

中华人民共和国工业和信息化部令

第 11 号

《通信网络安全防护管理办法》已经 2009 年 12 月 29 日中华人民共和国工业和信息化部第 8 次部务会议审议通过，现予公布，自 2010 年 3 月 1 日起施行。

部 长 李毅中

二〇一〇年一月二十一日

通信网络安全防护管理办法

第一条 为了加强对通信网络安全的管理，提高通信网络安全防护能力，保障通信网络安全畅通，根据《中华人民共和国电信条例》，制定本办法。

第二条 中华人民共和国境内的电信业务经营者和互联网域名服务提供者（以下统称“通信网络运行单位”）管理和运行的公用通信网和互联网（以下统称“通信网络”）的网络安全防护工作，适用本办法。

本办法所称互联网域名服务，是指设置域名数据库或者域名解析服务器，为域名持有者提供域名注册或者权威解析服务的行为。

本办法所称网络安全防护工作，是指为防止通信网络阻塞、中断、瘫痪或者被非法控制，以及为防止通信网络中传输、存储、处理的数据信息丢失、泄露或者被篡改而开展的工作。

第三条 通信网络安全防护工作坚持积极防御、综合防范、分级保护的原则。

第四条 中华人民共和国工业和信息化部（以下简称工业和信息化部）负责全国通信网络安全防护工作的统一指导、协调和检查，组织建立健全通信网络安全防护体系，制定通信行业相关标准。

各省、自治区、直辖市通信管理局（以下简称通信管理局）依据本办法的规定，对本行政区域内的通信网络安全防护工作进行指导、协调和检查。

工业和信息化部与通信管理局统称“电信管理机构”。

第五条 通信网络运行单位应当按照电信管理机构的规定和通信行业标准开展通信网络安全防护工作，对本单位通信网络安全负责。

第六条 通信网络运行单位新建、改建、扩建通信网络工程项目，应当同步建设通信网络安全保障设施，并与主体工程同时进行验收和投入运行。

通信网络安全保障设施的新建、改建、扩建费用，应当纳入本单位建设项目概算。

第七条 通信网络运行单位应当对本单位已正式投入运行的通信网络进行单元划分，并按照各通信网络单元遭到破坏后可能对国家安全、经济运行、社会秩序、公众利益的危害程度，由低到高分别划分为一级、二级、三级、四级、五级。

电信管理机构应当组织专家对通信网络单元的分级情况进行评审。

通信网络运行单位应当根据实际情况适时调整通信网络单元的划分和级别，并按照前款规定进行评审。

第八条 通信网络运行单位应当在通信网络定级评审通过后三十日内，将通信网络单元的划分和定级情况按照以下规定向电信管理机构备案：

（一）基础电信业务经营者集团公司向工业和信息化部申请办理其直接管理的通信网络单元的备案；基础电信业务经营者各省（自治区、直辖市）子公司、分公司向当地通信管理局申请办理其负责管理的通信网络单元的备案；

（二）增值电信业务经营者向作出电信业务经营许可决定的电信管理机构备案；

（三）互联网域名服务提供者向工业和信息化部备案。

第九条 通信网络运行单位办理通信网络单元备案，应当提交以下信息：

- (一) 通信网络单元的名称、级别和主要功能；
- (二) 通信网络单元责任单位的名称和联系方式；
- (三) 通信网络单元主要负责人的姓名和联系方式；
- (四) 通信网络单元的拓扑架构、网络边界、主要软硬件及型号和关键设施位置；
- (五) 电信管理机构要求提交的涉及通信网络安全的其他信息。

前款规定的备案信息发生变化的，通信网络运行单位应当自信息变化之日起三十日内向电信管理机构变更备案。

通信网络运行单位报备的信息应当真实、完整。

第十条 电信管理机构应当对备案信息的真实性、完整性进行核查，发现备案信息不真实、不完整的，通知备案单位予以补正。

第十一条 通信网络运行单位应当落实与通信网络单元级别相适应的安全防护措施，并按照以下规定进行符合性评测：

- (一) 三级及三级以上通信网络单元应当每年进行一次符合性评测；
- (二) 二级通信网络单元应当每两年进行一次符合性评测。

通信网络单元的划分和级别调整的，应当自调整完成之日起九十日内重新进行符合性评测。

通信网络运行单位应当在评测结束后三十日内，将通信网络单元的符合性评测结果、整改情况或者整改计划报送通信网络单元的备案机构。

第十二条 通信网络运行单位应当按照以下规定组织对通信网络单元进行安全风险评估，及时消除重大网络安全隐患：

- (一) 三级及三级以上通信网络单元应当每年进行一次安全风险评估；
- (二) 二级通信网络单元应当每两年进行一次安全风险评估。

国家重大活动举办前，通信网络单元应当按照电信管理机构的要求进行安全风险评估。

通信网络运行单位应当在安全风险评估结束后三十日内,将安全风险评估结果、隐患处理情况或者处理计划报送通信网络单元的备案机构。

第十三条 通信网络运行单位应当对通信网络单元的重要线路、设备、系统和数据等进行备份。

第十四条 通信网络运行单位应当组织演练,检验通信网络安全防护措施的有效性。

通信网络运行单位应当参加电信管理机构组织开展的演练。

第十五条 通信网络运行单位应当建设和运行通信网络安全监测系统,对本单位通信网络的安全状况进行监测。

第十六条 通信网络运行单位可以委托专业机构开展通信网络安全评测、评估、监测等工作。

工业和信息化部应当根据通信网络安全防护工作的需要,加强对前款规定的受托机构的安全评测、评估、监测能力指导。

第十七条 电信管理机构应当对通信网络运行单位开展通信网络安全防护工作的情况进行检查。

电信管理机构可以采取以下检查措施:

- (一) 查阅通信网络运行单位的符合性评测报告和风险评估报告;
- (二) 查阅通信网络运行单位有关网络安全防护的文档和工作记录;
- (三) 向通信网络运行单位工作人员询问了解有关情况;
- (四) 查验通信网络运行单位的有关设施;
- (五) 对通信网络进行技术性分析和测试;
- (六) 法律、行政法规规定的其他检查措施。

第十八条 电信管理机构可以委托专业机构开展通信网络安全检查活动。

第十九条 通信网络运行单位应当配合电信管理机构及其委托的专业机构开展检查活动,对于检查中发现的重大网络安全隐患,应当及时整改。

第二十条 电信管理机构对通信网络安全防护工作进行检查,不得影响通信网络的正常运行,不得收取任何费用,不得要求接受检查的单位购买指定品牌或者指定单位的安全软件、设备或者其他产品。

第二十一条 电信管理机构及其委托的专业机构的工作人员对于检查工作中获悉的国家秘密、商业秘密和个人隐私,有保密的义务。

第二十二条 违反本办法第六条第一款、第七条第一款和第三款、第八条、第九条、第十一条、第十二条、第十三条、第十四条、第十五条、第十九条规定的,由电信管理机构依据职权责令改正;拒不改正的,给予警告,并处五千元以上三万元以下的罚款。

第二十三条 电信管理机构的工作人员违反本办法第二十条、第二十一条规定的,依法给予行政处分;构成犯罪的,依法追究刑事责任。

第二十四条 本办法自 2010 年 3 月 1 日起施行。