杭州市计算机信息网络安全保护管理条例

（2008年12月23日杭州市第十一届人民代表大会常务委员会第十二次会议通过　2009年4月1日浙江省第十一届人民代表大会常务委员会第十次会议批准　2009年4月9日杭州市第十一届人民代表大会常务委员会公告第17号公布　自2009年5月1日起施行）

第一章　总则

第一条　为加强计算机信息网络安全的保护和管理，维护国家安全、公共利益和社会稳定，维护公民、法人和其他组织的合法权益，促进信息化建设的健康发展，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《互联网信息服务管理办法》等规定，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网络，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制作、采集、加工、存储、传输、检索等处理的人机

系统和运行体系。

计算机信息网络的安全，包括计算机信息系统及互联网络的运行安全和信息内容的安全。

第三条　杭州市行政区域内的计算机信息网络安全保护与管理活动，适用本条例。对涉及国家秘密的计算机信息系统（以下简称涉密信息系统）实行分级保护制度，按照国家保密法律法规和保密标准管理。

第四条　计算机信息网络安全坚持“保护与管理并重”和“谁主管、谁负责，谁运营、谁负责”的原则。

第五条　市公安局根据本条例规定主管全市计算机信息网络安全保护管理工作。市公安局公共信息网络安全监察分局具体负责全市计算机信息网络安全保护管理工作。

各县（市）公安局和萧山区、余杭区公安分局负责本行政区域范围内计算机信息网络安全保护管理工作。

国家安全机关、保密工作部门、密码管理部门、信息化行政主管部门、互联网新闻信息服务管理部门及其他有关行政主管部门，负责各自职责范围内的计算机信息网络安全保护管理工作。

第六条　单位和个人依法使用计算机信息网络的权利，受法律、法规和本条例保护。

任何单位和个人不得利用计算机信息网络从事危害国家安全、公共利益及社会秩序以及侵犯公民、法人和其他组织合法权益的

活动，不得危害计算机信息网络的安全。

第二章　安全保护和管理

第七条　计算机信息系统实行安全等级保护制度。

计算机信息系统的安全保护等级分为五个等级。等级确定的原则、标准、各级别安全保护和管理内容按照国家和省有关规定执行。

涉密信息系统应当根据国家等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护管理规定和技术标准，结合系统实际情况进行保护。

第八条　计算机信息系统的运营、使用单位作为安全等级保护的责任主体，应当按照国家有关管理规范、技术标准确定计算机信息系统的安全保护等级。对新建、改建、扩建的计算机信息系统，运营、使用单位应当在规划、设计阶段确定计算机信息系统的安全保护等级，并同步建设符合该安全保护等级要求的信息安全设施。

第九条　新建的第二级以上计算机信息系统，其运营、使用单位应当在系统投入运行后三十日内到市公安局办理备案手续。已运行的第二级以上计算机信息系统，其运营、使用单位应当在安全保护等级确定后三十日内到市公安局办理备案手续。

第十条　计算机信息系统运营、使用单位应当建立计算机信息系统安全状况日常检测工作制度。

计算机信息系统运营、使用单位应当按照国家有关管理规范和技术标准，定期对计算机信息系统安全等级状况开展等级测评，对计算机信息系统安全状况、安全保护制度及措施的落实情况进行自查。经测评或者自查，计算机信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

第十一条　计算机信息系统运营、使用单位应当建立并落实以下安全保护制度：

（一）安全责任制度和保密制度；

（二）核实、登记并及时更新用户注册信息制度；

（三）信息发布审核、登记、保存、清除和备份制度；

（四）信息网络安全教育和培训制度；

（五）信息网络安全应急处置制度；

（六）违法案件报告和协助查处制度；

（七）国家和省规定的其他安全保护制度。

第十二条　计算机信息系统运营、使用单位应当落实以下安全保护技术措施：

（一）系统重要数据备份、容灾恢复措施；

（二）计算机病毒等破坏性程序的防治措施；

（三）系统运行和用户使用日志备份并保存六十日以上的措

施；

（四）记录、监测网络运行状态和各种网络安全事件的安全审计措施；

（五）网络安全隔离以及防范网络入侵、攻击破坏等危害网络安全行为的措施；

（六）密钥、密码安全管理措施；

（七）国家和省规定的其他安全保护技术措施。

第十三条　计算机信息系统运营、使用单位应当制定重大突发事件应急处置预案。发生重大突发事件时，运营、使用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。

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。

第十四条　计算机信息系统中发生重大安全事故的，计算机信息系统运营、使用单位应当在二十四小时内向所在地公安机关报告，违反国家保密法规定泄露国家秘密的，应当向所在地保密工作部门报告，并保留有关原始记录。因计算机病毒等破坏性程序发生计算机信息系统瘫痪、程序和数据严重损坏等安全事故的，计算机信息系统运营、使用单位还应当向所在地公安机关提供计算机病毒等破坏性程序的样本。

公安机关、国家安全机关、保密工作部门对危害计算机信息网络安全和涉嫌违法犯罪的活动依法进行调查时，计算机信息系统运营、使用单位应当依法如实提供有关信息、资料及数据文件。

第十五条　计算机信息系统的规划、建设、运营和使用单位在计算机信息系统安全保护设施的规划、建设中，应当依照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定并满足计算机信息系统安全保护需求的信息安全产品。

第十六条　信息安全服务机构应当按照有关法律、法规和相关信息安全技术标准的规定提供信息安全服务，并保守计算机信息系统的技术秘密。

信息安全服务机构发现、掌握危害计算机信息网络安全的证据时，应当及时向所在地公安机关报告并提供所发现、掌握的计算机病毒等破坏性程序的样本。

第三章　公共秩序管理

第十七条　计算机信息系统运营、服务单位应当自网络联通之日起三十日内向所在地公安机关备案。

第十八条　互联网接入服务提供者及主机托管、租赁和虚拟空间租用等互联网数据中心服务提供者，应当建立并落实以下安全保护制度和安全保护技术措施：

（一）如实登记申请服务的用户基本情况、网络应用种类和范围以及身份证明，每月将用户登记情况及所分配的网络地址等有关情况报所在地公安机关备案；

（二）依法与用户签订服务协议，明确双方应当承担的信息安全法律责任；

（三）定期核查用户的网络应用种类和范围，发现用户的活动超出协议约定的应用种类和范围的，应当及时予以纠正；发现传输的内容明显属于本条例第二十三条规定情形的，应当立即停止传输违法内容，保存相关记录，并向所在地公安机关报告。

互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网网络地址或者域名、主叫电话号码等信息。

第十九条　互联网信息服务提供者应当建立信息审核制度，明确信息审核人员，发现属于本条例第二十三条规定情形信息的，应当立即删除违法内容，保存相关记录，并向所在地公安机关报告。涉及其他部门的，向有关主管部门报告。

互联网信息服务提供者应当建立并落实以下安全保护制度和安全保护技术措施：

（一）提供新闻、出版以及电子公告等服务的，能够记录所发布信息的内容、时间及互联网网络地址或者域名，并留存六十日以上；

（二）开办政务、新闻、重点商务网站的，能够防范网站、

网页被篡改，发现被篡改后能够立即恢复；

（三）提供电子公告、网络游戏和其他即时通信服务的，具有用户注册信息和发布信息审核功能，并如实登记向其申请开设上述服务的用户的有效身份证明；

（四）提供电子邮件和网上短信息服务的，具有信息群发限制措施，能够防范以群发方式发送伪造或者隐匿信息发送者真实标记的电子邮件或者短信息；

（五）提供电子公告服务或其他交互式信息服务的，其计算机信息网络应当使用固定的互联网网络地址。

前款所称的电子公告服务，是指在互联网上以论坛、聊天室、留言板、博客等交互形式为上网用户提供信息发布条件的行为。

第二十条　设立互联网上网服务营业场所的经营单位，应当在申领《网络文化经营许可证》之前到所在地公安机关申请信息网络安全审核。互联网上网服务营业场所经营单位变更营业场所或者对营业场所进行改建、扩建的，应当事先经原审核机关同意。

互联网上网服务营业场所经营单位变更名称、住所、法定代表人或者主要负责人、注册资本、网络地址或者终止经营活动的，应当依法到工商行政主管部门办理变更登记或者注销登记，并到文化行政部门、公安机关办理有关手续或者备案。

非经营性互联网上网服务提供单位应当自提供上网服务之日起十五日内向所在地公安机关备案，其法定代表人、营业场所、

网络地址等发生变更的，应当自变更之日起十五日内报原备案机关备案。

第二十一条　互联网上网服务提供单位应当建立并落实以下安全保护制度和安全保护技术措施：

（一）提供互联网上网服务的服务器应当使用固定的互联网网络地址；

（二）如实登记用户有效身份证明、上网时间等有关情况，登记记录应当保留六十日以上；

（三）安装具有防病毒、防入侵、防违法信息传播、记录上网用户日志等功能的安全保护技术设施，并保证其在线正常运行；

（四）发现法律、法规所禁止的行为和信息时，应当立即停止传播违法内容，保存有关日志和记录，并向所在地公安机关报告；

（五）提供无线接入服务的互联网上网服务场所，应当记录并留存用户信息及对应的计算机信息。

第二十二条　任何单位或者个人不得从事下列危害计算机信息网络安全和秩序的行为：

（一）擅自进入、使用他人计算机信息网络；

（二）擅自增加、修改、删除、复制他人计算机信息网络的数据；

（三）擅自增加、修改、删除、干扰他人计算机信息网络的

功能；

（四）破坏计算机信息网络运行环境、设备设施；

（五）窃取、盗用、篡改、破坏他人网络资源；

（六）故意制作、传播、使用计算机病毒、恶意软件等破坏性程序，或者制作、发布、复制、传播含破坏性程序或其机理、源程序的信息；

（七）故意阻塞、阻碍、中断计算机信息网络的信息传输，恶意占用网络资源；

（八）利用计算机信息网络大量或者多次发送电子邮件、短信息等，干扰他人正常生活秩序或者网络秩序；

（九）利用计算机信息网络违背他人意愿、冒用他人名义发布信息；

（十）明知本单位或本人的计算机信息网络的网络地址、主机空间等资源已被他人利用，从事可能危害计算机信息网络安全的活动而不予制止；

（十一）擅自利用计算机信息网络收集、使用、提供、买卖他人专有信息；

（十二）其他危害计算机信息网络安全和秩序的行为。

第二十三条　任何单位或者个人不得利用计算机信息网络制作、发布、传播含有下列内容的信息：

（一）反对宪法确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）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、封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）鼓动公众恶意评论他人、公开发布他人隐私或者通过暗示、影射等方式对他人进行人身攻击的；

（八）公然侮辱他人或者捏造事实诽谤他人的；

（九）以非法社团名义活动的；

（十）买卖法律、法规禁止流通的物品的；

（十一）非法买卖法律、法规限制流通的物品，对公共安全构成威胁的；

（十二）含有淫秽、色情、赌博、暴力、欺诈等内容，或者教唆犯罪、传授犯罪方法的；

（十三）含有法律、法规禁止的其他内容的。

第四章　监督管理

第二十四条　公安机关对计算机信息网络安全保护工作履行

以下监督管理职责：

（一）指导计算机信息系统运营、使用单位开展安全等级保护工作，接受第二级以上计算机信息系统的备案，并对其安全保护状况进行监督、检查；

（二）监督、检查、指导计算机信息系统运营、使用单位建立、落实各项安全保护制度和安全保护技术措施；

（三）依法对计算机信息网络中的公共信息服务实施监督、检查，发现公共信息中含有本条例第二十三条所列信息的，应当通知计算机信息系统运营、服务单位予以删除，必要时中止对发送者的网络服务；

（四）负责接受危害计算机信息网络安全的事件、案件的报告、举报，勘查现场并收集相关证据，提取疑似计算机病毒等破坏性程序的样本，依法查处计算机信息网络安全违法犯罪案件；

（五）向社会发布信息安全事件和计算机病毒疫情；

(六)与计算机信息网络安全保护工作相关的其他监督职责。公安机关发现计算机信息系统存在安全隐患，可能危及公共安全的，可以委托具有相应资质的测评机构进行测评。经测评发现存在安全问题的，计算机信息系统运营、使用单位应当立即予以整改。

第二十五条　公安机关、国家安全机关为保护计算机信息网络安全，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，可以对计算机信息系统运营、使用单位采取二十四小时内暂时停机、暂停联网、数据备份等措施。

第二十六条　公安机关应当组织计算机信息系统运营、使用单位的安全保护组织成员、管理责任人、信息审查员以及信息安全服务机构工作人员等从事计算机信息网络安全保护工作的人员参加计算机信息网络安全专业技术培训。

第二十七条　国家安全机关负责计算机信息网络国家安全事项管理工作，依法查处利用计算机信息网络危害国家安全的违法行为。

第二十八条　保密工作部门依法对有关计算机信息网络的保守国家秘密工作实施监督管理，并做好以下工作：

（一）指导、监督和检查涉密信息系统安全分级保护工作；

（二）指导涉密信息系统建设、使用单位规范信息定密，合理确定安全保护等级；

（三）参与涉密信息系统安全分级保护方案论证，指导涉密信息系统建设、使用单位做好保密设施的同步规划设计；

（四）指导涉密信息系统安全保护等级测评工作，监督、检查涉密信息系统安全分级保护管理制度和技术措施的落实情况；

（五）对涉密信息系统按照国家规定进行投入使用前审批，并对其管理使用情况进行检查；

（六）依法查处违反保密法律法规的行为。

第二十九条　密码管理部门应当加强对计算机信息系统内使用密码产品的单位的监督、检查和指导，定期对计算机信息系统安全等级保护工作中密码配备、使用和管理的情况进行检查和测评，同时对密码产品使用单位的操作人员和管理人员进行培训。

密码管理部门在监督检查过程中，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查处。

第三十条　信息化行政主管部门负责组织、协调和指导计算机信息网络安全工作，组织信息网络安全技术、设备和产品的监督管理，组织、指导和管理计算机病毒防范工作，并根据信息安全发展形势和信息安全保障要求，组织有关部门编制全市信息安全保障规划，报市政府批准后实施。

第三十一条　互联网新闻信息服务管理部门负责指导、协调互联网新闻信息管理工作，协调处理计算机信息网络传播违法新闻信息的行为。

第五章　法律责任

第三十二条　计算机信息系统运营、使用单位违反本条例第八条规定，未建立计算机信息系统安全保护等级的，由公安机关给予警告，责令其限期改正；逾期不改正的，处以一千元以上五

千元以下的罚款；情节严重的，给予六个月以内停机整顿的处罚。

第三十三条　第二级以上计算机信息系统运营、使用单位违反本条例第九条规定的，由市公安局给予警告，责令其限期改正；逾期不改正的，处以一千元以上五千元以下的罚款。

第三十四条　计算机信息系统运营、使用单位违反本条例第十条第一款规定的，由公安机关给予警告，责令其限期改正；逾期不改正的，处以一千元以上五千元以下的罚款。

计算机信息系统运营、使用单位违反第十条第二款、第十五条规定的，由公安机关给予警告，责令其限期改正；逾期不改正的，对经营性单位处以二千元以上二万元以下的罚款，对非经营性单位处以二千元的罚款。

第三十五条　计算机信息系统运营、使用单位违反本条例第十一条、第十二条规定的，由公安机关给予警告，责令其限期改正；逾期不改正的，处以二千元以上五万元以下的罚款；情节严重的，给予六个月以内停机整顿的处罚；对单位直接负责的主管人员和直接责任人员可处以五百元以上五千元以下的罚款。

第三十六条　计算机信息系统运营、使用单位违反本条例第十三条、第十四条规定的，由公安机关给予警告，责令其限期改正，并处以一千元以上一万元以下的罚款。

第三十七条　信息安全服务机构违反本条例第十六条第二款规定的，由公安机关给予警告，责令其限期改正，并处以一千元

以上一万元以下的罚款。

第三十八条　计算机信息系统运营、服务单位违反本条例第十七条规定的，由公安机关给予警告或者六个月以内停机整顿的处罚。

第三十九条　互联网接入服务和数据中心服务提供者、互联网信息服务提供者或者互联网上网服务提供单位违反本条例第十八条、第十九条或者第二十一条规定的，由公安机关给予警告，责令其限期改正，并可处以一千元以上一万五千元以下的罚款；情节严重的，给予六个月以内停机整顿的处罚；对单位直接负责的主管人员和直接责任人员可处以五百元以上五千元以下的罚款。

第四十条　单位或者个人违反本条例第二十条规定，未经信息网络安全审核从事互联网上网服务经营活动的，由公安机关责令其停业，并可处以一千元以上一万五千元以下的罚款。

第四十一条　单位或者个人违反本条例第二十二条、第二十三条规定，由公安机关给予警告，有违法所得的，没收其违法所得；对单位可并处以一千元以上一万五千元以下的罚款，对个人可并处以五百元以上五千元以下的罚款；情节严重的给予六个月以内停业整顿、停机联网的处罚。其中，危害国家安全的行为由国家安全机关依照有关法律法规规定查处。

第四十二条　违反本条例规定的行为，涉及其他法律法规的，由有关部门依法处罚；构成犯罪的，依法追究其刑事责任。

第四十三条　公安机关及其他部门工作人员违反本条例规定，玩忽职守、滥用职权或者徇私舞弊的，由其所在单位或者上级主管部门、监察机关依法追究其行政责任；构成犯罪的，由司法机关依法追究其刑事责任。

第六章　附则

第四十四条　本条例所称“以上”、“以下”包含本数。

第四十五条　本条例自2009年5月1日起施行。