

国际标准

信息安全、网络安全与隐私保护

隐私信息安全管理——要求与指南

ISO/IEC 27701

第二版 2025-10

受版权保护的文档

ISO/IEC 2025

版权所有。除非另有规定或实施过程中需要，未经事先书面许可，不得以任何形式或任何方式（包括电子或机械手段，如复印、发布于互联网或内联网）复制或以其他方式使用本出版物的任何部分。许可申请可向以下地址的 ISO 组织或请求者所在国的 ISO 成员机构提出。

国际版权局

CP 401 Ch. de Blandonnet 8

日内瓦 CH-1214 维尔尼尔

电话：+41227490111

Email:copyright@iso.org

Website:www.iso.org

在瑞士出版

目 录

1 范围	10
2 规范性参考文献	10
3 术语、定义和缩写	10
3.1 organization 组织	10
3.2 interested party 相关方	11
3.3 top management	11
3.4 management system 管理体系	11
3.5 policy 方针	11
3.6 objective result to be achieved 要实现的目标	11
3.7 risk 风险	12
3.8 process 过程	12
3.9 competence 能力	12
3.10 documented information 文件信息	12
3.11 performance 绩效	13
3.12 continual improvement 持续改进	13
3.13 effectiveness 有效	13
3.14 requirement 要求	13
3.15 conformity 符合	13
3.16 nonconformity 不符合性	13
3.17 corrective action 纠正措施	13
3.18 audit 审核	13

3.19 measurement 测量	14
3.20 monitoring 监视	14
3.21 joint PII controller 联合 PII 控制者	14
3.22 customer 顾客	14
3.23 privacy information management system PIMS 隐私信息安全管理体系 PIMS	14
3.24 information security programme 信息安全方案	14
3.25 statement of applicability 适用性声明	15
4 组织环境	15
4.1 理解组织及其环境	15
4.2 理解相关方的需求和期望	16
4.3 确定隐私信息安全管理体系的范围	16
4.4 隐私信息安全管理体系	17
5. 领导力	17
5.1 领导力与承诺	17
5.2 隐私方针	17
5.3 角色、职责与权限	18
6 策划	18
6.1 应对风险和机遇的措施	18
6.1.1 总则	18
6.1.2 隐私风险评估	19
6.1.3 隐私风险处理	20

6.2 隐私目标及实现策划	22
6.3 变更策划	22
7 支持	22
7.1 资源	22
7.2 能力	22
7.3 意识	23
7.4 沟通	23
7.5 文件化信息	23
7.5.1 总则	23
7.5.2 创建和更新	24
7.5.3 文件化信息的控制	24
8 运行	24
8.1 运行策划与控制	25
8.3 隐私风险处理	25
9 绩效评价	25
9.1 监测、测量、分析和评价	25
9.2 内部审核	26
9.2.1 总则	26
9.2.2 内部审核策划	26
9.3 管理评审	26
9.3.1 总则	26
9.3.2 管理评审的输入信息	27

9.3.3 管理评审结果	27
10 改进	27
10.1 持续改进	27
10.2 不符合项及纠正措施	27
11 附件的进一步信息	28
附录 A (规范性) PIMS PII 控制者和 PII 处理者的参考控制目标和控制	29
附录 B(规范性附录) PII 控制者和 PII 处理者的实施指南	40
附录 E (参考性附录) ISO/IEC27018 与 ISO/IEC29151 的对应关系	93
附录 F (参考性附录) ISO/IEC 27701:2019 标准对应关系	95
参考文献	103