



国际标准

信息安全、网络安全和隐私保护-
隐私信息管理体系-要求和指南

ISO/IEC 27701

第二版
2025-10

目录

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩写	1
3.1 组织	1
3.2 相关方	1
3.3 最高管理者	1
3.4 管理体系	1
3.5 策略	1
3.6 目标	1
3.7 风险	2
3.8 过程	2
3.9 能力	2
3.10 成文信息	2
3.11 绩效	2
3.12 持续改进	2
3.13 有效性	2
3.14 要求	2
3.15 符合性	3
3.16 不符合性	3
3.17 纠正措施	3
3.18 审核	3
3.19 测量	3
3.20 监视	3
3.21 联合 PII 控制者	3
3.22 客户	3
3.23 隐私信息管理体系 PIMS	3
3.24 信息安全计划	3
3.25 适用性声明	4
4 组织环境	4
4.1 了解组织及其环境	4
4.2 了解相关方的需求和期望	4
4.3 确定隐私信息管理体系的范围	5
4.4 隐私信息管理体系	5
5 领导作用	5
5.1 领导作用和承诺	5
5.2 隐私方针	5
5.3 岗位、职责和权限	5
6 策划	6
6.1 应对风险和机遇的措施	6
6.2 隐私目标及其实现策划	7
6.3 变更策划	8

7 支持	8
7.1 资源	8
7.2 能力	8
7.3 意识	8
7.4 沟通	8
7.5 成文信息	8
8 运行	9
8.1 运行策划与控制	9
8.2 隐私风险评价	9
8.3 隐私风险处理	9
9 绩效评价	10
9.1 监视、测量、分析和评价	10
9.2 内部审核	10
9.3 管理评审	10
10 改进	11
10.1 持续改进	11
10.2 不符合与纠正措施	11
11 附件中的进一步说明	11
附录 A PIMS 参考控制目标以及 PII 控制者和 PII 处理者的控制措施	12
附录 B PII 控制者和 PII 处理者的实施指南	18
B.1 PII 控制者的实施指南	18
B.2 PII 处理者的实施指南	27
B.3 PII 控制者和 PII 处理者的实施指南	31
附录 C 对应关系到 ISO/IEC 29100	41
附录 D 与通用数据保护条例的对应关系	43
附录 E 与 ISO/IEC 27018 和 ISO/IEC 29151 的对应关系	47
附录 F 与 IEC 27701:2019 ISO 的对应关系	49
参考文献	55