**《中华人民共和国网络安全法》关于**

**网络安全等级保护制度的解读**

2015年6月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》。网络安全法草案于2015年7月6日至2015年8月5日在中国人大网上全文公布，并向社会公开征求意见。2016年11月7日，十二届全国人大常委会第二十四次会议经表决，通过了《中华人民共和国网络安全法》。2017年6月1日起正式施行。其中对网络安全等级保护制度作了明确规定。

**第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：**

**（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；**

**（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；**

**（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；**

**（四）采取数据分类、重要数据备份和加密等措施；**

**（五）法律、行政法规规定的其他义务。**

**条文解读：**

一、网络安全等级保护制度

网络安全等级保护制度是我国现行的网络安全领域的一项重要制度。1994年国务院制定的《计算机信息系统安全保护条例》规定: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。2007年公安部等部门制定的《信息安全等级保护管理办法》规定,信息系统的安全保护等级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,分为五级,从第一级至第五级的保护要求渐次提高,并规定了每个等级的范围、信息系统运营者的义务及应对措施等。公安部和标准化主管部门制定了相关标准,明确了网络安全等级定级标准、程序以及各个方面的具体要求。网络安全法总结实践经验,对该制度的名称作了调整,改为网络安全等级保护制度,对其主要内容作了规定。国务院有关部门将逐步完善相关配套规定,确保网络安全等级保护制度落到实处。

二、网络安全等级保护制度的主要内容

网络安全等级保护制度的主要内容可以分为技术类安全要求和管理类安全要求两大类。技术类安全要求主要从物理安全、网络安全、主机安全、应用安全和数据安全几层面提出,通过在信息系统中部署软硬件并正确配置其安全功能来实现;管理类安全要求主要从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出,通过控制各种角色的活动,从政策、制度、规范、流程以及记录等方面作出规定来实现。本条根据网络安全等级保护制度,对网络运营者的安全保护义务作了基本规定,主要包括以下几个方面:

1.制定内部安全管理制度和操作规程,确定网络安全负责人,落实网络安全保护责任。内部安全管理制度是网络运营者制定的有关网络安全管理组织架构、人员配备、行为规范、管理责任的规则；操作规程是网络运营者制定的有关人员在操作设备或办理业务时应当遵守的程序或者步骤。网络运营者应当依照法律、行政法规及网络安全等级保护制度的规定,制定内部安全管理制度和操作规程,细化并落实安全管理义务,根据不同保护等级设置安全管理机构、安全管理人员、安全主管、安全管理负责人等,并明确相关机构和人员的职责。安全管理制度和操作规程规定的每一项具体制度、每一个操作步骤都应当有具体的责任人,哪个环节出了责任事故都要有相应的人员负责。

2.采取防范危害网络安全行为的技术措施。网络运营者应当依照法律、行政法规及网络安全等级保护制度的规定,切实采取技术防范措施,从技术上防范计算病和网络攻击、网络侵入等网络安全风险。例如,安装防病毒软件,防范计算机病毒;安装网络身份认证系统、网络入侵检测系统、网络风险审计系统等,防范网络攻击、侵入；安装自动报警系统,当检测到安全风险时自动报警等。

3.配备相应的硬件和软件监测、记录网络运行状态、网络安全事件,按照规定留存相关网络日志。网络日志是对网络信息系统的用户访问、运行状态、系统维护等情况的记录,对于追溯非法操作、未经授权的访问,并维护网络安全以及调查网络违法犯罪活动具有重要作用。我国相关行政法规和标准对网络日志的留存及其期限作了规定，一些国家的法律也对留存网络日志作了规定。网络安全法根据维护网络安全的需要,借鉴有关国家的做法,对网络日志留存及留存的期限作了规定。同时,考虑到网络日志的种类较多,哪些需要按照本条规定留存不少于六个月,需要根据维护网络安全的实际来确定,因此,本条规定,网络运营者应当按照规定留存相关的网络日志不少于六个月。

4.采取数据分类、重要数据备份和加密等措施。数据分类就是按照某种标准,例如重要程度,对数据进行区分、归类。数据备份就是为防止系统故障或者其他安全事件导致数据丢失,而将数据从应用主机的硬盘或阵列复制、存储到其他存储介质。数据加密就是通过加密算法和密钥将明文数据转变为密文数据,从而实现数据的保密性。网络运营者应当依照本法和有关法律、行政法规以及网络安全等级保护制度的规定，采取数据分类、重要数据备份和加密措施，保护网络数据安全。

5.网络运营者的其他义务。除了本法规定的义务外，网络运营者还应当履行其他有关法律、行政法规规定的网络安全保护义务。