

国家安全审查)

第三十六条 关键信息基础设施的运营者采购网络产品和服务, 应当按照规定与提供者签订安全保密协议, 明确安全和保密义务与责任。(外包服务安全, 防范服务商)

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要, 确需向境外提供的, 应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估; 法律、行政法规另有规定的, 依照其规定。(数据留存和提供)

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估, 并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。(等级测评, 风险评估, 渗透测试)

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施:

(一) 对关键信息基础设施的安全风险进行抽查检测, 提出改进措施, 必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估;

(二) 定期组织关键信息基础设施的运营者进行网络安全应急演练, 提高应对网络安全事件的水平和协同配合能力;

(三) 促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享;

(四) 对网络安全事件的应急处置与网络功能的恢复等, 提供技术支持和协助。

第四章 网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密, 并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息, 应当遵循合法、正当、必要的原则, 公开收集、使用规则, 明示收集、使用信息的目的、方式和范围, 并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息, 不得违反法律、行政法规的规定和双方的约定收集、使用个人信息, 并应当依照法律、行政法规的规定和与用户的约定, 处理其保存的个人信息。(强化个人信息保护)

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息; 未经被收集者同意, 不得向他人提供个人信息。但是, 经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施, 确保其收集的个人信息安全, 防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时, 应当立即采取补救措施, 按照规定及时告知用户并向有关主管部门报告。(网络运营者对个人信息保护责任)

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的, 有权要求网络运营者删除其个人信息; 发现网络运营者收集、存储的其个人信息有错误的, 有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息, 不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员, 必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密, 不得泄露、出售或者非法向他人提供。(监管人员责任)

第四十六条 任何个人和组织应当对其使用网络的行为负责, 不得设立用于实施诈骗, 传授犯罪方法, 制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组, 不得利用网络发布涉及实施诈骗, 制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理, 发现法律、行政法规禁止