



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
——要求与指南

信息安全、网络安全与隐私保护——隐私信息管理体系——要求与建议

ISO/IEC 27701

第二版 **2025-10**



版权保护文件

© ISO/IEC 2025

保留所有权利。除非另有说明，或实施过程中有特殊要求，未经事先书面许可，不得以任何形式或任何手段（包括电子或机械方式）复制或使本出版物的任何部分，包括影印、在互联网或内联网上发布。许可申请可向下述地址的ISO或申请者所在国的ISO成员机构提出。

ISO版权办公室
CP 401 • 布兰东内街8号 CH-1214 韦尔
尼耶，日内瓦电话：+41 22 749 01 11
电子邮箱：copyright@iso.org 网站：
www.iso.org

瑞士出版

目录

页码

前言.....	v
导言.....	vi
1 范围.....	1
2 规范性引用.....	1
3 术语、定义和缩写.....	1
4 组织背景.....	4
4.1 理解组织及其背景.....	4
4.2 理解相关方的需求和期望.....	5
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.....	6
5 领导层.....	6
5.1 领导力与承诺.....	6
5.2 隐私政策.....	6
5.3 角色、职责与权限.....	7
6 规划.....	7
6.1 应对风险与机遇的行动方案.....	7
6.1.1 一般性.....	7
6.1.2 隐私风险评估.....	7
6.1.3 隐私风险处理.....	8
6.2 隐私目标及实现规划.....	9
6.3 变更规划.....	10
7 支持.....	10
7.1 资源.....	10
7.2 能力.....	10
7.3 意识.....	10
7.4 沟通.....	10
7.5 文件化信息.....	11
7.5.1 一般.....	11
7.5.2 创建和更新文件化信息.....	11
7.5.3 文件信息的控制.....	11
8 操作.....	12
8.1 运行计划与控制.....	12
8.2 隐私风险评估.....	12
8.3 隐私风险处理.....	12
9 绩效评估.....	12
9.1 监测、测量、分析和评估.....	12
9.2 内部审计.....	13
9.2.1 一般.....	13
9.2.2 内部审计计划.....	13
9.3 管理层评审.....	13
9.3.1 一般.....	13
9.3.2 管理评审输入.....	13
9.3.3 管理评审结果.....	14
10 改进.....	14
10.1 持续改进.....	14
10.2 不符合项与纠正措施.....	14
11 附件的进一步信息.....	14
附件A（规范性）PIMS参考控制目标及PII控制器与PII处理器的控制措施.....	15

附件B（规范性）PII控制器和PII处理器的实施指南.....	21
附件C（信息性）与ISO/IEC 29100的映射关系.....	51
附录D（信息性）与《通用数据保护条例》的对照关系.....	53
附录E（说明性）与ISO/IEC 27018和ISO/IEC 29151的映射关系.....	56
附录F（信息性）与ISO/IEC 27701:2019的对应关系.....	58
参考文献.....	64

前言

国际标准化组织（ISO）与国际电工委员会（IEC）共同构成全球标准化专业体系。作为ISO或IEC成员的国家机构，通过各组织为特定技术领域设立的技术委员会参与国际标准制定工作。ISO与IEC技术委员会在共同关注领域开展协作。其他与ISO和IEC保持联络的国际组织（包括政府组织和非政府组织）也参与相关工作。

本文件的编制程序及其后续维护程序详见ISO/IEC指令第1部分。特别需要注意的是，不同类型的文件需满足不同的批准标准。本文件的起草遵循了ISO/IEC指令第2部分的编辑规则（详见www.iso.org/directives或www.iec.ch/members_experts/refdocs）。

ISO和IEC提醒注意，实施本文件可能涉及使用一项或多项专利。ISO和IEC对任何相关专利权主张的证据、有效性或适用性不持任何立场。截至本文件发布之日，ISO和IEC尚未收到实施本文件可能涉及的专利通知。但需提醒实施者注意，此信息可能并非最新状态，最新专利信息可通过www.iso.org/patents和<https://patents.iec.ch>查询。ISO和IEC不承担识别任何或所有此类专利权利的责任。

本文件中使用的任何商标名称仅为方便用户而提供，并不构成推荐。

关于标准自愿性的说明、ISO特定术语及符合性评估相关表述的含义，以及ISO在《技术性贸易壁垒协定》(TBT)中遵循世界贸易组织(WTO)原则的信息，请参阅www.iso.org/iso/foreword.html。在IEC中，请参阅www.iec.ch/understanding-standards。

本文件由国际标准化组织/国际电工委员会联合技术委员会1（JTC 1）下属信息技术分技术委员会27（SC 27）——信息安全、网络安全与隐私保护分技术委员会，与欧洲标准化委员会（CEN）技术委员会CEN/CLC/JTC 13——网络安全与数据保护技术委员会共同编制，依据ISO与CEN技术合作协议（维也纳协议）完成。

本第二版取代并废止了经技术修订的第一版（ISO/IEC 27701:2019）。

主要变更如下：

- 本文件已重新编写为独立的管理体系标准。

关于本文件的任何反馈或疑问，请联系用户所在国家的国家标准机构。这些机构的完整列表可查阅www.iso.org/members.html和www.iec.ch/national-committees。

如需获取全文，请通过以下方式联系，经我公司确认后，将提供
相关文本信息：

- 通讯地址：浙江省杭州市萧山区盈丰街道左右商务中心 1 幢 2
单元 1201 室

- 联系电话：0571-82751996 82751997

- 官方网址：<http://www.cnesc.com.cn>

- 电子邮箱：cnescrz@163.com