公安院校
招录培养体制改革
试点专业
系列教材

计算机犯罪侦查方向

丛书主编 李锦

信息安全法律法规汇编与案例分析

黄波 刘洋洋 主编

清华大学出版社

公安院校招录培养体制改革试点专业系列教材

★ ★ ★ ★ ★ 计算机犯罪侦查方向 ★ ★ ★ ★ ★

丛书主编 李锦

信息安全
法律法规汇编与案例分析

黄波 刘洋洋 主编

清华大学出版社
北 京

内 容 简 介

本书介绍信息安全的概念及信息安全保障体系的构成、我国法律制度的构成和信息安全法律体系的建设过程，汇编了信息安全相关国家法律法规、信息安全相关行政法规、信息安全相关部门规范、信息安全相关问题司法解释以及典型信息网络安全违法犯罪的相关案例，并针对案例简要分析了法律法规的应用。

本书比较全面地汇编了信息安全涉及的各方面法律法规和行业规范，内容详实，涵盖面广。

本书既可以作为公安体改生（网络安全与计算机犯罪侦查专业）本科学生、信息安全专业本科学生教材，也可作为普通高校电子商务、电子政务、信息管理与信息系统等计算机专业本科与专科学生的教材，以及公安干警初任警培训、公安一线干警普及信息安全法律法规知识与了解信息安全法律法规及案例的参考书。

图书在版编目(CIP)数据

信息安全法律法规汇编与案例分析/黄波等主编. —北京：清华大学出版社，2012.12
公安院校招录培养体制改革试点专业系列教材
ISBN 978-7-302-28832-9

Ⅰ. ①信… Ⅱ. ①黄… Ⅲ. ①信息网络－安全管理－法规－汇编－中国－高等学校－教材 ②信息网络－安全管理－法规－案例－中国－高等学校－教材 Ⅳ. ①D922.17

中国版本图书馆 CIP 数据核字(2012)第 102466 号

责任编辑：闫红梅　薛　阳
封面设计：常雪影
责任校对：时翠兰
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：26.5　　**字　　数**：576 千字
版　　次：2012 年 12 月第 1 版　　**印　　次**：2012 年 12 月第1 次印刷
印　　数：1～2500
定　　价：44.00 元

产品编号：043367-01

序

期待已久的由李锦同志主编的《公安院校招录培养体制改革试点专业系列教材》终于出版了！该系列教材是我国第一套计算机犯罪侦查专业系列教材，它的出版解决了国内相关院校教师与学生急需的教课书问题，也为从事信息安全专业和侦查执法人员提供一套极有价值的参考丛书。这实属一件可喜可贺的事！

由于信息技术空前迅速的发展，极具挑战的计算机网络空间形成了一个变幻无穷的虚拟空间。现实社会中的犯罪越来越多地涉及到计算机、手机等工具，各种数字技术与网络虚拟空间的交汇，使计算机犯罪侦查技术变得空前重要与紧迫。从20世纪90年代兴起的数字取证调查，涌现出各种各样的技术和工具，使得数字取证成为计算机专业的一门新兴学科。国际上的一些大学近年来已设置了专门的系和研究生学位的授予，为计算机犯罪侦查的教学内容增添了丰富而又精彩的情景。他山之石可以攻玉，许多技术和教材可以借鉴，但数字取证牵涉到法学、法规，各国的国情不尽相同，唯一的解决办法就是必须自主创新、撰写适合国内需要的相应教材。

面临这一劈山开路的挑战，本教材从专业的技术层面为国内的本科生尝试提供全面的教学培训，内容包括了从互联网体系结构原理到电子商务应用与各种法规，以及计算机网络攻防技术与信息系统安全等级保护与管理等基础知识，重点围绕着计算机犯罪调查的手段、工具与方法以及数据证据的分析与鉴定等基础知识；教材注重在传授理论知识的同时，强化面向实战能力的培训，全套教材既适应了学科特点又考虑到学生层次的具体情况，处处反映出作者们的精心思索。

本系列教材参编的作者全部来自辽宁警官高等专科学校的师资队伍，该校地处辽东半岛，面临蓝色的大海，大浪淘沙涌现一批时代的人杰。庄严整洁的校园具有公安教育突出的特色，更为可贵的是他们倡导教学、科研、警务实践紧密结合，不断创新教学模式的一贯校风，每年从那里培养出大量信息时代专业特色明显、创新能力强的人才队伍。本套系列教材的出版充分体现了该校的学术水平与精神面貌，尤其映射出参编作者们拥有第一线资深的教学经验和扎实的实际专业知识，以及始终保持一股奋发上进、开拓创新的风范。我在此由衷地对本教材的出版表示祝贺，并预祝他们再接再厉，取得更加辉煌的成功！

许榕生

2012-6 写于北京

前言

随着社会的发展，人们已经步入了信息网络时代，信息网络的广泛应用使得信息网络安全发展现状有了很大的变化，不法分子利用网络以各种方式进行违法犯罪活动，让人们的互联网生活开始变得复杂，这些都严重危害了国家和社会的安全及秩序。近年来对于信息安全保障工作，应该从管理和技术并重的角度来维护，同时努力加强信息安全立法工作，完善信息安全法律体系，加大法律执行力度，才能有效地保障信息安全。

信息安全法律法规作为国家法律体系的重要组成部分之一，在维护和保障信息安全中占有举足轻重的地位。信息安全法律法规是信息安全保障体系建设中的必要环节，它明确了信息安全的基本原则和基本制度、信息安全相关行为的规范、信息安全中各方权利和义务以及违反信息安全的行为，并明确对这些行为进行相应的处罚。信息安全立法能够保护国家信息主权和社会公共利益，规范信息活动，保护信息权利，协调和解决信息网络社会产生的矛盾，打击、惩治信息网络空间的违法犯罪行为，同时依托信息安全的司法和执法来实施法定程序和法律活动。

我国的法律体系是由以宪法为核心的各个法律部门所组成的，作为维护信息网络的安全与秩序的信息安全法律规范是不可缺少的法律部分，它在保证信息网络稳步、健康发展，保障整个社会环境的稳定中发挥重要作用。同时国家、地方以及相关部门针对信息安全的需求，制定了一系列与信息安全相关的法律法规。从领域上看，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、证券、教育等特定领域的信息安全和信息安全犯罪制裁等多个方面；从形式上看，有法律、行政法规、部门规章规范、相关的决定、司法解释及相关文件、地方性法规与地方政府规章及相关文件等多个层次。与此同时，与信息安全相关的司法和行政管理体系在逐渐完善，信息安全法律体系已初步建立，但整体来看，与美国、欧盟等国家与地区比较，我国在信息安全相关法律法规方面还欠体系化、有效性、覆盖面与深度，缺乏相关的基本法，信息网络安全法律法规的建设与发达国家还有一定差距。

本书共包括 6 章内容，其中，第 1 章主要介绍信息安全基础知识、信息安全法律关系及我国信息安全法律保障体系的构成，由刘洋洋编写；第 2 章主要介绍我国法律制度中的立法、司法和执行组织，由黄波编写；第 3 章汇编信息安全相关国家法律法规，主要包括全国人民代表大会和全国人民代表大会常务委员会通过的法律法规，由黄波编写；第 4 章汇编

信息安全相关行政法规和部门规范，主要包括国务院、国务院组成部委、国务院直属特设机构、国务院直属机构、国务院部委管理的国家局发布和制定的规章规范，由黄波、刘洋洋共同编写；第5章汇编最高人民法院，最高人民检察院信息安全相关司法解释，由刘洋洋编写；第6章汇编典型的信息网络安全违法犯罪相关案例，并针对案例简要分析法律法规的应用，由刘洋洋、芦晓丹共同编写。全书由黄波统稿。

本书是编者在多年教学、研究积累的基础上，紧密围绕公安工作，利用深入公安一线实习和挂职锻炼的学习机会，深刻体会信息安全法律法规体系建设与应用的思路，紧密围绕信息安全法律法规在公安工作实践中的执行需要，汇编的一本涵盖了信息安全相关国家法律法规、信息安全相关行政法规和部门规章规范等内容的教程，本书既可以作为公安体改生（网络安全与计算机犯罪侦查专业）本科学生、信息安全专业本科学生教材，也可作为普通高校电子商务、电子政务、信息管理与信息系统等非计算机专业本科与专科学生的教材及公安干警初任警培训、公安一线干警普及信息安全法律法规知识与了解信息安全法律法规及案例的参考书。

由于编写水平和时间有限，书中难免有疏漏和欠缺之处，敬请广大读者提出宝贵意见。

编者

2012年3月

第 1 章

信息安全概述

1.1 信息安全基础

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。

信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。

1.1.1 信息

在最一般的意义上，亦即没有任何约束条件，可以将信息定义为事物存在的方式和运动状态的表现形式，是事物的一种属性。在引入必要的约束条件后可以形成特定的概念体系。通常情况下，可以把信息理解为消息、信号、数据、情报和知识。

对于现代企业来说，信息是一种资产，包括计算机和网络中的数据，还包括专利、标准、商业机密、文件、图纸、管理规章等。和其他重要的商业资产一样，信息资产具有重要的价值，因而需要进行妥善保护。

信息是有生命周期的，从创建到被使用或操作，到存储，再到被传递，直至生命周期结束而被销毁或丢弃，各个环节各个阶段都应该被仔细考虑到，安全保护应兼顾信息存在的各种状态，丝毫不能有所遗漏。

1.1.2 信息安全

1. 定义

信息安全是一个广泛而抽象的概念，不同领域不同方面对其概念的阐述有所不同。这里给出几个有代表性的定义方式。

建立在网络基础之上的现代信息系统的安全定义是指信息网络的硬件、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，信息服务不中断。

我国相关立法给出的定义是：保障计算机及其相关的和配套的设备、设施（网络）的安

全，运行环境的安全，保障信息安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全。

国家信息安全重点实验室给出的定义是：信息安全涉及信息的机密性、完整性、可用性、可控性。综合起来说，就是要保障电子信息的有效性。

2. 基本属性

不论信息入侵者的意图和手段如何，一般都是通过攻击信息的以下几个基本安全属性来达到目的。“信息安全”在技术层面上的含义就是保证在客观上杜绝对信息安全基本属性的威胁，从而使得信息的主人在主观上对信息的本源性放心。

信息安全的基本属性有以下几个：

(1) 机密性

机密性(confidentiality)是指确保信息不泄露给未授权用户、实体或进程，不被非法利用。机密性能够确保敏感或机密数据的传输和存储不遭受未授权的浏览，甚至可以做到不暴露保密通信的事实。

(2) 完整性

完整性(integrity)是指信息未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被偶然或蓄意删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性能够保障被传输、接收或存储的数据是完整的和未被篡改的，在被篡改的情况下能够发现篡改的事实或篡改的位置。

(3) 可用性

可用性(availability)是指可被授权实体访问并按需求使用的特性。可用性能够保证即使在突发事件下，依然能够保障数据和服务的正常使用。

(4) 可控性

可控性(access)是对信息及信息系统实施安全监控。管理机构对危害国家信息的来往、使用加密手段从事非法的通信活动等进行监视审计，对信息的传播及内容具有控制能力。可控性能够保证掌握和控制信息与信息系统的基本情况，可对信息和信息系统的使用实施可靠的授权、审计、责任认定、传播源跟踪和监管等控制。

1.1.3 信息安全保障体系的三大要素

信息安全不仅关系到某些个人或组织的发展，还将影响到国家的安全，社会的稳定。保障信息安全是一项复杂的系统工程，必须多管齐下，综合治理。

1. 信息安全技术

各种信息安全技术的应用主要在技术层面上为信息安全提供具体的保障。目前主要采用的信息安全技术有：信息加密技术、防火墙技术、入侵检测技术、身份认证技术、反病毒技术、反黑客技术、安全扫描及安全审计技术等。

值得说明的是，尽管信息安全技术的应用在一定程度上对信息的安全起了积极的保护

作用，但它并不是万能的，由于疏于管理等其他原因而引起的安全事故仍然不可完全避免。

2. 信息安全标准

信息安全标准是确保信息安全的产品和系统在设计、研发、生产、建设、使用、测评中解决其一致性、可靠性、可控性、先进性和符合性的技术规范、技术依据。要保证信息产品和信息系统的安全性、提高用户对信息产品和信息系统安全性的信心，必须对信息安全产品以及提供信息安全产品、信息安全技术与服务的组织进行评估，并提供统一的科学依据，即建立统一的信息安全标准。信息安全标准是信息安全管理体系中不可或缺的重要组成部分。

目前信息安全标准大致可分为信息安全产品标准、信息安全技术标准和信息安全管理标准三大类，随着信息技术的不断发展和信息安全形势的变化，信息安全标准的数量和版本也将不断更新和完善。

3. 信息安全法律

法律是保障信息安全的一道利器。近年来我国在信息安全领域的法制建设方面做了大量工作，但相对于信息网络技术的迅猛发展及其在经济社会生活各方面日益显著的作用，信息安全立法工作滞后和不完善的问题也日益突出。因此，应当充分认识加强信息安全立法的紧迫性、重要性，抓紧建立和完善国家信息安全法律框架。

目前，我国已经建立起基本的信息安全法律法规体系，国家、地方以及相关部门针对信息安全的需求，制定了一系列与信息安全相关的法律法规，从法律层面上来规范人们的行为，使信息安全工作有法可依，使相关违法犯罪能得到处罚，促使组织和个人依法制作、发布、传播和使用信息，从而达到保障信息安全的目的。

1.2　信息安全事件

信息安全事件的防范和处置是国家信息安全保障体系中的重要环节，也是重要的工作内容。信息安全事件的分类分级是快速有效处置信息安全事件的基础之一。

1.2.1　基本术语

根据国家标准化指导性技术文件《信息安全事件分类分级指南》，提供下列信息安全领域常用术语：

1. 信息系统

信息系统(information system)是指由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

2. 信息安全事件

信息安全事件(information security incident)是指由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

1.2.2 信息安全事件分类

信息安全事件可以是故意、过失或非人为原因引起的。综合考虑信息安全事件的起因、表现、结果等，可将信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等七个基本分类，每个基本分类分别包括若干个子类。

1. 有害程序事件

有害程序事件(malware incidents，MI)是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序，它危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行。有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其他有害程序事件等七个子类，说明如下：

(1) 计算机病毒事件

计算机病毒事件(computer virus incidents，CVI)是指蓄意制造、传播计算机病毒，或是因受到计算机病毒影响而导致的信息安全事件。计算机病毒是指编制或者在计算机程序中插入的一组计算机指令或者程序代码，它可以破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制。

(2) 蠕虫事件

蠕虫事件(worms incidents，WI)是指蓄意制造、传播蠕虫，或是因受到蠕虫影响而导致的信息安全事件。蠕虫是指除计算机病毒以外，利用信息系统缺陷，通过网络自动复制并传播的有害程序。

(3) 特洛伊木马事件

特洛伊木马事件(trojan horses incidents，THI)是指蓄意制造、传播特洛伊木马程序，或是因受到特洛伊木马程序影响而导致的信息安全事件。特洛伊木马程序是指伪装在信息系统中的一种有害程序，具有控制该信息系统或进行信息窃取等对该信息系统有害的功能。

(4) 僵尸网络事件

僵尸网络事件(botnets incidents，BI)是指利用僵尸工具软件，形成僵尸网络而导致的信息安全事件。僵尸网络是指网络上受到黑客集中控制的一群计算机，它可以被用于伺机发起网络攻击，进行信息窃取或传播木马、蠕虫等其他有害程序。

(5) 混合攻击程序事件

混合攻击程序事件(blended attacks incidents，BAI)是指蓄意制造、传播混合攻击程序，或是因受到混合攻击程序影响而导致的信息安全事件。混合攻击程序是指利用多种方法传播和感染其他系统的有害程序，可能兼有计算机病毒、蠕虫、木马或僵尸网络等多种特征。混合攻击程序事件也可以是一系列有害程序综合作用的结果，例如一个计算机病毒或蠕虫在侵入系统后安装木马程序等。

(6) 网页内嵌恶意代码事件

网页内嵌恶意代码事件(Web browser plug-ins incidents,WBPI)是指蓄意制造、传播网页内嵌恶意代码,或是因受到网页内嵌恶意代码影响而导致的信息安全事件。网页内嵌恶意代码是指内嵌在网页中,未经允许由浏览器执行,影响信息系统正常运行的有害程序。

(7) 其他有害程序事件

其他有害程序事件(other malware incidents,OMI)是指不能包含在以上六个子类之中的有害程序事件。

2. 网络攻击事件

网络攻击事件(network attacks incidents,NAI)是指通过网络或其他技术手段,利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击,并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等七个子类,说明如下:

(1) 拒绝服务攻击事件

拒绝服务攻击事件(denial of service attacks Incidents,DOSAI)是指利用信息系统缺陷或通过暴力攻击的手段,大量消耗信息系统的 CPU、内存、磁盘空间或网络带宽等资源,从而影响信息系统正常运行为目的的信息安全事件。

(2) 后门攻击事件

后门攻击事件(backdoor attacks incidents,BDAI)是指利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施攻击的信息安全事件。

(3) 漏洞攻击事件

漏洞攻击事件(vulnerability attacks incidents,VAI)是指除拒绝服务攻击事件和后门攻击事件之外,利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞,对信息系统实施攻击的信息安全事件。

(4) 网络扫描窃听事件

网络扫描窃听事件(network scan & eavesdropping incidents,NSEI)是指利用网络扫描或窃听软件,获取信息系统网络配置、端口、服务、存在的脆弱性等特征而导致的信息安全事件。

(5) 网络钓鱼事件

网络钓鱼事件(phishing incidents,PI)是指利用欺骗性的计算机网络技术,使用户泄漏重要信息而导致的信息安全事件。例如,利用欺骗性电子邮件获取用户银行账号密码等。

(6) 干扰事件

干扰事件(interference incidents,II)是指通过技术手段对网络进行干扰,或对广播电视有线或无线传输网络进行插播,对卫星广播电视信号非法攻击等导致的信息安全事件。

(7) 其他网络攻击事件

其他网络攻击事件(other network attacks incidents,ONAI)是指不能被包含在以上六

个子类之中的网络攻击事件。

3. 信息破坏事件

信息破坏事件(information destroy incidents,IDI)是指通过网络或其他技术手段,造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其他信息破坏事件等六个子类,说明如下:

(1) 信息篡改事件

信息篡改事件(information alteration incidents,IAI)是指未经授权将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件,例如网页篡改等导致的信息安全事件。

(2) 信息假冒事件

信息假冒事件(information masquerading incidents,IMI)是指通过假冒他人信息系统收发信息而导致的信息安全事件,例如网页假冒等导致的信息安全事件。

(3) 信息泄漏事件

信息泄漏事件(information leakage incidents,ILEI)是指因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者而导致的信息安全事件。

(4) 信息窃取事件

信息窃取事件(information interception incidents,III)是指未经授权用户利用可能的技术手段恶意主动获取信息系统中信息而导致的信息安全事件。

(5) 信息丢失事件

信息丢失事件(information loss incidents,ILOI)是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件。

(6) 其他信息破坏事件

其他信息破坏事件(other information destroy incidents,OIDI)是指不能被包含在以上五个子类之中的信息破坏事件。

4. 信息内容安全事件

信息内容安全事件(information content security incidents,ICSI)是指利用信息网络发布和传播危害国家安全、社会稳定和公共利益的内容的安全事件。信息内容安全事件包括以下四个子类,说明如下:

(1) 违反宪法和法律、行政法规的信息安全事件;

(2) 针对社会事项进行讨论、评论形成网上敏感的舆论热点,出现一定规模炒作的信息安全事件;

(3) 组织串连、煽动集会游行的信息安全事件;

(4) 其他信息内容安全事件。

5. 设备设施故障

设备设施故障(facilities faults,FF)是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件,以及人为使用非技术手段有意或无意地造成信息系统破坏而导致的信息安全事件。

设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障等四个子类,说明如下:

(1) 软硬件自身故障

软硬件自身故障(software and hardware faults,SHF)是指因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的信息安全事件。

(2) 外围保障设施故障

外围保障设施故障(periphery safeguarding facilities faults,PSFF)是指由于保障信息系统正常运行所必需的外部设施出现故障而导致的信息安全事件,例如电力故障、外围网络故障等导致的信息安全事件。

(3) 人为破坏事故

人为破坏事故(man-made destroy accidents,MDA)是指人为蓄意地对保障信息系统正常运行的硬件、软件等实施窃取和破坏造成的信息安全事件,或由于人为遗失、误操作以及其他无意行为造成信息系统硬件、软件等遭到破坏,影响信息系统正常运行的信息安全事件。

(4) 其他设备设施故障(IF-OT)

其他设备设施故障是指不能被包含在以上三个子类之中的设备设施故障而导致的信息安全事件。

6. 灾害性事件

灾害性事件(disaster incidents,DI)是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

7. 其他事件

其他事件类别(other incidents,OI)是指不能归为以上六个基本分类的信息安全事件。

1.3　信息安全法律规范

没有规矩,不成方圆。法律法规是指国家按照统治阶级的利益和意志制定、认可,并由国家强制力保障其实施的行为规范的总和,是人们在社会活动中必须遵守的纪律,是人们从事社会活动所不能逾越的行为底线,违犯了就要受到惩罚。

作为国家法律体系的重要组成部分之一,信息安全法律规范制度在国家法律体系中占有举足轻重的地位。信息安全能取得成绩,与相关"规矩"的不断建立和完善分不开。这些"规矩"大致可分成法律、法规、标准等部分。