内蒙古自治区计算机信息系统安全保护办法

（2011 年 12 月 6 日内蒙古自治区人民政府令第 183 号公布 自 2012 年 2 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，结合自治区实际，制定本办法。

第二条 本办法适用于自治区行政区域内计算机信息系统的安全保护。

第三条 旗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。

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。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造成严重损害，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。

第六条 计算机信息系统运营、使用单位应当遵守下列规定：

（一）对计算机信息系统安全保护等级准确定级，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，应当在规划、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系统安全保护设施，落实安全保护措施；

（三）计算机信息系统的结构、处理流程、服务内容等发生重大变化，或者公安机关要求重新确定等级的，应当重新定级；

（四）按照计算机信息系统安全保护等级要求，使用符合国家及自治区规定并取得国家计算机信息系统安全专用产品销售许可证的信息安全产品；

（五）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；

（六）建立安全保护组织，确定安全管理责任人，指定专职人员负责本单位计算机信息系统的安全管理。

第七条 第二级以上计算机信息系统运营、使用单位，应当自确定安全保护等级之日起30日内，到所在地盟行政公署、设区的市人民政府公安机关或者其指定的受理机构备案；属于自治区统一联网、跨盟市或者中央驻自治区、自治区直属单位的计算机信息系统，应当到自治区人民政府公安机关或者其指定的受理机构备案。

第八条 公安机关应当在收到备案材料之日起10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，应当书面通知报送单位予以纠正。

第九条 计算机信息系统涉及国家安全、社会公共利益、重大经济建设等信息的，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，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进行测评。

第二级以上计算机信息系统建设完成后，经测评合格方可投入使用。

第十条 计算机信息系统确定为第二级保护等级的，应当每

两年至少进行一次系统安全等级测评；确定为第三级的，应当每年至少进行一次系统安全等级测评；确定为第四级以上的，应当每半年至少进行一次系统安全等级测评。

第十一条 从事计算机信息系统安全等级测评工作的机构和人员应当遵守国家规定。

申请成立安全等级测评机构的单位应当经自治区人民政府公安机关初审，并通过公安部信息安全等级保护评估中心的测评能力评估。

自治区人民政府公安机关应当加强对安全等级测评机构的监督、检查和指导。

第十二条 旗县级以上人民政府公安机关应当对计算机信息系统运营、使用单位的信息安全等级保护情况进行检查。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。

第三章 安全管理

第十三条 公安机关应当为公众提供计算机信息系统安全保护指导，开展安全宣传教育。

第十四条 公安机关对计算机信息系统安全服务机构实行分级管理和推荐制度。

第十五条 计算机信息系统安全服务机构应当向盟市级以上公安机关备案。

计算机信息系统安全服务机构应当执行国家及自治区有关计算机信息系统安全标准，应当配备适应开展相应安全服务需要、掌握国家及自治区有关计算机信息系统安全标准的技术人员。

计算机信息系统安全服务机构及其工作人员不得泄露在开展安全服务过程中获悉的国家秘密、商业秘密以及计算机信息系统网络结构、配置等用户信息；不得非法占有、使用用户的信息资源；不得在计算机信息系统中设置隐蔽信道。

第十六条 发生重大突发事件，危及国家安全、公共安全、社会稳定及重要计算机信息系统安全的紧急情况时，盟市级以上公安机关可以按照有关法律、法规的规定，要求有关单位采取相应控制措施。计算机信息系统的运营、使用单位应当服从公安机

关和国家指定部门的调度。

第十七条 基础电信运营企业和计算机信息系统的运营、使用单位应当接受公安机关的安全监督、检查、指导，并如实提供有关计算机信息系统安全保护的信息资料、互联网基础数据及其他数据文件。

第十八条 基础电信运营企业等提供互联网接入服务的单位应当执行下列规定：

（一）配合公安机关做好接入本网络联网单位和用户的备案工作，真实、准确、完整登记联网单位和用户的名称、性质、有效证件、互联网地址、装机地址、上网电话、联系人等公安机关要求备案的信息，报送同级公安机关，并及时报告本网络中联网单位和用户的变更情况；

（二）记录并留存接入本网络的联网单位和用户登录、退出互联网时间及主叫号码、账号、互联网地址等上网日志信息，留存时间不少于1年；

（三）落实相关安全保护技术措施，通过互联网地址和相关网络应用信息能够对应联网单位和用户信息；

（四）协助公安机关查处涉及互联网的违法犯罪行为，并采取人工值守、远程联网查询等方式提供24小时快速查询支持；

（五）协助公安机关对接入本网络的联网单位和用户进行安全宣传教育，落实安全保护措施；

（六）互联网络拓扑结构、通信协议等拟进行重大调整的，应当报自治区人民政府公安机关备案后实施。

第十九条 提供互联网接入服务的单位、提供服务器托管或租赁空间服务的单位、互联网信息服务提供者及其他有关电信业务经营者应当建立安全管理制度，采取异常流量和违法信息监测等安全保护技术措施，及时发现危害信息网络安全、网上传播违法信息等违法犯罪活动，保留有关原始记录，及时采取删除、停止传输等措施，并在24小时内向当地公安机关报告。

第二十条 联网单位和用户应当采取设置安全性较高的密码等安全保护措施，定期更改密码，保障所使用上网账号的安全。

基础电信运营企业可以采取动态密码认证等技术措施为联网单位和用户提供互联网接入服务。

第二十一条 联网单位和用户向其他单位、个人提供互联网上网服务或者与其他单位、个人共用上网线路、账号的，应当遵守国家有关规定，并到旗县级以上人民政府公安机关备案。

第二十二条 提供互联网上网服务的单位和通过局域网接入互联网用户终端在10台以上的联网单位应当安装、运行符合

国家及自治区规定的安全管理系统。

第二十三条 宾馆、酒店、餐厅、机场、车站、阅览室等提供互联网上网服务的场所和通过无线方式接入互联网的地点管理者，应当采取用户登录认证安全技术措施，并对上网用户的身份证等有效证件进行核对、登记。

第二十四条 使用内部网络地址与互联网网络地址转换方式接入互联网的联网单位，应当记录并留存用户上网终端硬件地址等信息与内部网络地址和互联网网络地址的对应关系。留存时间不少于1年。

第二十五条 生产、销售或者提供具有计算机信息系统远程控制、密码猜解、漏洞检测、信息群发功能的产品和工具的，应当报自治区人民政府公安机关或者其指定的公安机关备案。

第四章 安全秩序

第二十六条 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）病毒、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）账号使用登记和操作权限管理制度；

（六）安全管理人员岗位工作职责；

（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；

（十）安全教育和培训制度；

（十一）案件、事件报告和协助查处制度；

（十二）其他与安全保护相关的管理制度。

第二十七条 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留存 1 年以上措施；

（六）记录用户账号、主叫电话号码和网络地址措施；

（七）身份登记和识别确认措施；

（八）垃圾信息、有害信息的防治、清理措施；

（九）信息群发限制措施；

（十）其他保护计算机信息系统安全的技术措施。

第二十八条 任何单位和个人不得利用计算机信息系统、移动通讯终端制作、传播、复制下列信息：

（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，破坏民族团结或者侵害民族风俗、习惯的；

（四）破坏国家宗教政策，宣扬邪教、封建迷信的；

（五）散布谣言，发布虚假信息，扰乱社会秩序，破坏社会稳定的；

（六）煽动聚众滋事，损害社会公共利益的；

（七）宣扬淫秽、色情、赌博、暴力、凶杀、恐怖的；

（八）教唆犯罪或者传授犯罪方法的；

（九）散布他人隐私，侮辱、诽谤、恐吓他人，侵害他人合法权益的；

（十）从事考试作弊相关活动的；

（十一）贩卖假币、假证件、假发票、假冒伪劣商品、枪支弹药、爆炸物、迷药、窃听器和其他法律、法规禁止流通的物品的；

（十二）法律、法规禁止制作、传播、复制的其他信息。

第二十九条 任何单位和个人不得实施下列行为：

（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）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；

（三）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；

（四）利用计算机信息系统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）非法截取、篡改、删除他人电子邮件或者其他数据资料；

（六）故意制作、传播计算机病毒、恶意软件等破坏性程序；

（七）利用计算机信息系统假冒他人名义制作、传播信息，或者以其他方式进行网络诈骗；

（八）建立或者管理主要用于传播、交流违法犯罪信息的网

站、群组、论坛等；

（九）允许、放任他人在自己所有或者管理的网站、网页、群组上发布第二十八条所禁止的信息；

（十）为非法网站提供服务器托管、虚拟主机、网络存储空间等服务，或者通过投放广告等方式向其直接、间接提供资金；

（十一）明知是非法网站，向其提供互联网接入、通讯传输通道、代收费、费用结算等服务；

（十二）以牟利为目的，在互联网上散布、删除信息，侵犯他人合法权益；

（十三）提供侵入、非法控制计算机信息系统的方法、程序、工具；

（十四）法律、法规禁止的其他利用计算机信息系统实施的行为。

第五章 法律责任

第三十条 违反本办法第六条、第九条、第十条、第十七条、第十八条第一至四项、第十九条、第二十六条、第二十七条规定的，由公安机关责令限期改正，给予警告，有违法所得的，没收

违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员处以5000元以下的罚款，对单位处以15000元以下的罚款，可以建议主管部门对相关单位的主要领导给予处分；情节严重的，并可以给予6个月以内停止联网、停机整顿的处罚。

第三十一条 违反本办法第十五条第三款规定的，由公安机关对单位的主管负责人员和其他直接责任人员处以5000元以下的罚款，对单位处以5000元以上15000元以下的罚款；有违法所得的，除没收违法所得外，可以处以违法所得1至3倍的罚款，但是最高不得超过30000元。

第三十二条 违反本办法第二十条第一款规定的，由公安机关责令限期改正，给予警告；在规定的限期内未改正的，可以给予6个月以内停止联网、停机整顿的处罚。

第三十三条 违反本办法第二十二条、第二十三条、第二十四条规定的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员处以5000元以下的罚款，对单位处以15000元以下的罚款；情节严重的，并可以给予6个月以内停止联网、停机整顿的处罚。

第三十四条 违反本办法第二十八条、第二十九条规定的，由公安机关给予警告，对个人可以并处5000元以下的罚款，对单位可以并处15000元以下的罚款；有违法所得的，除没收违法所得外，可以处以违法所得1至3倍的罚款，但是最高不得超过30000元；情节严重的，并可以给予6个月以内停止联网、停机整顿的处罚。

第三十五条 从事计算机信息系统安全等级测评工作的单位和人员有下列行为之一的，由公安机关对单位主管负责人员和其他直接责任人员处以5000元以下的罚款，对单位处以5000元以上15000元以下的罚款；有违法所得的，除没收违法所得外，可以处以违法所得1至3倍的罚款，但是最高不得超过30000元：

（一）未通过测评能力评估，从事测评活动的；

（二）影响被测评计算机信息系统正常运行，危害被测评计算机信息系统安全的；

（三）擅自向第三方泄露被测评计算机信息系统运营、使用单位秘密和其他信息的；

（四）故意隐瞒测评过程中发现的安全问题，或者在测评过程中弄虚作假，未如实出具测评报告的；

（五）擅自占有、使用测评相关资料及数据文件的；

（六）分包或者转包测评项目的；

（七）从事计算机信息系统安全专用产品的开发、销售及信息系统安全集成业务，或者限定被测评单位购买、使用其指定的信息安全专用产品的；

（八）其他可能影响测评结果客观、公正的行为，或者未按照国家规定开展测评工作的。

第三十六条 违反本办法规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚法》的规定处罚；给国家、其他组织或者他人财产造成损失的，应当依法承担民事责任；构成犯罪的，依法追究刑事责任。

第三十七条 公安机关和其他有关部门及其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依法给予行政处分；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

第三十八条　本办法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、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。

本办法所称的信息安全等级测评，是指对计算机信息系统的安全状况进行测试、评价、判断。

本办法所称的安全服务机构，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、培训等业务的单位。

本办法所称联网单位和用户包括通过计算机或者手机等通讯终端以有线、无线等方式接入互联网的单位和用户。

第三十九条　本办法自 2012 年 2 月 1 日起施行。