

重庆市计算机信息系统安全保护条例

(1998年8月1日重庆市第一届人民代表大会常务委员会第十次会议通过, 2001年11月30日重庆市第一届人民代表大会常务委员会第三十七次会议第一次修正, 2006年9月27日重庆市第二届人民代表大会常务委员会第二十六次会议修订, 2010年7月23日重庆市第三届人民代表大会常务委员会第十八次会议第二次修正)

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,根据《中华人民共和国治安管理处罚法》和《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、法规的规定,结合本市实际,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,应当保障计算机及配套设备、设施(含网络)的安全,运行环境以及计算机信息的安全,确保计算机信息系统安全运行。

第四条 本市行政区域内计算机信息系统安全保护工作,适用本条例。

第五条 公安机关是计算机信息系统安全保护工作的主管部门,其主要职责是:

- (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)宣传计算机信息系统安全保护法规,组织培训安全保护人员;
- (四)对重要的计算机信息系统新建、改建、扩建工程方案进行安全指导;
- (五)指导对计算机病毒和其它有害数据的防治工作;
- (六)监督、检查、指导计算机信息系统等级保护工作;
- (七)监督计算机信息系统安全专用产品的制造、销售;

(八)对国际联网的计算机信息系统进行备案审查及安全管理;

(九)对重要的计算机信息系统进行监控;

(十)法律、法规规定的其他职责。

国家安全机关、国家保密机关及政府有关部门,在规定的职责范围内负责计算机信息系统的安全保护工作。

第六条 信息系统的运营、使用单位应当履行下列计算机信息系统安全保护职责:

- (一)遵守计算机信息系统安全保护的有关法律、法规;
- (二)建立健全计算机信息系统安全管理制度和落实责任制;
- (三)对管理人员和应用操作人员进行计算机安全教育;
- (四)落实计算机信息系统安全保护技术措施;
- (五)按照法律、法规的规定要求如实提供有关计算机信息系统安全保护工作所需的信息、资料和数据文件;
- (六)协助公安机关查处涉及计算机信息系统安全的违法犯罪案件;
- (七)建立信息安全事件的等级响应、处置制度;
- (八)法律、法规规定的其他应当履行的安全保护职责。

第七条 任何单位和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。

第八条 计算机信息系统实行安全等级保护。建设和应用计算机信息系统必须符合国家规定的标准。

第九条 重要的计算机信息系统使用单位,应配备

安全保护人员;对可能遭受的侵害和破坏,应制定应急处置预案。

计算机信息系统的安全保护人员应接受计算机安全培训,未经培训不得上岗。

第十条 计算机机房应符合国家标准和国家有关规定。

在计算机机房附近施工或者进行其他活动,不得危害计算机信息系统的安全。

第十一条 未经市公安局批准,任何单位和个人不得从事下列活动:

(一)收集和保存计算机病毒;

(二)制作、传播、销售有关计算机病毒机理及病毒程序的书刊资料和计算机信息媒体;

(三)公开发布计算机病毒疫情信息;

开展计算机病毒防治研究,须报市公安局备案。

第十二条 任何单位和个人不得制造或故意输入、传播计算机病毒或其他有害数据,不得违法复制、截收、删除、增加、修改、查阅计算机信息系统中的数据。

第十三条 对计算机信息系统中发生的违法案件、计算机病毒和危害社会公共安全的其他有害数据,有关使用单位和个人应在发现后二十四小时内向所在地县级以上公安机关报告,并保护现场及相关资料,公安机关应立即采取措施进行处理。

第十四条 进行国际联网的计算机信息系统,互联单位、接入单位和网络信息服务单位应在网络正式联通后三十日内向市公安局备案。

进行国际联网,必须使用国家规定的国际出入信道,不得自行建立或者使用其他通道。

第十五条 重要计算机信息系统的使用单位发现计算机信息系统出现安全问题,应及时处理,并报告公安机关。

公安机关发现影响计算机信息系统的安全隐患时,应及时向使用单位发出整改通知书,限期整改。

第十六条 公安机关计算机安全监察人员履行职责时,应不少于二人并出示执法身份证件。

第十七条 市公安局在紧急情况下,可以在本市范围内就涉及计算机信息系统安全的特定事项发布专项命令。

第十八条 违反本条例的规定,有下列行为之一的,由县级以上公安机关责令限期改正,拒不改正的,处一千元以上三千元以下罚款,可并处停机整顿:

(一)未落实计算机信息系统安全保护技术措施的;

(二)未建立计算机安全管理制度和落实责任制的;

(三)不按法律、法规规定向公安机关备案的;

(四)破坏计算机信息系统安全保护技术措施或妨碍其功能正常发挥的。

第十九条 有下列行为之一的,由县级以上公安机关给予警告或对个人处一千元以上五千元以下罚款,对单位处三千元以上一万五千元以下的罚款,并没收其违法所得和违法工具:

(一)违法收集和保存计算机病毒的;

(二)违法制作、传播、销售有关计算机病毒机理及病毒源程序的书刊资料和计算机信息媒体的;

(三)违法公开发布计算机病毒疫情消息的;

(四)制造、故意输入和传播计算机病毒或其他有害数据的;

(五)违法入侵计算机信息系统或违法复制、截收、删除、增加、修改、查阅计算机信息系统中的数据的;

(六)进行国际联网,不使用国家规定的国际出入信道,自行建立或者使用其他信道的。

有前款(四)、(五)项行为之一的,可按《中华人民共和国治安管理处罚法》的规定,并处五日以下拘留;情节严重的,并处五日以上十日以下拘留。

第二十条 有重大计算机安全隐患,公安机关要求限期整改,仍不改正的,对单位处五千元以上一万元以下罚款,可并处停机整顿;对单位负责人处一千元以上三千元以下罚款。

第二十一条 运输、携带、邮寄计算机信息媒体出境,不如实向海关申报的,由海关依照《中华人民共和国海关法》等法律、法规的规定处理。

第二十二条 违反本条例的规定,构成犯罪的,依法追究刑事责任。

第二十三条 当事人对公安机关依照本条例作出的具体行政行为不服的,可以依法申请行政复议或向人民法院提起行政诉讼。

第二十四条 执行本条例的人民警察利用职权,索贿受贿、徇私舞弊、玩忽职守,构成犯罪的,依法追究刑事责任;未构成犯罪的,由所在单位给予行政处分。

第二十五条 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。

有害数据,是指计算机信息系统及其存储介质中存在、出现的,以计算机程序、图像、文字、声音等多种形式表示的危害国家及社会公共安全的信息,宣扬封建迷信、淫秽色情、凶杀、教唆犯罪等危害社会治安秩序的信息,以及危害计算机信息系统运行功能发挥,应用软件、数据可靠性、完整性和保密性,用于违法活动

的计算机程序(含计算机病毒)。

计算机信息媒体,是指可存储、携带计算机程序、数据和信息的计算机硬磁盘、软磁盘、光盘、磁卡、磁带、纸带、卡片、打印纸等。

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的安全专用硬件和软件产品。

第二十六条 本条例自 2006 年 12 月 1 日起施行。