高等职业教育精品示范教材 信息安全系列

信息安全基础

主　编　曹　敏　刘　艳
副主编　杨雅军　王爱菊

本书特色：

- 以就业为导向，以能力为本位
- 工作需求驱动　实训任务引领
- 核心内容为主　拓展内容为辅

中国水利水电出版社
www.waterpub.com.cn

高等职业教育精品示范教材（信息安全系列）

信息安全基础

主　编　曹　敏　刘　艳

副主编　杨雅军　王爱菊

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书作为信息安全知识普及与技术推广教材，涵盖信息安全概念、物理安全技术、密码技术、认证技术、访问控制与网络隔离技术、信息系统安全检测技术、恶意程序及防范技术、网络攻击与防护技术和无线网络安全技术等多方面的内容。不仅能够为初学信息安全技术的学生提供全面、实用的技术和理论基础，而且能有效培养学生信息安全的防御能力。

本书的编写融入了作者丰富的教学和企业实践经验，内容注重实用，结构清晰，图文并茂，通俗易懂，力求做到使读者在兴趣中学习信息安全技术。每章开始都列出本章的学习重点，首先让学生知道通过本章学习能解决什么实际问题，做到有的放矢，激发学生的学习热情，使学生更有目标地学习相关理念和技术操作。此外，每章还配有习题和实训，不仅可以巩固理论知识，而且也为技能训练提供了基础。

本书可作为高职高专院校计算机或信息安全类专业教材，也可作为培养技能型紧缺人才的相关院校及培训班教学用书。

本书配有电子教案，读者可以到中国水利水电出版社网站和万水书苑上免费下载，网址：http://www.waterpub.com.cn/softdown 和 http://www.wsbookshow.com。

图书在版编目（CIP）数据

信息安全基础 / 曹敏，刘艳主编. -- 北京 : 中国水利水电出版社，2015.6
高等职业教育精品示范教材. 信息安全系列
ISBN 978-7-5170-3142-0

Ⅰ. ①信… Ⅱ. ①曹… ②刘… Ⅲ. ①信息安全－安全技术－高等职业教育－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2015)第089150号

策划编辑：祝智敏　　责任编辑：陈　洁　　加工编辑：孙　丹　　封面设计：李　佳

书　　名	高等职业教育精品示范教材（信息安全系列） **信息安全基础**
作　　者	主　编　曹　敏　刘　艳 副主编　杨雅军　王爱菊
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京泽宇印刷有限公司
规　　格	184mm×240mm　16 开本　16.5 印张　361 千字
版　　次	2015 年 6 月第 1 版　2015 年 6 月第 1 次印刷
印　　数	0001—3000 册
定　　价	36.00 元

高等职业教育精品示范教材（信息安全系列）

丛书编委会

序　言

随着信息技术和社会经济的快速发展，信息和信息系统成为现代社会极为重要的基础性资源。信息技术给人们的生产、生活带来巨大便利的同时，计算机病毒、黑客攻击等信息安全事故层出不穷，社会对于高素质技能型计算机网络技术和信息安全人才的需求日益旺盛。党的十八大明确指出“高度关注海洋、太空、网络空间安全”，信息安全被提到前所未有的高度。加快建设国家信息安全保障体系，确保我国的信息安全，已经上升为我国的国家战略。

发展我国信息安全技术与产业，对确保我国信息安全有着极为重要的意义。信息安全领域的快速发展，亟需大量的高素质人才。但与之不相匹配的是，在高等职业教育层次信息安全技术专业的教学中，还更多地存在着沿用本科专业教学模式和教材的现象，对于学生的职业能力和职业素养缺乏有针对性的培养。因此，在现代职业教育体系的建立过程中，培养大量的技术技能型信息安全专业人才成为我国高等职业教育领域的重要任务。

信息安全是计算机、通信、数学、物理、法律、管理等学科的交叉学科，涉及计算机、通信、网络安全、电子商务、电子政务、金融等众多领域的知识和技能。因此，探索信息安全专业的培养模式、课程设置和教学内容就成为信息安全人才培养的首要问题。高等职业教育信息安全与管理专业丛书编委会的众多专家、一线教师和企业技术人员，依据最新的专业教学目录和教学标准、结合就业实际需求，组织了以就业为导向的高等职业教育精品示范教材（信息安全系列）的编写工作。该系列教材由《网络安全产品调试与部署》、《网络安全系统集成》、《Web 开发与安全防范》、《数字身份认证技术》、《计算机取证与司法鉴定》、《操作系统安全（Linux）》、《网络安全攻防技术实训》、《大型数据库应用与安全》、《信息安全工程与管理》、《信息安全法规与标准》、《信息安全风险评估》等组成，在紧跟当代信息安全研究发展的同时，全面、系统、科学地培养信息安全类技术技能型人才。

本系列教材在组织规划的过程中，遵循以下几个基本原则：

（1）体现就业为导向、产学结合的发展道路。学科和专业同步加强，按企业需要、按岗位需求来对接培养内容。既能反映信息安全学科的发展趋势，又能结合信息安全专业教育的改革，且及时反映教学内容和教学体系的调整更新。

（2）采用项目驱动、案例引导的编写模式。打破传统的以学科体系设置课程体系、以知识点为核心的框架，更多地考虑学生所学知识与行业需求及相关岗位、岗位群的需求相一致，坚持“工作流程化”、“任务驱动式”，突出“走向职业化”的特点，努力培养学生的职业素养、职业能力，实现教学内容与实际工作的高仿真对接，真正以培养技术技能型人才为核心。

（3）专家和教师共建团队，优化编写队伍。由来自信息安全领域的行业专家、院校教师、企业技术人员组成编写队伍，跨区域、跨学校进行交叉研究、协调推进，把握行业发展和创新

教材发展方向，融入信息安全专业的课程设置与教材内容。

（4）开发课程教学资源，推进专业信息化建设。从充分关注人才培养目标、专业结构布局等入手，开发补充性、更新性和延伸性教辅资料，开发网络课程、虚拟仿真实训平台、工作过程模拟软件、通用主题素材库以及名师讲义等多种形式的数字化教学资源，建立动态、共享的课程教材信息化资源库，服务于系统培养技术技能型人才。

信息安全类教材建设是提高信息安全专业技术技能型人才培养质量的关键环节，是深化职业教育教学改革的有效途径。为了促进现代职业教育体系的建设，使教材建设全面对接教学改革、行业需求，更好地服务区域经济和社会发展，我们殷切希望各位职教专家和老师提出建议，并加入到我们的编写队伍中来，共同打造信息安全领域的系列精品教材！

丛书编委会

2014 年 6 月

前　言

随着全球信息化技术的快速发展，在信息技术的广泛应用中，安全问题正面临着前所未有的挑战，信息安全日渐成为国家一个重点关注的研究领域，成为关系着国计民生的一个重要应用学科。

本书针对信息安全领域的安全技术进行全面系统的介绍。随着信息网络技术的快速发展，信息安全技术也不断丰富和完善。本书尽可能涵盖信息安全技术的主要内容，同时增加实践内容，介绍相关工具软件以及信息安全技术实施的具体方法。

本书涵盖信息安全概念、物理安全技术、密码技术、认证技术、访问控制与网络隔离技术、信息系统安全检测技术、恶意程序及防范技术、网络攻击与防护技术和无线网络安全技术等多方面的内容。不仅能够为初学信息安全技术的学生提供全面、实用的技术和理论基础，而且能有效培养学生信息安全的防御能力。

本书的编写融入了作者丰富的教学和企业实践经验，内容注重实用，结构清晰，图文并茂，通俗易懂，力求做到使读者产生学习信息安全技术的兴趣。本书内容翔实、讲解透彻，具有如下特色。

（1）每章开始都列出本章的学习重点。第一节介绍基本概念、背景知识。在此基础上对信息安全技术进行深入浅出的介绍。

（2）教材文字内容简洁、清晰，尽可能采用插图、表格、以及截图的方式进行说明。

（3）每章都有习题，帮助读者复习本章的主要内容，掌握基本概念和基本原理。

（4）每章都有实训，通过上机训练，切实提高读者的动手实践能力，为技能训练提供了基础。

本书由中州大学的曹敏、刘艳任主编并负责统稿，中州大学的杨雅军、王爱菊任副主编，参加编写的还有河南大学人民武装学院的王贝贝、南京邮电大学的吴振宇。具体编写分工为：曹敏负责编写第4、5章，刘艳负责编写第1、9章，杨雅军负责编写第2、3章，王爱菊负责编写第6、7章，王贝贝负责编写第8章，吴振宇提供素材、案例等基础内容并审核教材初稿。

由于时间仓促，不妥之处欢迎读者批评指正。

编　者

2015年3月

目　　录

1 信息安全概述

本章主要介绍信息安全的概念及发展历史，介绍了信息安全体系的五类安全服务以及八类安全机制，指出了信息安全存在的主要威胁和防御策略，最后给出了信息安全的评估标准。

通过本章的学习，使读者：

（1）了解信息安全的概念和发展历史；

（2）理解信息安全体系的五类安全服务以及八类安全机制；

（3）了解信息安全存在的主要威胁和防御策略；

（4）理解信息安全的评估标准。

在信息化飞速发展的今天，信息作为一种资源，其普遍性、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。随着现代通信技术的迅速发展和普及，互联网进入千家万户，计算机信息的应用与共享日益广泛和深入，信息技术已经成为一个国家的政治、军事、经济和文化等发展的决定性因素，但是信息系统或信息网络中的信息资源通常会受到各种类型的威胁、干扰和破坏，计算机信息安全问题已成为制约信息化发展的瓶颈，日渐成为我们必须面对的一个严峻问题，从大的方面说，国家的政治、经济、军事、文化、意识形态等领域的信息安全受到威胁；从小的方面说，计算机信息安全问题也涉及到人们的个人隐私和私有财产安全等。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。因此，加强计算机信息安全研究、营造计算机信息安全氛围，既是时代发展的客观要求，也是保证国家安全和个人财产安全的必要途径。

信息是社会发展的重要战略资源。信息安全已成为急待解决、影响国家大局和长远利益的重大关键问题，信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交世界各国在奋力攀登的制高点。信息安全问题如果解决不好将全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面，使国家处于信息战和高度经济金融风险的威胁之中。

1.1 信息安全的概念

1.1.1 信息的概念

信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。ISO/IEC 的 IT 安全管理指南（GMITS，即 ISO/IEC TR 13335）给出的信息（Information）解释是：信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。

计算机的出现和逐步的普及，使信息对整个社会的影响逐步提高到一种绝对重要的地位。信息量、信息传播的速度、信息处理的速度以及应用信息的程度等都以几何级数的方式在增长。

信息技术的发展对人们学习知识、掌握知识、运用知识提出了新的挑战。对我们每个人、每个企事业机构来说，信息是一种资产，包括计算机和网络中的数据，还包括专利、著作、文件、商业机密、管理规章等，就像其他重要的固定资产一样，信息资产具有重要的价值，因而需要进行妥善保护。

知己知彼，百战不殆，要保证信息的安全，就需要我们熟悉所保护的信息以及信息的存储、处理系统，熟悉信息安全性所面临的威胁，以便做出正确的决策。

1.1.2 信息安全的含义

信息安全的实质就是要保护信息资源免受各种类型的危险，防止信息资源被故意或偶然地非授权泄露、更改、破坏，或使信息被非法系统辨识、控制和否认，即保证信息的完整性、可用性、保密性和可靠性。信息安全本身包括的范围很大，从国家军事政治等机密安全，到防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。

信息安全包括软件安全和数据安全，软件安全是指软件的防复制、防篡改、防非法执行等。数据安全是指计算机中的数据不被非法读出、更改、删除等。

信息安全的含义包含如下方面：

1. 信息的可靠性

信息的可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。

2. 信息的可用性

信息的可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。

3. 信息的保密性

信息的保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

即防止信息泄露给非授权个人或实体，信息只为授权使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

4. 信息的完整性

信息的完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

5. 信息的不可抵赖性

信息的不可抵赖性也称作不可否认性。在网络信息系统的信息交互过程中，确信参与者的真实同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

6. 信息的可控性

信息的可控性是对信息的传播及内容具有控制能力的特性。

除此之外，信息安全还包括鉴别、审计追踪、身份认证、授权和访问控制、安全协议、密钥管理、可靠性等。

1.2 信息安全的发展历史

人类很早就在考虑怎样秘密地传递信息了。文献记载的最早有实用价值的通信保密技术是古罗马帝国时期的 Caesar 密码。它能够把明文信息变换为人们看不懂的称为密文的字符串，当把密文传递到自己伙伴手中的时候，又可方便地还原为原来的明文形式。Caesar 密码实际上非常简单，需要加密时，把字母 A 变成 D、B 变为 E、……、W 变为 Z、X 变为 A、Y 变为 B、Z 变为 C，即密文由明文字母循环移 3 位得到。反过来，由密文变为明文也相当简单。

随着 IT 技术的发展，各种信息电子化，可以更加方便地获取、携带与传输，相对于传统的信息安全保障，需要更加有力的技术保障，而不单单是对接触信息的人和信息本身进行管理，介质本身的形态已经从“有形”到“无形”。在计算机支撑的业务系统中，正常业务处理的人员都有可能接触、获取这些信息，信息的流动是隐性的，对业务流程的控制就成了保障涉密信息的重要环节。

在不同的发展时期，信息安全的侧重点和控制方式是有所不同的，大致说来，信息安全的发展过程经历了三个阶段。

早在 20 世纪初期，通信技术还不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，人们强调的主要是信息的保密性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单称为通信安全（COMSEC，Communication Security）。

20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机得到广泛应用，人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息

安全阶段（INFOSEC，Information Security）。

20 世纪 80 年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点从传统的保密性、完整性和可用性的原则衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障（Information Assurance）阶段。

开放复杂的信息系统面临着诸多风险，而为了解决这些风险问题，人们一直在寻找问题的解决之道，最直接的做法就是各种安全技术和产品的选择使用，密码产品、防火墙、病毒防护、入侵检测、终端接入控制、网络隔离、安全审计、安全管理、备份恢复等技术领域产品研发取得明显进展，产品功能逐步向集成化、系统化方向发展。

随着信息技术的快速发展和广泛应用，基础信息网络和重要信息系统安全、信息资源安全以及个人信息安全等问题与日俱增，应用安全日益受到关注，主动防御技术成为信息安全技术发展的重点，信息安全产品与服务演化为多技术、多产品、多功能的融合，多层次、全方位、全网络的立体监测和综合防御趋势不断加强。信息安全保障逐步由传统的被动防护转向“监测—响应式”的主动防御，信息安全技术正朝着构建完整、联动、可信、快速响应的综合防护防御系统方向发展。信息技术网络化、服务化等都在积极推动信息安全服务化，信息安全服务在产业中的比重将不断提高，将逐渐主导产业的发展。

1.3 信息系统安全体系结构

研究信息系统安全体系结构，就是将普遍性安全体系原理与自身信息系统的实际相结合，形成满足信息系统安全需求的安全体系结构。

1989 年 12 月，国际标准化组织 ISO 颁布了 ISO7498-2 标准，该标准首次确定了 OSI 参考模型的计算机信息安全体系结构，并于 1995 年再次在技术上进行了修正。OSI 安全体系结构包括五类安全服务以及八类安全机制。

1.3.1 五类安全服务

五类安全服务包括认证（鉴别）服务、访问控制服务、数据保密性服务、数据完整性服务和抗否认性服务。

（1）认证（鉴别）服务：提供对通信中对等实体和数据来源的认证（鉴别）。

（2）访问控制服务：用于防治未授权用户非法使用系统资源，包括用户身份认证和用户权限确认。

（3）数据保密性服务：为防止网络各系统之间交换的数据被截获或被非法存取而泄密，提供机密保护。同时，对有可能通过观察信息流就能推导出信息的情况进行防范。

（4）数据完整性服务：用于组织非法实体对交换数据的修改、插入、删除以及在数据交换过程中的数据丢失。

（5）抗否认性服务：用于防止发送方在发送数据后否认发送和接收方在收到数据后否认收到或伪造数据的行为。

1.3.2 八类安全机制

八大类安全机制包括加密机制、数据签名机制、访问控制机制、数据完整性机制、认证机制、业务流填充机制、路由控制机制、公正机制。

（1）加密机制：是确保数据安全性的基本方法，在OSI安全体系结构中应根据加密所在的层次及加密对象的不同，而采用不同的加密方法。

（2）数字签名机制：是确保数据真实性的基本方法，利用数字签名技术可进行用户的身份认证和消息认证，它具有解决收、发双方纠纷的能力。

（3）访问控制机制：从计算机系统的处理能力方面对信息提供保护。访问控制按照事先确定的规则决定主体对客体的访问是否合法，当以主题试图非法使用一个未经给出的报警并记录日志档案。

（4）数据完整性机制：破坏数据完整性的主要因素有数据在信道中传输时受信道干扰影响而产生错误，数据在传输和存储过程中被非法入侵者篡改，计算机病毒对程序和数据的传染等。纠错编码和差错控制是对付信道干扰的有效方法。对付非法入侵者主动攻击的有效方法是保温认证，对付计算机病毒有各种病毒检测、杀毒和免疫方法。

（5）认证机制：在计算机网络中，认证主要有用户认证、消息认证、站点认证和进程认证等，可用于认证的方法有已知信息（如口令）、共享密钥、数字签名、生物特征（如指纹）等。

（6）业务流填充机制：攻击者通过分析网络中有一路径上的信息流量和流向来判断某些事件的发生，为了对付这种攻击，一些关键站点间再无正常信息传送时，持续传递一些随机数据，使攻击者不知道哪些数据是有用的，哪些数据是无用的，从而挫败攻击者的信息流分析。

（7）路由控制机制：在大型计算机网络中，从源点到目的地往往存在多条路径，其中有些路径是安全的，有些路径是不安全的，路由控制机制可根据信息发送者的申请选择安全路径，以确保数据安全。

（8）公正机制：在大型计算机网络中，并不是所有的用户都是诚实可信的，同时也可能由于设备故障等技术原因造成信息丢失、延迟等，用户之间很可能引起责任纠纷，为了解决这个问题，就需要有一个各方都信任的第三方以提供公证仲裁，仲裁数字签名技术是这种公正机制的一种技术支持。

1.4 信息安全的防御策略

计算机信息系统安全保护工作的任务，就是不断发现、堵塞系统安全漏洞，预防、发现、制止利用或者针对系统进行的不法活动，预防、处置各种安全事件和事故，提高系统安全系数，确保计算机信息系统安全可用。

1.4.1 信息安全存在的主要威胁

1. 失泄密

失泄密是指计算机网络信息系统中的信息，特别是敏感信息被非授权用户通过侦收、截获、窃取或分析破译等方法恶意获得，造成信息泄露的事件。造成失泄密以后，计算机网络一般会继续正常工作，所以失泄密事故往往不易被察觉，但是失泄密所造成的危害却是致命的，其危害时间也往往会持续很长。失泄密主要有六条途径：一是电磁辐射泄漏；二是传输过程中失泄密；三是破译分析；四是内部人员的泄密；五是非法冒充；六是信息存储泄漏。

2. 数据破坏

数据破坏是指计算机网络信息系统中的数据由于偶然事故或人为破坏，被恶意修改、添加、伪造、删除或者丢失。信息破坏主要存在六个方面：一是硬件设备的破坏；二是程序方式的破坏；三是通信干扰；四是返回渗透；五是非法冒充；六是内部人员造成的信息破坏。

3. 计算机病毒

计算机病毒是指恶意编写的破坏计算机功能或者破坏计算机数据，影响计算机使用并且能够自我复制的一组计算机程序代码。计算机病毒具有以下特点：一是寄生性；二是繁殖力特别强；三是潜伏期特别长；四是隐蔽性高；五是破坏性强；六是计算机病毒具有可触发性。

4. 网络入侵

网络入侵是指计算机网络被黑客或者其他对计算机网络信息系统进行非授权访问的人员，采用各种非法手段侵入的行为。他们往往会对计算机信息系统进行攻击，并对系统中的信息进行窃取、篡改、删除，甚至使系统部分或者全部崩溃。

5. 后门

后门是指在计算机网络信息系统中人为的设定一些“陷阱”，从而绕过信息安全监管而获取对程序或系统访问的权限，以达到干扰和破坏计算机信息系统正常运行的目的。后门一般可分为硬件后门和软件后门两种。硬件后门主要指蓄意更改集成电路芯片的内部设计和使用规程的“芯片捣鬼”，以达到破坏计算机网络信息系统的目的。软件后门主要是指程序员按特定的条件设计的，并蓄意留在软件内部的特定源代码。

1.4.2 保障信息安全的主要防御策略

尽管计算机网络信息安全受到威胁，但是采取恰当的防护措施也能有效地保护网络信息的安全。信息系统的安全策略是为了保障规定级别下的系统安全而制定和必须遵守的一系列准则和规定，它考虑到入侵者可能发起的任何攻击，以及为使系统免遭入侵和破坏而必然采取的措施。实现信息安全不但靠先进的技术，也得靠严格的安全管理、法律约束和安全教育。

本策略文件主要包括：物理安全策略、运行管理策略、信息安全策略、备份与恢复策略、应急计划和相应策略、计算机病毒与恶意代码防护策略、身份鉴别策略、访问控制策略、信息完整性保护策略、安全审计策略。

1. 物理安全策略

计算机信息和其他用于存储、处理或传输信息的物理设施，例如硬件、磁介质、电缆等，对于物理破坏来说是易受攻击的，同时也不可能完全消除这些风险。因此，应该将这些信息及物理设施放置于适当的环境中并在物理上给予保护，使之免受安全威胁和环境危害。

2. 运行管理策略

为避免信息遭受人为过失、窃取、欺骗、滥用的风险，应加强计算机信息系统运行管理，提高系统安全性、可靠性，减少恶意攻击、各类故障带来的负面效应，全体相关人员都应该了解计算机及系统的网络与信息安全需求，建立行之有效的系统运行维护机制和相关制度。比如，建立健全中心机房管理制度、信息设备操作使用规程、信息系统维护制度、网络通信管理制度、应急响应制度等。

3. 信息安全策略

为保护存储计算机的数据信息的安全性、完整性、可用性，保护系统中的信息免受恶意的或偶然的篡改、伪造和窃取，有效控制内部泄密的途径和防范来自外部的破坏，可借助数据异地容灾备份、密文存储、设置访问权限、身份识别、局部隔离等策略提高安全防范水平。

在设计信息系统时，选用相对成熟、稳定和安全的系统软件并保持与其提供商的密切接触，通过官方网站或合法渠道，密切关注其漏洞及补丁发布情况，争取“第一时间”下载补丁软件，弥补不足。

4. 计算机病毒与恶意代码防护策略

病毒防范包括预防和检查病毒（包括实时扫描、过滤和定期检查），主要内容包括：控制病毒入侵途径；安装可靠的防病毒软件；对系统进行实时检测和过滤；定期杀毒；及时更新病毒库；详细记录；防病毒软件的安装和使用由信息安全管理员执行。

5. 身份鉴别和访问控制策略

为了保护计算机系统中信息不被非授权地访问、操作或被破坏，必须对信息系统实行控制访问。采用有效的口令保护机制，包括：规定口令的长度、有效期、口令规则。保障用户登录和口令的安全；用户选择和使用密码时应参考良好的安全惯例，严格设置对重要服务器、网络设备的访问权限。

6. 安全审计策略

计算机及信息系统的信息安全审计活动和风险评估应当定期执行。

特别是系统建设前或系统进行重大变更之前，必须进行风险评估工作。

定期进行信息安全审计和信息安全风险评估，并形成文档化的信息安全审计报告和风险评估报告。

1.5 信息安全的评估标准

信息安全评估是信息安全生命周期中的一个重要环节，是对企业的网络拓扑结构、重要