

<<安全策略与规程>>

图书基本信息

书名：<<安全策略与规程>>

13位ISBN编号：9787302179627

10位ISBN编号：730217962X

出版时间：2008-10

出版时间：格林 (Greene.S.S.)、陈宗斌 清华大学出版社 (2008-10出版)

作者：格林

页数：383

译者：陈宗斌

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<安全策略与规程>>

### 前言

随着Internet的迅速发展，信息安全正成为一个越来越受关注的话题。

本书遵循由一般到具体、由理论到实践的原则阐述了当前国内外信息安全领域的相关主题，探讨了信息安全平台建设的理论基础和设计思路，并从实际应用出发探讨如何切实地落实信息安全工作。

本书有助于组织构建符合IS( )17799：2000信息安全标准的系统，这个标准为开发信息安全策略和理解信息安全控制提供了一个框架。

在全书中，我们都会引用ISO 17799：2000标准。

本书提供了信息安全思想的总体描述，以便企业管理人员能够更好地评估他们的公司在处理信息安全问题上的表现。

同时本书也提供一些实用方法来协助各个公司改进其信息安全计划。

本书是按照为公司建立信息安全计划的步骤来组织内容的。

本书分为三个部分。

第1部分“策略简介”旨在为开发、引荐和实施策略提供基础。

第2部分“信息安全策略的各个领域”探讨了9个安全领域的信息安全策略和规程。

第3部分“合规性”是关于策略和规程遵从联邦规章以及行业最佳实践的实际应用。

本书各章都配有相关的习题，以指导读者深入地进行学习。

本书可作为高等学校计算机及相关专业的教材，也可作为信息安全及管理人士的参考书。

对于有志成为信息安全专业人员的人，掌握本书中介绍的信息是绝对必要的。

参加本书翻译的人员有陈宗斌、陈红霞、张景友、易小丽、陈婷、管学岗、王新彦、金惠敏、张海峰、徐晔、戴锋、张德福、张士华、张锁玲、杜明宗、高玉琢、王涛、申川、孙玲、李振国、高德杰、宫飞、侯经国、刘淑妮、张春林、李大成、程明、张路红、张淑芝、孙先国、刘冀得、梁永翔、张广东、郁琪琳、邵长凯、蒲书箴、潘曙光、刘瑞东、李军、焦敬俭。

由于时间紧迫，加之译者水平有限，错误在所难免，恳请广大读者批评指正。

## <<安全策略与规程>>

### 内容概要

《安全策略与规程：原理与实践》提供了信息安全思想的总体描述，以便企业管理人员能够更好地评估他们的公司在处理信息安全问题上的表现。

同时《安全策略与规程：原理与实践》也提供一些实用方法来协助各个公司改进其信息安全计划。

《安全策略与规程：原理与实践》是按照为公司建立信息安全计划的步骤来组织内容的。

《安全策略与规程：原理与实践》分为三个部分。

第1部分“策略简介”旨在为开发、引荐和实施策略提供基础。

第2部分“信息安全策略的各个领域”探讨了9个安全领域的信息安全策略和规程。

第3部分“合规性”是关于策略和规程遵从联邦规章以及行业最佳实践的实际应用。

《安全策略与规程：原理与实践》各章都配有相关的习题，以指导读者深入地进行学习。

《安全策略与规程：原理与实践》可作为高等学校计算机及相关专业的教材，也可作为信息安全及管理人士的参考书。

对于有志成为信息安全专业人员的人，掌握《安全策略与规程：原理与实践》中介绍的信息是绝对必要的。

## <<安全策略与规程>>

### 作者简介

作者：(美国)格林 (Greene.S.S.) 译者：陈宗斌Sari Stern Greene(CISSP、MCSE、MCT、MCNE、MCNI、CTT、NSA / IAM)是Sage Data Security公司的总裁。  
在Sage，Sari领导一个经验丰富的安全从业人员团队。  
Sari致力于提供信息安全服务，比如策略和规程开发、信息安全程序开发、风险和漏洞评估，以及金融、卫生保健和政府领域的灾难恢复 / 业务连续性计划。  
Sari积极参与技术和安全社区。  
她是MESDA理事会中的一员，并且是Maine ISSA支部的创始会员。  
她还经常在安全大会和研讨会上发言，并且撰写了众多信息安全文章、教程和培训材料。

## &lt;&lt;安全策略与规程&gt;&gt;

## 书籍目录

第1部分 策略简介第1章 策略定义1.1 简介1.2 定义策略1.3 探讨有史以来的策略1.3.1 将《圣经》作为古代的策略1.3.2 将美国宪法作为策略革命1.4 定义策略在政府中的作用1.5 定义策略在企业文化中的作用1.5.1 服务、产品和企业文化中的一致性1.5.2 遵从政府策略1.6 理解策略的心理学1.6.1 使那些知道什么是可能的人参与进来1.6.2 环境中的变化1.7 引荐策略1.7.1 获得批准1.7.2 把策略引荐给组织1.8 使策略被接受1.8.1 组织文化来源于最高层1.8.2 通过良好的交流强化策略1.8.3 响应环境变化1.9 执行信息安全策略1.9.1 执行行为性策略1.9.2 执行技术性策略1.10 本章小结1.11 自测题1.11.1 多项选择题1.11.2 练习题1.11.3 项目题1.11.4 案例研究第2章 策略的元素2.1 简介2.2 定义策略配套文档：标准、准则和规程2.2.1 标准2.2.2 准则2.2.3 规程2.3 开发策略风格和格式2.3.1 在编写策略之前做出计划2.4 定义策略元素2.4.1 策略标题2.4.2 策略目标2.4.3 策略目的声明2.4.4 策略受众2.4.5 策略声明2.4.6 策略例外情况2.4.7 策略执行条款2.4.8 策略定义2.5 本章小结2.6 自测题2.6.1 多项选择题2.6.2 练习题2.6.3 项目题2.6.4 案例研究第2部分 信息安全策略的各个领域第3章 信息安全框架3.1 简介3.2 计划信息安全计划的目标3.2.1 C代表保密性3.2.2 I代表完整性3.2.3 A代表可用性3.2.4 信息安全的5个A：另外一些有意义的字母及其含义3.3 对数据和信息进行分类3.4 确定信息所有权角色3.5 ISO17799/BS7799信息安全管理实施细则3.6 使用ISO17799：2000的10个安全领域3.6.1 安全策略3.6.2 组织安全3.6.3 资产分类和控制3.6.4 人员安全3.6.5 物理和环境安全3.6.6 通信和运营管理3.6.7 访问控制3.6.8 系统开发和维护3.6.9 业务连续性管理3.6.10 合规性3.6.11 可能具有这么多策略吗3.7 本章小结3.8 自测题3.8.1 多项选择题3.8.2 练习题3.8.3 项目题3.8.4 案例研究第4章 安全策略文档和组织的安全策略4.1 简介4.2 撰写权威声明4.2.1 谁应该签署权威声明4.2.2 权威声明应该传达什么消息4.2.3 安全斗士的角色4.3 安全策略文档策略——关于策略的策略4.3.1 组织的安全策略文档与美国联邦法律之间有关系吗4.3.2 安全策略的雇员版本的要求4.3.3 策略是动态的4.4 管理组织的安全4.4.1 创建支持信息安全目标的组织结构4.4.2 其他人有访问权限吗4.4.3 外包日益成为一种趋势4.5 本章小结4.6 自测题4.6.1 多项选择题4.6.2 练习题4.6.3 项目题4.6.4 案例研究第5章 资产分类5.1 简介5.2 我们在尝试保护什么5.2.1 信息系统5.2.2 谁负责信息资产5.3 信息分类5.3.1 政府和军队的分类系统5.3.2 商业分类系统5.4 信息分类标记和处理5.4.1 信息标记5.4.2 熟悉的标签5.4.3 信息处理5.5 信息分类计划生命周期5.5.1 信息分类规程5.5.2 重新分级/撤销密级5.6 信息系统的价值和关键程度5.6.1 我们如何知道我们拥有什么5.6.2 资产清单方法5.6.3 资产清单的特征和属性5.6.4 系统表征5.7 本章小结5.8 自测题5.8.1 多项选择题5.8.2 练习题5.8.3 项目题5.8.4 案例研究第6章 人员安全6.1 简介6.2 初次接触6.2.1 工作说明6.2.2 面试6.3 这个人是谁6.3.1 背景检查的类型6.4 雇员协议的重要性6.4.1 保密性协议6.4.2 信息安全确认协议6.5 培训重要吗6.5.1 适用于各种计划的SETA6.5.2 利用安全意识影响行为6.5.3 利用安全培训传授技能6.5.4 安全教育是知识驱动的6.5.5 投资于培训6.6 安全事件报告是每个人的责任6.6.1 事件报告培训6.6.2 安全报告机制6.6.3 测试规程6.7 本章小结6.8 自测题6.8.1 多项选择题6.8.2 练习题6.8.3 项目题6.8.4 案例研究第7章 物理与环境安全策略和规程7.1 简介7.2 设计安全区域7.2.1 保护周界安全7.2.2 实施物理入口控制7.2.3 保护办公室、房间和设施安全7.2.4 在安全区域中工作7.3 保护设备安全7.3.1 设备安置和保护7.3.2 无电不工作7.3.3 安全地处置和重用设备7.4 一般控制7.4.1 清扫桌面和清除屏幕7.4.2 移走公司财产7.5 本章小结7.6 自测题7.6.1 多项选择题7.6.2 练习题7.6.3 项目题7.6.4 案例研究第8章 通信和运营管理8.1 简介8.2 标准操作规程8.2.1 为什么要编制操作规程的文档8.2.2 开发标准操作规程文档编制8.2.3 授权SOP文档编制8.2.4 保护SOP文档编制8.2.5 SOAP更改管理8.3 操作更改控制8.3.1 第1步：评估8.3.2 第2步：记录更改8.3.3 第3步：交流8.4 事件响应计划8.4.1 事件和严重性级别8.4.2 指定的事件处理者是谁8.4.3 事件报告、响应和处理规程8.4.4 分析事件和故障8.4.5 报告可疑的或者观察到的安全弱点8.4.6 测试可疑的或观察到的安全弱点8.5 恶意软件8.5.1 什么是恶意软件8.5.2 恶意软件控制8.6 信息系统备份8.6.1 定义备份策略8.6.2 测试恢复的重要性8.7 管理便携式存储设备8.7.1 控制非公司所有的可移动介质8.7.2 控制公司所有的可移动介质离开公司建筑物8.7.3 存储可移动介质8.7.4 安全地重用和处置介质8.7.5 外包介质拆除8.7.6 当感到怀疑时就检查日志8.7.7 运输过程中的介质安全8.7.8 仅适用于经过授权的快递员8.7.9 在运输期间物理地保护介质8.7.10 与运输介质相关的安全控制8.7.11 保护公共可用系统上的数据安全8.7.12 发布数据和遵守法律8.7.13 对渗透测试的要求8.8 保护电子邮件安全8.8.1 电子邮件不同于其他通信形式吗8.8.2 我们可能是我们自己最坏的敌人8.8.3 危及电子邮件服务器8.9 本章小结8.10 自测题8.10.1 多项选

## &lt;&lt;安全策略与规程&gt;&gt;

择题8.10.2 练习题8.10.3 项目题8.10.4 案例研究第9章 访问控制9.1 简介9.2 什么是安全姿态9.2.1 拒绝全部或者不拒绝全部.....这是一个问题9.2.2 执行业务活动的最少特权9.2.3 你需要知道吗,或者只是想知道9.2.4 我们如何知道谁需要什么9.2.5 谁决定谁需要什么9.3 管理用户访问9.3.1 一个人授权,一个人实施,另一个人监督9.3.2 用户访问管理9.3.3 晋升.解雇和其他变化9.3.4 特权伴随有责任9.4 保持密码安全9.4.1 不要问,也不要讲9.4.2 保护密钥9.4.3 其他密码策略问题9.5 用于远程连接的用户身份验证9.5.1 IPSec和虚拟专用网9.5.2 RADIUS和TACACS+9.5.3 硬件令牌9.5.4 质询/响应协议9.5.5 专用线路9.5.6 地址检查和回拨控制9.5.7 准备测试9.6 移动计算9.6.1 仍然是另一种风险评估9.6.2 批准还是禁止9.7 远程工作9.7.1 远程工作环境9.8 监视系统访问和使用9.8.1 我们需要监视什么9.8.2 审阅和保持9.8.3 监视合法吗9.9 本章小结9.10自测题9.10.1 多项选择题9.10.2 练习题9.10.3 项目题..29.10.4 案例研究第10章 系统开发和维护10.1 简介10.2 机构的风险是什么10.2.1 系统开发10.2.2 系统维护10.3 系统的安全需求10.3.1 风险评估10.3.2 独立的第三方顾问:需要吗10.3.3 实现完成后添加控制10.4 永远不能在敏感数据上发生的事情10.4.1 数据丢失10.4.2 数据修改10.4.3 数据滥用10.5 随意代码与安全代码10.5.1 系统所有者10.5.2 输入验证:简介10.5.3 高级输入验证10.5.4 测试数据输入的可信度10.5.5 输出验证10.6 风险评估和加密术10.6.1 风险评估10.6.2 保密性.完整性.身份验证.认可10.6.3 密钥的保管人10.6.4 密钥管理10.6.5 加密术与业务合作伙伴10.7 操作系统与应用软件的稳定性10.7.1 唯有稳定版本才应在生产服务器上部署10.7.2 更新:必需的.不安全的,还是两者兼备10.7.3 更新:应当部署的时机10.7.4 更新:应当执行部署的人10.7.5 测试环境所关心的内容10.8 本章小结10.9 自测题10.9.1 多项选择题10.9.2 练习题10.9.3 项目题10.9.4 案例研究第11章 业务连续性管理11.1 简介11.2 什么是灾难11.2.1 风险评估和业务影响分析(BIA)11.3 无警告的灾难打击11.3.1 行动计划11.3.2 业务连续性计划(BCP)组成11.4 理解角色和职责11.4.1 定义例外情况11.4.2 由谁负责11.5 灾难准备11.5.1 组织机构11.5.2 指挥中心位置11.5.3 通知全体人员11.5.4 业务的重新部署11.5.5 备用数据中心站11.6 响应灾难11.6.1 发现11.6.2 通知11.6.3 宣布11.6.4 启动11.7 应急计划11.7.1 业务应急规程11.7.2 业务应急文档11.8 灾难恢复11.8.1 恢复策略11.8.2 规程11.8.3 恢复手册11.9 计划的测试与维护11.9.1 测试方法11.9.2 计划的维护11.9.3 与卖主达成一致11.9.4 计划的审计11.10 本章小结11.11 自测题11.11.1 多项选择题11.11.2 练习题11.11.3 项目题11.11.4 案例研究第3分 合规性第12章 金融机构的合规性12.1 简介12.2 什么是格雷姆-里奇-比利雷法案12.2.1 GLBA的适用范围12.2.2 GLBA的执行人12.2.3 FFIEC的救赎12.2.4 GLBA安全条例的理解12.2.5 什么是部门间的指导原则12.2.6 信息安全计划的开发与实现12.3 涉及的董事会12.3.1 委托信息安全任务12.4 评估风险12.4.1 信息和信息系统的详细清单12.4.2 识别和评估威胁12.4.3 减损控制12.5 管理风险12.5.1 将ISO框架用于完成风险管理的目标12.5.2 逻辑与管理访问控制12.5.3 物理安全12.5.4 数据安全12.5.5 恶意代码12.5.6 系统开发.获取和维护12.5.7 人员安全12.5.8 电子与纸质介质的处理12.5.9 日志记录与数据收集12.5.10 服务提供商监管12.5.11 入侵检测和响应12.5.12 业务连续性考虑12.5.13 培训.培训.再培训12.5.14 测试控制12.6 调整计划.报告董事会并实现标准12.6.1 调整计划12.6.2 报告董事会12.6.3 合规性的有效期12.7 与FTC保护法案的不同之处12.7.1 目标12.7.2 元素12.8 身份盗窃和合规性12.8.1 身份盗窃的响应12.8.2 FTC与身份盗窃12.9 本章小结12.10 自测题12.10.1 多项选择题12.10.2 练习题12.10.3 项目题12.10.4 案例研究第13章 医疗卫生领域的合规性13.1 简介13.2 理解安全法规13.2.1 HIPAA的目标与目的13.2.2 HIPAA的关键原则13.2.3 达不到合规性导致的惩罚13.2.4 安全法规机构13.2.5 实现规范13.3 管理保护13.3.1 安全管理过程 § 164.308 (a) (1) 13.3.2 指派安全责任 § 164.308 (a) (2) 13.3.3 员工安全 § 164.308 (a) (3) 13.3.4 信息访问管理 § 164.308 (a) (4) 13.3.5 安全意识和培训 § 164.308 (a) (5) 13.3.6 安全事件规程 § 164.308 (a) (6) 13.3.7 意外事故计划 § 164.308 (a) (7) 13.3.8 评估 § 184.308 (a) (8) 13.3.9 业务合作合同和其他安排 § 164.308 (b) (1) 13.4 物理保护13.4.1 设施访问控制 § 164.310 (a) (1) 13.4.2 工作站的使用 § 164.310 (b) 13.4.3 工作站的安全 § 164.310 (b) 13.4.4 设备与介质控制 § 164.310 (d) (1) 13.5 技术保护13.5.1 访问控制 § 164.312 (a) (1) 13.5.2 审计控制 § 164.312 (b) 13.5.3 完整性控制 § 164.312 (c) (1) 13.5.4 人员或身份验证 § 164.312 (d) 13.5.5 传输安全 § 164.312 (e) (1) 13.6 机构要求13.6.1 业务合作合同 § 164.314 (a) (1) 13.6.2 对组健康计划的标准要求 § 164.314 (b) (1) 13.7 策略和规程13.7.1 策略和规程 § 164.316 (a) 13.7.2 文档 § 164.316 (b) (1) 13.8 本章小结13.9 自测题13.9.1 多项选择题13.9.2 练习题13.9.3 项目题13.9.4 案例研究第14章 关键基础设施领域的信息安全合规性14.1 简介14.2 电子政务成为现实14.2.1 国家级的安全性14.2.2 合规性必需的元素14.2.3 用于援救的NIST14.2.4 从事FISMA的NIST出版物14.2.5

## &lt;&lt;安全策略与规程&gt;&gt;

FISMA实现项目14.2.6 FISMA的未来14.3 保护学生记录的隐私14.3.1 FERPA的目标是什么14.3.2 教育记录是什么14.3.3 教育记录的类型14.3.4 FERPA与信息安全的关系如何14.4 一切皆从一件公司丑闻开始14.4.1 SOX与信息安全的关系如何14.4.2 采用控制框架14.5 与ISO17799:2000的关联14.5.1 ISO17799安全领域概述14.6 本章 小结14.7 自测题14.7.1 多项选择题14.7.2 练习题14.7.3 项目题14.7.4 案例研究第15章 小企业的  
安全策略与实践15.1 简介15.2 什么是小企业15.2.1 小企业应当做什么15.2.2 额外考虑15.2.3 小企业应当拥  
有什么策略15.2.4 策略应当如何提出15.3 为何要拥有一项保密性策略15.3.1 合法化15.3.2 不是一种,也不  
是两种,而是五种15.3.3 协议的结构15.3.4 保护协议15.4 什么是可接受的行为15.4.1 所有权15.4.2 硬件和软  
件15.4.3 资源滥用15.5 互联网的使用——在哪里划定最后界限15.5.1 互联网通信量的监控.记录日志及阻  
塞15.5.2 传输数据15.6 确保公司电子邮件的安全15.6.1 只供业务使用15.6.2 明文通信15.6.3 资源滥用15.7  
意外事件的报告与响应15.7.1 意外事件报告15.7.2 意外事件响应15.7.3 意外事件响应计划15.8 口令管  
理15.8.1 口令特征15.8.2 口令检查15.9 保护信息15.9.1 分类的确是必需的吗15.9.2 信息标记15.9.3 信息保  
护15.10防止恶意软件15.10.1 病毒.蠕虫.特洛伊木马以及间谍软件15.10.2 保护要求15.10.3 不要忘记用  
户15.10.4 补丁管理15.11保护远程访问15.11.1 扩展内部网络15.12控制更改15.12.1 小企业为何需要一套变  
更控制策略15.13数据备份与恢复15.13.1 企业依赖于访问数据的能力15.13.2 备份的类型15.13.3 备份介  
质的存储15.13.4 测试恢复15.14本章 小结15.15自测题15.15.1 多项选择题15.15.2 练习题15.15.3 项目题15.15.4  
案例研究附录A 访问控制附录B 雇员信息安全策略批准协议B.1 策略综述B.2 董事长的声明B.2.1 可接  
受的信息资源使用B.2.2 互联网使用B.2.3 电子邮件使用策略B.2.4 信息资源的临时使用B.2.5 口令策略B.2.6  
便携式计算策略B.2.7 发布B.2.8 认可协议B.2.9 标准定义术语表

<<安全策略与规程>>

章节摘录

插图：



## <<安全策略与规程>>

### 编辑推荐

《安全策略与规程原理与实践》：清华大学计算机安全译丛。

<<安全策略与规程>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>