

信息安全、网络安全和隐私保护

信息安全管理体系 要求

Information security,cybersecurity and privacy protection

-Information security management systems-Requirements

(ISO/IEC 27001:2022)

目 录

目 录.....	2
0 引言	1
0.1 总则.....	1
0.2 与其他管理体系标准的兼容性.....	1
1. 范围.....	2
2 规范性引用文件.....	2
3 术语和定义.....	3
4 组织环境.....	3
4.1 理解组织及其环境.....	3
4.2 理解相关方的需求和期望.....	4
4.3 确定信息安全管理体范围.....	4
4.4 信息安全管理体.....	5
5 领导力.....	5
5.1 领导力和承诺.....	5
5.2 方针.....	6
5.3 组织的角色，职责和权限.....	7
6.规划	8
6.1 应对风险和机会的措施.....	8
6.2 信息安全目标和实现规划.....	11
6.3 策划变更.....	12
7 支持	12
7.1 资源.....	12
7.2 能力.....	13
7.3 意识.....	13
7.4 沟通.....	14
7.5 文件化信息.....	14
8 运行	16
8.1 运行规划和控制.....	16
8.2 信息安全风险评估.....	17
8.3 信息安全风险处置.....	17
9 绩效评价.....	18
9.1 监视、测量、分析和评价.....	18
9.2 内部审核.....	19
9.3 管理评审.....	20
10 改进.....	21
10.1 持续改进.....	21
10.2 不符合和纠正措施.....	22