ISO/IEC 27001
2022-10

信息安全 网络安全 隐私保护

信息安全管理体系

要求

中文翻译稿

盟标国际认证有限公司

目录

前言 I
引言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 组织环境 1
4.1 理解组织及其环境 1
4.2 理解相关方的需求和期望 1
4.3 确定信息安全管理体系范围 1
4.4 信息安全管理体系 1
5 领导 2
5.1 领导和承诺 2
5.2 方针 2
5.3 组织的角色，责任和权限 2
6 策划 2
6.1 应对风险和机会的措施 2
6.1.1 总则 2
6.1.2 信息安全风险评估 3
6.1.3 信息安全风险处置 3
6.2 信息安全目标及其实现规划 4
6.3 变更规划 4
7 支持 4
7.1 资源 4
7.2 能力 4
7.3 意识 4
7.4 沟通 4
7.5 文件化信息 5
7.5.1 总则 5
7.5.2 创建和更新 5
7.5.3 文件化信息的控制 5
8 运行 5
8.1 运行规划和控制 5
8.2 信息安全风险评估 5
8.3 信息安全风险处置 6
9 绩效评价 6

9.1 监视、测量、分析和评价 6
9.2 内部审核 6
9.2.1 总则 6
9.2.2 内部审核方案 6
9.3 管理评审 6
9.3.1 总则 6
9.3.2 管理评审的输入 6
9.3.3 管理评审的输出 7
10 改进 7
10.1 持续改进 7
10.2 不符合及纠正措施 7
附录 A（规范性附录）信息安全控制参考 8
参考文献 15

盟标国际认证有限公司
Mengbiao International Certification Co.,Ltd

公开文件说明

本机构按照《国家认监委关于加强认证规则管理的公告》（认监委公告 2025 年第 9 号）对于本机构认证规则、认证依据文件进行公示，保障公众知情权与监督权，鉴于部分文件内容涉及本机构知识产权信息，为避免因信息过度披露对公司合法权益造成损害，依据法律法规规定，经公司内部审慎评估，决定仅对不涉及产权保护的部分内容进行公开上传至公司官网，公开的内容包括认证规则、认证依据目录页面等，您可通过访问公司官网，查阅已公开的文件资料。

若您对公开文件有任何疑问或建议，或需要获得公开文件完整内容的，欢迎通过公司官方客服电话【020-62355389】或官方邮箱【mbgjrz@163.com】与我们联系。

我们承诺，公开内容真实、准确，且符合国家法律法规及行业规范。

承诺单位：盟标国际认证有限公司

承诺日期：2025 年 06 月 13 日