信息安全等级保护
商用密码管理法规汇编

吉林省密码管理局　翻印
二〇一三年九月

目　录

1、中华人民共和国国务院令（第 273 号）　…（1）
2、商用密码管理条例　……（2）
3、国家密码管理局公告（第 8 号）　……（10）
4、商用密码产品使用管理规定 ……（11）
5、信息安全等级保护管理办法 ……（15）
6、信息安全等级保护商用密码管理办法 ……（35）
7、《信息安全等级保护商用密码管理办法》
　　实施意见 ……（38）

中华人民共和国国务院令

第 273 号

现发布《商用密码管理条例》，自发布之日起实施。

总理　朱镕基

1999 年 10 月 7 日

商用密码管理条例

第一章　总　则

第一条　为了加强商用密码管理，保护信息安全，保护公民和组织的合法权益，维护国家的安全和利益，制定本条例。

第二条　本条例所称商用密码，是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。

第三条　商用密码技术属于国家秘密。国家对商用密码产品的科研、生产、销售和使用实行专控管理。

第四条　国家密码管理委员会及其办公室（以下简称国家密码管理机构）主管全国的商用密码管理工作。

省、自治区、直辖市负责密码管理的机构根据国家密码管理机构的委托，承担商用密码的有关管理工作。

第二章　科研、生产管理

第五条　商用密码的科研任务由国家密码管理机构指定的单位承担。

商用密码指定科研单位必须具有相应的技术力量和设备，能够采用先进的编码理论和技术，编制的商用密码算法具有较高的保密强度和抗攻击能力。

第六条　商用密码的科研成果，由国家密码管理机构组织专家按照商用密码技术标准和技术规范审查、鉴定。

第七条　商用密码产品由国家密码管理机构指定的单位生产。未经指定，任何单位或者个人不得生产商用密码产品。

商用密码产品指定生产单位必须具有与生产商用密码产品相适应的技术力量以及确保商用密码产品质量的设备、生产工艺和质量保证体系。

第八条　商用密码产品指定生产单位生产的商用密码产品的品种和型号，必须经国家密码管理机构批准，并不得超过批准范围生产商用密码产品。

第九条　商用密码产品，必须经国家密码管理机构指定的产品质量检测机构检测合格。

第三章　销售管理

第十条　商用密码产品由国家密码管理机构许可的单位销售。未经许可，任何单位或者个人不得销售商用密码产品。

第十一条　销售商用密码产品，应当向国家密码管理机构提出申请，并应当具备下列条件：

（一）有熟悉商用密码产品知识和承担售后服务的人员；

（二）有完善的销售服务和安全管理规章制度；

（三）有独立的法人资格。

经审查合格的单位，由国家密码管理机构发给《商用密码产品销售许可证》。

第十二条　销售商用密码产品，必须如实登记直接使用商用密码产品的用户的名称（姓名）、地址（住址）、组织机构代码（居民身份证号码）以及每台商用密码产品的用途，并将登记情况报国家密码管理机构备案。

第十三条　进口密码产品以及含有密码技术的设备或者出口商用密码产品，必须报经国家密码管理机构批准。任何单位或者个人不得销售境外的密

码产品。

第四章　使用管理

第十四条　任何单位或者个人只能使用经国家密码管理机构认可的商用密码产品，不得使用自行研制的或者境外生产的密码产品。

第十五条　境外组织或者个人在中国境内使用密码产品或者含有密码技术的设备，必须报经国家密码管理机构批准；但是，外国驻华外交代表机构、领事机构除外。

第十六条　商用密码产品的用户不得转让其使用的商用密码产品。商用密码产品发生故障，必须由国家密码管理机构指定的单位维修。报废、销毁商用密码产品，应当向国家密码管理机构备案。

第五章　安全、保密管理

第十七条　商用密码产品的科研、生产，应当在符合安全、保密要求的环境中进行。销售、运输、保管商用密码产品，应当采取相应的安全措施。

从事商用密码产品的科研、生产和销售以及使用商用密码产品的单位和人员，必须对所接触和掌握的商用密码技术承担保密义务。

第十八条 宣传、公开展览商用密码产品，必须事先报国家密码管理机构批准。

第十九条 任何单位和个人不得非法攻击商用密码，不得利用商用密码危害国家的安全和利益、危害社会治安或者进行其他违法犯罪活动。

第六章 罚 则

第二十条 有下列行为之一的，由国家密码管理机构根据不同情况分别会同工商行政管理、海关等部门没收密码产品，有违法所得的，没收违法所得；情节严重的，可以并处违法所得 1 至 3 倍的罚款：

（一）未经指定，擅自生产商用密码产品的，或者商用密码产品指定生产单位超过批准范围生产商用密码产品的；

（二）未经许可，擅自销售商用密码产品的；

（三）未经批准，擅自进口密码产品以及含有

密码技术的设备、出口商用密码产品或者销售境外的密码产品的。

经许可销售商用密码产品的单位未按照规定销售商用密码产品的，由国家密码管理机构会同工商行政管理部门给予警告，责令改正。

第二十一条 有下列行为之一的，由国家密码管理机构根据不同情况分别会同公安、国家安全机关给予警告，责令立即改正：

（一）在商用密码产品的科研、生产过程中违反安全、保密规定的；

（二）销售、运输、保管商用密码产品，未采取相应的安全措施的；

（三）未经批准，宣传、公开展览商用密码产品的；

（四）擅自转让商用密码产品或者不到国家密码管理机构指定的单位维修商用密码产品的。

使用自行研制的或者境外生产的密码产品，转让商用密码产品，或者不到国家密码管理机构指定的单位维修商用密码产品，情节严重的，由国家密码管理机构根据不同情况分别会同公安、国家安全机关没收其密码产品。

第二十二条 商用密码产品的科研、生产、销

售单位有本条例第二十条、第二十一条第一款第（一）、（二）、（三）项所列行为，造成严重后果的，由国家密码管理机构撤销其指定科研、生产单位资格，吊销《商用密码产品销售许可证》。

第二十三条 泄露商用密码技术秘密、非法攻击商用密码或者利用商用密码从事危害国家的安全和利益的活动，情节严重，构成犯罪的，依法追究刑事责任。

有前款所列行为尚不构成犯罪的，由国家密码管理机构根据不同情况分别会同国家安全机关或者保密部门没收其使用的商用密码产品，对有危害国家安全行为的，由国家安全机关依法处以行政拘留；属于国家工作人员的，并依法给予行政处分。

第二十四条 境外组织或者个人未经批准，擅自使用密码产品或者含有密码技术的设备的，由国家密码管理机构会同公安机关给予警告，责令改正，可以并处没收密码产品或者含有密码技术的设备。

第二十五条 商用密码管理机构的工作人员滥用职权、玩忽职守、徇私舞弊，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，依法给予行政处分。

第七章　附　则

第二十六条　国家密码管理委员会可以依据本条例制定有关的管理规定。

第二十七条　本条例自发布之日起施行。

国家密码管理局公告

（第 8 号）

现公布《商用密码产品使用管理规定》，自 2007 年 5 月 1 日起施行。

国家密码管理局

2007 年 3 月 24 日

商用密码产品使用管理规定

第一条 为了规范商用密码产品使用行为，根据《商用密码管理条例》，制定本规定。

第二条 中国公民、法人和其他组织使用商用密码产品的行为适用本规定。

第三条 本规定所称商用密码产品，是指采用密码技术对不涉及国家秘密内容的信息进行加密保护或安全认证的产品。

第四条 国家密码管理局主管全国的商用密码产品使用管理工作。

省、自治区、直辖市密码管理机构依据本规定承担有关管理工作。

第五条 中国公民、法人和其他组织需要对不涉及国家秘密内容的信息进行加密保护或安全认证的，均可以使用商用密码产品。

使用商用密码产品，应当遵守国家法律，不得损害国家利益、社会公共利益和其他公民的合法权益，不得利用商用密码产品进行违法犯罪活动。

第六条 中国公民、法人和其他组织都应当使

用国家密码管理局准予销售的商用密码产品，不得使用自行研制的或境外生产的密码产品。

国家密码管理局定期公布准予销售的商用密码产品目录。

第七条 需要使用商用密码产品的，应当到商用密码产品销售许可单位购买。

购买商用密码产品应当向商用密码产品销售许可单位出示本人身份证，说明直接使用商用密码产品的用户名称（姓名）、地址（住址）以及产品用途，提供用户组织机构代码证（居民身份证）复印件。

第八条 需要维修商用密码产品的，应当交该产品的生产单位或销售单位维修。

第九条 外商投资企业（包括中外合资经营企业、中外合作经营企业、外资企业、外商投资股份有限公司等）确因业务需要，必须使用境外生产的密码产品与境外进行互联互通的，经国家密码管理局批准，可以使用境外生产的密码产品。

外商投资企业申请使用境外生产的密码产品，应当事先填写《使用境外生产的密码产品登记表》，交所在地的省、自治区、直辖市密码管理机构。

省、自治区、直辖市密码管理机构自受理申请

之日起5个工作日内，对《使用境外生产的密码产品登记表》进行审查并报国家密码管理局。

国家密码管理局应当自省、自治区、直辖市密码管理机构受理申请之日起20个工作日内，对《使用境外生产的密码产品登记表》进行审核。准予使用的，发给《使用境外生产的密码产品准用证》。

《使用境外生产的密码产品准用证》有效期3年。

第十条 使用境外生产的密码产品的外商投资企业的名称、地址、密码产品用途发生变更的，应当自变更之日起10日内，到所在地的省、自治区、直辖市密码管理机构办理《使用境外生产的密码产品准用证》更换手续。

第十一条 外商投资企业终止使用境外生产的密码产品的，应当自终止使用之日起30日内，书面告知所在地的省、自治区、直辖市密码管理机构，并交回《使用境外生产的密码产品准用证》。

第十二条 外商投资企业申请使用的密码产品需要从境外进口的，应当申请办理《密码产品进口许可证》。

密码产品入境时，外商投资企业应当向海关如

实申报并提交《密码产品进口许可证》，海关凭此办理验放手续。

第十三条 用户不得转让其使用的密码产品。

第十四条 违反本规定的行为，依照《商用密码管理条例》予以处罚。

第十五条 《使用境外生产的密码产品登记表》、《使用境外生产的密码产品准用证》、《密码产品进口许可证》由国家密码管理局统一印制。

第十六条 本规定自 2007 年 5 月 1 日起施行。

信息安全等级保护管理办法

第一章　总　　则

第一条　为规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《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，制定本办法。

第二条　国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

第三条　公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。国务院信息化工作办公室及地方信息化

领导小组办事机构负责等级保护工作的部门间协调。

第四条 信息系统主管部门应当依照本办法及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

第五条 信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。

第二章 等级划分与保护

第六条 国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭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。

第七条 信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、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。

第二级，信息系统受到破坏后，会对公民、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。

第三级，信息系统受到破坏后，会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。

第四级，信息系统受到破坏后，会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。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第八条 信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

第三章　等级保护的实施与管理

第九条　信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。

第十条　信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。有主管部门的，应当经主管部门审核批准。

跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。

对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。

第十一条 信息系统的安全保护等级确定后，运营、使用单位应当按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，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

第十二条 在信息系统建设过程中，运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》（GB17859－1999）、《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术信息系统通用安全技术要求》（GB/T20271－2006）、《信息安全技术网络基础安全技术要求》（GB/T20270－2006）、《信息安全技术操作系统安全技术要求》（GB/T20272－2006）、《信息安全技术数据库管理系统安全技术要求》（GB/T20273－2006）、《信息安全技术服务器技术要求》、《信息安全技术终端计算机系统安全等级技术要求》（GA/T671－2006）等技术标准同步建设符合该等级要求

的信息安全设施。

第十三条 运营、使用单位应当参照《信息安全技术信息系统安全管理要求》（GB/T20269－2006）、《信息安全技术信息系统安全工程管理要求》（GB/T20282－2006）、《信息系统安全等级保护基本要求》等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。

第十四条 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本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。

信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据特殊安全需求进行自查。

经测评或者自查，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。

第十五条 已运营（运行）的第二级以上信息系统，应当在安全保护等级确定后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

新建第二级以上信息系统，应当在投入运行后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。

第十六条 办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料：

（一）系统拓扑结构及说明；

（二）系统安全组织机构和管理制度；

（三）系统安全保护设施设计实施方案或者改建实施方案；

（四）系统使用的信息安全产品清单及其认证、

销售许可证明；

（五）测评后符合系统安全保护等级的技术检测评估报告；

（六）信息系统安全保护等级专家评审意见；

（七）主管部门审核批准信息系统安全保护等级的意见。

第十七条 信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，应当在收到备案材料之日起的10个工作日内颁发信息系统安全等级保护备案证明；发现不符合本办法及有关标准的，应当在收到备案材料之日起的10个工作日内通知备案单位予以纠正；发现定级不准的，应当在收到备案材料之日起的10个工作日内通知备案单位重新审核确定。

运营、使用单位或者主管部门重新确定信息系统等级后，应当按照本办法向公安机关重新备案。

第十八条 受理备案的公安机关应当对第三级、第四级信息系统的运营、使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次，对第四级信息系统每半年至少检查一次。对跨省或者全国统一联网运行的信息系统的检查，应当会同其主管部门进行。

对第五级信息系统，应当由国家指定的专门部门进行检查。

公安机关、国家指定的专门部门应当对下列事项进行检查：

（一）信息系统安全需求是否发生变化，原定保护等级是否准确；

（二）运营、使用单位安全管理制度、措施的落实情况；

（三）运营、使用单位及其主管部门对信息系统安全状况的检查情况；

（四）系统安全等级测评是否符合要求；

（五）信息安全产品使用是否符合要求；

（六）信息系统安全整改情况；

（七）备案材料与运营、使用单位、信息系统的符合情况；

（八）其他应当进行监督检查的事项。

第十九条 信息系统运营、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，如实向公安机关、国家指定的专门部门提供下列有关信息安全保护的信息资料及数据文件：

（一）信息系统备案事项变更情况；

（二）安全组织、人员的变动情况；

（三）信息安全管理制度、措施变更情况；

（四）信息系统运行状况记录；

（五）运营、使用单位及主管部门定期对信息系统安全状况的检查记录；

（六）对信息系统开展等级测评的技术测评报告；

（七）信息安全产品使用的变更情况；

（八）信息安全事件应急预案，信息安全事件应急处置结果报告；

（九）信息系统安全建设、整改结果报告。

第二十条 公安机关检查发现信息系统安全保护状况不符合信息安全等级保护有关管理规范和技术标准的，应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求，按照管理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案。必要时，公安机关可以对整改情况组织检查。

第二十一条 第三级以上信息系统应当选择使用符合以下条件的信息安全产品：

（一）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和

国境内具有独立的法人资格；

（二）产品的核心技术、关键部件具有我国自主知识产权；

（三）产品研制、生产单位及其主要业务、技术人员无犯罪记录；

（四）产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；

（五）对国家安全、社会秩序、公共利益不构成危害；

（六）对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

第二十二条 第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：

（一）在中华人民共和国境内注册成立（港澳台地区除外）；

（二）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

（三）从事相关检测评估工作两年以上，无违法记录；

（四）工作人员仅限于中国公民；

（五）法人及主要业务、技术人员无犯罪记录；

（六）使用的技术装备、设施应当符合本办法对信息安全产品的要求；

（七）具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

（八）对国家安全、社会秩序、公共利益不构成威胁。

第二十三条 从事信息系统安全等级测评的机构，应当履行下列义务：

（一）遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；

（二）保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险；

（三）对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

第四章 涉及国家秘密信息系统的分级保护管理

第二十四条 涉密信息系统应当依据国家信息安全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的管理规定和技术标

准，结合系统实际情况进行保护。

非涉密信息系统不得处理国家秘密信息。

第二十五条 涉密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。

涉密信息系统建设使用单位应当在信息规范定密的基础上，依据涉密信息系统分级保护管理办法和国家保密标准 BMB17－2006《涉及国家秘密的计算机信息系统分级保护技术要求》确定系统等级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定保护等级。

保密工作部门和机构应当监督指导涉密信息系统建设使用单位准确、合理地进行系统定级。

第二十六条 涉密信息系统建设使用单位应当将涉密信息系统定级和建设使用情况，及时上报业务主管部门的保密工作机构和负责系统审批的保密工作部门备案，并接受保密部门的监督、检查、指导。

第二十七条 涉密信息系统建设使用单位应当选择具有涉密集成资质的单位承担或者参与涉密信息系统的设计与实施。

涉密信息系统建设使用单位应当依据涉密信息

系统分级保护管理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。

第二十八条 涉密信息系统使用的信息安全保密产品原则上应当选用国产品，并应当通过国家保密局授权的检测机构依据有关国家保密标准进行的检测，通过检测的产品由国家保密局审核发布目录。

第二十九条 涉密信息系统建设使用单位在系统工程实施结束后，应当向保密工作部门提出申请，由国家保密局授权的系统测评机构依据国家保密标准 BMB22－2007《涉及国家秘密的计算机信息系统分级保护测评指南》，对涉密信息系统进行安全保密测评。

涉密信息系统建设使用单位在系统投入使用前，应当按照《涉及国家秘密的信息系统审批管理规定》，向设区的市级以上保密工作部门申请进行系统审批，涉密信息系统通过审批后方可投入使用。已投入使用的涉密信息系统，其建设使用单位在按照分级保护要求完成系统整改后，应当向保密

工作部门备案。

第三十条 涉密信息系统建设使用单位在申请系统审批或者备案时，应当提交以下材料：

（一）系统设计、实施方案及审查论证意见；

（二）系统承建单位资质证明材料；

（三）系统建设和工程监理情况报告；

（四）系统安全保密检测评估报告；

（五）系统安全保密组织机构和管理制度情况；

（六）其他有关材料。

第三十一条 涉密信息系统发生涉密等级、连接范围、环境设施、主要应用、安全保密管理责任单位变更时，其建设使用单位应当及时向负责审批的保密工作部门报告。保密工作部门应当根据实际情况，决定是否对其重新进行测评和审批。

第三十二条 涉密信息系统建设使用单位应当依据国家保密标准 BMB20－2007《涉及国家秘密的信息系统分级保护管理规范》，加强涉密信息系统运行中的保密管理，定期进行风险评估，消除泄密隐患和漏洞。

第三十三条 国家和地方各级保密工作部门依法对各地区、各部门涉密信息系统分级保护工作实施监督管理，并做好以下工作：

（一）指导、监督和检查分级保护工作的开展；

（二）指导涉密信息系统建设使用单位规范信息定密，合理确定系统保护等级；

（三）参与涉密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；

（四）依法对涉密信息系统集成资质单位进行监督管理；

（五）严格进行系统测评和审批工作，监督检查涉密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；

（六）加强涉密信息系统运行中的保密监督检查。对秘密级、机密级信息系统每两年至少进行一次保密检查或者系统测评，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；

（七）了解掌握各级各类涉密信息系统的管理使用情况，及时发现和查处各种违规违法行为和泄密事件。

第五章　信息安全等级保护的密码管理

第三十四条　国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象

在国家安全、社会稳定、经济建设中的作用和重要程度，被保护对象的安全防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。

信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

第三十五条 信息系统安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。

第三十六条 信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码管理局审批，密码的设计、实施、使用、运行维护和日常管理等，应当按照国家密码管理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码管理机构备案。

第三十七条 运用密码技术对信息系统进行系

统等级保护建设和整改的，必须采用经国家密码管理部门批准使用或者准于销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

第三十八条 信息系统中的密码及密码设备的测评工作由国家密码管理局认可的测评机构承担，其他任何部门、单位和个人不得对密码进行评测和监控。

第三十九条 各级密码管理部门可以定期或者不定期对信息系统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，对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和测评。在监督检查过程中，发现存在安全隐患或者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。

第六章 法律责任

第四十条 第三级以上信息系统运营、使用单位违反本办法规定，有下列行为之一的，由公安机

关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，并及时反馈处理结果：

（一）未按本办法规定备案、审批的；

（二）未按本办法规定落实安全管理制度、措施的；

（三）未按本办法规定开展系统安全状况检查的；

（四）未按本办法规定开展系统安全技术测评的；

（五）接到整改通知后，拒不整改的；

（六）未按本办法规定选择使用信息安全产品和测评机构的；

（七）未按本办法规定如实提供有关文件和证明材料的；

（八）违反保密管理规定的；

（九）违反密码管理规定的；

（十）违反本办法其他规定的。

违反前款规定，造成严重损害的，由相关部门依照有关法律、法规予以处理。

第四十一条 信息安全监管部门及其工作人员在履行监督管理职责中，玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第七章 附 则

第四十二条 已运行信息系统的运营、使用单位自本办法施行之日起180日内确定信息系统的安全保护等级；新建信息系统在设计、规划阶段确定安全保护等级。

第四十三条 本办法所称“以上”包含本数（级）。

第四十四条 本办法自发布之日起施行，《信息安全等级保护管理办法（试行）》（公通字〔2006〕7号）同时废止。

信息安全等级保护商用密码管理办法

第一条 为规范信息安全等级保护中使用商用密码的行为，依据《商用密码管理条例》和《信息安全等级保护管理办法》，制定本办法。

第二条 信息安全等级保护中使用商用密码对不涉及国家秘密内容的信息进行加密保护或者安全认证的行为，适用本办法。

第三条 国家密码管理局主管全国的信息安全等级保护中使用商用密码的管理工作。

省、自治区、直辖市密码管理机构，中央和国家机关有关部委密码管理机构负责本地区、本部门信息安全等级保护中使用商用密码的具体管理工作。

第四条 各级信息系统使用商用密码应当符合《信息安全等级保护商用密码技术要求》。

第五条 信息安全等级保护中使用的商用密码产品，应当是国家密码管理局准予销售的产品。

第六条 信息系统运营、使用单位应当按照《商用密码产品目录》选用商用密码产品。

第七条 信息安全等级保护中第二级及以上的信息系统使用商用密码产品应当备案，填写《信息安全等级保护商用密码产品备案表》。

中央和国家机关有关部委统一定级的信息系统使用商用密码产品，由本部门密码管理机构向国家密码管理局备案。

其他信息系统等级保护中使用商用密码产品，由信息系统所属单位向所在地的省、自治区、直辖市密码管理机构备案。

省、自治区、直辖市密码管理机构定期将备案汇总情况报国家密码管理局。

第八条 信息系统运行过程中，商用密码产品使用情况发生变化的，应重新备案。

第九条 国家密码管理局和省、自治区、直辖市密码管理机构对第三级以上信息系统使用商用密码情况进行检查。其中，第三级信息系统每两年检查一次，第四级、第五级信息系统每年检查一次；检查工作可以结合商用密码测评工作进行。

第十条 国家密码管理局和省、自治区、直辖市密码管理机构对未按照要求使用商用密码产品的，及时向备案单位发出整改通知，并对整改情况进行督促检查。

第十一条 信息安全等级保护商用密码测评工作由国家密码管理局指定的测评机构承担。

第十二条 信息安全等级保护商用密码测评机构应严格按照《信息安全等级保护商用密码技术要求》及相关规范进行测评。

第十三条 信息安全等级保护中违反商用密码管理规定的，由密码管理机构依据《商用密码管理条例》和《信息安全等级保护管理办法》及相关规定予以处罚。

第十四条 本办法由国家密码管理局负责解释。

第十五条 本办法自 2008 年 1 月 1 日起执行。

《信息安全等级保护商用密码管理办法》实施意见

为了配合《信息安全等级保护商用密码管理办法》（国密局发〔2007〕11号）的实施，进一步规范信息安全等级保护商用密码管理工作，特提出以下意见。

一、使用商用密码对信息系统进行密码保护，应当严格遵守国家商用密码相关政策和标准规范。

二、在实施信息安全等级保护的信息系统中，商用密码应用系统是指采用商用密码产品或者含有密码技术的产品集成建设的，实现相关信息的机密性、完整性、真实性、抗抵赖性等功能的应用系统。

三、商用密码应用系统的建设应当选择具有商用密码相关资质的单位。

四、使用商用密码开展信息安全等级保护应当制定商用密码应用系统建设方案。方案应当包括信息系统概述、安全风险与需求分析、商用密码应用方案、商用密码产品清单、商用密码应用系统的安

全管理与维护策略、实施计划等内容。

五、第三级以上信息系统的商用密码应用系统建设方案应当通过密码管理部门组织的评审后方可实施。

中央和国家机关各部委第三级信息系统的商用密码应用系统建设方案，由信息系统的责任单位向国家密码管理部门提出评审申请，国家密码管理部门组织专家进行评审。设有密码管理部门的中央和国家机关部委，其第三级信息系统的商用密码应用系统建设方案可由本部门密码管理部门组织专家进行评审。

各省（区、市）第三级信息系统的商用密码应用系统建设方案，由信息系统的责任单位向所在省（区、市）密码管理部门提出评审申请，所在省（区、市）密码管理部门组织专家进行评审。

第四级以上信息系统的商用密码应用系统建设方案，由信息系统的责任单位向国家密码管理部门提出评审申请，国家密码管理部门组织专家进行评审。

六、第三级以上信息系统的商用密码应用系统建设必须严格按照通过评审的方案实施。需变更商用密码应用系统建设方案的，应当按照上述第五条

的要求重新评审，评审通过后方可实施。

七、使用商用密码实施信息安全等级保护，选用的商用密码产品应当是国家密码管理部门准予销售的产品；选用的含有密码技术的产品，应当是通过国家密码管理部门指定测评机构密码测评的产品。

八、第三级以上信息系统的商用密码应用系统，应当通过国家密码管理部门指定测评机构的密码测评后方可投入运行。密码测评包括资料审查、系统分析、现场测评、综合评估等。信息系统的责任单位应当将测评结果报相应的密码管理部门备案。

九、第二级以上信息系统的责任单位，应当填写《信息安全等级保护商用密码产品备案表》，并按照《信息安全等级保护商用密码管理办法》的要求进行备案。

十、第三级以上信息系统的责任单位，应当建立完善的商用密码使用管理制度，保障商用密码应用系统的安全运行。

十一、第三级以上信息系统发生重大变更时，信息系统的责任单位应当将变更情况及时报相应的密码管理部门，并按照密码管理部门的要求办理相

关事项。

十二、第三级以上信息系统的商用密码应用系统需要由责任单位以外的单位负责日常维护的，应当选择具有商用密码相关资质的单位。

十三、第三级以上信息系统的责任单位，应当积极配合密码管理部门组织开展的商用密码检查工作。

十四、使用商用密码实施信息安全等级保护，应当符合《信息安全等级保护商用密码技术实施要求》（附后）。

十五、本意见施行前已建成的第三级以上信息系统的商用密码应用系统，应当按照本意见第八条的要求进行密码测评，并根据密码测评意见实施改造。

十六、本意见所称“以上”包含本级。

附件：《信息安全等级保护商用密码技术实施要求》

附件：

信息安全等级保护
商用密码技术实施要求

国家密码管理局

2009 年

目　录

引　言 …… 47

第一章　第一级信息系统商用密码技术实施要求 …… 49

1.1　商用密码技术基本要求 …… 49

1.1.1　功能要求 …… 49

1.1.2　密钥管理要求 …… 50

1.1.3　密码配用策略要求 …… 50

1.1.4　密码实现机制要求 …… 50

1.1.5　密码安全防护要求 …… 50

1.2　商用密码技术应用要求 …… 51

1.2.1　物理安全 …… 51

1.2.2　网络安全 …… 51

1.2.3　主机安全 …… 51

1.2.4　应用安全 …… 52

1.2.5　数据安全及备份恢复 …… 52

第二章　第二级信息系统商用密码技术实施要求 …… 53

2.1 商用密码技术基本要求 …… 53

2.1.1 功能要求 …… 53

2.1.2 密钥管理要求 …… 54

2.1.3 密码配用策略要求 …… 55

2.1.4 密码实现机制 …… 56

2.1.5 密码安全防护要求 …… 56
2.2 商用密码技术应用要求 …… 56
2.2.1 物理安全 …… 57
2.2.2 网络安全 …… 57
2.2.3 主机安全 …… 57
2.2.4 应用安全 …… 58
2.2.5 数据安全及备份恢复 …… 59
第三章 第三级信息系统商用密码技术实施要求 …… 60
3.1 商用密码技术基本要求 …… 60
3.1.1 功能要求 …… 60
3.1.2 密钥管理要求 …… 62
3.1.3 密码配用策略要求 …… 64
3.1.4 密码实现机制 …… 65
3.1.5 密码安全防护要求 …… 65
3.2 商用密码技术应用要求 …… 65
3.2.1 物理安全 …… 65
3.2.2 网络安全 …… 66
3.2.3 主机安全 …… 67
3.2.4 应用安全 …… 67
3.2.5 数据安全及备份恢复 …… 68
第四章 第四级信息系统商用密码技术实施要求 …… 70
4.1 商用密码技术基本要求 …… 70
4.1.1 功能要求 …… 70
4.1.2 密钥管理要求 …… 73

4.1.3 密码配用策略要求 …… 75
4.1.4 密码实现机制 …… 76
4.1.5 密码安全防护要求 …… 76
4.2 商用密码技术应用要求 …… 76
4.2.1 物理安全 …… 76
4.2.2 网络安全 …… 77
4.2.3 主机安全 …… 77
4.2.4 应用安全 …… 78
4.2.5 数据安全及备份恢复 …… 79

引言

密码技术作为信息安全的基础性核心技术，是信息保护和网络信任体系建设的基础，是实行信息安全等级保护不可或缺的关键技术，充分利用密码技术能够有效地保障信息安全等级保护制度的落实，科学合理地采用密码技术及其产品，是落实信息安全等级保护最为有效、经济和便捷的手段。

国家标准《GB/T 22239－2008 信息安全技术 信息系统安全等级保护基本要求》（以下简称“《基本要求》”）规定了对不同安全保护等级信息系统的基本安全要求，对于涉及到身份的真实性、行为的抗抵赖、内容的机密性和完整性的要求项，密码技术都可以直接或间接地为满足这些要求提供支持，因此如何科学合理地应用密码技术对信息系统进行安全保护就成为实施等级保护的关键工作内容，直接影响着信息安全等级保护的全面推进。为此，我们以《商用密码管理条例》和《信息安全等级保护商用密码管理办法》为指导，结合《基本要求》中的相关安全要求项，在《信息安全等级保护

商用密码技术要求》的基础上，编制了《信息安全等级保护商用密码技术实施要求》，用以规范使用商用密码实施等级保护的相关技术工作，并为商用密码产品的研发和系统的集成提供依据。

本要求明确了一、二、三、四级信息系统使用商用密码技术来实施等级保护的基本要求和应用要求。在基本要求中根据密码技术的特点，从技术实施上对商用密码应用系统的功能、密钥管理、密码配用、密码实现和密码保护等方面提出了相关要求和规定。在应用要求中，从应用密码技术来实现相应等级的物理安全、网络安全、主机安全、应用安全和数据安全提出了要求。为方便使用，我们将各级信息系统的商用密码需求和相关技术实施要求按照不同安全等级集中进行编排。

第一章　第一级信息系统商用密码技术实施要求

1.1 商用密码技术基本要求

1.1.1　功能要求

1.1.1.1　真实性

第一级信息系统使用商用密码进行真实性保护时，应提供以下功能：

1）提供基于实体的身份标识和鉴别服务；

2）为访问网络设备提供身份鉴别服务；

3）为登录操作系统和数据库提供身份鉴别服务；

4）为访问应用系统提供身份鉴别服务；

5）向访问控制系统提供身份真实性的凭证。

1.1.1.2　完整性

第一级信息系统使用商用密码进行完整性保护时，应提供以下功能：

1）应提供数据完整性校验服务；

2）为通信过程和数据传输提供完整性校验服务；

3）为访问控制系统提供访问控制信息的完整性校验服务。

1.1.2 密钥管理要求

密钥管理至少应包括密钥的生成、存储和使用等过程，并满足：

1）**密钥生成**：密钥应具有一定的随机性；

2）**密钥存储**：采取必要的安全防护措施，防止密钥被轻易非授权获取；

3）**密钥使用**：采取必要的安全防护措施，防止密钥被非法使用。

1.1.3 密码配用策略要求

采用国家密码管理部门批准使用的算法。

1.1.4 密码实现机制要求

不做强制性要求。

1.1.5 密码安全防护要求

不做强制性要求。

1.2 商用密码技术应用要求

1.2.1 物理安全

第一级物理安全基本技术要求的实现不需使用密码技术。

1.2.2 网络安全

实现第一级网络安全基本技术要求在访问控制和身份鉴别方面可以使用密码技术。

在访问控制机制中，可以使用密码技术的完整性服务来保证访问控制列表的完整性。

在身份鉴别机制中，可以使用密码技术的真实性服务来实现鉴别信息的防假冒，可以使用密码技术的机密性服务来实现鉴别信息的防泄露。

1.2.3 主机安全

实现第一级主机安全基本技术要求在身份鉴别和访问控制方面可以使用密码技术。

在身份鉴别机制中，可以使用密码技术的真实性服务来实现鉴别信息的防假冒。

在访问控制机制中，可以使用密码技术的完整性服务来保证访问控制信息的完整性。

1.2.4 应用安全

实现第一级应用安全基本技术要求在身份鉴别、访问控制和通信安全方面可以使用密码技术。

在身份鉴别机制中，可以使用密码技术的真实性服务来实现鉴别信息的防假冒，保证应用系统用户身份的真实性。

在访问控制机制中，可以使用密码技术的完整性服务来保证系统功能和用户数据访问控制信息的完整性。

在通信安全方面，可以使用密码技术的完整性服务来实现对通信过程中数据完整性。

1.2.5 数据安全及备份恢复

第一级数据安全及备份恢复基本技术要求在数据传输安全方面，可以使用密码技术的完整性服务来实现对重要用户数据在传输过程中完整性检测。

第二章　第二级信息系统商用密码技术实施要求

2.1 商用密码技术基本要求

2.1.1　功能要求

2.1.1.1　真实性

第二级信息系统使用商用密码进行真实性保护时，应提供以下功能：

1）提供基于单个实体的身份鉴别功能；

2）能唯一标识并有效区分实体，包括用户、设备、系统等；

3）为建立网络会话提供身份鉴别服务；

4）为访问网络设备提供身份鉴别服务；

5）保证身份鉴别信息的唯一性；

6）向访问控制系统提供身份真实性的凭证。

2.1.1.2　机密性

第二级信息系统使用商用密码进行机密性保护时，应提供以下功能：

1）提供数据机密性服务；

2）为初始化会话过程中提供加密保护；

3）对通信过程中的重要字段提供加密保护；

4）对存储的鉴别信息提供加密保护。

2.1.1.3 完整性

第二级信息系统使用商用密码进行完整性保护时，应提供以下功能：

1）对鉴别信息和重要业务数据在传输过程中提供完整性校验服务；

2）对系统资源的访问控制信息提供完整性校验服务；

3）对文件/数据库表等客体的访问控制信息提供完整性校验服务；

4）对审计记录提供完整性校验服务。

2.1.2 密钥管理要求

密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、更换等过程，并满足：

1）**密钥生成**：应使用随机数发生器产生密钥；

2）**密钥存储**：密钥应加密存储，并采取必要的安全防护措施，防止密钥被非法获取。

3）**密钥分发**：密钥分发应采取有效的安全措施，防止

在分发过程中泄露。

4）**密钥导入与导出**：密钥的导入与导出应采取有效的安全措施，保证密钥的导入与导出安全，以及密钥的正确。

5）**密钥使用**：密钥必须明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；应按照密钥更换周期要求更换密钥，密钥更换允许系统中断运行。

6）**密钥备份与恢复**：应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制；对密钥进行备份或恢复。

2.1.3 密码配用策略要求

2.1.3.1 密码算法配用策略

采用国家密码管理部门批准使用的算法。

2.1.3.2 密码协议使用策略

采用经国家密码管理部门安全性评审的密码协议实现密码功能。

2.1.3.3 密码设备使用策略

使用密码设备时应符合以下要求：

1）应选用国家密码管理部门批准的密码设备；

2）信源加密、完整性校验、身份鉴别应选用智能密码钥匙、智能 IC 卡、可信密码模块 TCM、密码卡、密码机等密码设备；

3）信道加密应选用链路密码机、网络密码机、VPN 密码机等密码设备。

2.1.4 密码实现机制

应采用专用固件或硬件方式实现。

2.1.5 密码安全防护要求

密码安全防护应符合以下要求：

1）专用固件或硬件应具有有效的物理安全保护措施；

2）专用固件或硬件应满足相应运行环境的可靠性要求。

2.2 商用密码技术应用要求

2.2.1 物理安全

实现第二级物理安全基本技术要求不需使用密码技术。

2.2.2 网络安全

实现第二级网络安全基本技术要求在访问控制和身份鉴别方面推荐使用密码技术。

在访问控制方面，推荐使用密码技术的完整性服务来保证网络边界访问控制信息、系统资源访问控制信息的完整性。

在身份标识与鉴别方面，推荐使用密码技术的真实性服务来实现鉴别信息的防重用和防冒用，保证网络设备用户身份的真实性；推荐使用密码技术的机密性服务来保证网络设备远程管理时，鉴别信息传输过程中的机密性。

2.2.3 主机安全

实现第二级主机安全基本技术要求在身份鉴别、访问控制和审计记录方面推荐使用密码技术。

在身份鉴别方面，推荐使用密码技术的真实性服务来实现鉴别信息的防冒用和防重用，保证操作系统和数据库

系统用户身份的真实性；推荐使用密码技术的机密性服务来实现鉴别信息远程传输过程中的机密性。

在访问控制方面，推荐使用密码技术的完整性服务来保证系统资源访问控制信息的完整性。

在审计记录方面，推荐使用密码技术的完整性服务来对审计记录进行完整性保护。

2.2.4 应用安全

实现第二级应用安全基本技术要求在身份鉴别、访问控制、审计记录和通信安全方面推荐使用密码技术。

在身份鉴别方面，推荐使用密码技术的真实性服务来实现鉴别信息的防重用和防冒用，保证应用系统用户身份的真实性和通信双方身份的真实性。

在访问控制方面，推荐使用密码技术的完整性服务来保证文件、数据库表等客体访问控制信息的完整性。

在审计记录方面，推荐使用密码技术的完整性服务来保证审计记录的完整性，防止对审计记录的非法修改。

在通信安全方面，推荐使用密码技术的完整性服务来保证通信过程中数据的完整性；推荐使用密码技术的机密性服务来对通信过程中敏感数据加密，保证通信过程中敏感信息的机密性。

2.2.5 数据安全及备份恢复

实现第二级数据安全及备份恢复基本技术要求在数据传输安全和数据存储安全方面可以使用密码技术。

在数据传输安全方面，推荐使用密码技术的完整性服务来实现对鉴别信息和重要业务数据在传输过程中完整性检测。

在数据存储安全方面，推荐使用密码技术的机密性服务来实现鉴别信息的存储机密性。

第三章　第三级信息系统商用密码技术实施要求

3.1 商用密码技术基本要求

3.1.1　功能要求

3.1.1.1　真实性

第三级信息系统使用商用密码进行真实性保护时，应提供以下功能：

1）提供重要区域进入人员身份真实性鉴别服务；

2）提供安全访问路径中通信主体身份的真实性鉴别服务；

3）提供访问网络设备用户身份的真实性鉴别服务；

4）提供登录操作系统和数据库系统用户的身份真实性的鉴别服务；

5）提供应用系统用户身份真实性鉴别服务；

6）提供通信双方身份真实性鉴别服务；

7）能够提供组合鉴别方式；

8）在建立网络会话时提供身份鉴别服务；

9）保证身份鉴别信息的唯一性；

10）向访问控制系统提供身份真实性的凭证。

3.1.1.2 机密性

第三级信息系统使用商用密码进行机密性保护时，应提供以下功能：

1）提供通信过程中整个报文或会话过程的机密性保护服务；

2）提供存储过程中系统管理数据、鉴别信息和重要业务数据的机密性保护服务；

3）提供传输过程中系统管理数据、鉴别信息和重要业务数据的机密性保护服务。

3.1.1.3 完整性

第三级信息系统使用商用密码进行完整性保护时，应提供以下功能：

1）提供电子门禁系统记录的完整性服务；

2）提供安全访问路径中路由信息的完整性服务；

3）提供网络边界和系统资源访问控制信息的完整性服务；

4）提供审计记录的完整性服务；

5）提供系统资源访问控制信息的完整性服务；

6）提供重要信息资源敏感标记的完整性服务；

7）提供重要程序的完整性服务；

8）提供文件、数据库表等客体访问控制信息的完整性服务；

9）提供重要信息资源敏感标记的完整性服务；

10）提供通信过程中所有数据的完整性服务；

11）提供存储过程中系统管理数据、鉴别信息和重要业务数据的完整性服务。

3.1.1.4 抗抵赖性

第三级信息系统使用商用密码进行抗抵赖保护时，应提供以下功能：

1）提供进入重要区域人员行为的抗抵赖服务；

2）支持原发抗抵赖服务；

3）支持接收抗抵赖服务。

3.1.2 密钥管理要求

密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档和销毁等环节进行管理和策略制定的全过程，并满足：

1）**密钥生成**：应使用国家密码管理部门批准的硬件物理噪声源产生随机数；密钥必须在密码设备内部产生，不得以明文方式出现在密码设备之外；应具备

检查和剔除弱密钥的能力

2）**密钥存储**：密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在专用硬件中。

3）**密钥分发**：密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

4）**密钥导入与导出**：密钥的导入与导出应采取有效的安全措施，保证密钥的导入与导出安全，以及密钥的正确。

5）**密钥使用**：密钥必须明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；应按照密钥更换周期要求更换密钥，密钥更换允许系统中断运行；密钥泄露时，必须停止使用，并启动相应的应急处理和响应措施。

6）**密钥备份与恢复**：应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

7）**密钥归档**：应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密

钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

8）**密钥销毁**：应具有在紧急情况下销毁密钥的措施。

3.1.3 密码配用策略要求

3.1.3.1 密码算法配用策略

采用国家密码管理部门批准使用的算法。

3.1.3.2 密码协议使用策略

采用经国家密码管理部门安全性评审的密码协议实现密码功能。

3.1.3.3 密码设备使用策略

使用密码设备时应符合以下要求：

1）应选用国家密码管理部门批准的密码设备；

2）信源加密、完整性校验、身份鉴别、抗抵赖应选用可信密码模块 TCM、智能密码钥匙、智能 IC 卡、密码卡、密码机等密码设备；

3）信道加密应选用链路密码机、网络密码机、VPN 密码机等密码设备；

4）需要配用独立的密钥管理系统或使用数字证书认证系统提供的密钥管理服务。

3.1.4 密码实现机制

必须采用专用固件或硬件方式实现。

3.1.5 密码安全防护要求

密码安全防护应符合以下要求：

1）专用固件或硬件以及密码设备应具有有效的物理安全保护措施；

2）专用固件或硬件以及密码设备应满足相应运行环境的可靠性要求；

3）应建立有效的密码设备安全管理制度。

3.2 商用密码技术应用要求

3.2.1 物理安全

第三级物理安全基本技术要求在电子门禁系统方面推

荐使用密码技术。

在电子门禁系统中，推荐使用密码技术的真实性服务来保护身份鉴别信息，保证重要区域进入人员身份的真实性；推荐使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性。

3.2.2 网络安全

第三级网络安全基本技术要求在安全访问路径、访问控制和身份鉴别方面应当使用密码技术。

在建立安全访问路径过程中，应当使用密码技术的真实性服务来保证通信主体身份鉴别信息的可靠，实现安全访问路径中通信主体身份的真实性；应当使用密码技术的完整性服务来保证安全访问路径中路由控制信息的完整性。

在访问控制机制中，应当使用密码技术的完整性服务来保证网络边界和系统资源访问控制信息的完整性。

在审计记录方面，应当使用密码技术的完整性服务来对审计记录进行完整性保护。

在身份标识与鉴别方面，应当使用密码技术来实现组合鉴别，使用密码技术的机密性和真实性服务来实现防窃听、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备用户身份的真实性。

3.2.3 主机安全

第三级主机安全基本技术要求在身份鉴别、访问控制、审计记录和程序安全方面应当使用密码技术。

在身份标识与鉴别方面，应当使用密码技术来实现组合鉴别，使用密码技术的真实性服务来实现鉴别信息的防假冒和防重用，保证操作系统和数据库系统用户身份的真实性，并在远程管理时使用密码技术的机密性服务来实现鉴别信息的防窃听。

在访问控制方面，应当使用密码技术的完整性服务来保证系统资源访问控制信息的完整性，并使用密码技术的完整性服务来保证重要信息资源敏感标记的完整性。

在审计记录方面，应当使用密码技术的完整性服务来对审计记录进行完整性保护。

在程序安全方面，推荐使用密码技术的完整性服务来实现对重要程序的完整性检测。

3.2.4 应用安全

第三级应用安全基本技术要求在身份鉴别、访问控制、审计记录和通信安全方面应当使用密码技术。

在身份鉴别方面，应当使用密码技术来实现组合鉴别，使用密码技术的机密性和真实性服务来实现防窃听、防假

冒和防重用，保证应用系统用户身份的真实性。

在访问控制方面，应当使用密码技术的完整性服务来保证文件、数据库表访问控制信息和重要信息资源敏感标记的完整性。

在审计记录方面，应使用密码技术的完整性服务来实现对审计记录完整性的保护。

在通信安全方面，应当使用密码技术的完整性服务来保证通信过程中数据完整性；应当使用密码技术的真实性服务来实现通信双方会话初始化验证；应当使用密码技术的机密性服务来实现对通信过程中整个报文或会话过程加密保护；应当使用密码技术的抗抵赖服务来提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

3.2.5 数据安全及备份恢复

第三级数据安全及备份恢复基本技术要求在数据传输安全和数据存储安全方面应当使用密码技术。

在数据传输安全方面，应当使用密码技术的完整性服务来实现对系统管理数据、鉴别信息和重要业务数据在传输过程中完整性的检测。应当使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的传输机密性。

在数据存储安全方面，应当使用密码技术的完整性服

务来实现对系统管理数据、鉴别信息和重要业务数据在存储过程中完整性的检测。应当使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的存储机密性。

第四章　第四级信息系统商用密码技术实施要求

4.1 商用密码技术基本要求

4.1.1　功能要求

4.1.1.1　真实性

第四级信息系统使用商用密码进行真实性保护时，应提供以下功能：

1）应提供基于单个实体（用户、主机）的身份鉴别功能；

2）能唯一标识并有效区分实体，包括用户、设备、系统等；

3）能够提供两种或两种以上的身份鉴别方式；

4）身份鉴别信息具备不易被冒用的防范能力；

5）身份鉴别信息具备不可伪造性；

6）保证身份鉴别信息的唯一性；

7）提供进入重要区域人员身份真实性鉴别服务；

8）在建立网络会话时提供身份鉴别服务；

9）提供安全访问路径中通信主体身份的真实性鉴别服务；

10）提供通信双方身份真实性鉴别服务；
11）支持在网络设备身份鉴别时提供身份鉴别服务；
12）提供主机平台基于可信密码模块 TCM 的身份真实性鉴别服务；
13）提供登录操作系统和数据库系统用户的身份真实性的鉴别服务；
14）提供应用系统用户身份真实性鉴别服务；
15）应向访问控制系统提供身份真实性的凭证。

4.1.1.2 机密性

第四级信息系统使用商用密码进行机密性保护时，应提供以下功能：
1）能提供数据机密性服务；
2）提供通信过程中整个报文或会话过程的机密性保护服务；
3）提供存储过程中系统管理数据、鉴别信息和重要业务数据的机密性保护服务；
4）提供传输过程中系统管理数据、鉴别信息和重要业务数据的机密性保护服务。

4.1.1.3 完整性

第四级信息系统使用商用密码进行完整性保护时，应

提供以下功能：

1）能够提供对数据的完整性保护；

2）支持对重要信息资源敏感标记提供完整性服务；

3）提供电子门禁系统记录的完整性服务；

4）支持对通信过程数据提供完整性服务；

5）提供安全访问路径中数据的完整性服务；

6）提供网络边界和系统资源访问控制信息的完整性服务；

7）提供系统资源访问控制信息的完整性服务；

8）支持对系统管理数据、鉴别信息和业务数据在传输过程中提供完整性服务，并能够检测完整性错误，提供必要的恢复手段；

9）支持对系统管理数据、鉴别信息和业务数据在存储过程中提供完整性服务，并能够检测完整性错误，提供必要的恢复手段；

10）提供主机平台基于可信密码模块 TCM 的完整性服务；

11）提供重要程序的完整性服务；

12）提供文件、数据库表等客体访问控制信息的完整性服务；

13）提供审计记录的完整性服务。

4.1.1.4 抗抵赖

第四级信息系统使用商用密码进行抗抵赖保护时，应提供以下功能：

1）提供进入重要区域人员行为的抗抵赖服务；

2）支持原发抗抵赖服务；

3）支持接收抗抵赖服务。

4.1.2 密钥管理要求

密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档和销毁等环节进行管理和策略制定的全过程，并满足：

1）**密钥生成**：应使用国家密码管理部门批准的硬件物理噪声源产生随机数；密钥必须在密码设备内部产生，不得以明文方式出现在密码设备之外；应具备检查和剔除弱密钥的能力；生成密钥审计信息，密钥审计信息包括：种类、长度、拥有者信息、使用起始时间、使用终止时间。

2）**密钥存储**：密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在专用硬件中：应具有密钥可能泄露时的应急处理和响应措施。

3）**密钥分发**：密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截获、假冒、篡改、重放等攻击，保证密钥的安全性。应具有密钥可能泄露时的应急处理和响应措施。

4）**密钥导入与导出**：密钥的导入与导出应采取有效的

安全措施，保证密钥的导入与导出安全，以及密钥的正确；密钥的导入与导出应采用密钥分量的方式或者专用设备的方式；密钥的导入与导出应保证系统密码服务功能不间断。

5）**密钥使用**：密钥必须明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；应按照密钥更换周期要求更换密钥，密钥更换允许系统中断运行；密钥泄露时，必须停止使用，并启动相应的应急处理和响应措施。

6）**密钥备份与恢复**：应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

7）**密钥归档**：应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归挡的密钥、归档的时间等：归档密钥应进行数据备份，并采用有效的安全保护措施。

8）**密钥销毁**：应具有在紧急情况下销毁密钥的措施。

4.1.3 密码配用策略要求

4.1.3.1 密码算法配用策略

采用国家密码管理部门批准使用的算法。

4.1.3.2 密码协议使用策略

采用经国家密码管理部门安全性评审的密码协议实现密码功能。

4.1.3.3 密码设备使用策略

使用密码设备时应符合以下要求：

1）应选用国家密码管理部门批准的密码设备；

2）信源加密、完整性校验、身份鉴别、抗抵赖应选用可信密码模块 TCM、智能密码钥匙、智能 IC 卡、密码卡、密码机等密码设备；

3）信道加密应选用链路密码机、网络密码机、VPN 密码机等密码设备；

4）需要配用独立的密钥管理系统或使用数字证书认证系统提供的密钥管理服务。

4.1.4 密码实现机制

必须采用专用硬件或固件方式实现。

4.1.5 密码安全防护要求

密码安全防护应符合以下要求：

1）专用硬件或固件以及密码设备应具有严格的物理安全保护措施；

2）专用硬件或固件以及密码设备应满足相应运行环境的可靠性要求；

3）应建立严格的密码设备安全管理制度。

4.2 商用密码技术应用要求

4.2.1 物理安全

第四级物理安全基本技术要求在电子门禁系统方面应当使用密码技术。

在电子门禁系统中，应当使用密码技术的真实性服务来实现对进入重要区域人员的身份鉴别，并使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性。

4.2.2 网络安全

第四级网络安全基本技术要求在安全访问路径、访问控制和身份鉴别方面应当使用密码技术。

在建立安全访问路径过程中，应当使用密码技术的真实性服务来保证通信主体身份鉴别信息的可靠，实现安全访问路径中通信主体身份的真实性应当使用密码技术的完整性服务来保证安全访问路径中路由控制信息的完整性。

在访问控制方面，应当使用密码技术的完整性服务来保证网络边界访问控制信息和数据敏感标记的完整性。

在审计记录方面，应当使用密码技术的完整性服务来对审计记录进行完整性保护。

在身份标识与鉴别方面，应当采用密码技术实现组合鉴别，使用密码技术的机密性和真实性服务来实现传输过程中鉴别信息防窃听、防假冒和防重用，保证网络设备用户身份的真实性。

4.2.3 主机安全

第四级主机安全基本技术要求在身份鉴别、访问控制、安全信息传输路径、审计记录和程序安全方面可以使用密码技术。

在身份鉴别方面，应当采用密码技术来实现组合鉴别，使用密码技术的真实性服务来实现鉴别信息的防假冒和防

重用，并在远程管理时使用密码技术的机密性服务来实现鉴别信息的防窃听。

在访问控制方面，应当使用密码技术的完整性服务来保证细粒度访问控制信息的完整性和所有主体和客体敏感标记的完整性。

在审计记录方面，应当使用密码技术的完整性服务来实现对审计记录和重要程序的完整性检测。

4.2.4 应用安全

第四级应用安全基本技术要求在身份鉴别、访问控制、审计记录和通信安全方面应当使用密码技术。

在身份鉴别方面，应当采用密码技术来实现组合鉴别，使用密码技术的真实性和机密性服务来实现鉴别信息的防重用、防冒用、防泄露，保证应用系统用户身份的真实性。

在访问控制方面，应使用密码技术的完整性服务来保证主体对客体访问控制信息和敏感标记的完整性。

在建立安全的信息传输路径过程中，应当使用密码技术的真实性服务来实现通信主体身份鉴别，并综合使用密码技术的机密性和完整性服务来建立安全通道。

在审计记录方面，应使用密码技术的完整性服务来对审计记录进行完整性保护。

在通信安全方面，应当使用密码技术的完整性服务来保证通信过程中数据完整性；应当使用密码技术的真实性

服务来实现通信双方会话初始化验证；应当使用密码技术的机密性服务来实现对通信过程中整个报文或会话过程加密保护；应当使用密码技术的抗抵赖服务来提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

4.2.5 数据安全及备份恢复

第四级数据安全及备份恢复基本技术要求在数据传输安全、数据存储安全和安全通信协议方面应当使用密码技术。

在数据传输安全方面，应使用密码技术的完整性服务来实现对系统管理数据、鉴别信息和重要业务数据在传输过程中完整性的检测；应使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的传输机密性。

在数据存储安全方面，应使用密码技术的完整性服务来实现对系统管理数据、鉴别信息和重要业务数据在存储过程中完整性的检测；应使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的存储机密性。

在安全通信协议方面，应综合使用密码技术的真实性、完整性和机密性服务来建立安全通信协议。