宁夏回族自治区人民代表大会
常务委员会公告

第六十二号

《宁夏回族自治区计算机信息系统安全保护条例》已由宁夏回族自治区第十届人民代表大会常务委员会第十一次会议于2009年7月31日通过，现予公布，自2009年10月1日起施行。

宁夏回族自治区人民代表大会常务委员会

二〇〇九年七月三十一日

宁夏回族自治区
计算机信息系统安全保护条例

（2009年7月31日宁夏回族自治区第十届人民代表大会常务委员会第十一次会议通过）

第一章　总　则

第一条　为加强计算机信息系统安全保护，促进计算机应用和信息化建设的健康发展，维护国家安全、社会公共利益和公民、法人及其他组织的合法权益，根据《中华人民共和国计算机信息系统安全保护条例》及有关法律、行政法规的规定，制定本条例。

第二条　自治区行政区域内对计算机信息系统的安全保护，适用本条例。

第三条　公安机关主管计算机信息系统的安全保护工作。

国家安全机关、保密行政管理部门、密码管理部门、信息化行政主管部门及其他有关部门，在各自职责范围内，依法负责计算机信息系统安全保护的相关工作。

第四条　计算机信息系统运营、使用单位，应当依法履行计算机信息系统安全保护义务。

任何组织或者个人，不得利用计算机信息系统从事危害国家利益、社会公共利益和公民、法人及其他组织的合法权益的活动，不得危害计算机信息系统的安全。

第二章　安全等级保护

第五条　计算机信息系统实行安全等级保护制度。

计算机信息系统安全等级保护坚持自主定级、自主保护原则，由运营、使用单位按照下列标准自主定级：

（一）计算机信息系统受到破坏后，可能对公民、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的，为第一级；

（二）计算机信息系统受到破坏后，可能对公民、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，但不损害国家安全的，为第二级；

（三）计算机信息系统受到破坏后，可能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的，为第三级；

（四）计算机信息系统受到破坏后，可能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的，为第四级；

（五）计算机信息系统受到破坏后，可能对国家安全造成特别严重损害的，为第五级。

第六条 计算机信息系统涉及国家安全、社会公共利益、重大经济建设信息的，其运营、使用单位或者主管部门应当选择符合法定条件的安全等级测评机构，对计算机信息系统安全等级状况进行测评，准确核定信息系统安全保护等级。

第七条 计算机信息系统运营、使用单位应当遵守下列规定：

（一）对计算机信息系统进行定级，并按照等级保护管理规范和技术标准实施保护；

（二）新建计算机信息系统的，在规划、设计阶段确定安全保护等级，同步建设符合该安全保护等级要求的信息安全保护设施，落实安全保护措施；

（三）按照计算机信息系统安全保护等级要求，使用取得国家销售许可证的信息安全专用技术产品；

（四）定期对本单位计算机信息系统的安全状况、保护制度和措施进行自查和整改；

（五）计算机信息系统确定为第二级以上保护等级的，应当制定重大突发事件应急处置预案；确定为第三级以上的，应当每年至少进行一次系统安全等级测评；

（六）指定专职人员负责本单位计算机信息系统的安全管理。专职人员应当通过设区的市以上公安机关、人力资源和社会保障部门的专业培训，并取得合格证。

第八条 第二级以上计算机信息系统运营、使用单位，应当自确定安全等级之日起三十日内，将信息系统保护的具体措施，向所在地设区的市以上公安机关报送备案；属于跨设区的市或者自治区统一联网的计算机信息系统，还应当向自治区公安机关报送备案。

计算机信息系统的结构、处理流程、服务内容等发生变化，致使安全保护等级发生变化，或者因实际需要公安机关要求重新定级的，计算机信息系统运营、使用单位应当重新定级、重新备案。

第九条 公安机关应当自收到备案材料之日起在十五个工作日内对报送备案的材料进行审查，对符合等级保护要求的，出具备案证明；对定级不准确或者保护措施不符合技术规范的，应当自收到备案材料之日起十五个工作日内书面通知报送单位予以纠正。

第十条 计算机信息系统运营、使用单位应当落实下列安全保护技术措施：

（一）重要数据库和系统主要设备的冗余或者备份；

（二）计算机病毒的防治；

（三）网络攻击的防范和追踪；

（四）网络安全事件的监测和记录；

（五）身份登记和识别确认；

（六）用户账号和网络地址的记录；

（七）安全审计和预警；

（八）系统运行和用户使用日志记录的保

存；

（九）信息群发的控制；

（十）有害信息、垃圾信息的防治；

（十一）法律、法规规定的其他技术保护措施。

鼓励计算机信息系统运营、使用单位采取先进的安全保护技术措施。

第三章　涉及国家秘密计算机信息系统管理

第十一条　涉及国家秘密计算机信息系统（以下简称涉密系统）应当依据涉密信息系统分级保护的管理规定和技术标准，按照秘密、机密、绝密三个等级的不同要求，实施分级保护。

涉密系统的安全保护水平，应当不低于计算机信息系统安全等级保护第三级以上的水平。

第十二条　涉密系统使用单位应当遵守下列规定：

（一）规划、设计和建设涉密系统时，应当按照国家保密标准配备设施和设备，同步设计和建设，同步运行；

（二）对已建成使用的涉密系统，定期进行安全保密性能测评；

（三）依法对涉密系统存储、处理和传输的信息，按照系统处理信息的最高密级确定保护等级和技术措施，并报保密行政管理部门备案。

第十三条　承担规划、设计、建设和维护涉密系统的单位，应当具有涉密集成资质。

涉密系统的安全保密设计方案和实施方案应当经过保密行政管理部门的审查。

第十四条　涉密系统投入使用前，建设使用单位应当向设区的市以上保密行政管理部门申请批准，非经保密行政管理部门批准的涉密系统不得投入使用。

设区的市以上保密行政管理部门应当自受理申请之日起二十日内，依据保密技术标准，对涉密系统进行审查。对不符合标准的，不予批准并提出书面整改意见，由使用单位进行整改后重新报批。

未经审查批准的涉密系统，不得存储、处理和传输涉密信息，不得与其他涉密系统互联。

第十五条　涉密系统使用单位应当根据实际需要采取下列保密防护措施：

（一）物理隔离；

（二）恶意代码的防护；

（三）身份鉴别和访问控制防护；

（四）涉密移动存储设备监管；

（五）密码保护；

（六）电磁泄漏发射防护；

（七）边界安全防护；

（八）其他需要的保密防护措施。

第十六条　涉密系统运营、使用单位采用密码进行等级保护的，应当执行国家密码管理的有关规定。

第四章　安全秩序

第十七条　任何单位或者个人不得利用计算机信息系统制作、传播、复制下列有害信息：

（一）危害国家统一、主权和领土完整的；

（二）泄露国家秘密、危害国家安全或者损害国家荣誉和利益的；

（三）煽动民族仇恨、民族歧视，或者故意侵害民族风俗、习惯，破坏民族团结的；

（四）煽动聚众滋事，损害社会公共利益的；

（五）散布谣言，扰乱社会秩序、破坏社会稳定的；

（六）宣扬邪教、封建迷信的；

（七）宣扬暴力、凶杀、恐怖、淫秽、色情、赌博的；

（八）教唆犯罪或者传授犯罪方法的；

（九）侮辱、诽谤、恐吓他人，侵害他人合法权益的；

（十）法律、法规禁止制作、传播、复制的其他信息。

第十八条　任何单位或者个人不得利用计

算机信息系统实施下列行为：

（一）未经允许，进入计算机信息系统或者非法占有、窃取、使用计算机信息系统资源；

（二）未经允许，对计算机信息系统的功能或者存储、处理、传输的数据和应用程序进行控制、删除、修改或者增加；

（三）故意制作、传播计算机病毒、恶意软件等破坏性程序；

（四）提供专门用于侵入、非法控制他人计算机信息系统的程序或者工具；

（五）窃取他人账号和密码，或者擅自向第三方公开他人账号和密码；

（六）非法截取、篡改、删除他人电子邮件或者其他数据资料；

（七）假冒他人名义发布、发送信息，或者以其他方式进行网络诈骗；

（八）擅自公开他人的信息资料；

（九）买卖法律、法规禁止流通的物品；

（十）非法提供虚假票据、证件；

（十一）其他危害国家、社会和他人合法权益的行为。

第十九条 提供互联网公共上网服务的单位，应当遵守下列规定：

（一）安装并运行国家规定的计算机信息安全管理系统；

（二）对上网人员进行实名登记并记录其上网信息，登记和记录的内容保存时间不少于六十日，在保存期内不得修改或者删除。

第二十条 互联网服务提供者应当自网络正式联通之日起三十日内，到所在地的设区的市以上公安机关备案，并应当将接入本网络系统的接入单位和用户数据资料及其变更情况备案。

互联网服务提供者应当对交互式服务栏目管理者的真实资料和信息发布者的注册信息进行登记，并对发布的信息进行审核。提供互联网接入、服务器托管、虚拟空间出租的单位，应当登记用户的真实资料。

第二十一条 生产、销售具有计算机信息网络远程控制、密码猜解、漏洞检测、信息群发等功能的产品和工具的单位，应当向设区的市以上公安机关备案。

第二十二条 互联网服务提供者和联网使用单位，应当落实互联网安全保护制度和技术措施，保障网络运行安全和信息安全，发现有本条例第十七条规定有害信息之一的，应当及时采取删除、停止传输、保存记录等技术措施，并报告公安机关；发现有危害国家安全的，同时报国家安全机关；发现有涉及泄露国家秘密的，同时报国家安全机关和保密行政管理部门；发现有本条例第十八条规定行为之一的，应当予以制止，并向公安机关举报。

公安机关和国家安全机关查处违法行为时，互联网服务提供者和联网使用单位应当如实提供有关数据文件、原始记录等信息资料。

第二十三条 互联网服务提供者和联网使用单位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，未经用户同意，不得公开、泄露用户注册信息。

第二十四条 计算机信息系统安全等级测评机构和从事计算机信息系统安全保护工作的人员，应当保守用户秘密，不得泄露用户信息，不得擅自占有、使用用户的信息资源。

第五章 安全管理

第二十五条 公安机关、国家安全机关、保密行政管理部门、密码管理部门及其他有关部门，应当依法对计算机信息系统运营、使用单位信息系统的安全保护工作进行监督检查；对发现的泄密、失密行为，应当依法查处。

实施监督检查时不得妨碍运营、使用单位的正常工作秩序。能够联合进行监督检查的，应当联合进行。

第二十六条 设区的市以上公安机关应当对第三级以上计算机信息系统的运营、使用单

位的信息安全等级保护工作情况定期进行检查。

设区的市以上公安机关应当对计算机信息系统安全等级测评工作进行监督管理。

第二十七条 保密行政管理部门应当对秘密级、机密级信息系统每年至少进行一次保密检查，每两年进行一次保密系统测评；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。

第二十八条 公安机关、国家安全机关和保密行政管理部门，发现计算机信息系统的安全保护、保密等级和安全措施不符合国家信息安全等级保护、保密管理规范和技术标准，或者存在安全隐患的，应当通知运营、使用单位限期进行整改。运营、使用单位应当按照整改通知书要求进行整改，并将整改情况向监管部门报告。

第二十九条 发生危及国家安全、公共安全及社会稳定的重大信息网络安全事故，计算机信息系统运营、使用单位应当立即报告公安机关和国家安全机关，并启动应急预案。公安机关可以对运营、使用单位采取二十四小时内停机检查、暂停联网、备份数据等应急措施。

第三十条 密码管理部门应当对计算机信息系统密码使用和管理的情况进行监督检查，发现存在安全隐患、违反密码管理有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。

第三十一条 公民、法人和其他组织发现有危害计算机信息系统安全违法行为的，有权向公安机关举报。公安机关应当公布接受举报电子邮箱、电话等，并为举报人保守秘密。

第六章 法律责任

第三十二条 计算机信息系统运营、使用单位以及互联网服务提供者和联网使用单位有违反本条例第十条、第二十条第二款规定行为之一的，对单位的主管负责人和其他直接责任人员可以处五千元以下罚款，对单位可以处五千元以上一万五千元以下罚款；不履行第七条、第八条、第二十条第一款、第二十二条和第二十三条规定的，由公安机关责令限期改正；逾期不改正的，给予警告；情节严重的，处以五日至三十日停止联网、停机整顿的处罚。

第三十三条 单位和个人违反本条例第十七条、第十八条规定的，由公安机关给予警告，责令限期改正，有违法所得的，没收违法所得，对个人可以并处以五千元以下罚款，对单位并处以五千元以上一万五千元以下罚款，情节严重的，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、审批机构吊销许可或者取消联网资格。

违反《中华人民共和国治安管理处罚法》和《中华人民共和国国家安全法》的，由公安机关和国家安全机关依法予以处罚；构成犯罪的，依法追究刑事责任。

第三十四条 提供互联网公共上网服务的单位违反本条例第十九条规定的，由公安机关给予警告，责令限期改正，逾期不改正的，处以五千元以上一万五千元以下的罚款；情节严重的，给予六个月以内的停止联网、停业整顿的处罚，并可以建议原许可机关吊销许可或者取消联网资格。

第三十五条 生产、销售或者提供含有计算机信息网络远程控制、密码猜解、漏洞检测、信息群发技术等功能的产品和工具的单位违反本条例第二十一条规定的，由公安机关给予警告，责令限期改正，处以五千元以上一万五千元以下罚款。

第三十六条 计算机信息系统安全等级测评机构和从事计算机信息系统安全保护工作的人员违反本条例第二十四条规定的，由公安机关处以三千元以上一万元以下罚款；给单位或者他人财产造成损失的，应当依法承担赔偿责任。

第三十七条 涉密系统使用单位违反本条例第十二条、第十四条第三款、第十五条规定的，由保密行政管理部门责令限期改正；逾期不改的，给予警告，并向其上级主管部门通报情况；情节严重的，建议对主管人员和其他直接责任人员给予处分；构成犯罪的，依法追究刑事责任。

第三十八条 公安机关、国家安全机关、保密行政管理等部门的工作人员有下列行为之一的，对直接负责的主管人员和其他直接责任人员给予处分；构成犯罪的，依法追究刑事责任：

（一）不履行监督检查职责，造成严重后果的；

（二）收到备案材料，不按照规定期限和要求办理的；

（三）接到举报，未依职责处理的；

（四）泄露计算机信息系统运营、使用单位或者个人的有关信息、资料及数据文件的；

（五）有其他徇私舞弊、滥用职权、玩忽职守行为的。

第七章 附 则

第三十九条 本条例下列用语的含义是：

（一）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。

（二）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。

（三）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。

第四十条 本条例自2009年10 月1日起施行。