



International
Standard

ISO/IEC 27701

**Information security, cybersecurity
and privacy protection – Privacy
information management systems –
Requirements and guidance**

信息安全，网络安全和隐私保护 – 隐私信息
– 要求

第 二 版
2025 - 10

查阅全文请联系北京海德国际认证有限公司
联系电话：010-84905056，010-65817800
邮箱地址：common@hicchina.com.cn

参考编号
ISO/IEC 27701:2025

© ISO/IEC 2025

目

页码

前言

引言

范围

规范性引用文件

术语，定义和缩写

组织环境

4.1 理解组织及其环境.....	10
4.2 理解相关方的需求和期望.....	10
4.3 确定隐私信息管理体系范围.....	11
4.4 隐私信息管理体系.....	11

5 领导作用

5.1 领导作用和承诺.....	11
5.2 隐私政策.....	11
5.3 组织的角色，责任和权限.....	12

6 策划

6.1 应对风险和机会的措施.....	12
6.1.1 总则.....	12
6.1.2 隐私风险评估.....	12
6.1.3 隐私风险处置.....	13
6.2 隐私信息目标及其实现策划.....	14
6.3 变更策划.....	15

7 支持

7.1 资源.....	15
7.2 能力.....	15
7.3 意识.....	15
7.4 沟通.....	15
7.5 文件化信息.....	15
7.5.1 总则.....	15
7.5.2 创建和更新.....	15
7.5.3 文件化信息的控制.....	16

8 运行

8.1 运行规划和控制.....	16
8.2 隐私风险评估.....	17
8.3 隐私风险处置.....	17

9 绩效评价

ISO/IEC 27

9.1 监视、测量、分析和评价	17
9.2 内部审核	17
9.2.1 总则	17
9.2.2 内部审核方案	17
9.3 管理评审	18
9.3.1 总则	18
9.3.2 管理评审输入	18
9.3.3 管理评审结果	18
10 改进	1
10.1 持续改进	18
10.2 不符合及纠正措施	18
11 关于附录的更多信息	1
附录 A（规范性附录） PII 控制者和 PII 处理者的 PIMS 参考控制目标及控制	20
附录 B（规范性附录） PII 控制者和 PII 处理者的实施指南	25
附录 C（资料性附录） 与 ISO/IEC 29100 的映射	53
附录 D（资料性附录） 与通用数据保护条例 GDPR 的映射	55
附录 E（资料性附录） 与 ISO/IEC 27018 和 ISO/IEC 29151 的映射	59
附录 F（资料性附录） 与 ISO/IEC 27701:2019 的对应关系	61
参考文献	