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。**（实名制要求）**

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。**（网络身份认证）**

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。（应急预案、应急处置）**

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。 **（第三方服务要守法）**

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。**（禁止网络犯罪和支持协助犯罪）**

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。**（支持协助义务）**

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。 **（必须落实国家等级保护制度，突出保护重点）**

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。**（制定规划）**

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。 （三同步原则）**

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。**（非常态的网络产品和服务的**