广东省计算机信息系统安全保护条例

（2007年12月20日广东省第十届人民代表大会常务委员会第三十六次会议通过　2007年12月20日公布　自2008年4月1日起施行）

第一章　总　则

第一条　为保护计算机信息系统安全，根据《中华人民共和国计算机信息系统安全保护条例》及有关法律法规，结合本省实际，制定本条例。

第二条　本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施构成的，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或者网络。

第三条　本条例适用于本省行政区域内计算机信息系统的安全保护。

第四条　计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施、网络的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第五条　县级以上人民政府公安机关主管本行政区域内计算机信息系统的安全保护工作。

县级以上人民政府国家安全机关、保密工作部门、密码管理部门和其他有关部门在各自职责范围内做好计算机信息系统的安全保护工作。

第六条 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活动，不得危害计算机信息系统的安全。

第二章 安全管理

第七条 计算机信息系统实行安全等级保护。

计算机信息系统安全等级保护按照国家规定的标准和要求，坚持自主定级、自主保护的原则。

第八条 计算机信息系统安全保护等级根据计算机信息系统在国家安全、经济建设、社会生活中的重要程度，计算机信息系统受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：

（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，或者可能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，或者可能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，或者可能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。

第九条 计算机信息系统规划、设计、建设和维护应当同步落实相应的安全措施，使用符合国家有关规定、满足计算机信息系统安全保护需求的信息技术产品。

第十条 计算机信息系统的运营、使用单位应当按照国家有关规定，建立、健全计算机信息系统安全管理制度，确定安全管理责任人，负责计算机信息系统的安全保护工作。

计算机信息系统信息服务提供者应当设立信息审查员，负责信息审查工作。

第十一条 第二级以上计算机信息系统的运营、使用单位应当建立安全保护组织，并报地级以上市人民政府公安机关备案。

第十二条 第二级以上计算机信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合国家规定的安全等级测评机构，依据国家规定的技术标准，对计算机信息系统安全等级状况开展等级测评，测评合格后方可投入使用。

第十三条 计算机信息系统的运营、使用单位及其主管部门应当按照国家规定定期对计算机信息系统开展安全等级测评，并

对计算机信息系统安全状况、安全管理制度及措施的落实情况进行自查。

计算机信息系统安全状况经测评或者自查，未达到安全等级保护要求的，运营、使用单位应当进行整改。

第十四条 第二级以上计算机信息系统，由运营、使用单位在投入运行后三十日内，到地级市以上人民政府公安机关备案。

第十五条 计算机信息系统备案后，对符合安全等级保护要求的，公安机关应当在收到备案材料之日起十个工作日内颁发计算机信息系统安全等级保护备案证明；对不符合安全等级保护要求的，应当在收到备案材料之日起十个工作日内通知备案单位予以纠正。

运营、使用单位或者其主管部门重新确定计算机信息系统等级的，应当按照本条例向公安机关重新备案。

第十六条 计算机信息系统的运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导，按照国家有关规定如实提供有关计算机信息系统安全保护的信息、资料及数据文件。

对计算机信息系统中发生的案件和重大安全事故，计算机信息系统的运营、使用单位应当在二十四小时内报告县级以上人民政府公安机关，并保留有关原始记录。

第十七条 第二级以上计算机信息系统的运营、使用单位应当制定重大突发事件应急处置预案。

第二级以上计算机信息系统发生重大突发事件，有关单位应当按照应急处置预案的要求采取相应的处置措施，并服从公安机关和国家指定的专门部门的调度。

第十八条 第二级以上计算机信息系统的运营、使用单位应当建立并执行下列安全管理制度:

（一）计算机机房安全管理制度;

（二）安全责任制度;

（三）网络安全漏洞检测和系统升级制度;

（四）系统安全风险管理和应急处置制度;

（五）操作权限管理制度;

（六）用户登记制度;

（七）重要设备、介质管理制度;

（八）信息发布审查、登记、保存、清除和备份制度;

（九）信息群发服务管理制度。

第十九条 第二级以上计算机信息系统的运营、使用单位应当采取下列安全保护技术措施:

（一）系统重要部分的冗余或者备份措施;

（二）计算机病毒防治措施;

（三）网络攻击防范和追踪措施;

（四）安全审计和预警措施;

（五）系统运行和用户使用日志记录保存六十日以上措施;

（六）记录用户账号、主叫电话号码和网络地址的措施;

（七）身份登记和识别确认措施；

（八）垃圾信息、有害信息防治措施；

（九）信息群发限制措施。

第二十条 涉密计算机信息系统应当依据国家信息安全等级保护的要求，按照国家有关涉密计算机信息系统分级保护的管理规定和技术标准，结合计算机信息系统实际情况进行保护。

第二十一条 涉密计算机信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密三个等级，并实行涉密计算机信息系统分级保护。

第二十二条 涉密计算机信息系统建设使用单位应当将涉密计算机信息系统定级和建设使用情况，及时报业务主管部门和负责系统审批的保密工作部门备案，并接受保密工作部门的监督、检查、指导。

第二十三条 涉密计算机信息系统投入使用前，应当按照国家有关规定报地级市以上人民政府保密工作部门审批，通过审批后方可投入使用。

第二十四条 计算机信息系统安全等级保护中密码的配备、使用和管理等，应当按照国家密码管理的有关规定执行。

第三章 安全秩序

第二十五条 任何单位和个人不得利用计算机信息系统制作、传播、复制下列信息：

（一）反对宪法确定的基本原则的；

（二）危害国家统一、主权和领土完整的；

（三）泄露国家秘密，危害国家安全或者损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结或者侵害民族风俗、习惯的；

（五）破坏国家宗教政策，宣扬邪教、迷信的；

（六）散布谣言，发布虚假信息，扰乱社会秩序，破坏社会稳定的；

（七）煽动聚众滋事，损害社会公共利益的；

（八）宣扬淫秽、色情、赌博、暴力、凶杀、恐怖的；

（九）教唆犯罪的；

（十）侮辱或者诽谤他人，侵害他人合法权益的；

（十一）其他法律法规禁止的内容。

第二十六条 任何单位和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、使用、窃取计算机信息系统资源；

（二）窃取、骗取、夺取计算机信息系统控制权；

（三）擅自向第三方公开他人电子邮箱地址和其他个人信息资料；

（四）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；

（五）假冒他人名义发送信息；

（六）未经允许，对计算机信息系统功能进行删除、修改、增加或者干扰；

（七）未经允许，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改或者增加；

（八）故意制作、传播计算机病毒、恶意软件等破坏性程序；

（九）危害计算机信息系统安全的其他行为。

第二十七条 任何单位和个人不得利用计算机信息系统非法传递或者交易涉及国家秘密的文件、资料和其他物品，不得将涉密计算机信息系统与国际互联网、其他公共信息网络相联接，不得利用非涉密计算机信息系统处理涉及国家秘密的信息。

第二十八条 提供互联网上网服务的场所应当安装国家规定的安全管理系统。

接入互联网的计算机信息系统的运营、使用单位和互联网服务单位采取的安全保护技术措施，应当具有符合公共安全行业技术标准的联网接口。

第二十九条 接入服务提供者、信息服务提供者以及数据中心服务提供者应当加强对本网络用户的安全宣传，落实安全保护措施，确保网络正常运行。发现有害信息应当保存有关记录，及时采取删除、停止传输等技术措施，同时报告公安机关，配合公安机关查处违法犯罪行为。

第三十条 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、信息群发技术的产品和工具的，应当报地级以上市人民政府公安机关备案。

第三十一条 计算机信息系统安全等级测评机构等安全服务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，不得擅自向第三方泄露用户信息，不得非法占有、使用用户的信息资源。

第四章 安全监督

第三十二条 公安机关、国家安全机关、保密工作部门、密码管理部门等有关部门应当按照国家规定，对计算机信息系统运营、使用单位的安全保护工作进行监督管理。

第三十三条 公安机关应当为公众提供计算机信息系统安全指导，加强安全动态分析，积极开展安全宣传，推动计算机信息系统安全保护能力的提高。

公安机关应当加强对计算机信息系统安全服务机构的指导，推动安全服务质量和技术水平的提高。

第三十四条 地级市以上人民政府公安机关、国家安全机关为保护计算机信息系统安全，在发生重大突发事件，危及国家安全、公共安全及社会稳定的紧急情况下，可以采取二十四小时内暂时停机、暂停联网、备份数据等措施。

第三十五条 地级市以上人民政府公安机关应当对第三级、

第四级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进行检查。对第三级计算机信息系统每年至少检查一次，对第四级计算机信息系统每半年至少检查一次。

对第五级计算机信息系统，应当由国家指定的专门部门进行检查。

第三十六条 公安机关发现计算机信息系统的安全保护等级和安全措施不符合国家信息安全等级保护管理规范和技术标准，或者存在安全隐患的，应当通知运营、使用单位进行整改。运营、使用单位应当按照整改通知要求进行整改，并将整改报告向公安机关备案。

第三十七条 地级市以上人民政府公安机关和人事部门应当组织计算机信息系统的运营、使用单位的安全保护组织成员、管理责任人、信息审查员参加信息安全专业技术培训。

第三十八条 保密工作部门依法对涉密计算机信息系统分级保护工作实施指导、监督和检查，具体负责下列工作：

（一）指导涉密计算机信息系统建设使用单位规范信息定密，合理确定系统保护等级；

（二）参与涉密计算机信息系统分级保护方案论证，指导建设使用单位做好保密设施的同步规划设计；

（三）依法对涉密计算机信息系统集成资质单位进行监督管理；

（四）按照国家规定进行系统测评和审批工作并监督检查涉

密计算机信息系统建设使用单位分级保护管理制度和技术措施的落实情况；

（五）按照国家规定定期对涉密计算机信息系统进行监督检查；

（六）了解各级各类涉密计算机信息系统的管理使用情况，查处各种违法行为和泄密事件。

第三十九条 密码管理部门应当对计算机信息系统安全保护工作中密码配备、使用和管理的情况进行检查和测评，发现存在安全隐患、违反密码管理相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。

第五章 法律责任

第四十条 违反本条例，有下列行为之一的，由公安机关责令限期改正，给予警告；逾期不改的，对单位的主管人员、其他直接责任人员可以处五千元以下罚款，对单位可以处一万五千元以下罚款：

（一）第二级以上计算机信息系统的运营、使用单位违反本条例第十一条规定，未建立安全保护组织的；

（二）第二级以上计算机信息系统的运营、使用单位违反本条例第十二条规定，计算机信息系统投入使用前未经符合国家规定的安全等级测评机构测评合格的；

（三）计算机信息系统的运营、使用单位未依照本条例第十

六条第一款规定如实提供有关计算机信息系统安全保护的信息、资料及数据文件的；

（四）第二级以上计算机信息系统的运营、使用单位违反本条例第十七条规定，在重大突发事件应急处置中不服从公安机关和国家指定的专门部门调度的；

（五）第二级以上计算机信息系统的运营、使用单位未依照本条例第十八条规定建立安全管理制度的；

（六）第二级以上计算机信息系统的运营、使用单位未依照本条例第十九条规定采取安全保护技术措施的；

（七）接入互联网的计算机信息系统的运营、使用单位和互联网服务单位违反本条例第二十八条第二款规定，采取的安全保护技术措施不具有符合公共安全行业技术标准的联网接口的；

（八）接入服务提供者、信息服务提供者以及数据中心服务提供者违反本条例第二十九条规定，发现有害信息不及时采取删除、停止传输等技术措施的；

（九）含有计算机信息网络远程控制、密码猜解、漏洞检测、信息群发技术的产品和工具的生产者、销售者或者提供者违反本条例第三十条规定，没有向地级以上市人民政府公安机关备案的。

前款第（一）项至第（八）项行为，有违法所得的，没收违法所得；情节严重的，并给予六个月以内的停止联网、停机整顿的处罚；必要时公安机关可以建议原许可机构撤销许可或者取消联网资格。

第四十一条 违反本条例第二十五条、第二十六条第（一）项、第（二）项、第（五）项、第（六）项、第（七）项、第（八）项、第（九）项规定的，违反第二十六条第（三）项、第（四）项规定窃取他人账号和密码、以营利或者非正当使用为目的擅自向第三方公开他人电子邮箱地址和其他个人信息资料、以非正当使用为目的擅自向第三方公开他人账号和密码的，由公安机关给予警告，有违法所得的，没收违法所得；对个人可以并处五千元以下罚款，对单位可以并处一万五千元以下罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚；必要时公安机关可以建议原许可机构撤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》的，依法予以处罚；构成犯罪的，依法追究刑事责任。

第四十二条 计算机信息系统的运营、使用单位违反本条例第十四条规定，没有向地级市以上人民政府公安机关备案的，或者违反本条例第三十六条规定，接到公安机关要求整改的通知后拒不按要求整改的，由公安机关处以警告或者停机整顿。

第四十三条 违反本条例第二十二条、第二十三条、第二十四条、第二十七条和其他有关保密管理和密码管理规定的，由保密工作部门或者密码管理部门按照职责分工责令限期改正；逾期不改的，给予警告，并向其上级主管部门通报情况，建议对其主管人员和其他直接责任人员予以处理；构成犯罪的，依法追究刑事责任。

第四十四条 公安机关、保密工作部门、密码管理部门和政府其他有关部门及其工作人员有下列行为之一的，对主管人员、其他直接责任人员，或者有关工作人员给予处分；构成犯罪的，依法追究刑事责任：

（一）利用职权索取、收受贿赂，或者玩忽职守、滥用职权的；

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

（三）其他不履行法定职责的。

第六章 附 则

第四十五条 本条例所称的安全等级测评，是指对计算机信息系统的安全状况进行测试、评价、判断。

本条例所称的安全服务，是指从事计算机信息系统安全设计、建设、检测、维护、监理、咨询、培训等业务。

本条例所称的重大突发事件，是指有害信息大范围传播、大规模网络攻击、计算机病毒疫情等危害计算机信息系统安全的重大事件。

第四十六条 本条例自2008年4月1日起施行。