国际标准

ISO/IEC 27701
第二版
2025-10

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

Innovation management system—Requirements

目 次

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hts://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(JTC1)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。

引 言

0.1 概述

几乎所有组织都会处理个人身份信息(PI)。随着组织间协作处理PII 的情形日益增多，所处理PII 的数量与类型也在持续增长。在处理PII过程中保障隐私既是社会需求，也是全球专项法律要求的核心议题。

本文档包含以下映射关系：

——ISO/IEC29100 中定义的隐私框架和原则；

——ISO/IEC27018；

——ISO/IEC29151；

—— 欧盟《通用数据保护条例》。

注：这些映射可根据当地法律要求进行解释。

本文件适用于个人身份信息(PII)控制者 (包括共同控制者)及处理者(包括使用分包处理者的控制者，以及作为处理者分包商的处理者) 。

通过遵守本文件的要求，组织可生成其处理个人身份信息(PII) 方式的证据。此类证据可用于促进与业务伙伴的协议达成，尤其在双方均涉及PII 处理时。这亦有助于维护与其他相关方的关系。采用本文件可为该证据提供独立验证。

0.2 与其他管理体系标准的兼容性

本文件采用ISO 制定的框架，旨在提升其管理体系标准间的协调性。

本文件使组织能够将其隐私信息管理体系(PIMS) 与其他管理体系标准的要求进行协调或整合，特别是与ISO/IEC 27001 中规定的信息安全管理体系相协调。

信息安全、网络安全与隐私保护——隐私信息管理体系——要求与指南

1 范围

本文件规定了建立、实施、维护和持续改进隐私信息管理体系(PIMS) 的要求。

同时提供实施指南以协助落实本文件要求。

本文件适用于对个人身份信息(PII) 处理负有责任和问责的PII控制者和PII处理者。

本文件适用于所有类型和规模的组织，包括公共和私营公司、政府实体和非营利组织。

2 规范性引用

以下文件在本文中被引用，其部分或全部内容构成本文件的要求。对于带日期的引用，仅适用所引用的版本。对于不带日期的引用，适用被引文件的最新版本(包括任何修订)。

ISO/IEC29100, 信息技术——安全技术——隐私框架

3 术语、定义和缩写

为本文件之目的，除另有规定外，采用ISO/IEC 29100所载术语及定义。 ISO 与IEC 在下列网址维护标准化用术语数据库：

—ISO 在线浏览平台：可访问https://www.iso.org/obp

—IEC Electropedia: 访问地址https://www.electropedia.org/

3.1 组织

具有自身职能、责任、权限及关系以实现其目标(3.6)的个人或群体

注1:组织的概念包括但不限于个体经营者、公司、企业、机构、企业、当局、合伙企业、慈善机构或机构，或其部分或组合，无论是否注册 成立，无论公营还是私营。

注2:若该组织隶属于更大实体，则"组织"仅指该实体中属于隐私信息管理体系(3.23)范围的部分。

3.2 相关方

能够影响、受影响或认为自己受某项决定或活动影响的个人或组织(3.1)。

3.3 最高管理层

在最高层级指导和控制组织的人或群体(3.1)

注1:最高管理层有权在组织内部授权并提供资源。

注2:若管理体系(3.4)的范围仅覆盖组织的部分领域，则最高管理层指该部分领域的决策控制者。

3. 4 管理体系

组 织 (3.1)中相互关联或相互作用的要素集合，用于制定政策(3.5)和目标 (3.6),以及实现这些目标的过程(3.8)

注1:管理体系可涉及单一领域或多个领域。

注2:管理体系要素包括组织的结构、角色与职责、规划和运作。

3. 5 政策

组织 (3.1)的意图和方向，由其最高管理层(3.3)正式表达。

3.6 目标

需达成的结果

注1:目标可分为战略目标、战术目标或操作目标。

条目注释2:目标可涉及不同领域(如财务、 健康与安全、环境)。 例如，目标可以是全组织性的，也可以针对特定项目、产品或流程(3.8)。

注3:目标可通过其他形式表达，例如作为预期结果、宗旨、操作标准、隐私目标，或使用其他含义相近的词语(如宗旨、目标或指标)。

注4:在隐私信息管理体系(3.23)的背景下，隐私目标由组织(3.1)设定， 组织(3.1)根据隐私政策(3.5)制定，以实现特定结果。

3.7 风险

不确定性的影响

注1:效应是指与预期值的偏差 - 可能是正向或负向偏差。

注释2:不确定性是指对某事件、其后果或发生概率的信息、理解或认知存在不足的状态，即使这种不足是部分性的。

注3:风险通常通过潜在事件及其后果，或二者的组合来表征。

注4:风险通常通过事件后果(包括环境变化)与发生概率的组合来表述。

通讯地址：四川省成都市成华区东华一路 47 号中国铁建广场 1 栋 25 楼

邮　　编：610051

电　　话：028-62521000

网　　址：https://www.ztccc.cn/

E-mail：ztc62521000@163.com