

ICS 75 - 010

E 07

备案号: 29417—2010



# 中华人民共和国石油天然气行业标准

**SY/T 5231—2010**

代替 SY/T 5231—1999

---

## 石油工业计算机信息系统安全管理规范

Security management standard for computer information system  
of petroleum industry

2010—05—01 发布

2010—10—01 实施

---

国家能源局 发布

目 次

前言 ..... II

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 体系概述 ..... 2

5 物理安全 ..... 2

6 网络安全 ..... 2

7 信息加密 ..... 2

8 运行安全 ..... 3

9 访问控制 ..... 3

10 安全架构和评估..... 3

11 业务连续性计划和灾难性恢复计划..... 3

12 遵守法律与犯罪调查管理..... 3

13 用户管理..... 3

参考文献..... 4

## 前 言

本标准代替 SY/T 5231—1999《石油工业计算机安全保密规程》。

本标准由石油信息与计算机应用专业标准化技术委员会提出并归口。

本标准起草单位：中国石油勘探开发研究院。

本标准主要起草人：靖小伟、冯梅、刘磊、石国伟、杨志贤、王峰、刘晓、郭以东、张克春、刘建兵、郭晓东、王雷、滕征岑、叶铭。

本标准所代替标准的历次版本发布情况为：

——SY/T 5231—1991，SY/T 5231—1999。

# 石油工业计算机信息系统安全管理规范

## 1 范围

石油工业计算机信息系统安全涵盖信息的存储、传输及应用的各环节，涉及到以下 10 个方面：

- 体系概述；
- 物理安全；
- 网络安全；
- 信息加密；
- 访问控制；
- 运行安全；
- 安全架构和评估；
- 业务连续性计划和灾难性恢复计划；
- 遵守法律及犯罪调查管理；
- 用户管理。

本标准为指导性标准，适用于石油工业企业，具体的信息系统按照各自的特点制定详细安全技术规范。

## 2 规范性引用文件

下列文件中的条款通过在本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 17859—1999 计算机信息系统 安全保护等级划分准则

ISO/IEC 15408 信息技术安全评估准则

信息安全等级保护管理办法 公通字（2007）43 号

## 3 术语和定义

下列术语和定义适用于本标准。

### 3.1

**客体 object**

信息的被动载体，如计算机、文件、数据库、目录、程序等。

### 3.2

**主体 subject**

存取客体中信息或客体的主动实体，如用户、程序、进程或设备等。

### 3.3

**安全策略 security policies**

由最高管理层做出的关于信息安全的最广泛、最概括的定义，明确指定了企业信息安全的作用、价值与意义。

### 3.4

**安全域 security domains**

可供主体访问的一组资源，这一资源工作于同一安全策略之下、被统一管理。

### 3.5

#### 业务连续性计划 business continuity planning

为保护信息系统，降低关键业务应用活动受到灾难影响，制定的保证业务应用连续性的技术方案。

### 3.6

#### 灾难性恢复计划 disaster recovery planning

灾难来临后，为保护信息系统，使企业关键业务应用不受灾难破坏，并在企业所能容忍的时间间隔内实施恢复，制定的业务恢复正常的技术方案。

## 4 体系概述

4.1 依据国家的相关法律、法规及国际标准，建立适合本企业的信息系统安全策略体系。

4.2 依据 GB/T 17859—1999 及《信息安全等级保护管理办法》[公通字(2007)43号]的规定，划分企业信息系统的等级。

4.3 建立信息系统安全等级的风险评估与管理制度，定期分析面临的威胁，进行风险评估。

4.4 根据风险评估及费用分析，选择安全措施。

4.5 建立信息系统安全管理机构，设置相应的安全岗位，明确应尽的责任与义务。

4.6 信息系统安全管理机构负责制定企业信息系统安全管理目标，划分信息系统的安全等级，建立风险评估与管理制度，制定用户管理规范，进行信息系统安全教育和培训，在聘用、保密和解聘等协议中加入关于信息系统安全的条款。

## 5 物理安全

5.1 依据国家相关规范及标准，对信息系统所处环境进行安全保护。

5.2 依据国家的相关法律、法规及国际标准，对信息系统的承载设备实行电源保护、防盗、防毁、防电磁信息辐射泄漏及抗电磁干扰。

5.3 制定适合本企业信息系统安全等级的物理安全策略。

5.4 建立企业信息存储介质安全管理规定。

5.5 对不同安全等级的信息系统环境安全、设备安全及介质安全定期进行威胁评估，分析面临的风险。

5.6 依据本企业物理安全策略，实施物理安全保护措施，包括对人、设备、环境、介质等。

## 6 网络安全

6.1 分析评估信息系统在网络传输过程中面临的威胁与风险，按照不同的信息系统安全等级，划分网络安全域。针对不同的安全域，制定不同的安全策略。

6.2 依据网络安全策略，采用合适的网络安全技术与设备，实现网络安全域的保障与防护。可采用的网络安全技术与设备，如加密技术、访问控制技术、防火墙设备、入侵检测设备、流量监控与审计系统、网络设备与链路的冗余技术、QOS技术等。

6.3 定期进行模拟攻击测试，发现网络安全漏洞，及时修补。

6.4 根据网络安全最佳实践，定期审核网络设备的部署情况及运行状态，检查网络安全的合规性，对网络安全进行优化。

## 7 信息加密

7.1 分析评估信息在网络传输和存储中面临的威胁与风险，制定适合信息系统安全等级的信息加密策略。

7.2 依据信息加密策略，选择加密类型、加密算法和密钥关键字长度。

7.3 依据信息系统的安全等级，制定相应的信息加密和密钥关键字有效性的管理措施。

## 8 运行安全

8.1 分析运行过程中所面临的威胁与风险，制定不同安全等级信息系统的运行安全策略。

8.2 依据运行安全策略，制定相应的员工工作规范，明确责任与义务。

8.3 对相关人员进行背景检查，实行最小权限管理、权职分离、工作轮换和强制休假制度。

8.4 依据运行安全策略，制定信息系统的变更管理、资源保护、输入/输出控制、介质控制等管理规范。

8.5 依据运行安全策略，建立相应的员工与信息系统的监控与审计规范。

## 9 访问控制

9.1 分析评估信息系统面临的威胁与风险，按照不同的信息系统等级，制定整体访问控制策略。

9.2 建立身份识别、认证、授权与审计体系。

9.3 依据访问控制策略采用合适的访问控制技术，实现不同信任级别的主体对不同安全域的访问控制。

9.4 定期进行穿透测试，寻找访问控制的漏洞，完善访问控制策略和方法，保护客体的机密性、完整性与可用性。

## 10 安全架构和评估

10.1 依据信息系统安全等级，确定安全模型与安全架构，建立信息系统安全体系。

10.2 参照 ISO/IEC 15408，分析信息系统所面临的威胁与风险，制定信息系统安全评估策略。

10.3 依据信息安全评估策略，制定适合信息系统的安全评估计划。

## 11 业务连续性计划和灾难性恢复计划

11.1 依据信息系统安全等级，分析业务应用连续性以及灾难恢复面临的威胁与风险，制定业务应用连续性与灾难恢复策略。

11.2 依据业务应用连续性策略，制定业务应用连续性计划。

11.3 依据业务应用灾难恢复策略，制定灾难性恢复计划。

## 12 遵守法律与犯罪调查管理

12.1 保证信息系统的设计、运行、使用和管理不违反国家法律和法规。

12.2 保证信息系统的设计、运行、使用和管理合同约定受法律保护。

12.3 依据信息系统安全等级划分，建立应急处理队伍和管理规范，进行相关计算机信息犯罪识别、证据搜集、证据质量和完备性保护。

## 13 用户管理

13.1 遵守国家相关的法律法规。

13.2 不得利用计算机危害企业业务运行、损害企业利益。

13.3 不得非法获得权限，不得越权使用、滥用、妨碍、窃取企业及其他用户的信息和相关资源。

13.4 防止企业信息、个人信息及设备被他人非法使用或盗用。

13.5 非本企业用户不能访问、使用企业内部网络上的信息及相关资源。

参 考 文 献

- [1] ISO/IEC 17799: 2000 (E) 信息技术 信息安全管理用实施规程 (*Information technology—Code of practice for information security management*)
  - [2] ISO/IEC 27001: 2005 信息安全管理体系
  - [3] ISO/IEC 27002 信息安全管理实用规则
  - [4] ISO/IEC 27003 信息安全管理体系实施指南
  - [5] ISO/IEC 27004 信息安全管理测量
  - [6] ISO/IEC 27005 信息安全风险管理
-

中华人民共和国  
石油天然气行业标准  
石油工业计算机信息系统安全管理规范  
SY/T 5231—2010

石油工业出版社出版  
(北京安定门外安华里二区一号楼)  
石油工业出版社印刷厂排版印刷  
新华书店北京发行所发行

880×1230 毫米 16 开本 0.75 印张 15 千字 印 1—2000  
2010 年 8 月北京第 1 版 2010 年 8 月北京第 1 次印刷  
书号: 155021·6476

版权专有 不得翻印