电子科技大学
University of Electronic Science and Technology of China

信息安全导论

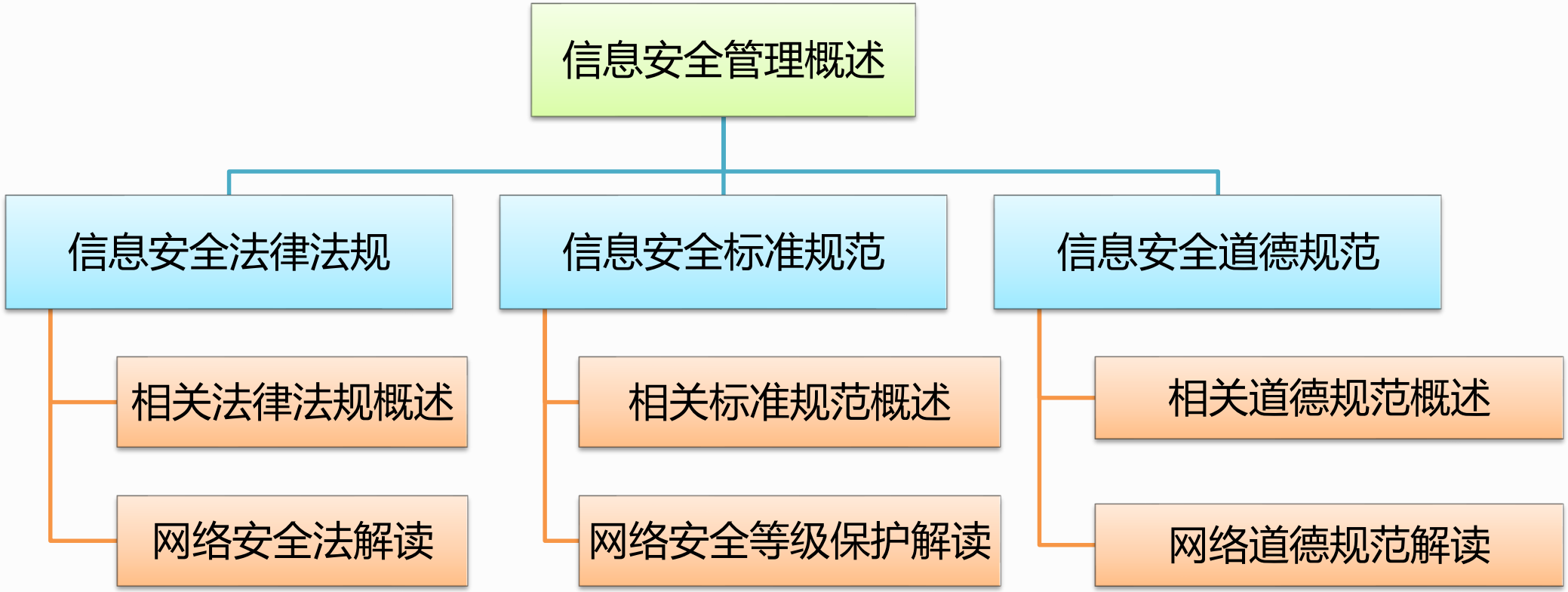
教学模块四：信息安全管理概述

赵洋 副教授

电子科技大学 信息与软件工程学院

2022年10月8日

内容安排


信息安全管理概述
信息安全法律法规
信息安全标准规范
信息安全道德规范
相关法律法规概述
网络安全法解读
相关标准规范概述
网络安全等级保护解读
相关道德规范概述
网络道德规范解读

引言

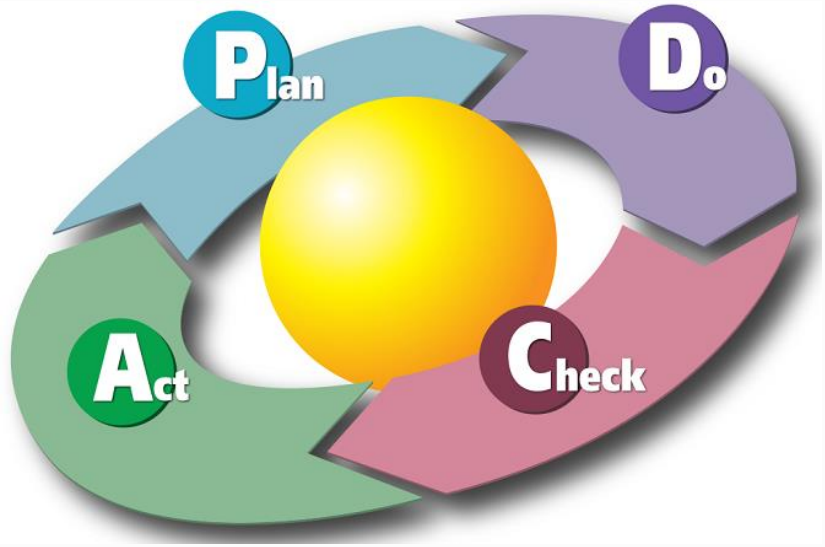
- 信息安全保障是一项复杂的系统工程，仅凭技术手段很难达成达成预期的安全保障目标。统计结果表明，在所有信息安全事故中，只有20%~30%是由于黑客入侵或其他外部原因造成的，70%~80%是由于内部员工的疏忽或有意泄密造成的。

保险柜就一定安全吗？

- 如果你把钥匙落在锁眼上会怎样？
- 技术措施需要配合正确的使用才能发挥作用。

引言

- 信息安全管理是一个十分复杂的综合管理体系，法律法规、规章制度和道德规范是管理的基础，标准规范是信息系统实施和安全运行的保障，其最终的目标是实现对安全风险的有效管理。



- 信息安全管理体系ISMS（Information Security Management System）是从管理学惯用的过程模型PDCA（Plan、Do、Check、Act）发展演化而来。
  - 规划（Plan）通过风险评估，了解安全需求，制订解决方案；
  - 实施（Do）将解决方案付诸实施；
  - 检查（Check）监视评审方案的有效性；
  - 处置（Act）对发现的问题予以解决，产生新的需求则再次进入规划阶段。

推进网络安全法治建设
提高网络治理能力

第一部分 信息安全法律法规管理

重点掌握信息安全法律法规的体系构成，了解我国网络安全法的主要内容

一、信息安全法律法规管理

1、相关法律法规概述

- 信息安全法律法规是指国家和相关职能部门为维护信息安全，预防信息犯罪的法律规范的总称。
- 目前我国现行法律法规中，与信息安全有关的已有近百部。
  - 涉及网络与信息系统安全、信息内容安全、信息安全系统与产品、保密及密码管理、计算机病毒与危害性程序防治、金融等特定领域的信息安全、信息安全犯罪制裁等多个领域，初步形成了我国信息安全的法律体系。

《中华人民共和国网络安全法》是为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定的法律。由全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行。

一、信息安全法律法规管理

1、相关法律法规概述

我国信息安全法律法规体系构成

- 通用性法律法规
  - 这类法律包括《宪法》、《国家安全法》、《国家秘密法》等，这些法律没有专门针对信息安全的规定，但约束的对象包括危害信息安全行为。
- 惩戒信息犯罪的法律
  - 这类法律包括《中华人民共和国刑法》、《中华人民共和国网络安全法》等。这类法律中的有关法律条文可以作为规范和惩罚网络犯罪的法律规定。
- 针对信息网络安全的特别规定
  - 这类法规主要有《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中华人民共和国计算机软件保护条例》，这些法规指定的目的是明确哪些行为构成违反法律法规，并可能被追究相关民事或刑事责任。

一、信息安全法律法规管理

1、相关法律法规概述

◘ 通用性法律法规中相关规定

- 《中华人民共和国宪法》对公民通信自由和通信秘密权有充分的保障
  - 《中华人民共和国宪法》的第四十条规定“中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。”
- 《中华人民共和国保守国家秘密法》对保守国家秘密有严格的要求
  - 《中华人民共和国保守国家秘密法》的第三条规定“一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务”。

一、信息安全法律法规管理

1、相关法律法规概述

◘ 案例思考 （一）—— 网络反恐

- 2014年我国公安机关通过网络监控，在掌握大量有力证据的情况下，将利用互联网鼓吹“新疆独立”，利用讲堂煽动“推翻政府”，利用教师身份从事分裂活动的中央民族大学的某教师绳之以法。
  - 观点一：网络空间是自由的空间，国家对网络空间的监管侵犯了公民的言论自由权
  - 观点二：网络空间不是法外之地，公民在网络空间中的言行也不能突破法律的底线

哪种观点是正确的?

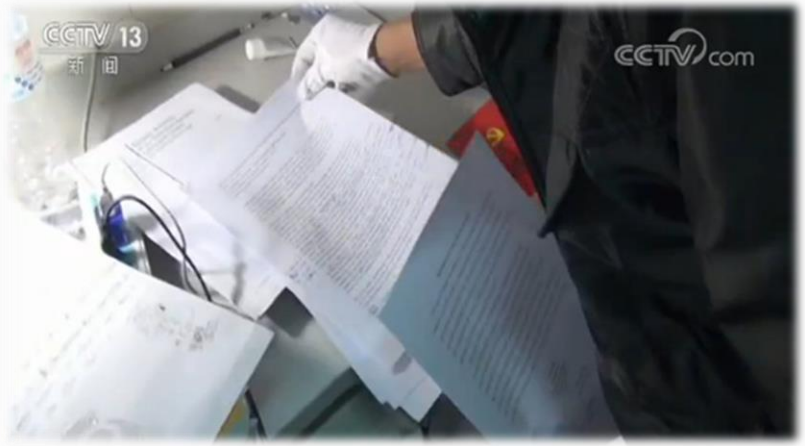
美国政府制定的《爱国者法》等反恐法案，规定政府可以合法监听公民，并要求所有大企业必须和政府合作，全方位为政府提供情报。

一、信息安全法律法规管理

1、相关法律法规概述

◘ 案例思考（二）—— 泄露国家机密

- 据有关报道，2011年正在一所重点大学机械专业读二年级的小哲，因为学习成绩优异，得到了去台湾义守大学学习交流的机会。而他所学习的专业，可以接触到不少国防科工的机密，因此在台期间成为重要目标，被间谍人员策反。小哲结束交流返回学校后，多次向境外人员提供了涉及我国防科工的近百份情报，最终受到了法律的严惩。



这个案例有什么值得思考的地方？

一、信息安全法律法规管理

- 测试点4-1
  - 什么是信息安全管理中的PDCA模型?
  - 我国的信息安全法律法规体系是如何构成的?
  - 有人说西方的网络环境是开放自由的，公民在网络空间中的行为不会受到管理和监控，这种观点是正确的吗？请查阅相关资料，谈谈自己的看法。

2、《中华人民共和国网络安全法》解读

□ 《网络安全立法》立法的必须性

- 当今社会，随着网络的快速发展，存在的网络安全问题也是接踵而来：网络入侵、网络攻击等非法活动威胁信息安全；非法获取公民信息、侵犯知识产权、损害公民合法利益；宣扬恐怖主义、极端主义，严重危害国家安全和社会公共利益。

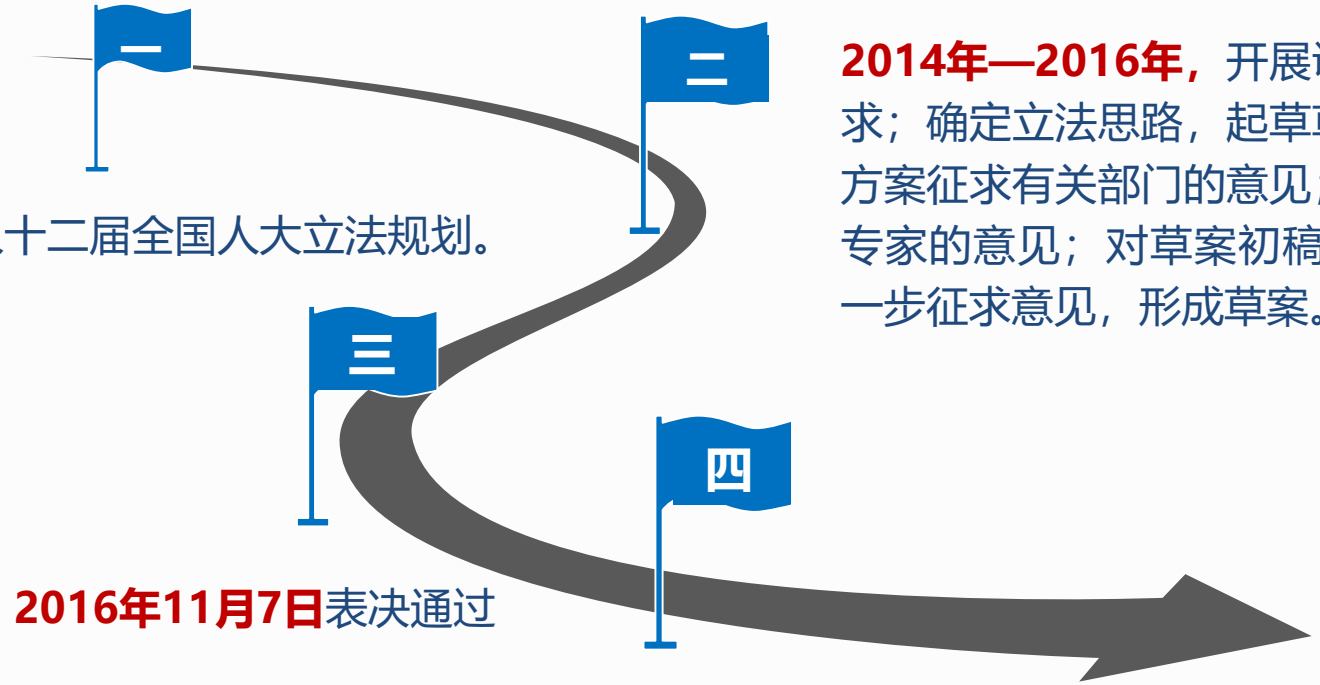
立法的必要性

- 是维护网络安全的客观需要
- 是维护广大人民群众切身利益的必然要求
- 是参与互联网国际竞争和国际治理的必然选择

一、信息安全法律法规管理

2、《中华人民共和国网络安全法》解读

□ 网络安全法审议流程



2013年10月列入十二届全国人大立法规划。

2014年—2016年，开展调查研究，掌握各方面立法需求；确定立法思路，起草草案大纲；拟订主要制度初步方案征求有关部门的意见；起草草案初稿征求有关部门专家的意见；对草案初稿进行修改形成征求意见稿;进一步征求意见，形成草案。

2016年11月7日表决通过

2017年6月1日，正式施行。

2、《中华人民共和国网络安全法》解读

《网络安全法》的基本原则

- 网络空间主权原则
  - 《网络安全法》第1条“立法目的”开宗明义，明确规定要维护我国网络空间主权。
- 网络安全与信息化发展并重原则
  - 《网络安全法》第3条明确规定，国家坚持网络安全与信息化并重，遵循积极利用、科学发展、依法管理、确保安全的方针；既要推进网络基础设施建设，鼓励网络技术创新和应用，又要建立健全网络安全保障体系，提高网络安全保护能力，做到“双轮驱动、两翼齐飞”。
- 共同治理原则
  - 《网络安全法》坚持共同治理原则，要求采取措施鼓励全社会共同参与。

2、《中华人民共和国网络安全法》解读

□ 《网络安全法》影响及重要性

➢ 当前，网络和信息技术迅猛发展、已经深度融入我国经济社会的各个方面，极大地改变和影响人们的社会活动和生活方式、在促进技术创新、经济房展、文化繁荣、社会进步的同时，网络安全问题也日益凸显。

对个人	**从源头杜绝个人信息泄露，违法必究** 《网络安全法》进一步完善了个人信息保护规则，可从源头杜绝个人信息泄露，如规定网络运营者收集、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。
对企业	**网络安全产业将迎发展，这些机会要抓住** 《网络安全法》在规范一般企业网络安全义务的基础上，特别针对三类企业，即网络运营者，比如通信运营商等；网络产品、服务的提供者，比如网购平台等；关键信息基础设施运营者，比如电力公司、股票交易中心等做了强制性的义务规范内容。

一、信息安全法律法规管理

2、《中华人民共和国网络安全法》解读

□ 《网络安全法》基本架构

中华人民共和国
网络安全法

第一章	第二章	第三章	第四章	第五章	第六章	第七章
总　则	网络安全支持与促进	网络运行安全	网络信息安全	监测预警与应急处置	法律责任	附　则

9800余字

总则 + 6章 = 79条

一、信息安全法律法规管理

2、《中华人民共和国网络安全法》解读

□ 《网络安全法》八大亮点

将信息安全等级保护制度上升为法律

对支持、促进网络安全发展的措施作了规定

明确了网络产品和服务提供者的安全义务和个人信息保护义务

明确建立国家统一的监测预警、信息通报和应急处置制度和体系

明确了关键信息基础设施的范围和关键信息基础设施保护制度的主要内容

进一步完善了网络运营者收集、使用个人信息的规则及其保护个人信息安全的义务与责任

明确了国家网信部门对网络安全工作的统筹协调职责和相关监督管理职责

确定网络实名制，并明确了网络运营者对公安机关、国际安全机关维护网络安全和侦查犯罪的活动提供技术支持和协助的义务

2、《中华人民共和国网络安全法》解读

《网络安全法》六大看点

- ★ 不得出售个人信息
- ★ 以法律形式明确“网络实名制”
- ★ 惩治攻击破坏我国关键信息基础设施的境外组织和个人
- ★ 严厉打击网络诈骗
- ★ 重点保护关键信息基础设施
- ★ 重大突发事件可采取“网络通信管制”

2、《中华人民共和国网络安全法》解读

□ 不得出售个人信息

➢ 根据中国互联网协会发布的《２０１６中国网民权益保护调查报告》，８４％的网民曾亲身感受到由于个人信息泄露带来的不良影响。从２０１５年下半年到今年上半年的一年间，我国网民因垃圾信息、诈骗信息、个人信息泄露等遭受的经济损失高达９１５亿元。近年来，警方查获曝光的大量案件显示，公民个人信息的泄露、收集、转卖，已经形成了完整的黑色产业链。

一	网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意
二	网络运营者不得泄露、篡改、毁损其收集的个人信息
三	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，并规定了相应法律责任。

2、《中华人民共和国网络安全法》解读

□ 严厉打击网络诈骗

- 个人信息的泄露是网络诈骗泛滥的重要原因。诈骗分子通过非法手段获取个人信息，包括姓名、电话、家庭住址等详细信息后，再实施精准诈骗，令人防不胜防。广受舆论关注的山东两名大学生遭电信诈骗死亡案、清华大学教授遭电信诈骗案，都是因为信息泄露之后的精准诈骗造成。
- 网络安全法针对层出不穷的新型网络诈骗犯罪还规定：任何个人和组织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，不得利用网络发布与实施诈骗，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。

2、《中华人民共和国网络安全法》解读

- 以法律形式明确“网络实名制”
  - “垃圾评论”充斥论坛，“一言不合”就恶意辱骂，更有甚者“唯恐天下不乱”传播制造谣言……一段时间以来，种种乱象充斥着虚拟的网络空间。
  - 网络安全法以法律的形式对“网络实名制”作出规定：网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

一、信息安全法律法规管理

2、《中华人民共和国网络安全法》解读

◘ 重点保护关键信息基础设施

- “物理隔离”防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取……这些信息基础设施的安全隐患，不出问题则已，一出就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。
- 网络安全法专门单列一节，对关键信息基础设施的运行安全进行明确规定，指出国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域的关键信息基础设施实行重点保护。

一、信息安全法律法规管理

2、《中华人民共和国网络安全法》解读

- 惩治攻击破坏我国关键信息基础设施的境外组织和个人
  - ２０１４年国家网信办曾披露数据显示，我国一直是网络攻击的受害国，每个月有１万多个网站被篡改，８０％的政府网站受到过攻击，这些网络攻击主要来自美国。
  - 网络安全法规定，境外的个人或者组织从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该个人或者组织采取冻结财产或者其他必要的制裁措施。

2、《中华人民共和国网络安全法》解读

◘ 重大突发事件可采取“网络通信管制”

- 现实社会中，出现重大突发事件，为确保应急处置、维护国家和公众安全，有关部门往往会采取交通管制等措施。网络空间也不例外。
- 网络安全法中，对建立网络安全监测预警与应急处置制度专门列出一章作出规定，明确了发生网络安全事件时，有关部门需要采取的措施。特别规定：因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

2、《中华人民共和国网络安全法》解读

《网络安全法》应用案例一

- 2017年7月20日，广东汕头网警支队在对该市网络安全等级保护重点单位进行执法检查时发现，汕头市某信息科技有限公司于2015年11月向公安机关报备的信息系统安全等级为第三级，经测评合格后投入使用，但2016年至今未按照规定定期开展等级测评。根据网络安全法第 五十九条规定，广东汕头网警支队依法对该单位给予警告处罚并责令其改正。
- 法律依据：《网络安全法》第21条、第59条第1款
  - 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

2、《中华人民共和国网络安全法》解读

□ 《网络安全法》应用案例二

- 重庆公安局网安总队在日常检查中发现，重庆市某科技发展有限公司自《网络安全法》正式实施以来，在提供互联网数据中心服务时，存在未依法留存用户登录相关网络日志的违法行为。公安机关根据《网络安全法》相关规定，决定给予该公司警告处罚，并责令限期15日内进行整改。
- 法律依据：《网络安全法》第21条、第59条
  - 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

2、《中华人民共和国网络安全法》解读

《网络安全法》应用案例三

- 江苏宿迁市某科技有限公司服务器内接入一违法网站被民警发现，民警经勘验取证后，立即传唤该公司法人代表王某，要求对提供互联网接入服务的服务器内涉及法律、行政法规禁止传输的信息立即予以停止传输、采取消除等处置措施并保存有关记录，并根据《网络安全法》规定， 给予上述公司警告处罚并要求其立即整改到位。
- 法律依据：《网络安全法》第47、第68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。

2、《中华人民共和国网络安全法》解读

《网络安全法》应用案例三

- 2016年6月22日，“智联招聘”向公安机关报案称，公司发现员工申某私下出售几十万条网站的个人简历，内容包括姓名、身份证号、住址、电话、受教育程度、工作单位、薪资收入等个人信息。2017年6月2日，申某因涉嫌非法获取公民信息罪，在朝阳法院出庭受审。经审理，法院认定其行为构成非法获取公民信息罪，判处申某有期徒刑三年六个月
- 法律依据：《网络安全法》第44、第74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。

一、信息安全法律法规管理

- 测试点4-2
  - 请查阅《中华人民共和国网络安全法》，回答以下问题：
    - 网络安全法是如何规范个人信息收集行为的?
    - 网络安全法是如何斩断信息买卖利益链的?
    - 网络安全法是如何防范个人信息泄露的?
    - 网络安全法是如何对网络诈骗溯源追责?

网络安全为人民

网络安全靠人民

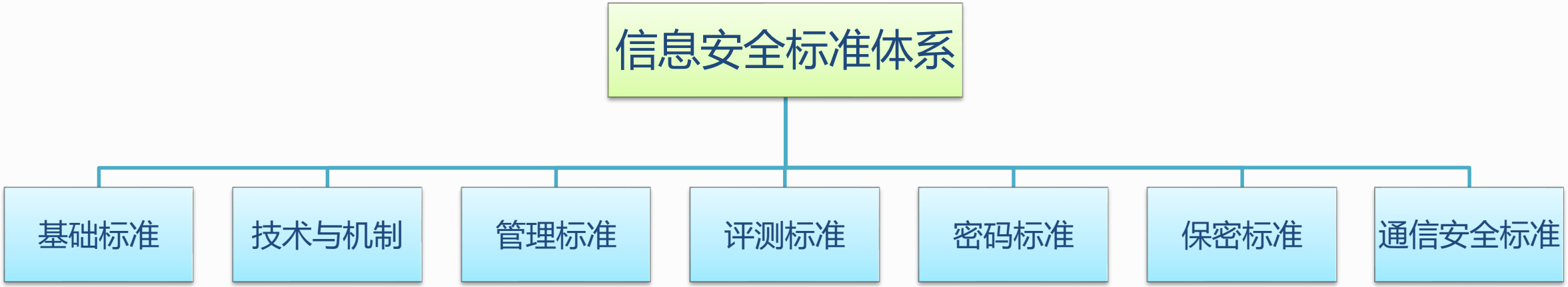
第二部分 信息安全标准规范管理

重点掌握信息安全标准规范的体系构成，了解我国网络安全等级保护的主要内容

二、信息安全标准规范管理

1、信息安全标准规范概述

- 标准规范管理可理解为在规划实施信息安全解决方案时，各项工作遵循国际或国家相关标准规范，建立完善的信息安全保障和审核机制。
- 我国信息安全标准体系



二、信息安全标准规范管理

1、信息安全标准规范概述

◘ 信息安全标准规范分类

- 互操作标准
  - 主要是非标准组织研发的算法和协议经过自发的选择过程，成为了所谓的“事实标准”，如AES、RSA、SSL以及通用脆弱性描述标准CVE等。
- 技术与工程标准
  - 主要指由标准化组织制定的用于规范信息安全产品、技术和工程的标准，如信息产品通用评测准则、安全系统工程能力成熟度模型等。
- 信息安全管理与控制标准
  - 由标准化组织制定的用于指导和管理信息安全解决方案实施过程的标准规范，如信息安全管理体系标准、信息安全管理标准以及信息和相关技术控制目标等。

二、信息安全标准规范管理

1、信息安全标准规范概述

□ 我国信息安全标准规范建设

一 1985年发布了第一个标准GB4943“信息技术设备的安全”

二 1994年发布了第一批信息安全技术标准。

三 截止2008年11月，国家共发布有关信息安全技术、产品、测评和管理的国家标准69项（不包括密码与保密标准）。

四 2019年5月，全国信息安全标准化技术委员会发布《 网络安全等级保护基本要求》系列标准。

二、信息安全标准规范管理

2、网络安全等级保护解读

- 等保1.0
  - 在我国众多的信息安全标准中，公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准GB17895-1999《计算机信息系统安全保护等级划分准则》、《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求 》为代表的等级保护系列配套标准被认为我国信息安全标准的奠基石，习惯称为等保1.0。
- 等保2.0
  - 2017年1月至2月，全国信息安全标准化技术委员会发布与等级保护相关的系列标准“征求意见稿”， 2019年5月13日，GB/T 22239-2019 《网络安全等级保护基本要求》正式颁布。
  - 2017年5月，国家公安部发布《GA/T 1389—2017 网络安全等级保护定级指南》、《GA/T 1390.2—2017 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求》等4个公共安全行业等级保护标准， 习惯称为等保2.0 。

二、信息安全标准规范管理

2、网络安全等级保护解读

◘ 等保1.0→2.0

GB 17859-1999 《计算机信息系统安全保护等级划分准则》

- ◘ 正式更名为网络安全等级保护标准；
- ◘ 横向扩展了对云计算、移动互联网、物联网、工业控制系统的安全要求；
- ◘ 纵向扩展了对等保测评机构的规范管理。

《信息系统安全等级保护定级指南》

《网络安全等级保护基本要求》

- 第1部分：安全通用要求
- 第2部分：云计算安全扩展要求
- 第3部分：移动互联安全扩展要求
- 第4部分：物联网安全扩展要求
- 第5部分：工业控制系统安全扩展要求

《网络安全等级保护实施指南》

《网络安全等级保护安全设计技术要求》

- 第1部分：安全通用要求
- 第2部分：云计算安全扩展要求
- 第3部分：移动互联安全扩展要求
- 第4部分：物联网安全扩展要求
- 第5部分：工业控制系统安全扩展要求

《网络安全等级保护测评要求》

- 第1部分：安全通用要求
- 第2部分：云计算安全扩展要求
- 第3部分：移动互联安全扩展要求
- 第4部分：物联网安全扩展要求
- 第5部分：工业控制系统安全扩展要求

《网络安全等级保护测评过程指南》

《网络安全等级保护测试评估技术指南》

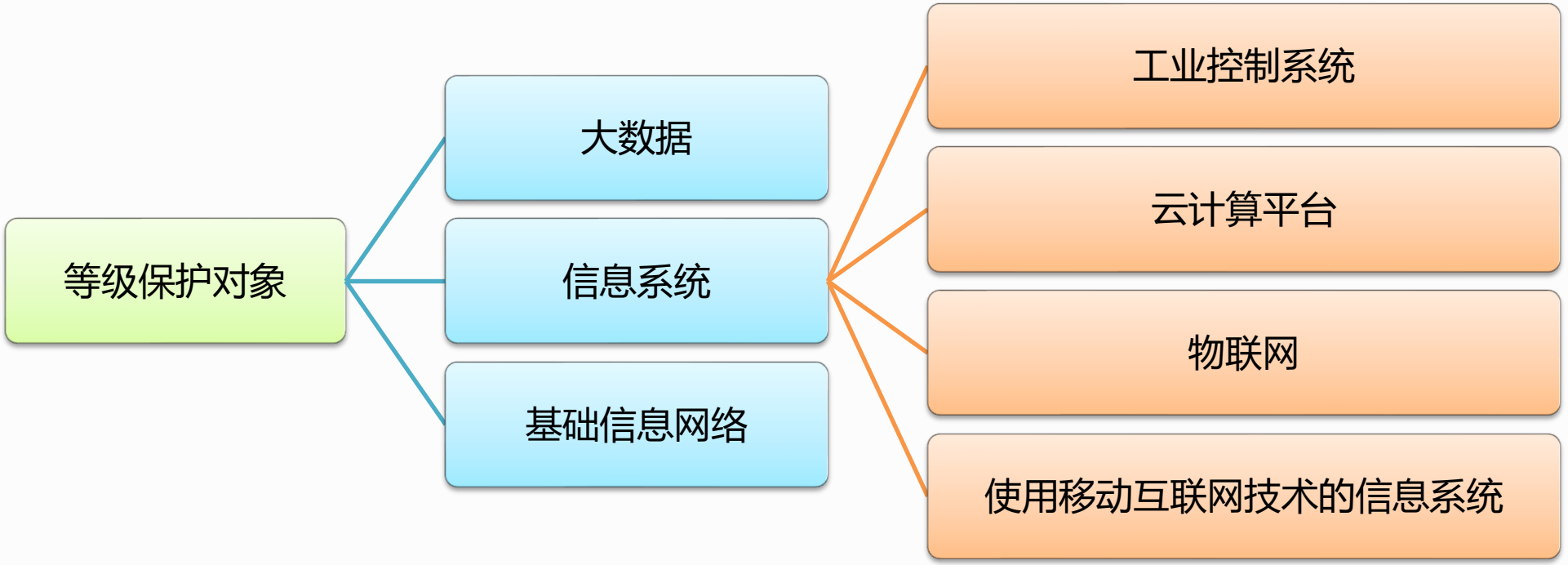
《网络安全等级保护安全管理中心技术要求》

《网络安全等级测评机构能力要求和评估规范》

未变化
修订内容
新增

2、网络安全等级保护解读

保护对象



2、网络安全等级保护解读

- GB17895-1999《计算机信息系统安全保护等级划分准则》
  - 第一级 用户自主保护级：提供用户和数据隔离功能。
  - 第二级 系统审计保护级：实施粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。
  - 第三级 安全标记保护级：具有系统审计保护的功能。
  - 第四级 结构化保护级：建立在一个明确定义的形式化安全策略模型之上，要求将第三级系统中的访问控制扩展到所有主体与客体。
  - 第五级 访问验证保护级：满足访问监控器需求，由访问监控器仲裁主体对客体的全部访问。

2、网络安全等级保护解读

- GA/T 1389—2017《信息安全技术　网络安全等级保护定级指南》
  - 一般损害：工作职能受到局部影响，业务能力下降，但不影响主要功能执行；
  - 严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行；
  - 特别严重损害：工作职能收到特别严重影响或丧失行使能力，业务能力严重下降或功能无法执行。

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织	第一级	第二级	第三级
社会秩序和公共利益	第二级	第三极	第四级
国家安全	第三极	第四级	第五级

2、网络安全等级保护解读

◘ 等级保护建设核心思想

➢信息系统的安全设计应基于业务流程自身特点，建立“可信、可控、可管”的安全防护体系，使得系统能够按照预期运行，免受信息安全攻击和破坏。

可信 1

即以可信认证为基础，构建一个可信的业务系统执行环境，即用户、平台、程序都是可信的，确保用户无法被冒充、病毒无法执行、入侵行为无法成功。可信的环境保证业务系统永远都按照设计预期的方式执行，不会出现非预期的流程，从而保障了业务系统安全可信。

可控 2

即以访问控制技术为核心，实现主体对客体的受控访问，保证所有的访问行为均在可控范围之内进行，在防范内部攻击的同时有效防止了从外部发起的攻击行为。对用户访问权限的控制可以确保系统中的用户不会出现越权操作，永远都按系统设计的策略进行资源访问，保证了系统的信息安全可控。

可管 3

即通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建一个工作平台，使其可以进行技术平台支撑下的安全策略管理，从而保证信息系统安全可管。

二、信息安全标准规范管理

2、网络安全等级保护解读

◘ 等级保护工作流程（等保五部曲）

➢网络安全等级保护工作包括定级、备案、安全建设、等级测评、监督检查五个阶段。

①定级

- 确认定级对象,参考《定级指南》等初步确认等级,组织专家评审,主管单位审核,公安机关备案审查。

②备案

- 持定级报告和备案表等材料到公安机关网安部门进行备案。

③安全建设

- 以《基本要求》中对应等级的要求为标准,对定级对象当前不满足要求的进行建设整改。

④等级评测

- 委托具备测评资质的测评机构对定级对象进行等级测评,形成正式的测评报告。

⑤监督检查

- 向当地公安机关网安部门提交测评报告,配合完成对网络安全等级保护实施情况的检查。

2、网络安全等级保护解读

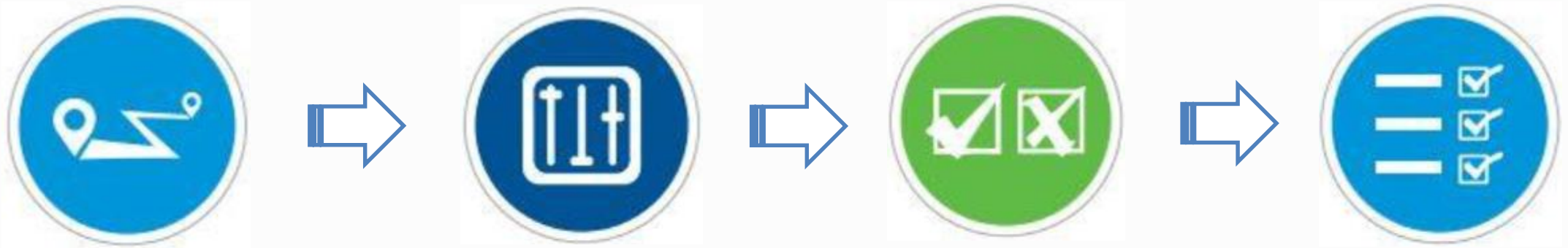
□ 步骤一：定级与备案流程

- 第二级以上网络运营者应当在网络的安全保护等级确定后10个工作日内，到县级以上公安机关备案。

二、信息安全标准规范管理

2、网络安全等级保护解读

- 步骤二：安全建设 —— 差距评估：人工检查、漏洞扫描、渗透测试
  - 差距评估过程



确定等级保护对象的基本安全需求

依据等级保护对象确定的安全等级，从《基本要求》中选择相应等级的基本安全需求。

选择调整基本安全需求

依据等级保护对象确定的安全等级，从《基本要求》中选择相应等级的基本安全需求。

明确特殊安全需求

针对《基本要求》中不能满足单位等级保护对象保护要求的部分，提供特殊保护措施。

根据各项安全要求逐项分析

对比等级保护对象现状和安全要求之间的差距，确定不满足标准的要求项。

2、网络安全等级保护解读

□ 步骤三：安全建设 ——方案设计及整改实施

安全策略配置

根据用户单位的实际情况及等级保护要求，制定相关设备的安全配置策略要求，并合理进行配置；

安全加固

对差距评估中自身安全策略配置不当和版本补丁问题进行处理，对等级保护对象进行安全加固，并形成安全加固报告

安全管理制度完善

针对用户目前缺少的安全管理制度进行补充，形成安全管理制度汇编

安全设备采购部署

最后根据设计方案内容，完成安全设备的采购及部署。

2、网络安全等级保护解读

- 步骤四：等级测评，结论分为符合、基本符合、不符合。

测评方法	测评对象范围	测评实施	测评方法使用
• 第一级以访谈为主 • 第二级以核查为主 • 第三级和第四级在核查的基础上进行测试验证	• 第一级和第二级为关键设备 • 第三级为主要设备 • 第四级为所有设备	• 第一级和第二级以核查安全机制为主 • 第三极和第四级先核查安全机制，在检查策略有效性	• 安全技术方面的测评以配置核查和测试验证为主 • 安全管理方面可以使用访谈方式进行测评

二、信息安全标准规范管理

2、网络安全等级保护解读

◘ 步骤五：监督检查





检查对象

- 非涉密重要信息系统运营使用单位

检查内容

- 等级保护工作开展和落实情况

检查目的

- 督促、检查其建设安全设施、落实安全措施、管理制度、安全责任和责任人

工作划分

- 谁受理备案、谁负责检查

检查方法

- 询问情况
- 查阅、核对资料
- 调看记录、资料
- 现场验查等方式

2、网络安全等级保护解读

□ 总结

➢ 等级保护上升为法律

《中华人民共和国网络安全法》第21条规定“国家实行网络安全等级保护制度”，要求“网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；第31条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

➢ 等级保护对象将不断拓展

随着云计算、移动互联、大数据、物联网、人工智能等新技术不断涌现，计算机信息系统的概念已经不能涵盖全部，特别是互联网快速发展带来大数据价值的凸显，等保保护对象的外延将不断拓展。

➢ 等级保护工作内容将持续扩展

在定级、备案、建设整改、等级测评和监督检查等规定动作基础上，2.0时代风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等这些与网络安全密切相关的措施都将全部纳入等级保护制度并加以实施。

➢ 等级保护体系将进行重大升级

2.0时代，主管部门将继续制定出台一系列政策法规和技术标准，形成运转顺畅的工作机制，在现有体系基础上，建立完善等级保护政策体系、标准体系、测评体系、技术体系、服务体系、关键技术研究体系、教育训练体系等。

二、信息安全标准规范管理

- 测试点4-3
  - GB17895-1999《计算机信息系统安全保护等级划分准则》中划分了哪几种安全等级?
  - GB/T 22239-2019 《网络安全等级保护基本要求》中分别对哪几类信息系统做出了专门规定?
  - 概述等级保护的工作流程。
  - 假定有一个由银行提供代水电代收费服务的信息系统，如果该系统受到破坏，将导致个人或企业无法通过银行网点缴纳相关费用，水电公司的收费业务只能在其处理能力有限营业厅进行，导致业务能力大幅度下降，依据等级保护的定级规则，思考该系统应属于几级保护的对象?

网络安全为人民
网络安全靠人民

第三部分 信息安全道德规范管理

了解我国信息安全道德规范的主要内容

三、信息安全道德规范管理

1、信息安全道德规范概述

□ 什么是信息安全道德规范?

- 道德是社会意识的总和，是在一定条件下调整人与人之间以及人与社会之间的行为规范的总和，宏观世界通过各种形式的教育及社会力量，使人们形成一个良好的信念和习惯 。
- 信息安全道德规范就是在网络环境或网络条件下调整人和人之间以及人和社会之间关系的一种行为规范。这种“规范”从其功能来看，就是通过引导和约束网上人和人之间的行为，达到保障网络正常运行的目的。

三、信息安全道德规范管理

1、信息安全道德规范概述

信息安全道德规范遵循的原则

- 整体原则
  - 指一切信息活动必须服从于社会国家等团体的整体利益。个体利益服从整体利益，不得以损害团体整体利益为代价谋取个人利益。
- 兼容原则
  - 指社会的各主体间的信息活动方式应符合某种公认的规范和标准，个人的具体行为应该被他人及整个社会所接受，最终实现信息活动的规范化和信息交流的无障碍化。
- 互惠原则
  - 指任何一个使用者必须认识到，每个个体均是信息资源使用者和享受者，也是信息资源的生产者和提供者，在拥有享用信息资源的权利同时，也应承担信息社会对其成员所要求的责任。

三、信息安全道德规范管理

1、信息安全道德规范概述

□ 典型不当网络行为及危害

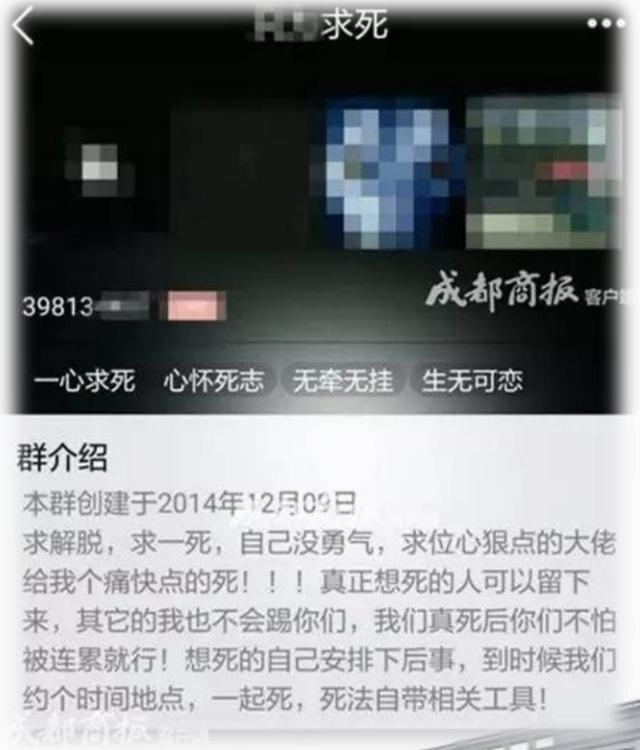
不当行为类型	造成的危害
传播不良信息	污染网络环境，散布负能量
传播虚假消息	影响网络可信度，混淆视听
传播垃圾信息	干扰正常信息获取，影响他人
实施舆论攻击	导致网络暴力等严重后果

三、信息安全道德规范管理

1、信息安全道德规范概述

□ 典型案例 — 散布消极厌世思想

- 记者卧底“相约自杀群”：竟有人提供“自杀攻略”！实在是太可怕!
  - 20岁的湖南大学生小伟通过QQ群和网友相约去峨眉山跳崖，小伟父亲李朝晖假扮女网友卧底该QQ群，成功救下另一名轻生者，但第二天，李朝晖就收到警方消息：小伟已另约他人在长沙双双跳楼身亡。连日来，记者卧底了多个“相约自杀群”，群内成员之间约定自杀的对话，令人触目惊心，甚至有网友还为轻生者出谋划策，提供自杀攻略。（2016年12月5日《成都商报》）



三、信息安全道德规范管理

1、信息安全道德规范概述

- 典型案例 —— 散布谣言，破坏社会安定
  - 谎称地震，导致社会恐慌
    - 2010年2月20日至21日，关于山西一些地区要发生地震的消息通过短信、网络等渠道疯狂传播，由于听信“地震”传言，山西太原、晋中、长治、晋城、吕梁、阳泉六地几十个县市数百万群众2月20日凌晨开始走上街头“躲避地震”，山西地震官网一度瘫痪。21日上午，山西省地震局发出公告辟谣。山西省公安机关立即对谣言来源展开调查，后查明造谣者共5人。

三、信息安全道德规范管理

1、信息安全道德规范概述

- 典型案例 —— 网络暴力，逼人走上不归路
  - 一家三口在湖南自杀，此前在海南自杀被解救，他们究竟经历了什么？
    - 2016年5月20日晚，一年轻女孩在微博发布一篇遗书，称因为父亲欠下高利贷一家人不胜其扰，决定自杀。后经海南警方救援，转危为安。但是后来网友质疑女孩发微博的动机，并通过“人肉搜索”在网络上曝光女孩及家人信息，引发一边倒的网络舆论攻击，最终导致一家三口再次选择了自杀的不归路。

三、信息安全道德规范管理

2、网络道德规范解读

- 对服务提供者的道德规范
  - 《中国互联网行业自律公约》2002年
  - 《互联网新闻信息服务自律公约》2003年
  - 《互联网站禁止传播淫秽、色情等不良信息自律规范》2004年
  - 《中国互联网协会互联网公共电子邮件服务规范》2004年
  - 《搜索引擎服务商抵制违法和不良信息自律规范》2004年
  - 《中国互联网网络版权自律公约》2005年
  - 《中国互联网协会反垃圾短信息自律公约》2008年
  - 《中国互联网协会短信息服务规范（试行）》2008年
- 对使用者的道德规范
  - 《全国青少年网络文明公约》2001年
  - 《文明上网自律公约》2006年
  - 《抵制恶意软件自律公约》2006年
  - 《博客服务自律公约》2007年

三、信息安全道德规范管理

2、网络道德规范解读

- 《文明上网自律公约》
  - 自觉遵纪守法，倡导社会公德，促进绿色网络建设；
  - 提倡先进文化，摒弃消极颓废，促进网络文明健康；
  - 提倡自主创新，摒弃盗版剽窃，促进网络应用繁荣；
  - 提倡互相尊重，摒弃造谣诽谤，促进网络和谐共处；
  - 提倡诚实守信，摒弃弄虚作假，促进网络安全可信；
  - 提倡社会关爱，摒弃低俗沉迷，促进少年健康成长；
  - 提倡公平竞争，摒弃尔虞我诈，促进网络百花齐放；
  - 提倡人人受益，消除数字鸿沟，促进信息资源共享。

三、信息安全道德规范管理

- 测试点4-4
  - 作为一名从事信息安全专业的人员，应该如何从自身做起，共同营造清朗的网络环境？

结束语

感 谢 聆 听!

zhaoyang@uestc.edu.cn