ISO/IEC 27001标准

第三版

2022-10-25

信息安全、网络安全和隐私保护——信息安全管理体系——要求

目　　录

前言 3
简介 4
0.1 总则 4
0.2 与其他管理体系标准的兼容性 4
1 范围 5
2 规范性引用文件 5
3 术语和定义 5
4 组织环境 5
4.1 理解组织及其环境 5
4.2 理解相关方的需求和期望 5
4.3 确定信息安全管理体系的范围 6
4.4 信息安全管理体系 6
5 领导 6
5.1 领导力和承诺 6
5.2 方针 6
5.3 组织角色、职责和权限 7
6 策划 7
6.1 应对风险和机遇的措施的策划 7
6.1.1 总则 7
6.1.2信息安全风险评估的策划 8
6.1.3信息安全风险控制的策划 8
6.2 信息安全目标及其实现的策划 9
6.3 变更的策划 9
7 支持 9
7.1 资源 9
7.2 能力 10
7.3 意识 10
7.4 沟通 10
7.5 文件化信息 10
7.5.1 总则 10
7.5.2 创建和更新 11
7.5.3文件化信息的控制 11
8 运行 11
8.1 运行策划和控制 11
8.2 信息安全风险评估 12
8.3 信息安全风险控制 12
9 绩效评价 12
9.1 监测、测量、分析和评价 12
9.2 内部审核 12
9.2.1 总则 12
9.2.2 内部审核方案 13
9.3 管理评审 13
9.3.1总则 13
9.3.2管理评审输入 13
9.3.3管理评审输出 13
10 改进 14
10.1 持续改进 14
10.2 不符合和纠正措施 14
参考文献 23