

发布或者传输的信息的,应当立即停止传输该信息,采取消除等处置措施,防止信息扩散,保存有关记录,并向有关主管部门报告。(违法信息传播的阻断义务)

第四十八条 任何个人和组织发送的电子信息、提供的应用软件,不得设置恶意程序,不得含有法律、行政法规禁止发布或者传输的信息。(禁止传播违法信息)

电子信息发送服务提供者和应用软件下载服务提供者,应当履行安全管理义务,知道其用户有前款规定行为的,应当停止提供服务,采取消除等处置措施,保存有关记录,并向有关主管部门报告。(违法信息传播的阻断义务)

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度,公布投诉、举报方式等信息,及时受理并处理有关网络信息安全的投诉和举报。网络运营者对网信部门和有关部门依法实施的监督检查,应当予以配合。(配合义务)

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责,发现法律、行政法规禁止发布或者传输的信息的,应当要求网络运营者停止传输,采取消除等处置措施,保存有关记录;对来源于中华人民共和国境外的上述信息,应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作,按照规定统一发布网络安全监测预警信息。(将信息通报制度上升为法律)

第五十二条 负责关键信息基础设施安全保护工作的部门,应当建立健全本行业、本领域的网络安全监测预警和信息通报制度,并按照规定报送网络安全监测预警信息。(要求行业建立信息通报制度)

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制,制定网络安全事件应急预案,并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案,并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级,并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时,省级以上人民政府有关部门应当按照规定的权限和程序,并根据网络安全风险的特点和可能造成的危害,采取下列措施:

(一)要求有关部门、机构和人员及时收集、报告有关信息,加强对网络安全风险的监测;

(二)组织有关部门、机构和专业人员,对网络安全风险信息进行分析评估,预测事件发生的可能性、影响范围和危害程度;

(三)向社会发布网络安全风险预警,发布避免、减轻危害的措施。

第五十五条 发生网络安全事件,应当立即启动网络安全事件应急预案,对网络安全事件进行调查和评估,要求网络运营者采取技术措施和其他必要措施,消除安全隐患,防止危害扩大,并及时向社会发布与公众有关的警示信息。(事件应急处置)

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中,发现网络存在较大安全风险或者发生安全事件的,可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施,进行整改,消除隐患。(约谈)

第五十七条 因网络安全事件,发生突发事件或者生产安全事故的,应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家和社会公共秩序,处置重大突发社会安全事件的需要,经国务院