



国际标准

ISO/IEC 27701

信息安全、网络安全与隐私保护——
——隐私信息管理系统
——要求 and 指南

第二版
2025-10

信息安全、网络安全和隐私保护 — 隐私保护管理系统 — 要求和建议



受版权保护的文档

©ISO/IEC 2025

保留所有权利。除非另有规定，或在实施过程中要求，否则未经事先书面许可，不得以任何形式或任何方式（电子或机械）复制或使用本出版物的任何部分，包括复印或在互联网或内联网上发布。可向位于以下地址的ISO或请求者所在国家/地区的ISO成员机构请求许可：

ISO 版权办公室
CP401 • Ch.de Blandonnet
8CH-1214 Vernier, Geneva
电话：+41227490111
电子邮件：
copyright@iso.org 网站：
www.iso.org

瑞士出版

©ISO/IEC 2025-保留所有权利

目录页码

前言 V

简介 vi

1	范围	1
2	规范性引用文件	1
3	术语、定义和缩写	1
4	组织背景	4
4.1	了解组织及其背景	4
4.2	了解相关方的需求和期望	5
4.3	确定隐私信息管理系统的范围	5
4.4	隐私信息管理系统	6
5	领导力	6
5.1	领导力和承诺	6
5.2	隐私政策	6
5.3	角色、责任和权限	7
6	计划	7
6.1	应对风险和机遇的行动	7
6.1.1	一般	7
6.1.2	隐私风险评估	7
6.1.3	隐私风险处理	8
6.2	隐私目标和实现这些目标的计划	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	通讯	10
7.5	记录信息	11
7.5.1	一般	1
7.5.2	创建和更新文档化信息	11
7.5.3	文件化信息的控制	11
8	操作	12
8.1	运营规划和控制	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	管理评审	13
9.3.1	一般	13
9.3.2	管理评审投入	13
9.3.3	管理评审结果	14
10	改进	14
10.1	持续改进	14
10.2	不合格和纠正措施	14
11	关于附件 14 的更多信息	

附件 A（规范性）PIMS 参考控制目标以及 PII 控制者和 PII 处理者的控制。15

附件 B（规范性）PII 控制者和 PII 处理器实施指南 21

附录 C（资料性）映射到 ISO /IEC 2910 51

附录 D（资料性）与一般数据保护条例 53 的映射

附录 E（资料性）与 ISO/IEC 27018 和 ISO/IEC 2915 56 的映射

附录 F（资料性）与 ISO /IEC 27701:201 58 的对应关系

参考书目 64

本次公开认证标准封面及目录，本机构客户及相关单位，获取标准全文方式：联系电话：19012716898，邮箱：
18968044408@163.com