



中华人民共和国国家标准

GB/T 22081—2008/ISO /IEC 27002:2005
代替 GB/T 19716--2005

信息技术 安全技术 信息安全管理实用规则

Information technology—Security techniques—
Code of practice for information security management

(ISO/IEC 27002:2005, IDT)

2008-06-19 发布

2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

前言	III
引言	IV
1 范围	1
2 术语和定义	1
3 本标准的结构	2
3.1 章节	2
3.2 主要安全类别	3
4 风险评估和处理	3
4.1 评估安全风险	3
4.2 处置安全风险	3
5 安全方针	4
5.1 信息安全方针	4
6 信息安全组织	5
6.1 内部组织	5
6.2 外部各方	8
7 资产管理	12
7.1 对资产负责	12
7.2 信息分类	13
8 人力资源安全	14
8.1 任用之前	14
8.2 任用中	16
8.3 任用的终止或变更	17
9 物理和环境安全	18
9.1 安全区域	18
9.2 设备安全	20
10 通信和操作管理	23
10.1 操作规程和职责	23
10.2 第三方服务交付管理	25
10.3 系统规划和验收	26
10.4 防范恶意和移动代码	27
10.5 备份	28
10.6 网络安全管理	29
10.7 介质处置	30
10.8 信息的交换	31
10.9 电子商务服务	34
10.10 监视	36
11 访问控制	39
11.1 访问控制的业务要求	39

11.2	用户访问管理	39
11.3	用户职责	41
11.4	网络访问控制	43
11.5	操作系统访问控制	46
11.6	应用和信息访问控制	48
11.7	移动计算和远程工作	49
12	信息系统获取、开发和维护	51
12.1	信息系统的安全要求	51
12.2	应用中的正确处理	51
12.3	密码控制	53
12.4	系统文件的安全	55
12.5	开发和支持过程中的安全	56
12.6	技术脆弱性管理	58
13	信息安全事件管理	59
13.1	报告信息安全事态和弱点	59
13.2	信息安全事件和改进的管理	61
14	业务连续性管理	63
14.1	业务连续性管理的信息安全方面	63
15	符合性	66
15.1	符合法律要求	66
15.2	符合安全策略和标准以及技术符合性	68
15.3	信息系统审计考虑	69
	参考文献	71