云南省网络与信息系统安全监察管理规定

（2004年11月7日云南省人民政府令130号公布　自2005年1月1日起施行。）

第一条　为了保护网络与信息系统安全，促进网络的应用和发展，根据《中华人民共和国计算机信息系统安全保护条例》和有关法律、法规，结合本省实际情况，特制定本规定。

第二条　县级以上人民政府领导和协调网络与信息系统安全工作。

县级以上公安机关主管本行政区域内网络与信息系统安全监察管理工作。

县级以上国家安全机关、国家保密工作部门、信息产业部门和其他有关部门，在各自职责范围内负责网络与信息系统安全管理的有关工作。

第三条　对网络与信息系统实行安全等级保护制度。

对下列单位涉及的基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全，实行重点保护:

（一）各级机关;

（二）银行、保险、证券等金融单位;

（三）邮政、电信单位;

（四）广播、电视、新闻出版单位;

（五）重点电力、煤炭、燃气、燃油等能源单位;

（六）航空、铁路和重点公路、水运等运输单位;

（七）水利及水源供给单位;

（八）重要物资储备单位;

（九）重点工程建设单位;

（十）大型工商、信息技术企业;

（十一）重点科研、教育机构;

（十二）医疗卫生、消防、紧急救援等社会应急服务机构;

（十三）需要实行重点保护的其他单位。

第四条　重点保护的网络与信息系统应当达到下列安全保护要求:

（一）机房及外部环境、设备及媒体的安全应当符合有关法律、法规、规章和标准的要求;

（二）具备风险分析、备份与恢复、容灾应急等信息运行安全保护措施;

（三）具有操作系统安全、数据库安全、网络安全、病毒防护、访问控制等信息安全保护措施和防范非法侵入、攻击网络与信息系统的安全保护措施;

（四）使用具有《计算机信息系统安全专用产品销售许可证》等行政许可证件的网络与信息系统安全专用产品;

（五）设置网络与信息系统安全管理机构或者配备专职或者兼职网络与信息系统安全员，具体负责网络与信息系统安全保护工作。

第五条　从事国际联网业务或者向公众提供上网服务的重点保护的网络与信息系统，除应当达到第四条规定的安全保护要求外，还应当达到下列安全保护要求:

（一）具有系统运行和用户使用日志记录保存 60 日以上的措施;

（二）具有记录用户主叫电话号码或者网络地址的措施;

（三）具有使用者身份登记和识别确认措施;

（四）具有垃圾邮件过滤、有害信息控制等安全防护措施;

（五）安装有国家规定的安全管理软硬件。

第六条　重点保护的网络与信息系统使用单位应当建立以下安全保护制度:

（一）计算机机房安全管理制度;

（二）安全管理责任人的任免和安全责任制度;

（三）网络安全漏洞检测和安全系统升级管理制度;

（四）操作权限管理制度;

（五）用户登记制度;

（六）信息发布的审查、登记、保存、清除和备份制度;

（七）信息群发服务管理制度。

第七条　重点保护的网络与信息系统配备的专职或者兼职网络与信息系统安全员应当取得国家认可的信息安全专业人员资格，未取得信息安全专业人员资格的，应当经过县级以上公安机关组织或者会同有关部门组织的专业培训，并考核合格。

网络与信息系统安全员实行年度专业考核制度。

第八条　网络与信息系统安全集成，由具有网络与信息系统安全集成能力的单位承担。

从事重点保护的网络与信息系统安全集成的单位应当取得国家有关部门认可的集成资质，并配备适应安全集成需要、掌握相关网络与信息系统安全标准的技术人员。

网络与信息系统安全集成单位应当向州（市）以上公安机关备案，并接受公安机关的监督检查。

第九条　安全集成单位在从事重点保护的网络与信息系统安全集成时，应当执行国家有关网络与信息系统安全保护的标准，在安全集成完成后及时将所有资料交网络与信息系统使用单位，并对安全集成系统的网络结构、配置以及在安全集成中获悉的国家秘密、商业秘密负有保密责任。禁止在安全集成的网络与信息系统中设置隐蔽信道。

第十条　重点保护的网络与信息系统在新建、改建、扩建之前，使用单位应当将安全措施方案报有管辖权的公安机

关备案。

第十一条　重点保护的网络与信息系统实行安全技术检测制度。安全技术检测执行有关国家标准和行业标准。经安全技术检测不符合安全要求的，应当进行整改。

重点保护的网络与信息系统应当在正式投入使用前进行首次安全技术检测；在本规定施行前已投入正式使用的，应当在本规定施行之日起6个月内完成首次安全技术检测。

重点保护的网络与信息系统在首次安全技术检测后，应当每年至少进行一次安全技术检测。

重点保护的网络与信息系统设备更新或者改造、网络结构变更，以及处理信息的种类、性质变更，对安全保护措施产生直接影响的，应当在投入运行前对受影响的部分进行安全技术检测。

重点保护以外的网络与信息系统应当加强安全技术检测，及时消除隐患。

第十二条　重点保护的网络与信息系统的使用单位发现危害网络与信息系统安全的隐患或者事故时，应当保留有关原始记录，并在24小时内向当地县级以上公安机关报告。公安机关发现危害网络与信息系统安全的隐患或者事故时，应当及时通知有关使用单位。

使用单位应当及时采取措施，消除、处理危害网络与信息系统安全的隐患或者事故。公安机关应当加强监督检查，

及时处理危害网络与信息系统安全的事件。

第十三条　网络与信息系统安全技术检测，由具有安全技术检测能力的单位承担。

从事重点保护的网络与信息系统安全技术检测的单位，应当经国家权威机构认可。因特殊情况自行完成安全技术检测的，应当具备开展计算机操作系统、数据库、网络、机房环境等安全检测的必要设备，配备适应安全技术检测需要、掌握网络与信息系统安全标准并经省级公安机关专业安全培训或者考核合格的技术人员。

网络与信息系统安全技术检测单位应当向州（市）以上公安机关备案，并接受公安机关的监督检查。

第十四条　安全技术检测单位对被检测单位网络与信息系统的检测内容、检测结果和所涉及的国家秘密、商业秘密等所有资料应当保密。禁止在所检测的网络与信息系统中设置隐蔽信道。

第十五条　从事网络与信息系统安全专用产品研究开发和从事计算机病毒等有害数据防治研究的单位，应当报省级公安机关备案。

第十六条　从事网吧等互联网上网服务营业场所经营活动的单位，应当按照《互联网上网服务营业场所管理条例》的规定及国家有关规定，履行信息网络安全职责，落实信息网络安全技术措施，接受公安机关和有关部门的监督管理。

第十七条　单位或者个人有下列行为之一的，由县级以上公安机关责令改正，给予警告或者对单位处15000元以下的罚款，对个人处5000元以下的罚款；构成犯罪的，依法追究刑事责任:

（一）非法侵入重点保护的网络与信息系统，修改、删除、增加、破坏网络与信息系统的功能、程序及数据的;

（二）制作、传播危害网络与信息系统安全的程序，或者恶意传授危害网络与信息系统安全的程序制作和使用等方法，造成网络与信息系统损害的;

（三）故意干扰网络与信息系统正常运行的;

（四）有其他危害网络与信息系统安全行为的。

第十八条　单位或者个人利用网络与信息系统实施下列行为之一的，由公安机关依法给予行政处罚；构成犯罪的，依法追究刑事责任:

（一）危害国家安全、破坏社会稳定、破坏民族团结、宣扬邪教、迷信的;

（二）宣传淫秽、赌博、暴力，实施诈骗活动，扰乱社会秩序，侵害他人合法权益的;

（三）法律、法规禁止的其他行为。

第十九条　重点保护的网络与信息系统使用单位有下列情形之一的，由县级以上公安机关责令限期改正，或者会同有关部门进行处理；逾期不改正的，对单位处1万元以下

的罚款，对直接负责的主管人员和其他直接责任人员可以处1000元以下的罚款；构成违纪的，依法给予行政处分或者纪律处分；构成犯罪的，依法追究刑事责任:

（一）未达到本规定第四条规定的网络与信息系统安全保护要求的;

（二）从事国际联网业务和向公众提供上网服务的网络与信息系统未达到本规定第四条和第五条规定的网络与信息系统安全保护要求的;

（三）未建立本规定第六条规定的安全保护制度的;

（四）未按规定进行网络与信息系统安全技术检测，或者经检测达不到安全要求而擅自使用的;

（五）发现危害网络与信息系统安全的隐患或者事故而隐瞒、缓报、谎报或者故意破坏原始记录的。

第二十条　网络与信息系统安全集成单位、安全技术检测单位在安全集成、安全技术检测活动中有下列情形之一的，由县级以上公安机关责令改正，对单位处3万元以下的罚款，对直接负责的主管人员和其他直接责任人员可以处5000元以下的罚款；构成犯罪的，依法追究刑事责任:

（一）不按照国家网络与信息系统安全标准进行安全集成或者安全技术检测，造成网络与信息系统损害的;

（二）故意在进行安全集成或者安全技术检测的网络与信息系统中设置隐蔽信道的;

（三）泄露安全集成系统的网络结构、配置或者在安全集成、安全技术检测过程中获取的其他国家秘密、商业秘密的；

（四）出具虚假安全集成、安全技术检测结果证明的。

第二十一条　国家机关工作人员在网络与信息系统安全监察管理工作中玩忽职守、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。

第二十二条　本规定自 2005 年 1 月 1 日起施行。