

信息安全策略编制指南

信息安全策略的一部完整总集

第 12 版

作者：查尔斯·克雷森·伍德
注册信息系统安全师
注册信息安全员
注册信息系统审计师
译者：高卓



InformationShield

美国 **Information Shield** 出版公司
得克萨斯州休斯顿

目录

第 12 版前言

第 1 章 引言

第 2 章 策略制定指引

信息安全策略定义

有别于指南和标准

有别于程序和控制

策略的重要性

确保控制得到适当执行

指导产品的挑选和开发流程

展示管理层的支持

避免承担法律责任

保护商业秘密

表 2-1：制定策略的理由

适应动态通信环境

实现始终如一和完备无缺的安全

协调内部和外部行动

制定策略的步骤

收集重要参考材料

构建策略框架

准备内容对象列表

处理关键系统设计决定

落实审查、批准和执行流程

通过策略服务器自动执行策略

制定策略的时间安排

策略文档的长度

确定适宜策略数量

确定策略长度

制定策略的反复推进过程

典型策略文档的目录

最初阐明的主题

第 3 章 本指南使用说明

预期目标读者

根据机构情况修改样本细节

利用关键词搜索功能

策略样本的编排

策略的目的和范围

激发性目的

运行性目的

范围

对不遵守策略规定的处理

免责声明

更改样本的需要

权衡取舍

专家帮助的需要

第4章 具体信息安全策略

第5章 安全策略

5.1 信息安全策略

5.1.1 信息安全策略文档

5.1.2 信息安全策略评审

第6章 信息安全的组织结构

6.1 内部组织

6.1.1 管理层的信息安全承诺

6.1.2 信息安全协调

6.1.3 信息安全责任分配

6.1.4 信息处理设施的授权流程

6.1.5 保密协议

6.1.6 与当局的关系

6.1.7 与特殊兴趣团体的联系

6.1.8 信息安全的独立评审

6.2 外部方

6.2.1 识别与外部方相关的风险

6.2.2 与客户交往时强调安全

6.2.3 与第三方签订协议时强调安全

第7章 资产管理

7.1 资产责任

7.1.1 资产清单

7.1.2 资产的所有者关系

7.1.3 资产的可接受使用

7.2 信息分类

7.2.1 分类指南

7.2.2 信息的标识和处置

第8章 人力资源安全

8.1 雇用前

8.1.1 角色和责任

8.1.2 筛选

8.1.3 雇用的条款和条件

8.2 受雇期间

8.2.1 管理责任

8.2.2 信息安全意识、教育和培训

8.2.3 违纪处罚流程

8.3 离职或雇用变更

8.3.1 离职手续

8.3.2 归还资产

8.3.3 撤销访问权

第9章 物理和环境安全

9.1 安全区

9.1.1 物理安全边界

9.1.2 物理进入控制

9.1.3 确保办公室、机房和设施安全

9.1.4 防范外部和环境威胁

9.1.5 在安全区工作

9.1.6 对外开放的货物交接区

9.2 设备安全

9.2.1 设备的安置和保护

9.2.2 支持性公用事业服务

9.2.3 电缆安全

9.2.4 设备维护

9.2.5 边界外设备的安全

9.2.6 设备的安全销毁或回收再利用

9.2.7 财产迁移

第10章 通信和操作管理

10.1 操作程序和责任

10.1.1 文档化操作程序

10.1.2 变更管理

10.1.3 职责分离

10.1.4 开发、测试和操作设施分离

10.2 第三方服务供应管理

10.2.1 服务供应

10.2.2 第三方服务的监督和评审

10.2.3 第三方服务变更管理

10.3 系统规划和验收

10.3.1 产能管理

10.3.2 系统验收

10.4 防范恶意和移动代码

10.4.1 防范恶意代码

10.4.2 防范移动代码

10.5 备份

10.5.1 信息备份

10.6 网络安全管理

10.6.1 网络控制

10.6.2 网络服务的安全

10.7 介质处理

10.7.1 可移动介质管理

10.7.2 介质销毁

10.7.3 信息处置程序

10.7.4 系统文档安全

10.8 信息交换

- 10.8.1 信息交换策略和程序
- 10.8.2 交换协议
- 10.8.3 物理介质传输
- 10.8.4 电子消息传递
- 10.8.5 业务信息系统

10.9 电子商务服务

- 10.9.1 电子商务
- 10.9.2 在线交易
- 10.9.3 公共可用信息

10.10 监视

- 10.10.1 审计日志
- 10.10.2 监视系统的使用
- 10.10.3 日志信息保护
- 10.10.4 管理员和操作员日志
- 10.10.5 故障日志
- 10.10.6 时钟同步

第 11 章 访问控制

11.1 访问控制的业务要求

- 11.1.1 访问控制策略

11.2 用户访问管理

- 11.2.1 用户注册
- 11.2.2 权限管理
- 11.2.3 用户口令管理
- 11.2.4 用户访问权限审查

11.3 用户责任

- 11.3.1 口令使用
- 11.3.2 无人值守的用户设备
- 11.3.3 办公桌和显示屏清除策略

11.4 网络访问控制

- 11.4.1 网络服务使用策略
- 11.4.2 外部连接的用户认证
- 11.4.3 网络设备识别
- 11.4.4 远程诊断和配置端口保护
- 11.4.5 网内隔离
- 11.4.6 网络连接控制
- 11.4.7 网络路由控制

11.5 操作系统访问控制

- 11.5.1 安全登录程序
- 11.5.2 用户的识别和认证
- 11.5.3 口令管理制度
- 11.5.4 系统公用程序的使用
- 11.5.5 会话超时

- 11.5.6 连接时间限制
- 11.6 应用和信息访问控制**
 - 11.6.1 信息访问限制
 - 11.6.2 敏感系统隔离
- 11.7 移动计算和远程办公**
 - 11.7.1 移动计算和通信
 - 11.7.2 远程办公
- 第 12 章 信息系统的采购、开发和维护**
 - 12.1 信息系统的安全要求**
 - 12.1.1 安全要求的分析和规定
 - 12.2 应用的正确处理**
 - 12.2.1 输入数据验证
 - 12.2.2 内部处理控制
 - 12.2.3 消息完整性
 - 12.2.4 输出数据验证
 - 12.3 加密控制**
 - 12.3.1 使用加密控制的策略
 - 12.3.2 密钥管理
 - 12.4 系统文档安全**
 - 12.4.1 操作软件控制
 - 12.4.2 系统测试数据保护
 - 12.4.3 程序源代码访问控制
 - 12.5 开发和支持流程的安全**
 - 12.5.1 变更控制程序
 - 12.5.2 操作系统变更后的应用技术评审
 - 12.5.3 软件包变更限制
 - 12.5.4 信息泄露
 - 12.5.5 外包软件开发
 - 12.6 技术脆弱性管理**
 - 12.6.1 技术脆弱性控制
- 第 13 章 信息安全事故管理**
 - 13.1 报告信息安全事件和弱点**
 - 13.1.1 报告信息安全事件
 - 13.1.2 报告安全弱点
 - 13.2 信息安全事故的管理和改进**
 - 13.2.1 责任和程序
 - 13.2.2 总结信息安全事件的经验教训
 - 13.2.3 收集证据
- 第 14 章 业务连续性管理**
 - 14.1 业务连续性管理涉及信息安全的方面**
 - 14.1.1 把信息安全纳入业务连续性管理流程
 - 14.1.2 业务连续性和风险评价
 - 14.1.3 制定和执行包含信息安全的业务连续性计划

- 14.1.4 业务连续性计划框架
- 14.1.5 业务连续性计划的测试、保持和再评价

第 15 章 合规

15.1 遵守法律要求

- 15.1.1 识别适用立法
- 15.1.2 知识产权
- 15.1.3 机构记录保护
- 15.1.4 个人信息的数据保护和隐私权
- 15.1.5 防范信息处理设施滥用
- 15.1.6 密码控件监管

15.2 遵守安全策略和标准及技术合规

- 15.2.1 遵守安全策略和标准
- 15.2.2 技术合规检查

15.3 信息系统审计的考虑因素

- 15.3.1 信息系统审计控制
- 15.3.2 信息系统审计工具保护

附录 A 信息安全策略参考文献列表

附录 B 信息安全期刊列表

附录 C 专业协会和相关组织列表

- 一般性组织
- 行业组织
- 按市场细分的组织

附录 D 安全意识教育方法建议列表

- 人员方面
- 书面材料方面
- 系统方面
- 其他方面

附录 E 与其他机构的联网安全策略协调一致

- 访问控制方面
- 加密和公钥基础设施方面
- 变更控制和应急预案方面
- 网络管理方面

附录 F 策略制定步骤检查列表

附录 G 策略制定流程简图

附录 H 因缺失策略而造成问题的真实案例

- 政府部门
- 律师事务所
 - 石油公司
 - 地方报社
 - 中西部制造公司
 - 西海岸制造公司
 - 著名互联网服务供应商

附录 I 后续步骤建议

附录 J 有关书面策略的法规要求

利用本指南满足法规要求

利用本指南满足 PCI-DSS 的要求

利用本指南满足 HIPAA/HiTEC 的安全要求

利用本指南满足《萨班斯-奥克斯利法案》的要求

利用本指南满足 NIST (FISMA) 的安全要求

附录 K 策略相关文档范本

遵守信息安全策略同意书

数据分类速查表范本

员工离职检查列表范本

安全事件报告表范本

经理接受风险备忘录范本

两页简化版不泄密协议范本

身份令牌责任书范本

信息安全策略术语表范本

附录 L 现成策略文档范本

资产可接受使用策略范本 (内部系统)

访问控制安全策略范本

账号和权限管理策略范本

资产管理策略范本

备份和恢复策略范本

业务连续性策略范本

详细版信息安全策略范本

电子邮件安全策略范本

外部网络连接安全策略范本

对外披露信息策略范本

防火墙管理策略范本

高层信息安全策略范本

信息分类策略范本

事故报告和响应策略范本

信息销毁策略范本

信息交换策略范本

信息拥有权策略范本

信息安全方案策略范本

互联网可接受使用策略范本

内联网安全策略范本

IT 风险管理安全策略范本

日志管理和监测策略范本

网络安全管理策略范本

恶意软件策略范本

移动计算机安全策略范本

口令管理策略范本

个人计算机安全策略范本

人员安全管理策略范本

物理安全策略范本

隐私权策略范本——较严格的

隐私权策略范本——较宽松的

远程访问管理策略范本

安全策略模板

社交网络可接受使用策略范本

远程办公安全策略范本

第三方安全管理策略范本

网站安全策略范本

无线网络安全策略范本

关于作者