信息安全等级保护管理办法

为加强信息安全等级保护,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》等国家有关法律法规,制定本办法。

第一章 总 则

第一条 为加强信息安全等级保护,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》等国家有关法律法规,制定本办法。

第二条 信息安全等级保护,是指对国家秘密信息及公民、法人和其他组织的专有信息以及

公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护,对信息系统中使用的信息安全产品实行按等级管理,对信息系统中发生的信息安全事件分等级响应、处置。

第三条 信息系统的安全保护等级应当根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度,信息和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,信息和信息系统应当达到的基本的安全保护水平等因素确定。

第四条 信息系统的安全保护等级分为以下五级:

(一) 第一级为自主保护级,适用于一般的信息系统,其受到破坏后,会对公民、法人和其他组织的合法权益产生损害,但不损害国家安全、社会秩序和公共利益。

(二) 第二级为指导保护级,适用于一般的信息系统,其受到破坏后,会对社会秩序和公共利益造成轻微损害,但不损害国家安全。

(三) 第三级为监督保护级,适用于涉及国家安全、社会秩序和公共利益的重要信息系统,其受到破坏后,会对国家安全、社会秩序和公共利益造成损害。

(四) 第四级为强制保护级,适用于涉及国家安全、社会秩序和公共利益的重要信息系统,其受到破坏后,会对国家安全、社会秩序和公共利益造成严重损害。

(五) 第五级为专控保护级,适用于涉及国家安全、社会秩序和公共利益的重要信息系统的核心子系统,其受到破坏后,会对国家安全、社会秩序和公共利益造成特别严重损害。

第五条 信息系统,运营、使用单位及个人依据本办法和相关技术标准对信息系统进行保护,国家有关信息安全职能部门对其信息安全等级保护工作进行监督管理。

(一) 第一级信息系统运营、使用单位或者个人可以依据国家管理规范和技术标准进行保护。

(二) 第二级信息系统运营、使用单位应当依据国家管理规范和技术标准进行保护。必要时,国家有关信息安全职能部门可以对其信息安全等级保护工作进行指导。

(三) 第三级信息系统运营、使用单位应当依据国家管理规范和技术标准进行保护,国家有关信息安全职能部门对其信息安全等级保护工作进行监督、检查。

(四) 第四级信息系统运营、使用单位应当依据国家管理规范和技术标准进行保护,国家有关信息安全职能部门对其信息安全等级保护工作进行强制监督、检查。

(五) 第五级信息系统运营、使用单位应当依据国家管理规范和技术标准进行保护,国家指定的专门部门或者专门机构对其信息安全等级保护工作进行专门监督、检查。

第六条 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。

第二章 信息安全等级保护的安全管理

第七条 信息系统的运营、使用单位应当依据本办法和有关标准，确定信息系统的安全保护等级。有主管部门的,应当报主管部门审核批准。

第八条 信息系统的运营、使用单位应当根据已确定的安全保护等级，依照本办法和有关技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求得信息技术产品，进行信息系统建设。

第九条 信息系统得运营、使用单位应当履行下列安全等级保护职责：

(一) 落实信息安全等级保护的责任部门和人员,负责信息系统的安全等级保护管理工作；

(二) 建立健全安全等级保护管理制度；

(三) 落实安全等级保护技术标准要求；

(四) 定期进行安全状况检测和风险评估；

(五) 建立信息安全事件的等级响应、处置制度；

(六) 负责对信息系统用户的安全等级保护教育和培训；

(七) 其他应当履行的安全等级保护职责。

第十条 信息系统建设完成后，其运营、使用单位应当依据本办法选择具有国家相关技术资质和安全资质的测评单位，按照技术标准进行安全测评，符合要求的，方可投入使用。

第十一条 从事信息系统安全等级测评的单位，应当遵守国家有关法律法规和技术标准规定，保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，提供安全、客观、公正的检测评估服务。

测评单位资质管理办法由有关部门另行制定。

第十二条 第三级以上信息系统的运营、使用单位应当自系统投入运行之日起三十日内,到所在地的省、自治区、直辖市公安机关指定的受理机构办理备案手续,填写《信息系统安全保护等级备案登记表》。国家另有规定的除外。

备案事项发生变更时,信息系统运营、使用单位或其主管部门应当自变更之日起三十日内将变更情况报原备案机关。

第十三条 公安机关应当掌握信息系统运营、使用单位的备案情况,建立备案档案,进行备案管理。发现不符合本办法及有关标准的,应通知其予以纠正。

第十四条 公安机关应当监督、检查第三级和第四级信息系统运营、使用单位履行安全等级保护职责的情况。

对安全保护等级为三级的信息系统每年至少检查一次,对安全保护等级为四级的信息系统每半年至少检查一次。

第十五条 公安机关发现信息系统运营、使用单位未履行安全等级保护职责或未达到安全保护要求的,应当书面通知其整改。

第三章 信息安全等级保护的保密管理

第十六条 涉及国家秘密的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。

不涉及国家秘密的信息系统不得处理国家秘密信息。

第十七条 涉及国家秘密的信息系统按照所处理信息的最高密级,由低到高划分为秘密级、机密级和绝密级三个级别,其总体防护水平分别不低于三级、四级、五级的要求。

涉及国家秘密的信息系统建设单位应当依据《中华人民共和国保守国家秘密法》和国家有关秘密及其密级具体范围的规定,确定系统处理信息的最高密级和系统的保护级别。

第十八条 涉及国家秘密的信息系统的设计实施、审批备案、运行维护和日常保密管理,按照国家保密工作部门的有关规定和技术标准执行。

第十九条 各级保密工作部门应当对已投入使用的涉及国家秘密的信息系统组织检查和测评。发现系统存在安全隐患或系统保护措施不符合分级保护管理规定和技术标准的,应当通知系统使用单位和管理部门限期整改。

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系统测评。

第四章 信息安全等级保护的密码管理

第二十条 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规定和相关标准。

第二十一条 信息系统安全等级保护中密码的配备、使用和管理等,应严格执行国家密码管理的有关规定。

第二十二条 要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,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,须遵照《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。

第二十三条 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 b 在监督检查过程中,发现存在安全隐患或违反密码管理相关规定或者未达到密码相关标准要求的,按照国家密码管理的相关规定进行处置。

第五章 法律责任

第二十四条 三级、四级信息系统和涉及国家秘密的信息系统的主管部门和运营、使用单位违反本办法规定,有下列行为之一造成严重损害的，由相关部门依照有关法律、法规予以处理：

(一) 未按本办法规定报请备案、审批的;

(二) 未按等级保护技术标准要求进行系统安全制度建设的;

(三) 接到整改通知后,拒不整改的;

(四) 违反保密管理规定的;

(五) 违反密码管理规定的;

(六) 违反本办法其他规定的。

第六章 附 则

第二十五条 军队的计算机信息系统安全保护工作,按照军队的有关法规执行。

第二十六条 本管理办法自 2006 年 3 月 1 日起施行。