘密，危害国家安全或者损害国家荣誉和利益的；
- (四) 煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗、习惯的；
- (五) 破坏国家宗教政策，宣扬邪教、迷信的；
- (六) 散布谣言，扰乱社会秩序，破坏社会稳定的；
- (七) 宣传淫秽、赌博、暴力或者教唆犯罪的；
- (八) 侮辱或者诽谤他人，侵害他人合法权益的；
- (九) 危害社会公德或者民族优秀传统文化的；
- (十) 含有法律、行政法规禁止的其他内容的。

第十五条 互联网上网服务营业场所经营单位和上网消费者不得进行下列危害信息网络安全的活动：

- (一) 故意制作或者传播计算机病毒以及其他破坏性程序的；
- (二) 非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序的；
- (三) 进行法律、行政法规禁止的其他活动的。

第十六条 互联网上网服务营业场所经营单位应当通过依法取得经营许可证的互联网接入服务提供者接入互联网，不得采取其他方式接入互联网。

互联网上网服务营业场所经营单位提供上网消费者使用的计算机必须通过局域网的方式接入互联网，不得直接接入互联网。

第十七条 互联网上网服务营业场所经营单位不得经营非网络游戏。

第十八条 互联网上网服务营业场所经营单位和上网消费者不得利用网络游戏或者其他方式进行赌博或者变相赌博活动。

第十九条 互联网上网服务营业场所经营单位应当实施经营管理技术措施，建立场内巡查制度，发现上网消费者有本条例第十四条、第十五条、第十八条所列行为或者有其他违法行为的，应当立即予以制止并向文化行政部门、公安机关举报。

第二十条 互联网上网服务营业场所经营单位应当在营业场所的显著位置悬挂《网络文化经营许可证》和营业执照。

第二十一条 互联网上网服务营业场所经营单位不得接纳未成年人进入营业场所。互联网上网服务营业场所经营单位应当在营业场所入口处的显著位置悬挂未成年人禁入标志。

第二十二条 互联网上网服务营业场所每日营业时间限于8时至24时。

第二十三条 互联网上网服务营业场所经营单位应当对上网消费者的身份证等有效证件进行核对、登记，并记录有关上网信息。登记内容和记录备份保存时间不得少于60日，并在文化行政部门、公安机关依法查询时予以提供。登记内容和记录备份在保存期内不得修改或者删除。

第二十四条 互联网上网服务营业场所经营单位应当依法履行信息网络安全、治安和消防安全职责，并遵守下列规定：

- (一)禁止明火照明和吸烟并悬挂禁止吸烟标志；
- (二)禁止带入和存放易燃、易爆物品；
- (三)不得安装固定的封闭门窗栅栏；
- (四)营业期间禁止封堵或者锁闭门窗、安全疏散通道和安全出口；
- (五)不得擅自停止实施安全技术措施。

第四章 罚则

第二十五条 文化行政部门、公安机关、工商行政管理部门或者其他有关部门及其工作人员，利用职务上的便利收受他人财物或者其他好处，违法批准不符合法定设立条件的互联网上网服务营业场所经营单位，或者不依法履行监督职责，或者发现违法行为不予依法查处，触犯刑律的，对直接负责的主管人员和其他直接责任人员依照刑法关于受贿罪、滥用职权罪、玩忽职守罪或者其他罪的规定，依法追究刑事责任；尚不够刑事处罚的，依法给予降级、撤职或者开除的行政处分。

第二十六条 文化行政部门、公安机关、工商行政管理部门或者其他有关部门的工作人员，从事或者变相从事互联网上网服务经营活动的，参与或者变相参与互联网上网服务营业场所经营单位的经营活动的，依法给予降级、撤职或者开除的行政处分。

文化行政部门、公安机关、工商行政管理部门或者其他有关部门有前款所列行为的，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依法给予行政处分。

第二十七条 违反本条例的规定，擅自从事互联网上网服务经营活动的，由文化行政部门或者由文化行政部门会同公安机关依法予以取缔，查封其从事违法经营活动的场所，扣押从事违法经营活动的专用工具、设备；触犯刑律的，依照刑法关于非法经营罪的规定，依法追究刑事责任；尚不够刑事处罚的，由文化行政部门没收违法所得及其从事违法经营活动的专用工具、设备；违法经营额1万元以上的，并处违法经营额5倍以上10倍以下的罚款；违法经营额不足1万元的，并处1万元以上5万元以下的罚款。

第二十八条 文化行政部门应当建立互联网上网服务营业场所经营单位的经营活动信用监管制度，建立健全信用约束机制，并及时公布行政处罚信息。

第二十九条 互联网上网服务营业场所经营单位违反本条例的规定，涂改、出租、出借或者以其他方式转让《网络文化经营许可证》，触犯刑律的，依照刑法关于伪造、变造、买卖国家机关公文、证件、印章罪的规定，依法追究刑事责任；尚不够刑事处罚的，由文化行政部门吊销《网络文化经营许可证》，没收违法所得；违法经营额5000元以上的，并处违法经营额2倍以上5倍以下的罚款；违法经营额不足5000元的，并处5000元以上1万元以下的罚款。

第三十条 互联网上网服务营业场所经营单位违反本条例的规定，利用营业场所制作、下载、复制、查阅、发布、传播或者以其他方式使用含有本条例第十四条规定禁止含有的内容的信息，触犯刑律的，依法追究刑事责任；尚不够刑事处罚的，由公安机关给予警告，没收违法所得；违法经营额1万元以上的，并处违法经营额2倍以上5倍以下的罚款；违法经营额不足1万元的，并处1万元以上2万元以下的罚款；情节严重的，责令停业整顿，直至由文化行政部门吊销《网络文化经营许可证》。

上网消费者有前款违法行为，触犯刑律的，依法追究刑事责任；尚不够刑事处罚的，由公安机关依照治安管理处罚条例的规定给予处罚。

第三十一条 互联网上网服务营业场所经营单位违反本条例的规定，有下列行为之一的，由文化行政部门给予警告，可以并处15000元以下的罚款；情节严重的，责令停业整顿，直至吊销《网络文化经营许可证》：

- (一)在规定的营业时间以外营业的；

- (二)接纳未成年人进入营业场所的；
- (三)经营非网络游戏的；
- (四)擅自停止实施经营管理技术措施的；
- (五)未悬挂《网络文化经营许可证》或者未成年人禁入标志的。

第三十二条 互联网上网服务营业场所经营单位违反本条例的规定，有下列行为之一的，由文化行政部门、公安机关依据各自职权给予警告，可以并处15000元以下的罚款；情节严重的，责令停业整顿，直至由文化行政部门吊销《网络文化经营许可证》：

- (一)向上网消费者提供的计算机未通过局域网的方式接入互联网的；
- (二)未建立场内巡查制度，或者发现上网消费者的违法行为未予制止并向文化行政部门、公安机关举报的；
- (三)未按规定核对、登记上网消费者的有效身份证件或者记录有关上网信息的；
- (四)未按规定时间保存登记内容、记录备份，或者在保存期内修改、删除登记内容、记录备份的；
- (五)变更名称、住所、法定代表人或者主要负责人、注册资本、网络地址或者终止经营活动，未向文化行政部门、公安机关办理有关手续或者备案的。

第三十三条 互联网上网服务营业场所经营单位违反本条例的规定，有下列行为之一的，由公安机关给予警告，可以并处15000元以下的罚款；情节严重的，责令停业整顿，直至由文化行政部门吊销《网络文化经营许可证》：

- (一)利用明火照明或者发现吸烟不予制止，或者未悬挂禁止吸烟标志的；
- (二)允许带入或者存放易燃、易爆物品的；
- (三)在营业场所安装固定的封闭门窗栅栏的；
- (四)营业期间封堵或者锁闭门窗、安全疏散通道或者安全出口的；
- (五)擅自停止实施安全技术措施的。

第三十四条 违反国家有关信息网络安全、治安管理、消防管理、工商行政管理、电信管理等规定，触犯刑律的，依法追究刑事责任；尚不够刑事处罚的，由公安机关、工商行政管理部门、电信管理机构依法给予处罚；情节严重的，由原发证机关吊销许可证件。

第三十五条 互联网上网服务营业场所经营单位违反本条例的规定，被吊销《网络文化经营许可证》的，自被吊销《网络文化经营许可证》之日起5年内，其法定代表人或者主要负责人不得担任互联网上网服务营业场所经营单位的法定代表人或者主要负责人。

擅自设立的互联网上网服务营业场所经营单位被依法取缔的，自被取缔之日起5年内，其主要负责人不得担任互联网上网服务营业场所经营单位的法定代表人或者主要负责人。

第三十六条 依照本条例的规定实施罚款的行政处罚，应当依照有关法律、行政法规的规定，实行罚款决定与罚款收缴分离；收缴的罚款和违法所得必须全部上缴国库。

第五章 附则

第三十七条 本条例自2002年11月15日起施行。2001年4月3日信息产业部、公安部、文化部、国家工商行政管理局发布的《互联网上网服务营业场所管理办法》同时废止。

最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释

最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释

(2017年3月20日最高人民法院审判委员会第1712次会议、2017年4月26日最高人民检察院第十二届检察委员会第63次会议通过，自2017年6月1日起施行)

为依法惩治侵犯公民个人信息犯罪活动，保护公民个人信息安全和合法权益，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》的有关规定，现就办理此类刑事案件适用法律的若干问题解释如下：

第一条 刑法第二百五十三条之一规定的“公民个人信息”，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特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

第二条 违反法律、行政法规、部门规章有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的“违反国

家有关规定”。

第三条 向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。

未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。

第四条 违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

第五条 非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

- （一）出售或者提供行踪轨迹信息，被他人用于犯罪的；
- （二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；
- （三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；
- （四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；
- （五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；
- （六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；
- （七）违法所得五千元以上的；
- （八）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；
- （九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；
- （十）其他情节严重的情形。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”：

- （一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；
- （二）造成重大经济损失或者恶劣社会影响的；
- （三）数量或者数额达到前款第三项至第八项规定标准十倍以上的；
- （四）其他情节特别严重的情形。

第六条 为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

- （一）利用非法购买、收受的公民个人信息获利五万元以上的；
- （二）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的；
- （三）其他情节严重的情形。

实施前款规定的行为，将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准适用本解释第五条的规定。

第七条 单位犯刑法第二百五十三条之一规定之罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

第八条 设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。

第九条 网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。

第十条 实施侵犯公民个人信息犯罪，不属于“情节特别严重”，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免于刑事处罚；确有必要判处刑罚的，应当从宽处罚。

第十一条 非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算。

向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算。

对批量公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。

第十二条 对于侵犯公民个人信息犯罪，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。罚金数额一般在违法所得的一倍以上五倍以下。

第十三条 本解释自2017年6月1日起施行。

☞ 最高人民法院、最高人民检察院关于利用网络云盘制作、复制、贩卖、传播淫秽电子信息牟利行为定罪量刑问题的批复

最高人民法院、最高人民检察院关于利用网络云盘制作、复制、贩卖、传播淫秽电子信息牟利行为定罪量刑问题的批复

（2017年8月28日最高人民法院审判委员会第1724次会议、2017年10月10日最高人民检察院第十二届检察委员会第70次会议通过，自2017年12月1日起施行法释〔2017〕19号）

各省、自治区、直辖市高级人民法院、人民检察院，解放军军事法院、军事检察院，新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院：

近来，部分高级人民法院、省级人民检察院就如何对利用网络云盘制作、复制、贩卖、传播淫秽电子信息牟利行为定罪量刑的问题提出请示。经研究，批复如下：

一、对于以牟利为目的，利用网络云盘制作、复制、贩卖、传播淫秽电子信息的行为，是否应当追究刑事责任，适用刑法和《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》（法释〔2004〕11号）、《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）》（法释〔2010〕3号）的有关规定。

二、对于以牟利为目的，利用网络云盘制作、复制、贩卖、传播淫秽电子信息的行为，在追究刑事责任时，鉴于网络云盘的特点，不应单纯考虑制作、复制、贩卖、传播淫秽电子信息数量，还应充分考虑传播范围、违法所得、行为人一贯表现以及淫秽电子信息、传播对象是否涉及未成年人等情节，综合评估社会危害性，恰当裁量刑罚，确保罪责刑相适应。此复。

☞ 最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见

最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见

（法发〔2016〕32号2016年12月20日实施）

为依法惩治电信网络诈骗等犯罪活动，保护公民、法人和其他组织的合法权益，维护社会秩序，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》等法律和有关司法解释的规定，结合工作实际，制定本意见。

一、总体要求

近年来，利用通讯工具、互联网等技术手段实施的电信网络诈骗犯罪活动持续高发，侵犯公民个人信息，扰乱无线电通讯管理秩序，掩饰、隐瞒犯罪所得、犯罪所得收益等上下游关联犯罪不断蔓延。此类犯罪严重侵害人民群众财产安全和其他合法权益，严重干扰电信网络秩序，严重破坏社会诚信，严重影响人民群众安全感和社会和谐稳定，社会危害性大，群众反映强烈。

人民法院、人民检察院、公安机关要针对电信网络诈骗等犯罪的特点，坚持全链条全方位打击，坚持依法从严从快惩处，坚持最大力度最大限度追赃挽损，进一步健全工作机制，加强协作配合，坚决有效遏制电信网络诈骗等犯罪活动，努力实现法律效果和社会效果的高度统一。

二、依法严惩电信网络诈骗犯罪

（一）根据《最高人民法院、最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》第一条的规定，利用电信网络技术手段实施诈骗，诈骗公私财物价值三千元以上、三万元以上、五十万元以上的，应当分别认定为刑法第二百六十六条规定的“数额较大”“数额巨大”“数额特别巨大”。

二年内多次实施电信网络诈骗未经处理，诈骗数额累计计算构成犯罪的，应当依法定罪处罚。

（二）实施电信网络诈骗犯罪，达到相应数额标准，具有下列情形之一的，酌情从重处罚：

1. 造成被害人或其近亲属自杀、死亡或者精神失常等严重后果的；
2. 冒充司法机关等国家机关工作人员实施诈骗的；
3. 组织、指挥电信网络诈骗犯罪团伙的；
4. 在境外实施电信网络诈骗的；
5. 曾因电信网络诈骗犯罪受过刑事处罚或者二年内曾因电信网络诈骗受过行政处罚的；
6. 诈骗残疾人、老年人、未成年人、在校学生、丧失劳动能力人的财物，或者诈骗重病患者及其亲属财物的；
7. 诈骗救灾、抢险、防汛、优抚、扶贫、移民、救济、医疗等款物的；
8. 以赈灾、募捐等社会公益、慈善名义实施诈骗的；
9. 利用电话追呼系统等技术手段严重干扰公安机关等部门工作的；
10. 利用“钓鱼网站”链接、“木马”程序链接、网络渗透等隐蔽技术手段实施诈骗的。

（三）实施电信网络诈骗犯罪，诈骗数额接近“数额巨大”“数额特别巨大”的标准，具有前述第（二）条规定的情形之一的，应当分别认定为刑法第二百六十六条规定的“其他严重情节”“其他特别严重情节”。

上述规定的“接近”，一般应掌握在相应数额标准的百分之八十以上。

（四）实施电信网络诈骗犯罪，犯罪嫌疑人、被告人实际骗得财物的，以诈骗罪（既遂）定罪处罚。诈骗数额难以查证，但具有下列情形之一的，应当认定为刑法第二百六十六条规定的“其他严重情节”，以诈骗罪（未遂）定罪处罚：

1. 发送诈骗信息五千条以上的，或者拨打诈骗电话五百人次以上的；
2. 在互联网上发布诈骗信息，页面浏览量累计五千次以上的。

具有上述情形，数量达到相应标准十倍以上的，应当认定为刑法第二百六十六条规定的“其他特别严重情节”，以诈骗罪（未遂）定罪处罚。

上述“拨打诈骗电话”，包括拨出诈骗电话和接听被害人回拨电话。反复拨打、接听同一电话号码，以及反复向同一被害人发送诈骗信息的，拨打、接听电话次数、发送信息条数累计计算。

因犯罪嫌疑人、被告人故意隐匿、毁灭证据等原因，致拨打电话次数、发送信息条数的证据难以收集的，可以根据经查证属实的日拨打人次数、日发送信息条数，结合犯罪嫌疑人、被告人实施犯罪的时间、犯罪嫌疑人、被告人的供述等相关证据，综合予以认定。

（五）电信网络诈骗既有既遂，又有未遂，分别达到不同量刑幅度的，依照处罚较重的规定处罚；达到同一量刑幅度的，以诈骗罪既遂处罚。

（六）对实施电信网络诈骗犯罪的被告人裁量刑罚，在确定量刑起点、基准刑时，一般应就高选择。确定宣告刑时，应当综合全案事实情节，准确把握从重、从轻量刑情节的调节幅度，保证罪责刑相适应。

（七）对实施电信网络诈骗犯罪的被告人，应当严格控制适用缓刑的范围，严格控制适用缓刑的条件。

（八）对实施电信网络诈骗犯罪的被告人，应当更加注重依法适用财产刑，加大经济上的惩罚力度，最大限度剥夺被告人再犯的能力。

三、全面惩处关联犯罪

（一）在实施电信网络诈骗活动中，非法使用“伪基站”“黑广播”，干扰无线电通讯秩序，符合刑法第二百八十八条规定的，以扰乱无线电通讯管理秩序罪追究刑事责任。同时构成诈骗罪的，依照处罚较重的规定定罪处罚。

（二）违反国家有关规定，向他人出售或者提供公民个人信息，窃取或者以其他方法非法获取公民个人信息，符合刑法第二百五十三条之一规定的，以侵犯公民个人信息罪追究刑事责任。

使用非法获取的公民个人信息，实施电信网络诈骗犯罪行为，构成数罪的，应当依法予以并罚。

(三) 冒充国家机关工作人员实施电信网络诈骗犯罪，同时构成诈骗罪和招摇撞骗罪的，依照处罚较重的规定定罪处罚。

(四) 非法持有他人信用卡，没有证据证明从事电信网络诈骗犯罪活动，符合刑法第一百七十七条之一第一款第(二)项规定的，以妨害信用卡管理罪追究刑事责任。

(五) 明知是电信网络诈骗犯罪所得及其产生的收益，以下列方式之一予以转账、套现、取现的，依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得、犯罪所得收益罪追究刑事责任。但有证据证明确实不知道的除外：

1. 通过使用销售点终端机具(PoS机)刷卡套现等非法途径，协助转换或者转移财物的；
2. 帮助他人将巨额现金散存于多个银行账户，或在不同银行账户之间频繁划转的；
3. 多次使用或者使用多个非本人身份证明开设的信用卡、资金支付结算账户或者多次采用遮蔽摄像头、伪装等异常手段，帮助他人转账、套现、取现的；
4. 为他人提供非本人身份证明开设的信用卡、资金支付结算账户后，又帮助他人转账、套现、取现的；
5. 以明显异于市场的价格，通过手机充值、交易游戏点卡等方式套现的。

实施上述行为，事前通谋的，以共同犯罪论处。

实施上述行为，电信网络诈骗犯罪嫌疑人尚未到案或案件尚未依法裁判，但现有证据足以证明该犯罪行为确实存在的，不影响掩饰、隐瞒犯罪所得、犯罪所得收益罪的认定。

实施上述行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。法律和司法解释另有规定的除外。

(六) 网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使诈骗信息大量传播，或者用户信息泄露造成严重后果的，依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪追究刑事责任。同时构成诈骗罪的，依照处罚较重的规定定罪处罚。

(七) 实施刑法第二百八十七条之一、第二百八十七条之二规定之行为，构成非法利用信息网络罪、帮助信息网络犯罪活动罪，同时构成诈骗罪的，依照处罚较重的规定定罪处罚。

(八) 金融机构、网络服务提供者、电信业务经营者等在经营活动中，违反国家有关规定，被电信网络诈骗犯罪分子利用，使他人遭受财产损失的，依法承担相应责任。构成犯罪的，依法追究刑事责任。

四、准确认定共同犯罪与主观故意

(一) 三人以上为实施电信网络诈骗犯罪而组成的较为固定的犯罪组织，应依法认定为诈骗犯罪集团。对组织、领导犯罪集团的首要分子，按照集团所犯的全部罪行处罚。对犯罪集团中组织、指挥、策划者和骨干分子依法从严惩处。

对犯罪集团中起次要、辅助作用的从犯，特别是在规定期限内投案自首、积极协助抓获主犯、积极协助追赃的，依法从轻或减轻处罚。

对犯罪集团首要分子以外的主犯，应当按照其所参与的或者组织、指挥的全部犯罪处罚。全部犯罪包括能够查明具体诈骗数额的事实和能够查明发送诈骗信息条数、拨打诈骗电话人次数、诈骗信息网页浏览次数的事实。

(二) 多人共同实施电信网络诈骗，犯罪嫌疑人、被告人应对其参与期间该诈骗团伙实施的全部诈骗行为承担责任。在其所参与的犯罪环节中起主要作用的，可以认定为主犯；起次要作用的，可以认定为从犯。

上述规定的“参与期间”，从犯罪嫌疑人、被告人着手实施诈骗行为开始起算。

(三) 明知他人实施电信网络诈骗犯罪，具有下列情形之一的，以共同犯罪论处，但法律和司法解释另有规定的除外：

1. 提供信用卡、资金支付结算账户、手机卡、通讯工具的；
2. 非法获取、出售、提供公民个人信息的；
3. 制作、销售、提供“木马”程序和“钓鱼软件”等恶意程序的；
4. 提供“伪基站”设备或相关服务的；

5. 提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供支付结算等帮助的；
6. 在提供改号软件、通话线路等技术服务时，发现主叫号码被修改为国内党政机关、司法机关、公共服务部门号码，或者境外用户改为境内号码，仍提供服务的；
7. 提供资金、场所、交通、生活保障等帮助的；
8. 帮助转移诈骗犯罪所得及其产生的收益，套现、取现的。

上述规定的“明知他人实施电信网络诈骗犯罪”，应当结合被告人的认知能力，既往经历，行为次数和手段，与他人关系，获利情况，是否曾因电信网络诈骗受过处罚，是否故意规避调查等主客观因素进行综合分析认定。

（四）负责招募他人实施电信网络诈骗犯罪活动，或者制作、提供诈骗方案、术语清单、语音包、信息等的，以诈骗共同犯罪论处。

（五）部分犯罪嫌疑人在逃，但不影响对已到案共同犯罪嫌疑人、被告人的犯罪事实认定的，可以依法先行追究已到案共同犯罪嫌疑人、被告人的刑事责任。

五、依法确定案件管辖

（一）电信网络诈骗犯罪案件一般由犯罪地公安机关立案侦查，如果由犯罪嫌疑人居住地公安机关立案侦查更为适宜的，可以由犯罪嫌疑人居住地公安机关立案侦查。犯罪地包括犯罪行为发生地和犯罪结果发生地。

“犯罪行为发生地”包括用于电信网络诈骗犯罪的网站服务器所在地，网站建立者、管理者所在地，被侵害的计算机信息系统或其管理者所在地，犯罪嫌疑人、被害人使用的计算机信息系统所在地，诈骗电话、短信息、电子邮件等的拨打地、发送地、到达地、接受地，以及诈骗行为持续发生的实施地、预备地、开始地、途经地、结束地。

“犯罪结果发生地”包括被害人被骗时所在地，以及诈骗所得财物的实际取得地、藏匿地、转移地、使用地、销售地等。

（二）电信网络诈骗最初发现地公安机关侦办的案件，诈骗数额当时未达到“数额较大”标准，但后续累计达到“数额较大”标准，可由最初发现地公安机关立案侦查。

（三）具有下列情形之一的，有关公安机关可以在其职责范围内并案侦查：

1. 一人犯数罪的；
2. 共同犯罪的；
3. 共同犯罪的犯罪嫌疑人还实施其他犯罪的；
4. 多个犯罪嫌疑人实施的犯罪存在直接关联，并案处理有利于查明案件事实的。

（四）对因网络交易、技术支持、资金支付结算等关系形成多层次链条、跨区域的电信网络诈骗等犯罪案件，可由共同上级公安机关按照有利于查清犯罪事实、有利于诉讼的原则，指定有关公安机关立案侦查。

（五）多个公安机关都有权立案侦查的电信网络诈骗等犯罪案件，由最初受理的公安机关或者主要犯罪地公安机关立案侦查。有争议的，按照有利于查清犯罪事实、有利于诉讼的原则，协商解决。经协商无法达成一致的，由共同上级公安机关指定有关公安机关立案侦查。

（六）在境外实施的电信网络诈骗等犯罪案件，可由公安部按照有利于查清犯罪事实、有利于诉讼的原则，指定有关公安机关立案侦查。

（七）公安机关立案、并案侦查，或因有争议，由共同上级公安机关指定立案侦查的案件，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理。

对重大疑难复杂案件和境外案件，公安机关应在指定立案侦查前，向同级人民检察院、人民法院通报。

（八）已确定管辖的电信诈骗共同犯罪案件，在逃的犯罪嫌疑人归案后，一般由原管辖的公安机关、人民检察院、人民法院管辖。

六、证据的收集和审查判断

（一）办理电信网络诈骗案件，确因被害人人数众多等客观条件的限制，无法逐一收集被害人陈述的，可以结合已收集的被害人陈述，以及经查证属实的银行账户交易记录、第三方支付结算账户交易记录、通话记录、电子数据等证据，综合认定被害人人数及诈骗资金数额等犯罪事实。

（二）公安机关采取技术侦查措施收集的案件证明材料，作为证据使用的，应当随案移送批准采取技术侦查措施的法律文书和所收集的证据材料，并对其来源等作出书面说明。

（三）依照国际条约、刑事司法协助、互助协议或平等互助原则，请求证据材料所在地司法机关收集，或通过国际警务合作机制、国际刑警组织启动合作取证程序收集的境外证据材料，经查证属实，可以作为定案的依据。公安机关应对其来源、提取人、提取时间或者提供人、提供时间以及保管移交的过程等作出说明。

对其他来自境外的证据材料，应当对其来源、提供人、提供时间以及提取人、提取时间进行审查。能够证明案件事实且符合刑事诉讼法规定的，可以作为证据使用。

七、涉案财物的处理

（一）公安机关侦办电信网络诈骗案件，应当随案移送涉案赃款赃物，并附清单。人民检察院提起公诉时，应一并移交受理案件的人民法院，同时就涉案赃款赃物的处理提出意见。

（二）涉案银行账户或者涉案第三方支付账户内的款项，对权属明确的被害人的合法财产，应当及时返还。确因客观原因无法查实全部被害人，但有证据证明该账户系用于电信网络诈骗犯罪，且被告人无法说明款项合法来源的，根据刑法第六十四条的规定，应认定为违法所得，予以追缴。

（三）被告人已将诈骗财物用于清偿债务或者转让给他人，具有下列情形之一的，应当依法追缴：

1. 对方明知是诈骗财物而收取的；
2. 对方无偿取得诈骗财物的；
3. 对方以明显低于市场的价格取得诈骗财物的；
4. 对方取得诈骗财物系源于非法债务或者违法犯罪活动的。

他人善意取得诈骗财物的，不予追缴。

最高人民法院

最高人民检察院

公安部

2016年12月19日

最高人民法院于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释

最高人民法院关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释

（2001年6月26日最高人民法院审判委员会第1182次会议通过法释[2001]24号）

为了正确审理涉及计算机网络域名注册、使用等行为的民事纠纷案件（以下简称域名纠纷案件），根据《中华人民共和国民事诉讼法通则》（以下简称民法通则）、《中华人民共和国反不正当竞争法》（以下简称反不正当竞争法）和《中华人民共和国民事诉讼法》

（以下简称民事诉讼法）等法律的规定，作如下解释：

第一条 对于涉及计算机网络域名注册、使用等行为的民事纠纷，当事人向人民法院提起诉讼，经审查符合民事诉讼法第一百零八条规定的，人民法院应当受理。

第二条 涉及域名的侵权纠纷案件，由侵权行为地或者被告住所地的中级人民法院管辖。对难以确定侵权行为地和被告住所地的，原告发现该域名的计算机终端等设备所在地可以视为侵权行为地。

涉外域名纠纷案件包括当事人一方或者双方是外国人、无国籍人、外国企业或组织、国际组织，或者域名注册地在外国的域名

纠纷案件。在中华人民共和国领域内发生的涉外域名纠纷案件，依照民事诉讼法第四编的规定确定管辖。

第三条 域名纠纷案件的案由，根据双方当事人争议的法律关系的性质确定，并在其前冠以计算机网络域名；争议的法律关系的性质难以确定的，可以通称为计算机网络域名纠纷案件。

第四条 人民法院审理域名纠纷案件，对符合以下各项条件的，应当认定被告注册、使用域名等行为构成侵权或者不正当竞争：

- （一）原告请求保护的民事权益合法有效；
- （二）被告域名或其主要部分构成对原告驰名商标的复制、模仿、翻译或音译；或者与原告的注册商标、域名等相同或近似，足以造成相关公众的误认；
- （三）被告对该域名或其主要部分不享有权益，也无注册、使用该域名的正当理由；
- （四）被告对该域名的注册、使用具有恶意。

第五条 被告的行为被证明具有下列情形之一的，人民法院应当认定其具有恶意：

- （一）为商业目的将他人驰名商标注册为域名的；
- （二）为商业目的注册、使用与原告的注册商标、域名等相同或近似的域名，故意造成与原告提供的产品、服务或者原告网站的混淆，误导网络用户访问其网站或其他在线站点的；
- （三）曾要约高价出售、出租或者以其他方式转让该域名获取不正当利益的；
- （四）注册域名后自己并不使用也未准备使用，而有意阻止权利人注册该域名的；
- （五）具有其他恶意情形的。

被告举证证明在纠纷发生前其所持有的域名已经获得一定的知名度，且能与原告的注册商标、域名等相区别，或者具有其他情形足以证明其不具有恶意的，人民法院可以不认定被告具有恶意。

第六条 人民法院审理域名纠纷案件，根据当事人的请求以及案件的具体情况，可以对涉及的注册商标是否驰名依法作出认定。

第七条 人民法院在审理域名纠纷案件中，对符合本解释第四条规定的情形，依照有关法律规定构成侵权的，应当适用相应的法律规定；构成不正当竞争的，可以适用民法通则第四条、反不正当竞争法第二条第一款的规定。

涉外域名纠纷案件，依照民法通则第八章的有关规定处理。

第八条 人民法院认定域名注册、使用等行为构成侵权或者不正当竞争的，可以判令被告停止侵权、注销域名，或者依原告的请求判令由原告注册使用该域名；给权利人造成实际损害的，可以判令被告赔偿损失。

通信短信息服务管理规定

通信短信息服务管理规定

第一章 总 则

第一条 为了规范通信短信息（以下简称短信息）服务行为，维护用户的合法权益，促进短信息服务市场的健康发展，根据《全国人民代表大会常务委员会关于加强网络信息保护的決定》、《中华人民共和国电信条例》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内提供、使用短信息服务，适用本规定。

第三条 工业和信息化部负责对全国的短信息服务实施监督管理。

省、自治区、直辖市通信管理局负责对本行政区域内的短信息服务实施监督管理。

工业和信息化部和省、自治区、直辖市通信管理局统称电信管理机构。

第四条 提供、使用短信息服务的，应当遵守法律、行政法规和电信管理机构的相关规定，不得利用短信息服务从事违法活动。

第五条 鼓励有关行业协会依法制定短信息服务的自律性管理制度，引导会员加强自律管理。

第二章 短信息服务规范

第六条 经营短信息服务的，应当依法取得电信业务经营许可。

基础电信业务经营者不得为未取得电信业务经营许可的单位或者个人提供用于经营短信息服务的网络或者业务接入服务。

第七条 基础电信业务经营者应当准确记录接入其网络的短信息服务提供者的名称、接入代码和接入地点等信息。

第八条 短信息服务提供者应当制定短信息服务规则，并将与用户相关的内容通过服务合同或者入网协议等方式告知用户，不得利用格式条款侵犯用户合法权益。

第九条 短信息服务需向用户收费的，短信息服务提供者应当保证计费符合相关法律规定和电信标准，并事先明确告知用户服务内容、资费标准、收费方式和退订方式等。

第十条 短信息服务提供者发送短信息，应当将发送端电话号码或者代码一并发送，不得发送缺少发送端电话号码或者代码的短信息，不得发送含有虚假、冒用的发送端电话号码或者代码的短信息。

第十一条 短信息服务提供者应当在其服务系统中记录短信息发送和接收时间、发送端和接收端电话号码或者代码、用户订阅和退订情况等信息，端口类短信息还应当保存短信息内容。

前款规定的记录应当保存至少5个月，其中用户订阅和退订情况应当保存至短信息服务提供者与用户服务关系终止后5个月。

第十二条 短信息服务提供者提供端口类短信息服务，应当要求短信息内容提供者提供真实身份信息，并进行查验和登记。

第十三条 短信息服务提供者提供端口类短信息服务，应当按照电信管理机构批准的码号结构、位长、用途和使用范围使用端口号。未经电信管理机构批准，不得转让或者出租端口号。

第十四条 短信息服务提供者在业务活动中收集、使用用户个人信息，应当严格遵守有关法律法规的规定。

第十五条 短信息服务提供者应当建立和执行网络与信息安全管理制度，采取安全防范措施，加强公共信息巡查。

第十六条 短信息服务提供者、短信息内容提供者不得制作、复制、发布和传播含有《中华人民共和国电信条例》等法律法规规定的禁止性内容的短信息。

第十七条 发送公益性短信息的，由省级以上人民政府有关部门提前10个工作日向电信管理机构提供短信息发送时间、发送内容、发送范围、发送机构等信息，电信管理机构协调短信息服务提供者发送；不属于公益性短信息的，及时告知有关部门并说明理由。

涉及自然灾害、事故灾难、公共卫生事件和社会安全事件预警和处置等应急公益性短信息，情况紧急需要先行发送的，短信息服务提供者应当按照有关应急预案和机制及时免费发送，有关部门事后应当向电信管理机构提供有关信息。

第三章 商业性短信息管理

第十八条 短信息服务提供者、短信息内容提供者未经用户同意或者请求，不得向其发送商业性短信息。用户同意后又明确表示拒绝接收商业性短信息的，应当停止向其发送。

短信息服务提供者、短信息内容提供者请求用户同意接收商业性短信息的，应当说明拟发送商业性短信息的类型、频次和期限等信息。用户未回复的，视为不同意接收。用户明确拒绝或者未回复的，不得再次向其发送内容相同或者相似的短信息。

基础电信业务经营者对通过其电信网发送端口类商业性短信息的，应当保证有关用户已经同意或者请求接收有关短信息。

第十九条 短信息服务提供者、短信息内容提供者用于发送业务管理和服务类短信息的端口，不得用于发送商业性短信息。

第二十条 短信息服务提供者、短信息内容提供者向用户发送商业性短信息，应当提供便捷和有效的拒绝接收方式并随短信息告知用户，不得以任何形式对用户拒绝接收短信息设置障碍。

第二十一条 短信息服务提供者、短信息内容提供者向用户发送商业性短信息，应当在短信息中明确注明短信息内容提供者的名称。

第二十二条 短信息服务提供者应当建立短信息管理制度和预警监测机制，通过规范管理、技术手段和合同约定等措施，防范未经用户同意或者请求发送的商业性短信息。

第二十三条 基础电信业务经营者发现短信息服务提供者、短信息内容提供者违反本规定第十八条发送商业性短信息的，应当采取必要的措施暂停或者停止为其提供相关的电信资源，并保存有关记录。

第二十四条 鼓励用户自主选择使用短信息安全应用软件等适当的安全防护手段，提高自我防护能力。

第四章 用户投诉和举报

第二十五条 短信息服务提供者应当建立投诉处理机制，公布有效、便捷的联系方式，接受与短信息服务有关的投诉。

第二十六条 工业和信息化部委托12321网络不良与垃圾信息举报受理中心（以下简称举报中心）受理短信息服务举报。

第二十七条 用户认为其受到商业性短信息侵扰或者收到含有法律法规规定的禁止性内容的短信息的，可以向短信息服务提供者投诉或者向举报中心举报。

举报中心受理用户举报后，应当在5个工作日内转送短信息服务提供者处理。发现存在违法行为的，应当及时报告国家有关部门处理。

短信息服务提供者收到用户投诉或者举报中心转办的举报，经核实后应当及时采取有效手段，并在15个工作日内向投诉方或举报中心反馈处置结果。

第二十八条 短信息服务提供者发现被投诉或者举报的短信息明显含有本规定第十六条规定的内容的，应当立即停止发送，保存有关记录，并及时向国家有关机关报告；涉及本单位的，应当立即开展调查，采取有效的防范或者处理措施，并及时将调查结果报告电信管理机构。

第二十九条 用户与短信息服务提供者发生短信息服务争议的，可以依法向电信管理机构委托的电信用户申诉受理机构申诉。

第五章 监督管理

第三十条 电信管理机构对短信息服务活动实施监督检查时，短信息服务提供者、短信息内容提供者应当予以配合并按照要求提供相关材料。

电信管理机构实施监督检查，应当记录监督检查的情况，不得妨碍短信息服务提供者、短信息内容提供者正常的经营或者服务活动，不得收取任何费用。

第三十一条 电信管理机构实施电信业务经营许可年检时，应当对短信息服务提供者执行本规定的情况进行审查。

第三十二条 电信管理机构应当将短信息服务提供者违反本规定的行为记入信用档案并予以公布。必要时，电信管理机构可以对短信息服务提供者的负责人进行监管谈话。

第六章 法律责任

第三十三条 违反本规定第六条第一款、第十三条规定的，由电信管理机构依据《中华人民共和国电信条例》第六十九条规定处罚。

第三十四条 基础电信业务经营者、短信息服务提供者违反本规定第七条至第十二条、第十五条、第十八条至第二十一条、第二十七条第三款规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以上三万元以下罚款，向社会公告。

短信息内容提供者违反本规定第十八条至第二十一条规定的，由有关部门按照国家有关法律、行政法规予以处罚。

第三十五条 违反本规定第十六条规定的，依据《中华人民共和国电信条例》第六十六条规定处罚。

第三十六条 电信管理机构、举报中心工作人员在短信息服务监督管理工作中滥用职权、玩忽职守、徇私舞弊的，依法给予处理；构成犯罪的，依法追究刑事责任。

第七章 附 则

第三十七条 本规定下列用语的含义是：

（一）短信息服务，是指利用电信网向移动电话、固定电话等通信终端用户，提供有限长度的文字、数据、声音、图像等信息的电信业务。

（二）短信息服务提供者，是指提供短信息发送、存储、转发和接收等基础网络服务，以及利用基础网络设施和服务为其他组织和个人发送短信息提供平台的电信业务经营者（包含但不限于基础电信业务、增值电信业务中的信息服务业务和移动通信转售业务经营者）。

（三）短信息内容提供者，是指将其短信息通过短信息服务提供者发送的组织或者个人。

(四) 端口类短信息，是指短信息服务提供者利用自有端口或者行业类应用端口发送的短信息。

(五) 商业性短信息，是指用于介绍、推销商品、服务或者商业投资机会的短信息。

(六) 公益性短信息，是指各级人民政府相关部门等单位向用户发送的，旨在服务社会公共利益，倡导社会公序良俗、预防或处置突发事件、提醒群众防灾减灾等非盈利性质的短信息。

第三十八条 利用互联网向固定电话、移动电话等通信终端用户提供文字、数据、声音、图像等具有短信息特征的信息递送类服务，参照本规定执行。依法需经有关主管部门审核同意的，应当经有关部门审核同意。

第三十九条 本规定自2015年6月30日起施行。

🔗 《电信业务经营许可管理办法》

《电信业务经营许可管理办法》

(中华人民共和国工业和信息化部令 第42号)

第一章 总则

第一条 为了加强电信业务经营许可管理，根据《中华人民共和国电信条例》及其他法律、行政法规的规定，制定本办法。

第二条 在中华人民共和国境内申请、审批、使用和管理电信业务经营许可证（以下简称经营许可证），适用本办法。

第三条 工业和信息化部和省、自治区、直辖市通信管理局（以下统称电信管理机构）是经营许可证的审批管理机构。

经营许可证审批管理应当遵循便民、高效、公开、公平、公正的原则。

工业和信息化部建立电信业务综合管理平台（以下简称管理平台），推进经营许可证的网上申请、审批和管理及相关信息公示、查询、共享，完善信用管理机制。

第四条 经营电信业务，应当依法取得电信管理机构颁发的经营许可证。

电信业务经营者在电信业务经营活动中，应当遵守经营许可证的规定，接受、配合电信管理机构的监督管理。

电信业务经营者按照经营许可证的规定经营电信业务受法律保护。

第二章 经营许可证的申请

第五条 经营基础电信业务，应当具备下列条件：

- (一) 经营者为依法设立的专门从事基础电信业务的公司，并且公司的国有股权或者股份不少于51%；
- (二) 有业务发展研究报告和组网技术方案；
- (三) 有与从事经营活动相适应的资金和专业人员；
- (四) 有从事经营活动的场地、设施及相应的资源；
- (五) 有为用户提供长期服务的信誉或者能力；
- (六) 在省、自治区、直辖市范围内经营的，注册资本最低限额为1亿元人民币；在全国或者跨省、自治区、直辖市范围经营的，注册资本最低限额为10亿元人民币；
- (七) 公司及其主要投资者和主要经营管理人员未被列入电信业务经营失信名单；
- (八) 规定的其他条件。

第六条 经营增值电信业务，应当具备下列条件：

- (一) 经营者为依法设立的公司；
- (二) 有与开展经营活动相适应的资金和专业人员；
- (三) 有为用户提供长期服务的信誉或者能力；
- (四) 在省、自治区、直辖市范围内经营的，注册资本最低限额为100万元人民币；在全国或者跨省、自治区、直辖市范围经营的，注册资本最低限额为1000万元人民币；
- (五) 有必要的场地、设施及技术方案；
- (六) 公司及其主要投资者和主要经营管理人员未被列入电信业务经营失信名单；
- (七) 规定的其他条件。

第七条 申请办理基础电信业务经营许可证的，应当向工业和信息化部提交下列申请材料：

- （一）公司法定代表人签署的经营基础电信业务的书面申请，内容包括：申请经营电信业务的种类、业务覆盖范围、公司名称和联系方式等；
- （二）公司营业执照副本及复印件；
- （三）公司概况，包括公司基本情况，拟从事电信业务的机构设置和管理情况、技术力量和经营管理人员情况，与从事经营活动相适应的场地、设施等情况；
- （四）公司章程、公司股权结构及股东的有关情况；
- （五）业务发展研究报告，包括：经营电信业务的业务发展和实施计划、服务项目、业务覆盖范围、收费方案、预期服务质量、效益分析等；
- （六）组网技术方案，包括：网络结构、网络规模、网络建设计划、网络互联方案、技术标准、电信设备的配置、电信资源使用方案等；
- （七）为用户提供长期服务和质量保障的措施；
- （八）网络与信息安全保障措施；
- （九）证明公司信誉的有关材料；
- （十）公司法定代表人签署的公司依法经营电信业务的承诺书。

第八条 申请办理增值电信业务经营许可证的，应当向电信管理机构提交下列申请材料：

- （一）公司法定代表人签署的经营增值电信业务的书面申请，内容包括：申请经营电信业务的种类、业务覆盖范围、公司名称和联系方式等；
- （二）公司营业执照副本及复印件；
- （三）公司概况，包括：公司基本情况，拟从事电信业务的人员、场地和设施等情况；
- （四）公司章程、公司股权结构及股东的有关情况；
- （五）经营电信业务的业务发展和实施计划及技术方案；
- （六）为用户提供长期服务和质量保障的措施；
- （七）网络与信息安全保障措施；
- （八）证明公司信誉的有关材料；
- （九）公司法定代表人签署的公司依法经营电信业务的承诺书。

申请经营的电信业务依照法律、行政法规及国家有关规定须经有关主管部门事先审核同意的，应当提交有关主管部门审核同意的文件。

第三章 经营许可证的审批

第九条 经营许可证分为《基础电信业务经营许可证》和《增值电信业务经营许可证》两类。其中，《增值电信业务经营许可证》分为《跨地区增值电信业务经营许可证》和省、自治区、直辖市范围内的《增值电信业务经营许可证》。

《基础电信业务经营许可证》和《跨地区增值电信业务经营许可证》由工业和信息化部审批。省、自治区、直辖市范围内的《增值电信业务经营许可证》由省、自治区、直辖市通信管理局审批。

外商投资电信企业的经营许可证，由工业和信息化部根据《外商投资电信企业管理规定》审批。

第十条 工业和信息化部应当对申请经营基础电信业务的申请材料进行审查。申请材料齐全、符合法定形式的，应当向申请人出具受理申请通知书。申请材料不齐全或者不符合法定形式的，应当当场或者在五日内一次告知申请人需要补正的全部内容。

工业和信息化部受理申请之后，应当组织专家对第七条第五项、第六项、第八项申请材料进行评审，形成评审意见。

工业和信息化部应当自受理申请之日起180日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发《基础电信业务经营许可证》。不予批准的，应当书面通知申请人并说明理由。

第十一条 电信管理机构应当对申请经营增值电信业务的申请材料进行审查。申请材料齐全、符合法定形式的，应当向申请人出具受理申请通知书。申请材料不齐全或者不符合法定形式的，应当当场或者在五日内一次告知申请人需要补正的全部内容。

电信管理机构根据管理需要，可以组织专家对第八条第五项、第六项和第七项申请材料进行评审，形成评审意见。

电信管理机构应当自收到全部申请材料之日起60日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发《跨地区增

增值电信业务经营许可证》或者省、自治区、直辖市范围内的《增值电信业务经营许可证》。不予批准的，应当书面通知申请人并说明理由。

第十二条 电信管理机构需要对申请材料实质内容进行核实的，可以自行或者委托其他机构对申请人实地查验，申请人应当配合。

电信管理机构组织专家评审的，专家评审时间不计算在本办法第十条第三款和第十一条第三款规定的审查期限内。

第十三条 经营许可证由正文和附件组成。

经营许可证正文应当载明公司名称、法定代表人、业务种类（服务项目）、业务覆盖范围、有效期限、发证机关、发证日期、经营许可证编号等内容。

经营许可证附件可以规定特别事项，由电信管理机构对电信业务经营行为、电信业务经营者权利义务等作出特别要求。

经营许可证应当加盖发证机关印章。

工业和信息化部可以根据实际情况，调整经营许可证的内容，重新公布。

第十四条 《基础电信业务经营许可证》的有效期限，根据电信业务种类分为5年、10年。《跨地区增值电信业务经营许可证》和省、自治区、直辖市范围内的《增值电信业务经营许可证》的有效期限为5年。

第十五条 经营许可证由公司法定代表人领取，或者由其委托的公司其他人员凭委托书领取。

第四章 经营许可证的使用

第十六条 电信业务经营者应当按照经营许可证所载明的电信业务种类，在规定的业务覆盖范围内，按照经营许可证的规定经营电信业务。

电信业务经营者应当在公司主要经营场所、网站主页、业务宣传材料等显著位置标明其经营许可证编号。

第十七条 获准经营无线电通信业务的，应当按照国家无线电管理相关规定，持经营许可证向无线电管理机构申请取得无线电频率使用许可。

第十八条 电信业务经营者经发证机关批准，可以授权其持股比例（包括直接持有和间接持有）不少于51%并符合经营电信业务条件的公司经营其获准经营的电信业务。发证机关应当在电信业务经营者的经营许可证中载明该被授权公司的名称、法定代表人、业务种类、业务覆盖范围等内容。

获准跨地区经营基础电信业务的公司在一个地区不能授权两家或者两家以上公司经营同一项基础电信业务。

第十九条 任何单位和个人不得伪造、涂改、冒用和以任何方式转让经营许可证。

第五章 经营行为的规范

第二十条 基础电信业务经营者应当按照公开、平等的原则为取得经营许可证的电信业务经营者提供经营相关电信业务所需的电信服务和电信资源，不得为无经营许可证的单位或者个人提供用于经营电信业务的电信资源或者提供网络接入、业务接入服务。

第二十一条 电信业务经营者不得以任何方式实施不正当竞争。

第二十二条 为增值电信业务经营者提供网络接入、代理收费和业务合作的基础电信业务经营者，应当对相应增值电信业务的内容、收费、合作行为等进行规范、管理，并建立相应的发现、监督和处置制度及措施。

第二十三条 基础电信业务经营者调整与增值电信业务经营者之间的合作条件的，应当事先征求相关增值电信业务经营者的意见。

有关意见征求情况及记录应当留存，并在电信管理机构监督检查时予以提供。

第二十四条 提供接入服务的增值电信业务经营者应当遵守下列规定：

- （一）应当租用取得相应经营许可证的基础电信业务经营者提供的电信服务或者电信资源从事业务经营活动，不得向其他从事

接入服务的增值电信业务经营者转租所获得的电信服务或者电信资源；

(二) 为用户办理接入服务手续时，应当要求用户提供真实身份信息并予以查验；

(三) 不得为未依法取得经营许可证或者履行非经营性互联网信息服务备案手续的单位或者个人提供接入或者代收收费等服务；

(四) 按照电信管理机构的规定，建立相应的业务管理系统，并按要求实现同电信管理机构相应系统对接，定期报送有关业务管理信息；

(五) 对所接入网站传播违法信息的行为进行监督，发现传播明显属于《中华人民共和国电信条例》第五十六条规定的信息的，应当立即停止接入和代收收费等服务，保存有关记录，并向国家有关机关报告；

(六) 按照电信管理机构的要求终止或者暂停对违法网站的接入服务。

第二十五条 电信管理机构建立电信业务市场监测制度。相关电信业务经营者应当按照规定向电信管理机构报送相应的监测信息。

第二十六条 电信业务经营者应当按照国家和电信管理机构的规定，明确相应的网络与信息安全管理机构和专职网络与信息安全管理机构，建立网络与信息安全保障、网络安全防护、违法信息监测处置、新业务安全评估、网络安全监测预警、突发事件应急处置、用户信息安全保护等制度，并具备相应的技术保障措施。

第六章 经营许可证的变更、撤销、吊销和注销

第二十七条 经营许可证有效期届满需要继续经营的，应当提前90日向原发证机关提出延续经营许可证的申请；不再继续经营的，应当提前90日向原发证机关报告，并做好善后工作。

未在前款规定期限内提出延续经营许可证的申请，或者在经营许可证有效期内未开通电信业务的，有效期届满不予延续。

第二十八条 电信业务经营者或者其授权经营电信业务的公司，遇有因合并或者分立、股东变化等导致经营主体需要变更的情形，或者业务范围需要变化的，应当自公司作出决定之日起30日内向原发证机关提出申请。

电信业务经营者变更经营主体、股东的，应当符合本办法第五条、第六条、第九条第三款的有关规定。

第二十九条 在经营许可证的有效期限内，变更公司名称、法定代表人、注册资本的，应当在完成公司的工商变更登记手续之日起30日内向原发证机关申请办理电信业务经营许可证变更手续。

第三十条 在经营许可证的有效期限内，电信业务经营者需要终止经营的，应当符合下列条件：

(一) 终止经营基础电信业务的，应当符合电信管理机构确定的电信行业管理总体布局；

(二) 有可行的用户妥善处理方案并已妥善处理用户善后问题。

第三十一条 在经营许可证的有效期限内，电信业务经营者需要终止经营的，应当向原发证机关提交下列申请材料：

(一) 公司法定代表人签署并加盖公章的终止经营电信业务书面申请，内容包括：公司名称、联系方式、经营许可证编号、申请终止经营的电信业务种类、业务覆盖范围等；

(二) 公司股东会或者股东大会关于同意终止经营电信业务的决定；

(三) 公司法定代表人签署的做好用户善后处理工作的承诺书；

(四) 公司关于解决用户善后问题的情况说明，内容包括：用户处理方案、社会公示情况说明、用户意见汇总、实施计划等；

(五) 公司的经营许可证原件、营业执照复印件。

原发证机关收到终止经营电信业务的申请后应当向社会公示，公示期为30日。自公示期结束60日内，原发证机关应当完成审查工作，作出予以批准或者不予批准的决定。对于符合终止经营电信业务条件的，原发证机关应当予以批准，收回并注销电信业务经营许可证或者注销相应的电信业务种类、业务覆盖范围；对于不符合终止经营电信业务条件的，原发证机关应当不予批准，书面通知申请人并说明理由。

第三十二条 有下列情形之一的，发证机关或者其上级机关可以撤销经营许可证：

(一) 发证机关工作人员滥用职权、玩忽职守作出准予行政许可决定的；

(二) 超越法定职权或者违反法定程序作出准予行政许可决定的；

(三) 对不具备申请资格或者不符合申请条件的申请人准予行政许可的；

(四) 依法可以撤销经营许可证的其他情形。

第三十三条 有下列情形之一的，发证机关应当注销经营许可证：

- （一）电信业务经营者依法终止的；
- （二）经营许可证有效期届满未延续的；
- （三）电信业务经营者被有关机关依法处罚或者因不可抗力，导致电信业务经营许可事项无法实施的；
- （四）经营许可证依法被撤销、吊销的；
- （五）法律、法规规定应当注销经营许可证的其他情形。

第三十四条 发证机关吊销、撤销或者注销电信业务经营者的经营许可证后，应当向社会公布。

电信业务经营者被吊销、撤销或者注销经营许可证的，应当按照国家有关规定做好善后工作。

被吊销、撤销或者注销经营许可证的，应当将经营许可证交回原发证机关。

第七章 经营许可的监督检查

第三十五条 电信业务经营者应当在每年第一季度通过管理平台向发证机关报告下列信息：

- （一）上一年度的电信业务经营情况；
- （二）网络建设、业务发展、人员及机构变动情况；
- （三）服务质量情况；
- （四）网络与信息安全保障制度和措施执行情况；
- （五）执行国家和电信管理机构有关规定及经营许可证特别事项的情况；
- （六）发证机关要求报送的其他信息

前款第一项至第三项规定的信息（涉及商业秘密的信息除外）应当向社会公示，第五项、第六项规定的信息由电信业务经营者选择是否向社会公示。

电信业务经营者应当对本条第一款规定的年报信息的真实性负责，不得弄虚作假或者隐瞒真实情况。

第三十六条 电信管理机构建立随机抽查机制，对电信业务经营者的年报信息、日常经营活动、执行国家和电信管理机构有关规定的情况等进行检查。

电信管理机构可以采取书面检查、实地核查、网络监测等方式，并可以委托第三方机构开展有关检查工作。

电信管理机构在抽查中发现电信业务经营者有违反电信管理规定的违法行为的，应当依法处理。

第三十七条 电信管理机构根据随机抽查、日常监督检查及行政处罚记录等情况，建立电信业务经营不良名单和电信业务经营失信名单。

电信业务经营不良名单和失信名单应当定期通过管理平台更新并向社会公示。

第三十八条 电信管理机构发现电信业务经营者未按照本办法第三十五条的规定报告年报信息的，应当要求其限期报告。电信业务经营者未按照电信管理机构要求的期限报告年报信息的，由电信管理机构列入电信业务经营不良名单。

依照前款规定列入电信业务经营不良名单的电信业务经营者，依照本办法规定履行报告年报信息义务的，经电信管理机构确认后移出。

第三十九条 获准跨地区经营电信业务的公司在有关省、自治区、直辖市设立、变更或者撤销分支机构的，应当自作出决定之日起30日内通过管理平台向原发证机关和当地电信管理机构报送有关信息。

省、自治区、直辖市通信管理局应当对跨地区电信业务经营者在当地开展电信业务的有关情况进行监督检查，并向工业和信息化部报告有关检查结果。

第四十条 电信管理机构开展监督检查，不得妨碍电信业务经营者正常的生产经营活动，不得收取任何费用。

电信管理机构开展监督检查时，应当记录监督检查的情况和处理结果，由监督检查人员签字后归档。

电信管理机构应当通过管理平台公示监督检查情况。

第四十一条 电信管理机构应当通过管理平台向社会公示电信业务经营者受到行政处罚的情况，并向相关基础电信业务经营者和

提供接入服务的增值电信业务经营者通报。

第四十二条 电信业务经营者受到电信管理机构行政处罚的，由电信管理机构自作出行政处罚决定之日起30日内列入电信业务经营不良名单，但受到电信管理机构吊销经营许可证的处罚或者具有本办法规定直接列入电信业务经营失信名单情形的，直接列入失信名单。

列入电信业务经营不良名单的电信业务经营者，一年内未再次受到电信管理机构行政处罚的，由电信管理机构移出不良名单；三年内再次受到电信管理机构责令停业整顿、吊销经营许可证的处罚，或者具有工业和信息化部规定的其他情形的，由电信管理机构列入电信业务经营失信名单。

列入电信业务经营失信名单后，三年内未再次受到电信管理机构行政处罚的，由电信管理机构移出失信名单。

列入或者移出电信业务经营失信名单，应当同时将电信业务经营者的主要经营管理人员列入或者移出。

第四十三条 电信管理机构对列入电信业务经营不良名单和失信名单的电信业务经营者实施重点监管。

基础电信业务经营者和提供接入服务的增值电信业务经营者向其他增值电信业务经营者提供网络接入、代收费和业务合作时，应当把电信业务经营不良名单和失信名单作为重要考量因素。

第四十四条 任何单位或者个人发现电信业务经营者违反电信管理规定应当受到行政处罚的，可以向有关电信管理机构举报。

第八章 法律责任

第四十五条 隐瞒有关情况或者提供虚假材料申请电信业务经营许可的，电信管理机构不予受理或者不予行政许可，给予警告，申请人在一年内不得再次申请该行政许可。

以欺骗、贿赂等不正当手段取得电信业务经营许可的，电信管理机构撤销该行政许可，给予警告并直接列入电信业务经营失信名单，并视情节轻重处5000元以上3万元以下的罚款，申请人在三年内不得再次申请该行政许可；构成犯罪的，依法追究刑事责任。

第四十六条 违反本办法第十六条第一款、第二十八条第一款规定，擅自经营电信业务或者超范围经营电信业务的，依照《中华人民共和国电信条例》第六十九条规定予以处罚，其中情节严重、给予责令停业整顿处罚的，直接列入电信业务经营失信名单。

第四十七条 违反本办法第十九条规定的，依照《中华人民共和国电信条例》第六十八条规定予以处罚。

第四十八条 违反本办法第四条第二款、第二十条、第二十二條、第二十三條、第二十四條、第二十九條、第三十一條或者第三十五條第三款规定的，由电信管理机构责令改正，给予警告，可以并处5000元以上3万元以下的罚款。

《中华人民共和国网络安全法》《中华人民共和国电信条例》对前款规定的情形规定法律责任的，电信管理机构从其规定处理。

第四十九条 当事人对电信管理机构作出的行政许可、行政处罚决定不服的，可以依法申请行政复议或者提起行政诉讼。

当事人逾期不申请行政复议也不提起行政诉讼，又不履行行政处罚决定的，由作出行政处罚决定的电信管理机构申请人民法院强制执行，并列入电信业务经营失信名单。

第五十条 电信管理机构的工作人员在经营许可证管理工作中，玩忽职守、滥用职权、徇私舞弊，构成犯罪的，移交司法机关依法追究刑事责任；尚不构成犯罪的，由所在单位或者上级主管部门依法给予处分。

第九章 附则

第五十一条 经营许可证由工业和信息化部统一印制。

第五十二条 电信管理机构可以参照本办法组织开展电信业务商用试验活动。

第五十三条 本办法自2017年9月1日起施行。2009年3月5日公布的《电信业务经营许可管理办法》（工业和信息化部令第5号）同时废止。

《电信用户申诉处理办法》

工业和信息化部令

第一章 总则

第一条 为了保护电信用户的合法权益，规范用户申诉处理行为，根据《中华人民共和国电信条例》及其他有关法律、行政法规的规定，制定本办法。

第二条 本办法适用于处理用户在接受电信服务的过程中与电信业务经营者发生的争议。

第三条 本办法所称电信管理机构，是指工业和信息化部或省、自治区、直辖市通信管理局。

本办法所称申诉受理机构，是指工业和信息化部电信用户申诉受理中心和省、自治区、直辖市电信用户申诉受理机构。

本办法所称申诉人，是指在使用电信业务、接受电信服务中，与电信业务经营者发生争议并向申诉受理机构提出申诉的电信用户。

本办法所称被申诉人，是指因与用户发生争议而被用户申告的电信业务经营者。

第四条 工业和信息化部对全国电信用户申诉处理工作进行监督指导。工业和信息化部电信用户申诉受理中心受工业和信息化部委托，依据本办法开展全国电信用户申诉受理工作。

省、自治区、直辖市通信管理局可以根据本地实际情况设立电信用户申诉受理机构。电信用户申诉受理机构受省、自治区、直辖市通信管理局的委托并在其监督指导下，依据本办法开展本行政区电信用户申诉受理工作。

第五条 申诉处理以事实为依据，以法律为准绳，坚持公正、合理、合法的原则。

第六条 申诉受理机构对电信用户申诉事项实行调解制度，并可以出具调解书。

第七条 申诉受理机构每季度将受理用户申诉的统计报表上报同级电信管理机构。

第二章 受理

第八条 电信业务经营者应当认真受理用户的投诉，并在接到用户投诉之日起15日内答复用户。用户对电信业务经营者的处理结果不满意或者电信业务经营者在接到投诉后15日内未答复的，可以向申诉受理机构提出申诉。

第九条 申诉人应当向被申诉人所在省、自治区、直辖市的申诉受理机构提出申诉。被申诉人所在省、自治区、直辖市没有设立申诉受理机构的，申诉人可以向工业和信息化部电信用户申诉受理中心提出申诉。

第十条 用户申诉应当符合下列条件：

- (一) 申诉人是与申诉事项有直接利害关系的当事人；
- (二) 有明确的被申诉人；
- (三) 有具体的申诉请求和事实根据；
- (四) 已经向被申诉人投诉且对其处理结果不满意或者其未在15日内答复。

第十一条 申诉受理机构对有下列情形之一的申诉事项不予受理：

- (一) 属于收费争议的申诉，申诉事项发生时距提起申诉时超过五个月的，其他申诉，申诉事项发生时距提起申诉时超过二年的；
- (二) 申诉人与被申诉人已经达成和解协议并执行的；
- (三) 申诉受理机构已经受理或者处理的；
- (四) 人民法院、仲裁机构、消费者组织或者其他行政机关已经受理或者处理的；
- (五) 不符合本办法第十条规定的申诉条件的；
- (六) 国家法律、行政法规及部门规章另有规定的。

第十二条 申诉采用书面形式。申诉材料应当包括下列内容：

- (一) 申诉人姓名或名称、地址、电话号码、邮政编码；

- (二) 被申诉人名称、地址；
- (三) 申诉要求、理由、事实根据；
- (四) 申诉日期。

第十三条 申诉受理机构在接到用户申诉时，应当询问用户是否就申诉事项向电信业务经营者提出过投诉，电信业务经营者是否给予处理或答复。

对于未经电信业务经营者处理的用户申诉，申诉受理机构应当告知用户先向电信业务经营者投诉。

对于咨询有关电信政策的用户申诉，申诉受理机构应当向用户作出解答。

第十四条 申诉受理机构应当自收到申诉材料之日起5个工作日内，作出受理或者不予受理的决定，并通知申诉人。对于不予受理的申诉，应当告知不予受理的理由。

第三章 办理

第十五条 对于决定受理的用户申诉，申诉受理机构应当在受理用户申诉后2个工作日内将用户申诉内容和转办通知书发送被申诉人。

转办通知书应当载明申诉受理机构名称及联系方式、申诉人名称及联系方式、申诉人的申诉请求摘要、申诉受理机构对申诉处理的要求等。

第十六条 对申诉受理机构要求回复处理意见的，被申诉人收到转办通知书后，应当在10日内将申诉事项的事实情况和处理结果或者处理意见以及申诉人对处理结果的意见（满意程度）反馈给申诉受理机构。

第十七条 申诉受理机构应当自收到全部申诉材料之日起30日内向申诉人作出答复，将申诉处理情况告知申诉人。

对于被申诉人与申诉人协商和解的申诉，申诉受理机构可以作办结处理。

对于被申诉人与申诉人未能协商和解的申诉，应任何一方申请，申诉受理机构在征得对方同意后应当进行调解。

第四章 调解

第十八条 对于属于民事争议的下列情形，申诉受理机构可以组织双方当事人进行调解：

- (一) 申诉人与被申诉人已经就申诉事项进行过协商，但未能和解的；
- (二) 申诉人、被申诉人同意由申诉受理机构进行调解的；
- (三) 工业和信息化部规定的其他情形。

第十九条 申诉受理机构应当自争议双方同意调解之日起30日内调解完毕。调解达成协议的，视为办结；调解不成的，应当终止调解并告知申诉人，视为办结。调解达成协议的，应任何一方请求，申诉受理机构应当制作调解书。

第二十条 申诉受理机构调解无效的，争议双方可以依照国家有关法律规定就申诉事项向仲裁机构申请仲裁或者向人民法院提起诉讼。

第五章 调查

第二十一条 申诉受理机构可以通过电话、传真、书信以及实地调查等方式向申诉人和被申诉人了解有关情况，要求提供有关证据；申诉受理机构可以根据有关法律、行政法规和部门规章的规定，收集证据或者召集有关当事人进行调查。

第二十二条 申诉受理机构的调查人员有权行使下列权利：

- (一) 询问当事人和有关人员；
- (二) 要求有关单位和个人提供书面材料和证明；
- (三) 要求当事人提供有关技术材料；
- (四) 查阅、复制有关文件等。

第二十三条 调查应当由两名工作人员共同进行，调查时应当出示有效证件和有关证明，并应当制作调查笔录。调查人员对涉及当事人隐私、商业秘密等事项负有保密义务。

第二十四条 被调查人员必须如实回答调查人员的询问，提供相关证据。

第二十五条 申诉受理机构认为需要对有关设备、系统进行检测或者鉴定的，经同级电信管理机构批准后，交由指定检测或者鉴定机构进行检测、鉴定。被申诉的电信业务经营者应当予以配合。

第六章 附则 第二十六条 申诉受理机构每季度将受理用户申诉的统计报表向电信业务经营者进行通报。

第二十七条 对于电信用户与公用电信等代办点的争议，电信用户可以向委托代办的电信业务经营者投诉；对于电信用户与宾馆、饭店等电信业务代办点的争议，电信用户可以直接向申诉受理机构提出申诉。

第二十八条 本办法自2016年7月30日起施行。原信息产业部2001年1月11日公布的《电信用户申诉处理暂行办法》（原信息产业部令第7号）同时废止。

《电信设备进网管理办法》

《电信设备进网管理办法》

（2001年5月10日中华人民共和国信息产业部令第11号公布。根据2014年9月23日中华人民共和国工业和信息化部令第28号公布的《工业和信息化部关于废止和修改部分规章的决定》修正）

第一条 为了保证公用电信网的安全畅通，加强电信设备进网管理，维护电信用户和电信业务经营者的合法权益，根据《中华人民共和国电信条例》，制定本办法。

第二条 本办法所称电信设备是指电信终端设备、无线电通信设备和涉及网间互联的设备。

电信终端设备是指连接在公用电信网末端，为用户提供发送和接收信息功能的电信设备。

无线电通信设备是指连接在公用电信网上，以无线电为通信手段的电信设备。

涉及网间互联的设备是指涉及不同电信业务经营者的网络之间或者不同电信业务的网络之间互联互通的电信设备。

第三条 国家对接入公用电信网的电信终端设备、无线电通信设备和涉及网间互联的电信设备实行进网许可制度。

实行进网许可制度的电信设备必须获得工业和信息化部颁发的进网许可证；未获得进网许可证的，不得接入公用电信网使用和在国内销售。

第四条 实行进网许可制度的电信设备目录由工业和信息化部会同国务院产品质量监督部门制定和公布。

第五条 电信设备生产企业（以下简称生产企业）申请电信设备进网许可必须符合国家法律、法规和政策规定。申请进网许可的电信设备必须符合国家标准、通信行业标准以及工业和信息化部的规定。电信设备生产企业应当具有完善的质量保证体系和售后服务措施。

第六条 生产企业申请电信设备进网许可，应当附送国务院产品质量监督部门认可的电信设备检测机构出具的检测报告或者认证机构出具的产品认证证书。检测机构对申请进网许可的电信设备进行检测的依据、检测规程和出具的检测报告应当符合国家或工业和信息化部的规定。

第七条 工业和信息化部电信管理局具体负责全国电信设备进网管理和监督检查工作。

省、自治区、直辖市通信管理局负责本行政区域内电信设备进网管理和监督检查工作。

经工业和信息化部授权的受理机构承担电信设备进网许可申请的具体受理事宜。

第二章 进网许可程序

第八条 生产企业申请电信设备进网许可，应当向工业和信息化部授权的受理机构提交下列申请材料：

（一）电信设备进网许可申请表（由工业和信息化部提供格式文本）。申请表应当由生产企业法定代表人或其授权人签字并加盖公章。境外生产企业应当委托中国境内的代理机构提交申请表，并出具委托书；

（二）企业法人营业执照。境内生产企业应当提供企业法人营业执照。受境外生产企业委托代理申请电信设备进网许可的代理机构，应当提供代理机构有效执照；

（三）企业情况介绍。包括企业概况、生产条件、仪表配备、质量保证体系和售后服务措施等内容。对国家规定包修、包换和

包退的产品，还应提供履行有关责任的文件；

（四）质量体系认证证书或审核报告。通过质量体系认证的，提供认证证书；未通过质量体系认证的，提供满足相关要求的质量体系审核机构出具的质量体系审核报告；

（五）电信设备介绍。包括设备功能、性能指标、原理框图、内外观照片和使用说明等内容；

（六）检测报告或产品认证证书。应当是国务院产品质量监督部门认可的电信设备检测机构出具的检测报告或者认证机构出具的产品认证证书。

申请进网许可的无线电发射设备，应当提供工业和信息化部颁发的“无线电发射设备型号核准证”。

无线电通信设备、涉及网间互联的设备或新产品应当提供总体技术方案和试验报告。

前列申请材料中证书、执照类材料应当提供原件和一份复印件，或者盖有发证机构证明印章的复印件；其它材料必须使用中文。

第九条 自受理机构收到完备的申请材料之日起60日内，工业和信息化部电信管理局对生产企业提交的申请材料进行审查，经审查符合条件的，颁发进网许可证并核发进网许可标志；不符合条件的，书面答复生产企业。

第十条 生产企业通过质量体系认证的，其提供检测机构检测的样品由生产企业按规定数量自行选取。生产企业未通过质量体系认证的，其提供检测机构检测的样品由省、自治区、直辖市通信管理局按工业和信息化部规定的抽样办法执行。

第十一条 申请进网许可的无线电通信设备、涉及网间互联的设备或者新产品，应当在中国境内的电信网上或者工业和信息化部指定的模拟实验网上进行至少三个月的试验，并由试验单位出具试验报告。

工业和信息化部电信管理局组织专家对前款电信设备总体技术方案、试验报告、检测报告等进行评审，根据专家评审意见，经审查符合条件的，颁发进网许可证。

第十二条 生产企业对获得进网许可证的电信设备进行技术、外型改动的，须进行检测或重新办理进网许可证。

对获得进网许可证的电信设备外型改动较小，生产企业要求减免测试项目的，可以将改动前后的照片、电路原理图、改动说明和改动后的样品等交检测机构进行审核。检测机构向工业和信息化部电信管理局出具审核意见，检测机构审核认为可以减免测试项目的，经工业和信息化部电信管理局同意，可以减免测试项目。

第十三条 实行进网许可制度但尚无国家标准、行业标准的电信新设备，由生产企业自行将样品送到检测机构，检测机构根据国际标准或者企业标准进行检测，并出具检测报告。

工业和信息化部电信管理局对检测报告和有关材料进行审查，在符合国家产业政策和不影响网络安全畅通的条件下，批准进网试验，待国家标准、行业标准颁布后再按程序办理进网许可证。

第十四条 我国与其它国家或地区政府间签署电信设备检测实验室和检测报告相互认可协议的，按协议规定执行。

第三章 进网许可证和进网许可标志

第十五条 生产企业应当在其获得进网许可的电信设备上粘贴进网许可标志。进网许可标志由工业和信息化部统一印制和核发。进网许可标志属于质量标志。

未获得进网许可和进网许可证失效的电信设备上不得加贴进网许可标志。

第十六条 进网许可证和进网许可标志不得转让、涂改、伪造和冒用。

第十七条 进网许可证的有效期为3年。

生产企业需要继续生产和销售已获得进网许可的电信设备的，在进网许可证有效期届满前三个月，应当重新申请办理进网许可证，并附送一年内的送样检测报告或产品质量监督抽查报告，原证交回。

第十八条 电信设备进网许可证中规定的内容发生变化的，生产企业应当重新办理进网许可证。

第十九条 获得进网许可证的生产企业应当向其经销商以及需要进网许可证复印件的用户提供复印件，复印件应当由生产企业负责人签字并加盖公章。生产企业应当对复印件编号登记。

第二十条 生产企业应当在获得进网许可的电信设备包装上和刊登的广告中标明进网许可证编号。

第四章 监督管理

第二十一条 工业和信息化部定期向社会公布获得进网许可证的电信设备和生产企业。

获得进网许可证的生产企业应当接受所在的省、自治区、直辖市通信管理局的监督管理。

任何单位不得对已获得进网许可证的电信设备进行重复检测、发证。

第二十二条 省、自治区、直辖市通信管理局应当于每年12月31日前，对本行政区域内获得进网许可的电信设备和生产企业进行年度检查，并于第二年1月31日前，将年度检查情况汇总报工业和信息化部电信管理局。

第二十三条 获得电信设备进网许可证的生产企业应当保证电信设备获得进网许可证前后的一致性，保证产品质量稳定、可靠，不得降低产品质量和性能。

工业和信息化部组织对电信设备获得进网许可证前后的一致性进行监督检查；配合国务院产品质量监督部门对获得进网许可证的电信设备进行质量跟踪和监督抽查，并向社会公布抽查结果。

第二十四条 获得进网许可的电信设备及其外包装必须标有国家规定的中文标识；产品必须附有中文说明书和保修卡；对国家规定包修、包换和包退的产品，还应有相应的凭证。

第二十五条 实行进网许可制度的电信设备未获得进网许可的，电信业务经营者不得使用。

第二十六条 用户有权自主选择电信终端设备，电信业务经营者不得拒绝用户使用自备的已经取得进网许可的电信终端设备。

第二十七条 电信设备检测机构或产品质量认证机构必须执行国家标准、行业标准和工业和信息化部规定。检测机构或产品质量认证机构及其工作人员不得弄虚作假，不得利用职务之便剽窃或泄露生产企业的技术秘密。

第五章 罚则

第二十八条 违反本办法规定，销售未获得进网许可的电信终端设备的，由省、自治区、直辖市通信管理局责令改正，并处1万元以上10万元以下罚款。

第二十九条 违反本办法规定，伪造、冒用、转让进网许可证，编造进网许可证编号或粘贴伪造的进网许可标志的，由工业和信息化部或者省、自治区、直辖市通信管理局没收违法所得，并处违法所得3倍以上5倍以下罚款；没有违法所得或者违法所得不足1万元的，处1万元以上10万元以下罚款。

第三十条 违反本办法规定，生产企业获得进网许可证后降低产品质量和性能的，由产品质量监督部门依照有关法律法規予以处罚。

第三十一条 违反本办法规定，生产企业未在获得进网许可的设备外包装和刊登的广告中注明进网许可证编号的，由工业和信息化部或者省、自治区、直辖市通信管理局责令改正，并给予警告。

第三十二条 违反本办法规定，生产企业有下列行为之一的，由工业和信息化部或者省、自治区、直辖市通信管理局责令限期改正；情节严重的，给予警告：

- （一）申请进网许可时提供不真实申请材料的；
- （二）不能保证电信设备获得进网许可证前后的一致性的；
- （三）售后服务不落实，对国家规定包修、包换和包退的产品不履行相应义务的；
- （四）不按规定参加年检或者年检结果不合格的；
- （五）不接受工业和信息化部对电信设备获得进网许可证前后的一致性组织进行的监督检查或者检查结果不合格的。

违反前款第一项规定，尚未取得进网许可证的，工业和信息化部不予受理或者不予许可，生产企业在一年内不得再次申请进网许可；已取得进网许可证的，工业和信息化部撤销进网许可证，生产企业在三年内不得再次申请进网许可。

第三十三条 违反本办法规定，电信业务经营者拒绝用户自备的获得进网许可的电信终端设备进网的，由省、自治区、直辖市通信管理局责令改正，并向电信用户赔礼道歉，赔偿电信用户损失；拒不改正并赔礼道歉、赔偿损失的，处以警告，并处1万元以上10万元以下的罚款；情节严重的，责令停业整顿。

第三十四条 违反本办法规定，对已获得进网许可证的电信设备进行重复检测、发证的，由工业和信息化部责令改正。

第三十五条 违反本办法规定，检测机构、产品质量认证机构有下列行为之一的，工业和信息化部对其出具的检测报告或认证证书不予承认：

- （一）弄虚作假，有作弊行为的；
- （二）不按规定标准进行检测或认证的；
- （三）不按工业和信息化部规定出具检测报告或认证证书的。

第三十六条 从事电信设备进网许可申请受理、检测、审批及有关工作的人员滥用职权、徇私舞弊或者利用职务之便剽窃、泄露生产企业技术秘密的，依法给予行政处分。构成犯罪的，依法追究刑事责任。

第六章 附则

第三十七条 对进入公用电信网的电信设备抗震性能的管理办法，工业和信息化部另行制定。

第三十八条 未实行进网许可制度的电信设备可以由生产企业自愿向国务院产品质量监督部门认可的电信设备进网认证机构申请产品认证。

第三十九条 本办法自发布之日起施行。1998年12月31日信息产业部发布的《电信设备进网审批管理办法》同时废止。

《电信和互联网用户个人信息保护规定》

《电信和互联网用户个人信息保护规定》

工业和信息化部令（第24号）

第一章 总则

第一条 为了保护电信和互联网用户的合法权益，维护网络信息安全，根据《全国人民代表大会常务委员会关于加强网络信息保护的決定》、《中华人民共和国电信条例》和《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内提供电信服务和互联网信息服务过程中收集、使用用户个人信息的活动，适用本规定。

第三条 工业和信息化部 and 各省、自治区、直辖市通信管理局（以下统称电信管理机构）依法对电信和互联网用户个人信息保护工作实施监督管理。

第四条 本规定所称用户个人信息，是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。

第五条 电信业务经营者、互联网信息服务提供者在提供服务的过程中收集、使用用户个人信息，应当遵循合法、正当、必要的原则。

第六条 电信业务经营者、互联网信息服务提供者对其在提供服务过程中收集、使用的用户个人信息的安全负责。

第七条 国家鼓励电信和互联网行业开展用户个人信息保护自律工作。

第二章 信息收集和使用规范

第八条 电信业务经营者、互联网信息服务提供者应当制定用户个人信息收集、使用规则，并在其经营或者服务场所、网站等予以公布。

第九条 未经用户同意，电信业务经营者、互联网信息服务提供者不得收集、使用用户个人信息。

电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的，应当明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等事项。

电信业务经营者、互联网信息服务提供者不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息。

电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。

法律、行政法规对本条第一款至第四款规定的情形另有规定的，从其规定。

第十条 电信业务经营者、互联网信息服务提供者及其工作人员对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十一条 电信业务经营者、互联网信息服务提供者委托他人代理市场销售和技术服务等直接面向用户的服务性工作，涉及收集、使用用户个人信息的，应当对代理人的用户个人信息保护工作进行监督和管理，不得委托不符合本规定有关用户个人信息保护要求的代理人代办相关服务。

第十二条 电信业务经营者、互联网信息服务提供者应当建立用户投诉处理机制，公布有效的联系方式，接受与用户个人信息保护有关的投诉，并自接到投诉之日起十五日内答复投诉人。

第三章 安全保障措施

第十三条 电信业务经营者、互联网信息服务提供者应当采取以下措施防止用户个人信息泄露、毁损、篡改或者丢失：

- (一) 确定各部门、岗位和分支机构的用户个人信息安全管理责任；
- (二) 建立用户个人信息收集、使用及其相关活动的工作流程和安全管理制；
- (三) 对工作人员及代理人实行权限管理，对批量导出、复制、销毁信息实行审查，并采取防泄密措施；
- (四) 妥善保管记录用户个人信息的纸介质、光介质、电磁介质等载体，并采取相应的安全储存措施；
- (五) 对储存用户个人信息的信息系统实行接入审查，并采取防入侵、防病毒等措施；
- (六) 记录对用户个人信息进行操作的人员、时间、地点、事项等信息；
- (七) 按照电信管理机构的规定开展通信网络安全防护工作；
- (八) 电信管理机构规定的其他必要措施。

第十四条 电信业务经营者、互联网信息服务提供者保管的用户个人信息发生或者可能发生泄露、毁损、丢失的，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予其许可或者备案的电信管理机构报告，配合相关部门进行的调查处理。

电信管理机构应当对报告或者发现的可能违反本规定的行为的影响进行评估；影响特别重大的，相关省、自治区、直辖市通信管理局应当向工业和信息化部报告。电信管理机构在依据本规定作出处理决定前，可以要求电信业务经营者和互联网信息服务提供者暂停有关行为，电信业务经营者和互联网信息服务提供者应当执行。

第十五条 电信业务经营者、互联网信息服务提供者应当对其工作人员进行用户个人信息保护相关知识、技能和安全责任培训。

第十六条 电信业务经营者、互联网信息服务提供者应当对用户个人信息保护情况每年至少进行一次自查，记录自查情况，及时消除自查中发现的安全隐患。

第四章 监督检查

第十七条 电信管理机构应当对电信业务经营者、互联网信息服务提供者保护用户个人信息的情况实施监督检查。

电信管理机构实施监督检查时，可以要求电信业务经营者、互联网信息服务提供者提供相关材料，进入其生产经营场所调查情况，电信业务经营者、互联网信息服务提供者应当予以配合。

电信管理机构实施监督检查，应当记录监督检查的情况，不得妨碍电信业务经营者、互联网信息服务提供者正常的经营或者服务活动，不得收取任何费用。

第十八条 电信管理机构及其工作人员对在履行职责中知悉的用户个人信息应当予以保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十九条 电信管理机构实施电信业务经营许可及经营许可证年检时，应当对用户个人信息保护情况进行审查。

第二十条 电信管理机构应当将电信业务经营者、互联网信息服务提供者违反本规定的行为记入其社会信用档案并予以公布。

第二十一条 鼓励电信和互联网行业协会依法制定有关用户个人信息保护的自律性管理制度，引导会员加强自律管理，提高用户个人信息保护水平。

第五章 法律责任

第二十二条 电信业务经营者、互联网信息服务提供者违反本规定第八条、第十二条规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以下的罚款。

第二十三条 电信业务经营者、互联网信息服务提供者违反本规定第九条至第十一条、第十三条至第十六条、第十七条第二款规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以上三万元以下的罚款，向社会公告；构成犯罪的，依法追究刑事责任。

第二十四条 电信管理机构工作人员在对用户个人信息保护工作实施监督管理的过程中玩忽职守、滥用职权、徇私舞弊的，依法给予处理；构成犯罪的，依法追究刑事责任。

第六章 附则

第二十五条 本规定自2013年9月1日起施行。

《通信网络安全防护管理办法》

《通信网络安全防护管理办法》

第一条 为了加强对通信网络安全的管理，提高通信网络安全防护能力，保障通信网络安全畅通，根据《中华人民共和国电信条例》，制定本办法。

第二条 中华人民共和国境内的电信业务经营者和互联网域名服务提供者（以下统称“通信网络运行单位”）管理和运行的公用通信网和互联网（以下统称“通信网络”）的网络安全防护工作，适用本办法。

本办法所称互联网域名服务，是指设置域名数据库或者域名解析服务器，为域名持有者提供域名注册或者权威解析服务的行为。

本办法所称网络安全防护工作，是指为防止通信网络阻塞、中断、瘫痪或者被非法控制，以及为防止通信网络中传输、存储、处理的数据信息丢失、泄露或者被篡改而开展的工作。

第三条 通信网络安全防护工作坚持积极防御、综合防范、分级保护的原则。

第四条 中华人民共和国工业和信息化部（以下简称工业和信息化部）负责全国通信网络安全防护工作的统一指导、协调和检查，组织建立健全通信网络安全防护体系，制定通信行业相关标准。

各省、自治区、直辖市通信管理局（以下简称通信管理局）依据本办法的规定，对本行政区域内的通信网络安全防护工作进行指导、协调和检查。

工业和信息化部与通信管理局统称“电信管理机构”。

第五条 通信网络运行单位应当按照电信管理机构的规定和通信行业标准开展通信网络安全防护工作，对本单位通信网络安全负责。

第六条 通信网络运行单位新建、改建、扩建通信网络工程项目，应当同步建设通信网络安全保障设施，并与主体工程同时进行验收和投入运行。

通信网络安全保障设施的新建、改建、扩建费用，应当纳入本单位建设项目概算。

第七条 通信网络运行单位应当对本单位已正式投入运行的通信网络进行单元划分，并按照各通信网络单元遭到破坏后可能对国家安全、经济运行、社会秩序、公众利益的危害程度，由低到高分别划分为一级、二级、三级、四级、五级。

电信管理机构应当组织专家对通信网络单元的分级情况进行评审。

通信网络运行单位应当根据实际情况适时调整通信网络单元的划分和级别，并按照前款规定进行评审。

第八条 通信网络运行单位应当在通信网络定级评审通过后三十日内，将通信网络单元的划分和定级情况按照以下规定向电信管理机构备案：

- （一）基础电信业务经营者集团公司向工业和信息化部申请办理其直接管理的通信网络单元的备案；基础电信业务经营者各省（自治区、直辖市）子公司、分公司向当地通信管理局申请办理其负责管理的通信网络单元的备案；

- (二) 增值电信业务经营者向作出电信业务经营许可决定的电信管理机构备案；
- (三) 互联网域名服务提供者向工业和信息化部备案。

第九条 通信网络运行单位办理通信网络单元备案，应当提交以下信息：

- (一) 通信网络单元的名称、级别和主要功能；
- (二) 通信网络单元责任单位的名称和联系方式；
- (三) 通信网络单元主要负责人的姓名和联系方式；
- (四) 通信网络单元的拓扑架构、网络边界、主要软硬件及型号和关键设施位置；
- (五) 电信管理机构要求提交的涉及通信网络安全的其他信息。

前款规定的备案信息发生变化的，通信网络运行单位应当自信息变化之日起三十日内向电信管理机构变更备案。

通信网络运行单位报备的信息应当真实、完整。

第十条 电信管理机构应当对备案信息的真实性、完整性进行核查，发现备案信息不真实、不完整的，通知备案单位予以补正。

第十一条 通信网络运行单位应当落实与通信网络单元级别相适应的安全防护措施，并按照规定进行符合性评测：

- (一) 三级及三级以上通信网络单元应当每年进行一次符合性评测；
- (二) 二级通信网络单元应当每两年进行一次符合性评测。

通信网络单元的划分和级别调整的，应当自调整完成之日起九十日内重新进行符合性评测。

通信网络运行单位应当在评测结束后三十日内，将通信网络单元的符合性评测结果、整改情况或者整改计划报送通信网络单元的备案机构。

第十二条 通信网络运行单位应当按照以下规定组织对通信网络单元进行安全风险评估，及时消除重大网络安全隐患：

- (一) 三级及三级以上通信网络单元应当每年进行一次安全风险评估；
- (二) 二级通信网络单元应当每两年进行一次安全风险评估。

国家重大活动举办前，通信网络单元应当按照电信管理机构的要求进行安全风险评估。

通信网络运行单位应当在安全风险评估结束后三十日内，将安全风险评估结果、隐患处理情况或者处理计划报送通信网络单元的备案机构。

第十三条 通信网络运行单位应当对通信网络单元的重要线路、设备、系统和数据等进行备份。

第十四条 通信网络运行单位应当组织演练，检验通信网络安全防护措施的有效性。

通信网络运行单位应当参加电信管理机构组织开展的演练。

第十五条 通信网络运行单位应当建设和运行通信网络安全监测系统，对本单位通信网络的安全状况进行监测。

第十六条 通信网络运行单位可以委托专业机构开展通信网络安全评测、评估、监测等工作。

工业和信息化部应当根据通信网络安全防护工作的需要，加强对前款规定的受托机构的安全评测、评估、监测能力指导。

第十七条 电信管理机构应当对通信网络运行单位开展通信网络安全防护工作的情况进行检查。

电信管理机构可以采取以下检查措施：

- (一) 查阅通信网络运行单位的符合性评测报告和风险评估报告；
- (二) 查阅通信网络运行单位有关网络安全防护的文档和工作记录；
- (三) 向通信网络运行单位工作人员询问了解有关情况；
- (四) 查验通信网络运行单位的有关设施；
- (五) 对通信网络进行技术性分析和测试；
- (六) 法律、行政法规规定的其他检查措施。

第十八条 电信管理机构可以委托专业机构开展通信网络安全检查活动。

第十九条 通信网络运行单位应当配合电信管理机构及其委托的专业机构开展检查活动，对于检查中发现的重大网络安全隐患，

应当及时整改。

第二十条 电信管理机构对通信网络安全防护工作进行检查，不得影响通信网络的正常运行，不得收取任何费用，不得要求接受检查的单位购买指定品牌或者指定单位的安全软件、设备或者其他产品。

第二十一条 电信管理机构及其委托的专业机构的工作人员对于检查工作中获悉的国家秘密、商业秘密和个人隐私，有保密的义务。

第二十二条 违反本办法第六条第一款、第七条第一款和第三款、第八条、第九条、第十一条、第十二条、第十三条、第十四条、第十五条、第十九条规定的，由电信管理机构依据职权责令改正；拒不改正的，给予警告，并处五千元以上三万元以下的罚款。

第二十三条 电信管理机构的工作人员违反本办法第二十条、第二十一条规定的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第二十四条 本办法自2010年3月1日起施行。

《工业和信息化部关于进一步规范因特网数据中心业务和因特网接入服务业务市场准入工作的通告》

《工业和信息化部关于进一步规范因特网数据中心业务和因特网接入服务业务市场准入工作的通告》

(工信部电管函[2012]552号)

为促进互联网行业健康发展，营造健康有序的市场环境，落实《工业和信息化部关于鼓励和引导民间资本进一步进入电信业的实施意见》（工信部通〔2012〕293号），依据《电信业务经营许可管理办法》（工业和信息化部令第5号）等相关规定，我部制定了《关于进一步规范因特网数据中心（IDC）业务和因特网接入服务（ISP）业务市场准入工作的实施方案》（以下简称《实施方案》，见附件）。现就有关事项通告如下：

一、规范范围及重点内容

本次规范范围是因特网数据中心（IDC）业务和因特网接入服务（ISP）业务。重点内容为明确IDC、ISP两项业务经营许可证申请条件 and 审查流程，同时进一步明确IDC、ISP申请企业资金、人员、场地、设施等方面的要求（具体内容见《实施方案》）。

二、工作安排

（一）自2012年12月1日起，拟经营IDC和ISP业务的电信企业，可按照《实施方案》及相关法规要求，向电信主管部门申请办理业务经营许可。电信主管部门受理申请并对申请企业是否满足申请条件进行审查，依法做出予以批准或者不予批准决定。

（二）电信主管部门在按照《实施方案》要求开展IDC、ISP业务许可申请受理工作后，将视实际情况开展规范、清理IDC、ISP市场工作。

三、其他相关事宜

（一）电信主管部门将研究建立IDC和ISP企业信誉评价和机房星级评定管理机制，并将此评价和评定结果作为电信市场监管的重要依据。定期发布IDC和ISP企业信誉积分排名，将信誉积分评估与IDC和ISP企业年检相结合。从机房环境安全、网络质量等方面对IDC机房进行星级评定，定期向社会公示评定情况。具体评价和评定标准和条件另行发布。

（二）电信业务经营许可证相关申请材料可在电信业务综合管理系统（网址为tsm.miit.gov.cn）查阅和下载。

许可证申请咨询电话：010-62304694。

《工业和信息化部关于清理规范互联网网络接入服务市场的通知》

工业和信息化部关于清理规范互联网网络接入服务市场的通知

工信部信管函[2017]32号

各省、自治区、直辖市通信管理局，中国信息通信研究院，中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司、中国广播电视网络有限公司、中信网络有限公司，各互联网数据中心业务经营者、互联网接入服务业务经营者、内容分发网络业务经营者：

近年来，网络信息技术日新月异，云计算、大数据等应用蓬勃发展，我国互联网网络接入服务市场面临难得的发展机遇，但无序发展的苗头也随之显现，亟须整治规范。为进一步规范市场秩序，强化网络信息安全管理，促进互联网行业健康有序发展，工业和信息化部决定自即日起至2018年3月31日，在全国范围内对互联网网络接入服务市场开展清理规范工作。现将有关事项通知如下：

一、目标任务

依法查处互联网数据中心（IDC）业务、互联网接入服务（ISP）业务和内容分发网络（CDN）业务市场存在的无证经营、超范围经营、“层层转租”等违法行为，切实落实企业主体责任，加强经营许可和接入资源的管理，强化网络信息安全管理，维护公平有序的市场秩序，促进行业健康发展。

二、工作重点

（一）加强资质管理，查处非法经营

1. 各通信管理局要对本辖区内提供IDC、ISP、CDN业务的企业情况进行摸底调查，杜绝以下非法经营行为：

- （1）无证经营。即企业未取得相应的电信业务经营许可证，在当地擅自开展IDC、ISP、CDN等业务。
- （2）超地域范围经营。即企业持有相应的电信业务经营许可证，业务覆盖地域不包括本地区，却在当地部署IDC机房及服务器，开展ISP接入服务等。
- （3）超业务范围经营。即企业持有电信业务经营许可证，但超出许可的业务种类在当地开展IDC、ISP、CDN等业务。
- （4）转租转让经营许可证。即持有相应的电信业务经营许可证的企业，以技术合作等名义向无证企业非法经营电信业务提供资质或资源等的违规行为。

2. 在《电信业务分类目录（2015年版）》实施前已持有IDC许可证的企业，若实际已开展互联网资源协作服务业务或CDN业务，应在2017年3月31日之前，向原发证机关书面承诺在2017年年底达到相关经营许可要求，并取得相应业务的电信经营许可证。

未按期承诺的，自2017年4月1日起，应严格按照其经营许可证规定的业务范围开展经营活动，不得经营未经许可的相关业务。未按承诺如期取得相应电信业务经营许可的，自2018年1月1日起，不得经营该业务。

（二）严格资源管理，杜绝违规使用

各基础电信企业、互联网网络接入服务企业对网络基础设施和IP地址、带宽等网络接入资源的使用情况进行全面自查，切实整改以下问题：

1. 网络接入资源管理不到位问题。各基础电信企业应加强线路资源管理，严格审核租用方资质和用途，不得向无相应电信业务经营许可的企业和个人提供用于经营IDC、ISP、CDN等业务的网络基础设施和IP地址、带宽等网络接入资源。
2. 违规自建或使用非法资源问题。IDC、ISP、CDN企业不得私自建设通信传输设施，不得使用无相应电信业务经营许可资质的单位或个人提供的网络基础设施和IP地址、带宽等网络接入资源。
3. 层层转租问题。IDC、ISP企业不得将其获取的IP地址、带宽等网络接入资源转租给其他企业，用于经营IDC、ISP等业务。
4. 违规开展跨境业务问题。未经电信主管部门批准，不得自行建立或租用专线（含虚拟专用网络VPN）等其他信道开展跨境经营活动。基础电信企业向用户出租的国际专线，应集中建立用户档案，向用户明确使用用途仅供其内部办公专用，不得用于连接境外的数据中心或业务平台开展电信业务经营活动。

（三）落实相关要求，夯实管理基础

贯彻落实《工业和信息化部关于进一步规范因特网数据中心（IDC）业务和因特网接入服务（ISP）业务市场准入工作的通告》（工信部电管函[2012]552号，以下简称《通告》）关于资金、人员、场地、设施、技术方案和信息安全管理的要求，强化事前、事中、事后全流程管理。

1. 2012年12月1日前取得IDC、ISP许可证的企业，应参照《通告》关于资金、人员、场地、设施、技术方案和信息安全管理等方面的要求，建设相关系统，通过评测，并完成系统对接工作。当前尚未达到相关要求的企业，应在2017年3月31日之前，向原发证机关书面承诺在2017年年底达到相关要求，通过评测，并完成系统对接工作。未按期承诺或者未按承诺如期通过评测完成系统对接工作的，各通信管理局应当督促相应企业整改。

其中，各相关企业应按照《关于切实做好互联网信息安全管理与系统建设与对接工作的通知》、《关于通报全国增值IDC/ISP企业互联网信息安全管理与系统对接情况的函》和《互联网信息安全管理与系统使用及运行管理办法（试行）》（工信厅网安〔2016〕135号）要求，按期完成互联网信息安全管理与系统建设、测评及系统对接工作。未按期完成的，企业2017年电信业务经营许可证年检不予通过。

2. 新申请IDC（互联网资源协作服务）业务经营许可证的企业需建设ICP/IP地址/域名信息备案系统、企业接入资源管理平台、信息安全管理与系统，落实IDC机房运行安全和网络信息安全要求，并通过相关评测。
3. 新申请CDN业务经营许可证的企业需建设ICP/IP地址/域名信息备案系统、企业接入资源管理平台、信息安全管理与系统，落实网络信息安全要求，并通过相关评测。
4. 现有持证IDC企业申请扩大业务覆盖范围或在原业务覆盖范围新增机房、业务节点的，需要在新增范围内达到《通告》关于IDC机房运行安全和网络信息安全管理的要求，并通过相关评测。
5. 现有持证ISP（含网站接入）企业申请扩大业务覆盖范围的，需要在新增业务覆盖地区内达到《通告》关于网络信息安全管理的要求，并通过相关评测。
6. 现有持证CDN企业申请扩大业务覆盖范围或在原业务覆盖范围增加带宽、业务节点的，需要在新增范围内达到《通告》关于网络信息安全管理的要求，并通过相关评测。

三、保障措施

（一）政策宣贯引导，做好咨询服务

各通信管理局要利用各种方式做好政策宣贯和解读工作，公布电话受理相关举报和解答企业问题咨询，引导企业按照要求合法开展经营活动。中国信息通信研究院要做好相关评测支撑工作，协助部和各通信管理局做好政策宣贯、举报受理、企业问题解答等工作。

（二）全面开展自查，自觉清理整顿

各基础电信企业集团公司要组织下属企业全面自查，统一业务规程和相关要求，从合同约定、用途复查、违规问责等全流程加强规范管理，严防各类接入资源违规使用；对存在问题的要立即予以改正，并追究相关负责人责任。

各IDC、ISP、CDN企业要落实主体责任，按照本通知要求全面自查清理，及时纠正各类违规行为，确保经营资质合法合规，网络设施和线路资源使用规范，加强各项管理系统建设并通过评测。

（三）加强监督检查，严查违规行为

各通信管理局加强对企业落实情况的监督检查，发现违规问题要督促企业及时整改，对拒不整改的企业要依法严肃查处；情节严重的，应在年检工作中认定为年检不合格，将其行为依法列入企业不良信用记录，经营许可证到期时依法不予续期，并且基础电信企业在与其开展合作、提供接入服务时应当重点考虑其信用记录。部将结合信访举报、舆情反映等情况适时组织开展监督抽查。

（四）完善退出机制，做好善后工作

对未达到相关许可要求或被列入因存在违规行为被列入不良信用记录的企业，不得继续发展新用户。发证机关督促相关企业在此期间按照《电信业务经营许可管理办法》有关规定做好用户善后工作。向发证机关提交经营许可证注销申请的，发证机关应依法注销该企业的IDC、ISP经营许可证。

（五）完善信用管理，加强人员培训

积极发挥第三方机构优势，研究建立IDC/ISP/CDN企业信用评价机制，从基础设施、服务质量、网络和信息安全保障能力等多维度综合评定，引导企业重视自身信用状况、完善管理制度建设、规范市场经营行为。各通信管理局要加强对相关从业人员的技能培训，不断提高从业人员的业务素质和能力水平。

四、工作要求

（一）提高认识，加强组织领导

开展互联网网络接入服务市场规范清理工作是加强互联网行业管理和基础管理的重要内容，对夯实管理基础、促进行业健康有序发展具有重要意义。各相关单位要指定相关领导牵头负责，加强组织保障，抓好贯彻落实。

（二）分工协作，落实各方责任

各通信管理局、基础电信企业集团公司、互联网网络接入服务企业要落实责任，按照本通知要求，制定工作方案，明确任务分工、工作进度和责任，细化工作、责任到人，确保本次规范清理工作各项任务按期完成。

（三）加强沟通，定期总结通报

各通信管理局、各基础电信企业集团公司要加强沟通协作，及时总结工作经验，每季度末向部（信息通信管理局）报送工作进展情况，发生重大问题随时报部。部（信息通信管理局）将建立情况通报制度，并定期向社会公示规范清理工作进展情况。

四、四部门关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告

四部门关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告

为加强网络关键设备和网络安全专用产品安全管理，依据《中华人民共和国网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录（第一批）》，现予以公布，自印发之日起施行。

一、列入《网络关键设备和网络安全专用产品目录》的设备和产品，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。

具备资格的机构指国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室按照国家有关规定共同认定的机构。

二、网络关键设备和网络安全专用产品认证或者检测委托人，选择具备资格的机构进行安全认证或者安全检测。

三、网络关键设备、网络安全专用产品选择安全检测方式的，经安全检测符合要求后，由检测机构将网络关键设备、网络安全专用产品检测结果（含本公告发布之前已经本机构安全检测符合要求、且在有效期内的设备与产品）依照相关规定分别报工业和信息化部、公安部。

选择安全认证方式的，经安全认证合格后，由认证机构将认证结果（含本公告发布之前已经本机构安全认证合格、且在有效期内的设备与产品）依照相关规定报国家认证认可监督管理委员会。

国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一发布。

特此公告。

附：网络关键设备和网络安全专用产品目录（第一批）

	设备或产品类别	范围
网络关键设备	1.路由器	整系统吞吐量（双向）≥12Tbps 整系统路由表容量≥55万条
-	2.交换机	整系统吞吐量（双向）≥30Tbps 整系统包转发率≥10Gpps
-	3.服务器（机架式）	CPU数量≥8个 单CPU内核数≥14个 内存容量≥256GB
-	4.可编程逻辑控制器（PLC设备）	控制器指令执行时间≤0.08微秒
网络安全专用产品	5.数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1小时
-	6.防火墙（硬件）	整机吞吐量≥80Gbps 最大并发连接数≥300万 每秒新建连接数≥25万
-	7.WEB应用防火墙（WAF）	整机应用吞吐量≥6Gbps 最大HTTP并发连接数≥200万
-	8.入侵检测系统（IDS）	满检速率≥15Gbps 最大并发连接数≥500万
-	9.入侵防御系统（IPS）	满检速率≥20Gbps 最大并发连接数≥500万
-	10.安全隔离与信息交换产品（网闸）	吞吐量≥1Gbps 系统延时≤5ms
-	11.反垃圾邮件产品	连接处理速率（连接/秒）>100 平均延迟时间<100ms
-	12.网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5万条/秒
-	13.网络脆弱性扫描产品	最大并行扫描IP数量≥60个
-	14.安全数据库系统	TPC-EtpsE（每秒可交易数量）≥4500个
-	15.网站恢复产品（硬件）	恢复时间≤2ms 站点的最长路径≥10级

国家互联网信息办公室 工业和信息化部

公安部 国家认证认可监督管理委员会

2017年6月1日

百度智能云账号注销协议

在您正式发起百度智能云账号注销程序前，请您务必认真阅读、充分理解本《百度智能云账号注销协议》内容。如您对本协议条款有任何疑问，请向我方咨询（客服电话：400-920-8999）。

【特别提示】当您按照注销页面提示开始填写信息，即表示您已充分阅读、理解并接受本协议的全部内容。阅读本协议的过程中，如果您不同意任何条款或条件约定，您有权立即停止账户注销程序。

一、协议主体、内容与生效

1.1 本协议是特定百度智能云账号的账号持有人（“您”）与北京百度网讯科技有限公司（“我方”）之间，就解除双方之前达成的《百度智能云用户服务协议》（“用户服务协议”）、《百度智能云线上订购协议》及相关事宜，所达成的一致条款。

1.2 本协议为附生效条件的协议。在您向我方提交账号注销申请后，我方将按照注销提示的相关说明，对您账号的相关情况进行逐一核查，通过核查确认您符合如下账号注销条件的，本协议即可生效：

1) 账号不存在诸如以下未完成的订单、服务：

- 账号本月有账期未出账
- 账号有资源运行未删除
- 账号有未完成订单
- 账号存在提现过程中未到账的金额

2) 账号不存在现金余额、返点余额，且不存在以下任何拖欠或者未缴纳的款项：

- 账号有欠款
- 账号账期未还
- 账号未确认入账金额
- 账号有欠票

3) 账号不存在企业组织关系。

二、账号注销的程序

我们在此善意提醒，账号一旦注销后，我们将无法协助您找回，请您备份好账号下所有业务信息后谨慎操作。您注销账户后，除满足《网络安全法》对于数据留存的强制性要求外，我们将在相关行为的诉讼时效届满后，对您的个人信息予以删除或匿名化处理。

2.1 按照注销页面提示，发起账号注销。

2.2 您发起账户注销之时起，系统将启动自动核查机制，该机制无法强行中止，如通过自动核查，且法律法规无相反规定的，账号将自动删除。

2.3 系统自动核查中，如发现相关账号下存在未完成的订单、服务，或其他不符合注销条件的，系统将提示错误信息，账号注销程序将自动中止，且不会自动恢复。如果您希望继续注销的，请您按照提示完成相关操作，符合注销条件后请您重新发起账号注销。

2.4 账号注销期间，如果我方发现您的百度智能云账号被他人投诉、被国家机关调查或者正处于诉讼、仲裁程序中，我方有权自行终止您账号注销进程而无需另行得到您的同意。

2.5 账号注销过程需要一定时间，请您耐心等待。

三、账号注销的后果

3.1 账号注销意味着账号协议及该账号下所有服务条款、协议、合同等一并解除，将对您造成如下后果：

3.1.1 您将无法再次登录百度智能云网站、论坛、APP等；

3.1.2 您将无法访问控制面板或云站点控制面板；

3.1.3 您将无法进行依赖于账号权限进行的其他操作；

3.1.4 您将无法找回该账号下的个人信息、交易记录、业务数据、历史信息等。

提示：账号注销并不代表您在该账号注销前的所有账号行为和相关责任得到豁免或减轻。

3.2 账号注销后，将对我方造成如下后果：

3.2.1 我方将无权继续收集、存储和使用您的个人信息和数据，但法律法规另有要求的情形除外，例如：为了税务合规而保留相应的发票信息等，因法律规定需要留存的个人信息，我们将妥善保管，不再将其应用于业务场景；

3.2.2 在遵守国家法律法规的前提下，我方有义务保障您在该账号下的所有数据在实现日常业务功能所涉及系统中不可被检索、访问；

3.2.3 我方不再负有向您提供与已注销账号相关的信息展示与披露、数据恢复与找回，或提供其他服务的义务。

提示：账号注销不影响我方在政府主管机关要求或其他合法场景下，依法确认该账号注销前的用户真实身份等相关义务的履行。

3.3 账号注销后，经过一定的注销保护期后，任何第三方均可使用同一用户名发起注册申请。账号新注册成功后，新的账号持有人对账号注销前的所有账户下行为不承担任何责任。若新旧账号持有人之间发生任何纠纷，由双方自行解决。

四、附则

4.1 您理解并接受，本协议的订立、执行和解释及争议的解决均应适用中华人民共和国法律，与法律规定不一致或存在冲突的，该不一致或冲突条款不具有法律约束力。

4.2 就本协议内容或其执行发生任何争议，双方应进行友好协商；协商不成时，任一方均可向我方所在地有管辖权的人民法院提起诉讼。

4.3 本协议如果与双方以前签署的有关条款或者我方的有关陈述不一致或者相抵触的，以本协议约定为准。

您在此再次保证已经完全阅读并理解了上述账号注销协议，并自愿正式进入账号注销的后续流程，接受上述条款的约束。

百度智能云账号实名认证相关协议

百度智能云主、子关联账户实名认证授权协议

《百度智能云主、子关联账户实名认证授权》(以下简称“本授权”)用户(以下简称“您”)提交给北京百度网讯科技有限公司(以下简称“百度智能云”或“我们”)的有效授权。本授权旨在解决您的子账户独立于您企业组织后可继续使用百度智能云的服务的问题。

根据本授权书，您确认子账户与您企业账户解除绑定关系后、子账户自行更新实名认证信息之前，该账户下的行为依旧由您(授权主体)承担法律责任或连带法律责任，您授权该子账户仍使用您的实名认证信息，直至其完成实名认证信息的更新并通过百度智能云实名审核。

本授权之效力、解释、变更、执行与争议解决均适用中华人民共和国法律。

接受账号主体变更协议

在您正式接受账号主体变更申请前，请您务必认真阅读本协议。本协议将通过加粗或加下划线的形式提示您特别关注对您的权利及义务将产生重要影响的相应条款。如果您对本协议的条款有疑问的，请向百度智能云咨询，如果您不同意本协议的内容，或者无法准确理解百度智能云对条款的解释，请不要进行后续操作。

当您通过网络页面直接确认、接受引用本页面链接及提示遵守内容、签署书面协议、以及百度智能云认可的其他方式，或以其他法律法规或惯例认可的方式选择接受本协议，即表示您与百度智能云已达成协议，并同意接受本协议的全部约定内容。自本协议约定的生效之日起，本协议对您具有法律约束力。

请您务必在接受本协议，且确信通过账号主体变更的操作，能够实现您所希望的目的，且您能够接受因本次变更行为的相关后果与责任后，再进行后续操作。

一、协议主体、内容与生效

1.1 本协议是特定百度智能云账号的账号持有人(“您”、“新主体”)与北京百度网讯科技有限公司(“百度智能云”)之间，就您

接受该账号的原持有人（“原主体”）将其与百度智能云之前就本次申请主体变更的百度智能云账号所达成的《百度智能云用户服务协议》的权利义务转让给您，及相关事宜所达成的一致条款。

1.2 您确认并认可，在确认本协议前：

1.2.1 您已经认真阅读《百度智能云用户服务协议》、《百度智能云线上订购协议》、《信息安全》及《隐私政策》的内容，并确认同意接受上述协议的约束；

1.2.2 您知晓并同意原主体向百度智能云提交该账号的主体变更申请，且您已经对该账号下的全部产品、服务、资金、债务等（统称为“账号下资源”）及其他相关事项有确切认知，并接受在该等状态下成为该账号的新主体；

1.2.3 只有在您通过百度智能云实名认证后，本协议才正式生效；如果您未能通过百度智能云的实名认证或实名审核，则本次账号实名认证主体变更流程将终止，该账号仍为原主体持有。

1.3 您与原主体就账号下所有的产品、服务、资金、债权、债务等（统称为“账号下资源”）转让等相关事项，由您与原主体之间另外自行约定。但如果您与原主体之间的约定如与本协议约定冲突的，应优先适用本协议的约定。

二、定义和解释

2.1 “百度智能云官网”：是指包含域名为cloud.baidu.com的网站以及百度智能云客户端，如APP。

2.2 “百度智能云账号”：是指百度智能云分配给注册用户的数字ID，以下简称为“百度智能云账号”、“账号”。

2.3 “百度智能云账号持有人”，是指注册、持有并使用百度智能云账号的百度智能云会员。已完成实名认证的账号，除有相反证据外，百度智能云将根据用户的实名认证信息来确定账号持有人，如用户填写信息与实名认证主体信息不同的，以实名认证信息为准；未完成实名认证的账号，百度智能云将根据用户的填写信息，结合其他相关因素合理判断账号持有人。

2.4 “账号实名认证主体变更”：是指某一百度智能云账号的实名认证主体（原主体），变更为另一实名认证主体（新主体），本协议中简称为“账号主体变更”。

2.5 本协议下的“账号主体变更”程序、后果，仅适用于依据账号原主体申请发起、且被账号新主体接受的百度智能云账号实名认证主体变更情形。

三、变更的条件及程序

3.1 百度智能云仅接受符合以下条件下的账号主体变更申请；

3.1.1 由于原账号主体发生合并、分立、重组、解散、死亡等原因，需要进行账号主体变更的；

3.1.2 根据生效判决、裁定、裁决、决定等生效法律文书，需要账号主体变更的；

3.1.3 账号实际持有人与账号实名认证主体不一致，且提供了明确证明的；

3.1.4 根据法律法规规定，应当进行账号主体变更的；

3.1.5 百度智能云经过审慎判断，认为可以进行账号主体变更的其他情形。

3.2 您接受账号主体变更，应遵循如下程序要求：

3.2.1 您应在原主体发起变更申请前，完成本协议第1.2.1条、第1.2.2条的全部要求；

3.2.2 您应同意本协议的约定，接受本协议对您具有法律约束力；

3.2.3 您应按照百度智能云的要求完成实名认证流程，使百度智能云能够确认您的真实身份；

3.2.4 百度智能云有权通过手机号、人脸识别等进行二次验证、要求您出具授权证明（当您通过账号管理人接受变更申请时）、以及其他百度智能云认为有必要的材料，确认本次接受账号主体变更的行为确系您本人意愿；

3.2.5 您应遵守与账号主体变更相关的其他百度智能云规则、制度等的要求。

3.3 您理解并同意，

3.3.1 在您确认本协议后，完成实名认证前，您可以取消本次账号主体变更程序；

3.3.2 当您完成实名认证后，您的撤销或取消请求百度智能云将不予支持；

3.3.3 您并不会自动获得该账号的实际管理权，您还应自行与原主体完成管理权交接的相关操作。您和变更前的主体之间因实名认证主体变更而发生纠纷的，您应自行处理和承担后果，百度智能云不介入您和变更前主体之间的账号及权益纠纷的调处，百度智能云依据账号实名规则判断账号的控制权和权益归属。

3.4 您理解并同意，如果发现以下任一情形的，百度智能云有权随时终止账号主体变更程序或采取相应处理措施：

3.4.1 第三方对该账号发起投诉，且尚未处理完毕的；

3.4.2 该账号正处于国家主管部门的调查中；

3.4.3 该账号正处于诉讼、仲裁或其他法律程序中；

3.4.4 该账号下存在与百度智能云给予的信用政策、伙伴关系等与原主体身份关联的合作关系的；

3.4.5 存在其他可能损害国家、社会利益，或者损害百度智能云、百度或其他第三方权利的情形的；

3.4.6 该账号因存在频繁变更引起的账号纠纷或账号归属不明确的情形。

四、账号主体变更的后果

4.1 当您接受原主体提出的账号主体变更申请，且完成实名认证后，该账号主体将立即完成变更，会对您产生如下后果：

4.1.1 除本协议另有约定外，您将获得原主体在本账号的权益，权益包括但不限于账号控制权、账号下已开通的服务、账号下未消耗的充值金额等；同时本账号下的责任从原主体转移给您，责任包括但不限于清偿账号欠费、解决侵权纠纷等；

4.1.2 账号主体变更发起前本账号下已经消费金额，如百度智能云已向原主体开具发票，则不再向您开具发票；如有未向原主体开具的发票，且原主体未在变更发起前申请开具，变更完成后您可向百度智能云申请开具发票；变更处理期间该账号下如产生消费，该部分消费金额由您向百度智能云支付并申请开具发票。

4.1.3 如账号主体变更发起当日原主体有后付费资源消费，对应消费金额将优先从剩余的账户余额中扣除，但在发起变更当日无法开票，该部分消费金额会于次日在该账号下产生相应金额的可开票额度，您可向百度智能云申请开具发票。

4.1.4 如该账号在账号主体变更发起当月有月结资源的订阅和消费，则当月的月结资源对应消费金额暂时无法生成应付账单，该部分消费金额由您向百度智能云支付并申请开具开票。

4.1.5 该账号及该账号下的全部资源的归属权将全部转由您拥有。但百度智能云有权终止，原主体通过该账号与百度智能云另行达成的关于优惠政策、信控、伙伴合作等相关事项的合作协议，或与其他百度智能云账号之间存在的关联关系等；

4.1.6 百度智能云不接受您以与原主体之间的协议为由或以其他理由，要求将该账号下一项或多项业务、权益转移给其他账号的要求；

4.1.7 百度智能云有权拒绝您以和原主体之间存在纠纷为由或以其他理由，要求撤销本次账号主体变更的请求。

4.2 您理解并确认，账号主体变更并不代表您仅对主体变更之后该账号下的所有行为和责任承担责任，您还应对该账号主体变更前该账号下发生的所有行为及后果，承担连带责任，例如您须对原主体在本账号下的欠费予以清偿。

4.3 原主体在开始实名认证主体变更操作时未关闭的百度智能云服务、未提现的资金均视为一并转移给您，您应自行核实您已经做好技术准备并具有相应的资质使用该等服务，且已跟原主体之间明确资金归属。百度智能云在此特别提醒您，在实名认证变更成功后，您应立即对账号原登录方式进行清理或变更，确保账号为您完全管控，避免原主体继续登录操作您的账号；若您对账号资金进行提现，应注意提前查询和核对资金退回路径，以免某些资金因按照其充值路径原路退回而脱离您的控制，请您特别关注资金安全，避免发生纠纷和资损；进一步地，您应第一时间核实本账号下已经开通的百度智能云服务，确保所有开通服务为您实际所需或关闭您不需要的服务。

五、双方权利与义务

5.1 您应承诺并保证，

5.1.1 您在账号主体变更流程中所填写的内容及提交的资料均真实、准确、有效，且不存在任何误导或可能误导百度智能云同

意接受该项账号主体变更申请的行为；

5.1.2 您不存在利用百度智能云的账号主体变更服务进行任何违反法律、法规、部门规章和国家政策等，或侵害任何第三方权利的行为；

5.1.3 您进行账号主体变更的操作不会置百度智能云于违约或者违法的境地。因该账号主体变更行为而产生的任何纠纷、争议、损失、侵权、违约责任等，百度智能云不承担法律明确规定外的责任。

您进一步承诺，如上述原因给百度智能云造成损失的，您应向百度智能云承担相应赔偿责任。

5.2 您理解并同意，

5.2.1 百度智能云有权在您接受账号主体申请后的任一时刻，要求您提供书面材料或其他证明，证明您有权进行变更账号主体的操作；

5.2.2 百度智能云有权依据自己谨慎的判断来确定该次账号主体变更行为是否符合法律法规或政策的规定及账号协议的约定，如存在违法违规或其他不适宜变更的情形的，百度智能云有权拒绝；

5.2.3 百度智能云有权记录账号实名认证主体变更前后的账号主体、交易流水、合同等相关信息，以遵守法律法规的规定，以及维护自身的合法权益；

5.2.4 如果您存在违反本协议第5.1条的行为的，百度智能云一经发现，有权直接终止账号主体变更流程，或者撤销已完成的账号主体变更操作，将账号主体恢复为没有进行变更前的状态。

六、附则

6.1 您理解并接受，本协议的订立、执行和解释及争议的解决均应适用中华人民共和国法律，与法律规定不一致或存在冲突的，该不一致或冲突条款不具有法律约束力。

6.2 就本协议内容或其执行发生任何争议，双方应进行友好协商；协商不成时，任一方均可向北京市海淀区人民法院提起诉讼。

6.3 本协议如果与双方以前签署的有关条款或者百度智能云的有关陈述不一致或者相抵触的，以本协议约定为准。

您在此再次保证已经完全阅读并理解了上述《接受账号主体变更协议》，并自愿正式进入账号主体变更的后续流程，接受上述条款的约束。

申请账号主体变更协议

在您正式提交账号主体变更申请前，请您务必认真阅读本协议。**本协议将通过加粗或加下划线的形式提示您特别关注对您的权利及义务将产生重要影响的相应条款。**如果您对本协议的条款有疑问的，请向百度智能云咨询，如果您不同意本协议的内容，或者无法准确理解百度智能云对条款的解释，请不要进行后续操作。

当您通过网络页面直接确认、接受引用本页面链接及提示遵守内容、签署书面协议、以及百度智能云认可的其他方式，或以其他法律法规或惯例认可的方式选择接受本协议，即表示您与百度智能云已达成协议，并同意接受本协议的全部约定内容。自本协议约定的生效之日起，本协议对您具有法律约束力。

请您务必在接受本协议，且确信通过账号主体变更的操作，能够实现您所希望的目的，且您能够接受因本次变更行为的相关后果与责任后，再进行后续操作。

一、协议主体、内容与生效

1.1 本协议是特定百度智能云账号的账号持有人（“您”、“原主体”）与百度智能云之间，就您申请将双方之前就本次申请主体变更的百度智能云账号所达成的《百度智能云用户服务协议》的权利义务转让给第三方，及相关事宜所达成的一致条款。

1.2 **本协议为附生效条件的协议，仅在以下三个条件同时满足的情况下，才对您及百度智能云产生法律效力：**

1.2.1 您所申请变更的百度智能云账号已完成了实名认证，且您为该实名认证主体；

1.2.2 百度智能云审核且同意您的账号主体变更申请；

1.2.3 您申请将账号下权利义务转让给第三方（“新主体”），且其同意按照《接受账号主体变更协议》的约定，接受账号主体变更。

1.3 您与新主体就账号下所有的产品、服务、资金、债权、债务等（统称为“账号下资源”）转让等相关事项，由您与新主体之间另外自行约定。但如果您与新主体之间的约定如与本协议约定冲突的，应优先适用本协议的约定。

二、定义和解释

2.1 “百度智能云官网”：是指包含域名为cloud.baidu.com的网站以及百度智能云客户端，如APP。

2.2 “百度智能云账号”：是指百度智能云分配给注册用户的数字ID，以下简称为“百度智能云账号”、“账号”。

2.3 “百度智能云账号持有人”，是指注册、持有并使用百度智能云账号的用户。已完成实名认证的账号，除有相反证据外，百度智能云将根据用户的实名认证信息来确定账号持有人，如用户填写信息与实名认证主体信息不同的，以实名认证信息为准；未完成实名认证的账号，百度智能云将根据用户的填写信息，结合其他相关因素合理判断账号持有人。

2.4 “账号实名认证主体变更”：是指某百度智能云账号的实名认证主体（原主体），变更为另一实名认证主体（新主体），本协议中简称为“账号主体变更”。

2.5 本协议下的“账号主体变更”程序、后果，仅适用于依据账号原主体申请发起、且被账号新主体接受的百度智能云账号实名认证主体变更情形。

三、变更的条件及程序

3.1 百度智能云仅接受符合以下条件下的账号主体变更申请；

3.1.1 由于原账号主体发生合并、分立、重组、解散、死亡等原因，需要进行账号主体变更的；

3.1.2 根据生效判决、裁定、裁决、决定等生效法律文书，需要账号主体变更的；

3.1.3 账号实际持有人与账号实名认证主体不一致，且提供了明确证明的；

3.1.4 根据法律法规规定，应当进行账号主体变更的；

3.1.5 百度智能云经过审慎判断，认为可以进行账号主体变更的其他情形。

3.2 您发起账号主体变更，应遵循如下程序要求：

3.2.1 您应在申请变更的百度智能云账号下发起账号主体变更申请；

3.2.2 百度智能云有权通过手机号、人脸识别等进行二次验证、要求您出具授权证明（当您通过账号管理人发起变更申请时）、以及其他百度智能云认为有必要的材料，确认本次申请账号主体变更的行为确系您本人意愿；

3.2.3 您应同意本协议的约定，接受本协议对您具有法律约束力；

3.2.4 您应遵守与账号主体变更相关的其他百度智能云规则、制度等的要求。

3.3 您理解并同意，

3.3.1 在新主体确认接受且完成实名认证前，您可以撤回、取消本账号主体变更流程；

3.3.2 当新主体确认接受且完成实名认证后，您的撤销或取消请求百度智能云将不予支持；

3.3.3 且您有义务配合新主体完成账号管理权的转交。

3.3.4 在您进行实名认证主体变更期间，本账号下的登录和操作行为均视为您的行为，您应注意和承担账号的操作风险。

3.4 您理解并同意，如果发现以下任一情形的，百度智能云有权随时终止账号主体变更程序或采取相应处理措施：

3.4.1 第三方对该账号发起投诉，且尚未处理完毕的；

3.4.2 该账号正处于国家主管部门的调查中；

3.4.3 该账号正处于诉讼、仲裁或其他法律程序中；

3.4.4 该账号下存在百度智能云给予的信用政策、伙伴关系等与原主体身份关联的合作关系的；

3.4.5 存在其他可能损害国家、社会利益，或者损害百度智能云、百度或其他第三方权利的情形的；

3.4.6 该账号因存在频繁变更引起的账号纠纷或账号归属不明确的情形。

四、账号主体变更的后果

4.1 当您的账号主体变更申请经百度智能云同意，且新主体确认并完成实名认证后，该账号主体将完成变更，变更成功以百度智能云系统记录为准，变更成功后会对您产生如下后果：

4.1.1 您本账号下的权益转让给变更后的实名主体，权益包括不限于账号控制权、账号下已开通的服务、账号下未消耗的充值金额等（关于购买产品服务的消费明细以百度智能云系统数据为准）；

4.1.2 账号主体变更发起前您本账号下已经消费的金额，如百度智能云已向您开具发票，则不再向新主体开具发票；如有未向您开具的发票，且您未在变更发起前申请开具，百度智能云不再向您就该部分已消费金额开具发票，变更完成后由变更后的新主体可向百度智能云申请开具发票；变更处理期间该账号下如产生消费，该部分消费金额由变更后的新主体向百度智能云支付并申请开具发票。

4.1.3 如账号主体变更发起当日原主体有后付费资源消费，对应消费金额将优先从剩余的账户余额中扣除，但在发起变更当日无法开票，该部分消费金额会于次日在该账号下产生相应金额的可开票额度，由变更后的新主体向百度智能云申请开具发票。

4.1.4 如该账号在账号主体变更发起当月有月结资源的订阅和消费，则当月的月结资源对应消费金额暂时无法生成应付账单，该部分消费金额由新主体向百度智能云支付并申请开具开票。

4.1.5 该账号及该账号下的全部资源的归属权全部转由新主体拥有。但百度智能云有权终止，原主体通过该账号与百度智能云另行达成的关于优惠政策、信控、伙伴合作等相关事项的合作协议，或与其他百度智能云账号之间存在的关联关系等；

4.1.6 百度智能云不接受您以和新主体之间的协议为由或以其他理由，要求将该账号下一项或多项业务、权益转移给您指定的其他账号的要求；

4.1.7 百度智能云有权拒绝您以和新主体之间存在纠纷为由或以其他理由，要求撤销该账号主体变更的请求；

4.1.8 百度智能云有权在您与新主体之间就账号管理权发生争议或纠纷时，采取相应措施使得新主体获得该账号的实际管理权。

4.2 您理解并确认，账号主体变更并不代表您自变更完成之时起已对该账号下的所有行为和责任得到豁免或减轻：

4.2.1 您仍应对账号主体变更完成前，该账号下发生的所有行为承担责任，包括但不限于对主体变更完成前的欠费承担清偿责任；

4.2.2 您还需要对于变更之前已经产生，变更之后继续履行的合同及其他事项，对新主体在变更之后的履行行为及后果承担连带责任。

五、双方权利与义务

5.1 您应承诺并保证，

5.1.1 您在账号主体变更流程中所填写的内容及提交的资料均真实、准确、有效，且不存在任何误导或可能误导百度智能云同意接受该项账号主体变更申请的行为；

5.1.2 您不存在利用百度智能云的账号主体变更服务进行任何违反法律、法规、部门规章和国家政策等，或侵害任何第三方权利的行为；

5.1.3 您进行账号主体变更的操作不会置百度智能云于违约或者违法的境地。因该账号主体变更行为而产生的任何纠纷、争议、损失、侵权、违约责任等，百度智能云不承担法律明确规定外的责任。

您进一步承诺，如上述原因给百度智能云造成损失的，您应向百度智能云承担相应赔偿责任。

5.2 您理解并同意，

5.2.1 百度智能云有权在您发起申请后的任一时刻，要求您提供书面材料或其他证明，证明您有权进行变更账号主体的操作；

5.2.2 百度智能云有权依据自己谨慎的判断来确定您的申请是否符合法律法规或政策的规定及账号协议的约定，如存在违法违规或其他不适宜变更的情形的，百度智能云有权拒绝；

5.2.3 百度智能云有权记录账号实名认证主体变更前后的账号主体、交易流水、合同等相关信息，以遵守法律法规的规定，以及维护自身的合法权益；

5.2.4 如果您存在违反本协议第5.1条的行为的，百度智能云一经发现，有权直接终止账号主体变更流程，或者撤销已完成的账号主体变更操作，将账号主体恢复为没有进行变更前的状态。

六、附则

6.1 您理解并接受，本协议的订立、执行和解释及争议的解决均应适用中华人民共和国法律，与法律规定不一致或存在冲突的，该不一致或冲突条款不具有法律约束力。

6.2 就本协议内容或其执行发生任何争议，双方应进行友好协商；协商不成时，任一方均可向北京市海淀区人民法院提起诉讼。

6.3 本协议如果与双方以前签署的有关条款或者百度智能云的有关陈述不一致或者相抵触的，以本协议约定为准。

您在此再次保证已经完全阅读并理解了上述《申请账号主体变更协议》，并自愿正式进入账号主体变更的后续流程，接受上述条款的约束。

百度智能云学生身份验证功能服务用户协议

欢迎您使用北京百度网讯科技有限公司（以下简称“百度智能云”）精心打造的学生身份验证功能服务（以下简称“本服务”）。在享受本服务之前，请您务必仔细阅读并理解《百度智能云学生身份验证功能服务用户协议》（以下简称“本协议”）的各项条款。特别是那些免除或限制责任的条款（可能已以加粗形式提示），请您格外留意。只有充分阅读并接受本协议的全部内容，您才有资格使用本服务。任何对本服务的查看、设置或使用行为，均视为您已阅读并同意接受本协议的约束。

若您为完全民事行为能力人，请自行阅读并决定是否同意本协议；若您不具备完全民事行为能力，请在法定监护人的陪同下阅读并判断是否同意本协议。您和您的监护人均应依法承担因使用本服务而产生的相关后果。

一、协议适用范围

1.1 本服务专为中华人民共和国境内（不含港澳台地区）的普通高等学校在校学生，以及已被录取并确认即将入学的准在校生（以下简称“高校在校生”）提供。若您不属于此范畴，请立即停止使用本服务。

1.2 本协议是您与百度智能云之间关于本服务的约定，具有法律约束力。

1.3 本协议作为《百度智能云用户服务协议》的补充，与之共同构成完整的协议体系。同时，百度智能云可能发布的与本服务相关的其他协议、服务声明、业务规则及公告等（以下统称“专项规则”），一经发布即成为本协议不可分割的一部分，您亦需遵守。

二、术语定义

2.1 学生身份验证功能：指百度智能云基于用户授权，提供的高校学生身份验证、绑定及查询学生身份绑定状态等技术服务。

2.2 用户：指开通并使用百度智能云学生身份验证功能服务的个人，即“您”。

2.3 学生身份绑定状态：指用户通过本服务完成学生身份验证后，账号与学生身份之间形成的绑定关系状态。

三、服务内容

3.1 百度智能云提供本服务，旨在确认您的高校学生身份，使您能够享受百度智能云上各类开发者提供的专属学生服务及优惠活动。

3.2 为实现服务目的，百度智能云将提供功能界面供您填写实名信息（包括姓名和身份证号）、edu邮箱、学校、专业、预计毕业时间及层次。

3.3 为保障用户和相关方的权益，本服务下同一学生身份仅支持绑定一个账号。若您希望将学生身份与其他账号绑定，需先解除已绑定账号的绑定关系，并通过“人脸识别”验证身份。

3.4 您通过本服务完成的学生身份验证具有有效期限制，到期后已验证的学生身份将自动失效。百度智能云将在有效期到期前通知您，您可通过补充信息重新进行验证。

3.5 百度智能云将结合您提供的信息及授权使用的数据进行身份验证，并反馈验证结果。验证成功后，您的账号将自动与学生身份绑定。

四、用户权利义务

4.1 在使用本服务时，您需要向百度智能云提供或授权并及时更新必要的个人信息，并确保所提供的信息真实、准确、合法、有效。若您提供的信息不完整或不准确，可能导致您无法使用服务或在服务使用过程中受到限制。关于本服务处理个人信息的具体情况，请参见《百度智能云学生身份验证功能服务个人信息处理规则》。

4.2 您不得利用本服务侵犯任何第三方的合法权益，包括禁止盗用、冒用或非法使用他人学生身份信息。一旦百度智能云发现此类违规行为，为保护服务及信息安全，我们将保留采取限制服务或终止服务的权利。对于因您的违规行为而产生的任何法律后果，包括但不限于刑事责任、民事赔偿或行政处罚，您需自行负责，并赔偿因此给其他用户或百度智能云带来的所有损失。

4.3 您应明确并接受，本服务旨在为您提供更加高效、便捷的学生身份验证体验。但鉴于技术和数据的限制，百度智能云不能保证验证结果的完全无误，百度智能云不对验证结果的准确性作出任何明示或默示的声明或保证。

五、百度智能云权利义务

5.1 您应明确理解，本服务仅为信息技术服务。百度智能云基于您的授权将学生身份绑定状态提供给具体服务的开发者，以帮助您享受服务。相关服务及商品由对应的开发者提供，百度智能云不与其他开发者的经营活动，也不承担与服务、商品交易相关的义务或责任。

5.2 鉴于互联网的特殊性及技术的不断发展变化，百度智能云的免责事由包括但不限于：因台风、地震、洪水、雷电或恐怖袭击等不可抗力原因；用户的电脑软硬件和通信线路、供电线路出现故障的；因病毒、木马、恶意程序攻击、网络拥堵、系统不稳定、系统或设备故障、通讯故障、电力故障、银行原因、第三方服务瑕疵或政府行为等原因。国家法律法规或政策的颁布、调整、变更等；以及其他非因百度智能云过错而导致的情况。尽管有前款约定，百度智能云将采取合理行动积极促使服务恢复正常。

5.3 百度智能云目前免费提供本服务。若未来决定收费，百度智能云将依法提前进行合理通知，以确保您有权选择是否继续使用。若您不同意付费服务，应停止使用本服务。

六、个人信息保护

关于本服务处理个人信息的情况，请详细参阅《百度智能云学生身份验证功能服务个人信息处理规则》。

七、知识产权声明

百度智能云在此明确声明，对于本服务中提供的所有技术服务内容，包括但不限于网页、文字、图片、音视频等素材及信息，其知识产权均归百度智能云所有。未经百度智能云明确授权，任何单位或个人不得以任何形式复制、修改、传播、出售或用于其他商业目的。同时，百度智能云提供本服务所依赖的软件平台，其著作权、专利权及其他相关知识产权，除非另有明确说明，均归百度智能云或其相关权利方所有。百度智能云保留对上述知识产权的一切法律权利，包括但不限于追究侵权行为的法律责任。用户在使用本服务时，应尊重并遵守上述知识产权约定，不得进行任何侵犯百度智能云或其相关权利方知识产权的行为。如有违反，百度智能云将依法追究其法律责任。

八、其他

8.1 本协议的成立、生效、履行、解释及纠纷解决均适用中华人民共和国大陆地区的法律（不包括冲突法）。

8.2 本协议的签订地为中华人民共和国北京市海淀区。因本协议引起的或与本协议有关的任何争议，将由协议签订地有管辖权

的人民法院管辖。

8.3 百度智能云未行使或执行本服务协议任何权利或规定，不构成对前述权利或权利之放弃。

8.4 如本协议中的任何条款无论因何种原因完全或部分无效或不具有执行力，本协议的其余条款仍应有效并且有约束力。

8.5 您使用本服务即视为已阅读并同意接受本协议的约束。百度智能云有权对本协议进行修改。您可在相关服务页面查阅最新版本的协议条款。协议变更后，若您继续使用服务，则视为接受修改后的协议；若您不接受修改后的协议，应停止使用服务。

百度智能云学生身份验证功能服务个人信息处理规则

百度智能云学生身份验证功能服务（以下简称“本服务”）是北京百度网讯科技有限公司（以下亦简称“我们”或“百度智能云”）提供的信息服务产品。为说明在您使用本服务过程中我们会如何收集、使用和存储您的个人信息及您享有何种权利，我们将通过《百度智能云学生身份验证功能服务个人信息处理规则》（以下简称“本规则”）向您阐述相关事宜：

1. 我们收集、使用的信息
2. 信息的储存
3. 信息安全
4. 信息共享
5. 您的权利
6. 变更
7. 未成年人保护
8. 其他
9. 联系我们

1. 我们收集、使用的信息

在您使用本服务过程中，为实现本服务所必需，我们会按照如下方式收集、使用您的个人信息：

- 1.1 为证明您的学生身份，您需要填写您的**实名信息（姓名、身份证号码）、edu邮箱、学校、专业、预计毕业时间及层次**。
- 1.2 为了验证操作者是您本人，我们将采用“人脸识别”技术来完成验证。

2. 信息储存

2.1 信息存储的地点

原则上，我们在中华人民共和国境内收集和产生的个人信息，将存储在中华人民共和国境内。在以下情形下，您的个人信息可能会被转移到您使用产品或服务所在国家/地区的境外管辖区，或者受到来自这些管辖区的访问：

1. 适用的法律法规有明确规定；
2. 获得您的单独同意；
3. 为了履行与您订立的合同。

针对以上情形，我们会严格履行法律法规规定的义务，并按照本政策保护您的个人信息安全。

2.2 信息存储的期限

我们仅在为实现目的所必需的时间及法律、行政法规所规定的保存期限内保留您的个人信息。当您的学生身份失效，我们将删除您的学生身份验证功能服务相关信息。当我们的产品或服务停止运营时，我们将以推送通知、公告等形式通知您，并在合理的期限内删除您的学生身份验证功能相关个人信息或进行匿名化处理。

3. 信息安全

3.1 我们会以“最小化”原则收集、使用、存储和传输用户信息，并通过用户协议和隐私政策告知您相关信息的使用目的和范围。

3.2 我们非常重视信息安全。我们成立了专责团队负责研发和应用多种安全技术和程序等，我们会对安全管理负责人和关键安全岗位的人员进行安全背景审查，我们建立了完善的信息安全管理制度和内部安全事件处置机制等。我们会采取适当的符合业界标准的安全措施和技术手段存储和保护您的个人信息，以防止您的信息丢失、遭到被未经授权的访问、公开披露、使用、毁损、丢失或泄露。我们会采取一切合理可行的措施，保护您的个人信息。我们会使用加密技术确保数据的保密性；我们会使用受信赖的保护机制防止数据遭到恶意攻击。

3.3 我们会对员工进行数据安全的意识培养和安全能力的培训和考核，加强员工对于保护个人信息重要性的认识。我们会对处理个人信息的员工进行身份认证及权限控制，并会与接触您个人信息的员工、合作伙伴签署保密协议，明确岗位职责及行为准则，确保只有授权人员才可访问个人信息。若有违反保密协议的行为，会被立即终止与百度公司的合作关系，并会被追究相关法律责任，对接触个人信息人员在离岗时也提出了保密要求。

3.4 我们也请您理解，在互联网行业由于技术的限制和飞速发展以及可能存在的各种恶意攻击手段，即便我们竭尽所能加强安全措施，也不可能始终保证信息的百分之百安全。请您了解，您使用我们的产品和/或服务时所用的系统和通讯网络，有可能在我们控制之外的其他环节而出现安全问题。

3.5 根据我们的安全管理制度，个人信息泄露、毁损或丢失事件被列为最特大安全事件，一旦发生将启动公司最高级别的紧急预案，由安全部、公共事务部、法务部等多个部门组成联合应急响应小组处理。

4. 信息共享

我们可能将您的学生身份信息提供给合作方，以便合作方验证确认您的学生身份，使您可使用面向高校学生的相关服务、优惠活动等。

5. 您的权利

5.1 在您使用本服务期间，为了您可以更加便捷地查阅、复制、更正、删除您的个人信息，同时保障您撤回对个人信息处理的同意及停用本服务的权利，我们在产品设计中为您提供了相应的操作设置，具体操作方式您可以参考 [《百度智能云隐私政策》](#)。此外，我们还设置了意见反馈的渠道。

5.2 特别提示您，您对学生身份信息和与学生身份信息相关联的实名认证信息的修改、删除等，可能导致您无法使用学生身份购买和使用百度智能云的相关产品和服务。

5.3 我们可能会适时对本规则进行修订。当规则的条款发生重大变更时，我们会以推送通知、弹窗或其他符合法律要求的适当形式向您展示变更后的指引。

6. 未成年人保护

6.1 百度公司非常重视对未成年人信息的保护。

6.2 我们的产品和服务主要面向成年人。我们只会在受到法律法规允许、父母或其他监护人同意的情况下处理未成年的个人信息。

6.3 如您是未满14周岁的未成年人，在使用【百度智能云】产品和服务前，应请您的父母或其他监护人仔细阅读，或在您的父母或其他监护人的监护、指导下共同仔细阅读本隐私政策以及 [《百度儿童个人信息保护声明》](#)，并在征得您的父母或其他监护人同意的前提下使用我们的产品和服务，或向我们提供信息。

6.4 如果我们发现在未事先获得可证实的父母或其他监护人同意的情况下收集了未满14周岁的未成年人的个人信息，我们将会采取措施尽快删除相关信息。如果任何时候监护人有理由相信我们在未获监护人同意的情况下收集了未成年人的个人信息，请通过本隐私政策【联系方式】联系我们，我们会采取措施尽快删除相关数据。

7. 其他

我们将严格按照本规则及 [《百度智能云隐私政策》](#) 等政策中约定的方式处理您的个人信息以及保障您的信息安全，除非依照法

法律法规规定另行取得您的同意。若本规则与《[百度智能云隐私政策](#)》等政策存在矛盾，以本规则为准。

8. 联系我们

8.1 【百度智能云】的成长离不开各方用户达人的共同努力，我们非常感谢您对【百度智能云】数据更新、使用反馈方面的贡献。

8.2 您可以通过个人信息保护问题反馈平台 <http://help.baidu.com/personalinformation> 同我们联系。

8.3 您也可以通过如下联络方式同我们联系：

中国北京市海淀区上地十街10号

北京百度网讯科技有限公司法务部

邮政编码：100085

8.4 为保障我们高效处理您的问题并及时向您反馈，我们可能需要您提交身份证明、有效联系方式和书面请求及相关证据，我们会在验证您的身份后于15个工作日内及时处理您的请求。

8.5 如果您对我们的回复不满意，特别是您认为我们的个人信息处理行为损害了您的合法权益，您还可以通过向有关政府部门投诉或者司法部门起诉的方式寻求解决方案，例如向北京市海淀区人民法院提起诉讼。