

网络安全法

课程目标：

随着互联网的快速发展和信息化程度的不断提高，互联网深刻影响着政治、经济、文化等各个方面，保障信息安全的重要性日益凸显，加强对互联网上各类信息的管理应引起高度重视。在系统安全方面，以提高防御、应急处置能力为主的传统安全管理已经不能适应新计算、新网络、新应用和新数据为新特征的信息安全产业发展的需要。

网络信息安全是一个关系国家安全和主权、社会稳定、民族文化继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快越来越重要。网络信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合学科。它主要是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

1月7日上午，十二届全国人大常委会第二十四次会议表决，正式的通过了《中华人民共和国网络安全法》。网络安全法将于2017年6月1日起施行。

适用学员：

企业信息安全主管，参与信息系统审计和管理体系规划的人员，提供信息安全咨询服务的专业人员，其他对信息安全全面的知识体系感兴趣的人员。具体培训对象包括：

- 政府机关信息安全员
- 事业单位
- 企业信息安全主管
- 信息安全业内人士
- IT 或安全顾问人员
- IT 审计人员
- 信息安全事件调查人员
- 其他从事与信息安全相关工作的人员（如系统管理员、程序员、保安人员等）

课程设计：

授课课时：	1-2 天
授课条件：	学员必须具有基本的计算机或网络操作知识
内容摘要：	第一章 我国网络安全立法体系框架

1、什么是网络？

- ✓ 什么是网络安全
- ✓ 网络安全目标
- ✓ 重要的概念

2、法律条文总览

- ✓ 总体框架
- ✓ 条文要点
- ✓ 网络安全法的适用范围

3、相关职责

- ✓ 国家职责
- ✓ 网络运营者职责
- ✓ 行业组织职责

第二章 网络运行安全

1、网络通信基础

- ✓ 世界网络概述
- ✓ 中国网络发展状态

2、网络安全等级保护制度

- ✓ 发达国家网络保护
- ✓ 网络攻击事件

3、网络产品和服务

- ✓ 现有典型产品
- ✓ VR 带来的变化

4、远程访问安全与管理

- ✓ 网络关键设备和网络安全专业产品
- ✓ 网络实名制

5、关键信息基础设施范围

- ✓ 建设要求
- ✓ 安全保护

- ✓ 安全审查
- ✓ 保密要求
- ✓ 境内存储

6、法律义务

- ✓ 检测评估
- ✓ 统筹协调

第三章 网络信息安全

1、数据保护范围

- ✓ 用户信息保护要点
- ✓ 个人信息保护
- ✓ 商业秘密保护要点

2、数据保护方式

- ✓ 数据本地化
- ✓ 数据异地化

3、网络行为要求

- ✓ 行为规范
- ✓ 自由化行为

4、国家及主管部门

- ✓ 部委级
- ✓ 地市级
- ✓ 公检法行为

第四章 监测预警与应急处置

1、什么是访问控制？

- ✓ 功能和分类
- ✓ 身份识别与认证技术：口令、一次性口令、生物识别

2、访问控制技术

- ✓ MAC
- ✓ DAC
- ✓ 基于角色 AC

3、访问控制模型

- ✓ 状态机模型
- ✓ BLP 模型
- ✓ Biba 模型

4、访问控制管理

- ✓ 账号管理
- ✓ 权限管理
- ✓ 跟踪审计

5、攻击手段

- ✓ 口令攻击
- ✓ 拒绝服务
- ✓ 欺骗攻击
- ✓ 渗透测试

第五章 法律责任

1、行政处罚

- ✓ 行政处罚法 相关
- ✓ 行政诉讼法 相关
- ✓ 行政复议法 相关

2、民事责任

- ✓ 治安管理处罚条例 相关
- ✓ 地方法规 相关

3、刑事责任

- ✓ 刑事诉讼法 相关
- ✓ 保守国家秘密法 相关
- ✓ 国家安全法 相关

- ✓ 刑法 相关

第六章 守法与机遇

1、网络运营者法律合规要求

- ✓ 各种应用于 Internet 的安全标准和协议
- ✓ 密码分析学和攻击手段
- ✓ 政府介入，密钥托管

2、产品研发

- ✓ 公钥基础设施 PKI，CA 证书
- ✓ 密钥管理：生成、交换、撤销、恢复

3、产业机会

- ✓ 创新应用

授课语言：

中文