# 安全技术
# 针对 ISO/IEC 27001 和 ISO/IEC 27002
# 在隐私信息管理的扩展
# 要求和指南

## ISO/IEC 27701：2019
## 发布单位：国际标准化组织

浙江公信认证有限公司

（仅供内部交流使用）

# 目 录


前言 ..... I
引言 ..... II
0.1 总则 ..... II
0.2 与其他管理体系标准的兼容性 ..... II
1 范围 ..... 1
2 规范性引用文件 ..... 1
3 术语，定义和缩写 ..... 1
3.1PII 联合控制者 ..... 1
3.2 隐私信息管理体系 PIMS ..... 2
4 总则 ..... 2
4.1 本标准的结构 ..... 2
4.2 ISO/IEC 27001:2013 要求的应用 ..... 3
4.3 ISO/IEC 27002：2013 指南的应用 ..... 3
4.4 客户 ..... 4
5 与 ISO/IEC 27001 相关的 PIMS 特定要求 ..... 4
5.1 总则 ..... 4
5.2 组织环境 ..... 4
5.2.1 了解组织及其环境 ..... 4
5.2.2 理解相关方的需求和期望 ..... 5
5.2.3 确定信息安全管理体系的范围 ..... 5
5.2.4 信息安全管理体系 ..... 5
5.3 领导 ..... 5
5.3.1 领导和承诺 ..... 5
5.3.2 方针 ..... 6
5.3.3 组织角色，职责和权限 ..... 6
5.4 规划 ..... 6
5.4.1 应对风险和机遇的措施 ..... 6
5.4.2 信息安全目标和实现规划 ..... 7
5.5 支持 ..... 7
5.5.1 资源 ..... 7
5.5.2 能力 ..... 7
5.5.3 意识 ..... 7
5.5.4 沟通 ..... 7
5.5.5 文件记录信息 ..... 7
5.6 运行 ..... 8
5.6.1 运行的规划和控制 ..... 8

5.6.2 信息安全风险评估 ..... 8
5.6.3 信息安全风险处置 ..... 8
5.7 绩效评价 ..... 8
5.7.1 监测，测量，分析和评价 ..... 8
5.7.2 内部审核 ..... 8
5.7.3 管理评审 ..... 8
5.8 改进 ..... 8
5.8.1 不符合和纠正措施 ..... 8
5.8.2 持续改进 ..... 8
6 与ISO/IEC 27002 相关的PIMS 特定指南 ..... 9
6.1 总则 ..... 9
6.2 信息安全策略 ..... 9
6.2.1 信息安全管理指导 ..... 9
6.3 信息安全组织 ..... 10
6.3.1 内部组织 ..... 10
6.3.2 移动设备和远程工作 ..... 11
6.4 人力资源安全 ..... 11
6.4.1 任用前 ..... 11
6.4.2 任用中 ..... 11
6.4.3 任用终止和变更 ..... 12
6.5 资产管理 ..... 12
6.5.1 资产责任 ..... 12
6.5.2 信息分类 ..... 12
6.5.3 介质处理 ..... 13
6.6 访问控制 ..... 14
6.6.1 访问控制的业务要求 ..... 14
6.6.2 用户访问管理 ..... 14
6.6.3 用户责任 ..... 15
6.6.4 系统和应用程序访问控制 ..... 15
6.7 密码 ..... 16
6.7.1 密码控制 ..... 16
6.8 物理和环境安全 ..... 16
6.8.1 安全区域 ..... 16
6.8.2 设备 ..... 17
6.9 运行安全 ..... 18
6.9.1 运行规程和责任 ..... 18
6.9.2 恶意软件防范 ..... 18
6.9.3 备份 ..... 18

6.9.4 日志和监视 ..... 19
6.9.5 运行软件的控制 ..... 20
6.9.6 技术脆弱性管理 ..... 20
6.9.7 信息系统审计的考虑 ..... 20
6.10 通信安全 ..... 21
6.10.1 网络安全管理 ..... 21
6.10.2 信息传输 ..... 21
6.11 系统获取，开发和维护 ..... 22
6.11.1 信息系统的安全要求 ..... 22
6.11.2 开发和支持过程中的安全 ..... 22
6.11.3 测试数据 ..... 24
6.12 供应商关系 ..... 24
6.12.1 供应商关系中的信息安全 ..... 24
6.12.2 供应商服务交付管理 ..... 25
6.13 信息安全事件管理 ..... 25
6.13.1 信息安全事件的管理和改进 ..... 25
6.14 业务连续性管理的信息安全方面 ..... 27
6.14.1 信息安全连续性 ..... 27
6.14.2 冗余 ..... 28
6.15 符合性 ..... 28
6.15.1 遵守法律和合同要求 ..... 28
6.15.2 信息安全评审 ..... 29
7 针对 PII 控制者的附加 ISO/IEC 27002 指南 ..... 29
7.1 总则 ..... 29
7.2 收集和处理的条件 ..... 29
7.2.1 识别并记录目的 ..... 30
7.2.2 确定合法的依据 ..... 30
7.2.3 确定何时以及如何获得同意 ..... 31
7.2.4 获取并记录同意 ..... 31
7.2.5 隐私影响评估 ..... 31
7.2.6 与 PII 处理者的合同 ..... 32
7.2.7PII 联合控制者 ..... 32
7.2.8 与处理 PII 有关的记录 ..... 33
7.3 对 PII 主体的主要义务 ..... 33
7.3.1 确定并履行对 PII 主体的义务 ..... 33
7.3.2 确定 PII 主体的信息 ..... 34
7.3.3 向 PII 主体提供信息 ..... 35
7.3.4 提供修改或撤销同意的机制 ..... 35

7.3.5 提供反对 PII 处理的机制 ..... 35
7.3.6 访问，更正和/或删除 ..... 36
7.3.7 PII 控制者告知第三方的义务 ..... 36
7.3.8 提供 PII 处置的副本 ..... 37
7.3.9 处理请求 ..... 37
7.3.10 自动决策 ..... 37
7.4 默认隐私和设计的隐私 ..... 38
7.4.1 限制收集 ..... 38
7.4.2 限制处理 ..... 38
7.4.3 准确性和质量 ..... 38
7.4.4 PII 最小化目标 ..... 39
7.4.5 PII 在处理结束时去标识化和删除 ..... 39
7.4.6 临时文件 ..... 40
7.4.7 保留 ..... 40
7.4.8 处置 ..... 40
7.4.9 PII 传输控制 ..... 41
7.5 PII 共享，转移和披露 ..... 41
7.5.1 识别司法管辖区之间 PII 传输的基础 ..... 41
7.5.2 PII 可以传输至的国家和国际组织 ..... 41
7.5.3 PII 转移记录 ..... 41
7.5.4 向第三方披露 PII 的记录 ..... 42
8 针对 PII 处理者的附加 ISO/IEC 27002 指南 ..... 42
8.1 总则 ..... 42
8.2 收集和处理的条件 ..... 42
8.2.1 客户协议 ..... 42
8.2.2 组织的目的 ..... 43
8.2.3 营销和广告使用 ..... 43
8.2.4 侵权指令 ..... 43
8.2.5 客户义务 ..... 44
8.2.6 与处理 PII 有关的记录 ..... 44
8.3 对 PII 主体的义务 ..... 44
8.3.1 对 PII 主体的义务 ..... 44
8.4 默认的隐私，设计的隐私 ..... 45
8.4.1 临时文件 ..... 45
8.4.2 回退，传输或处置 PII ..... 45
8.4.3 PII 传输控制 ..... 45
8.5 PII 共享，传输和披露 ..... 46
8.5.1 管辖区之间 PII 传输的基础 ..... 46

8.5.2 PII 可以传输至的国家和国际组织 ..... 46
8.5.3 向第三方披露 PII 的记录 ..... 47
8.5.4 PII 披露请求的通知 ..... 47
8.5.5 具有法律约束力的 PII 披露 ..... 47
8.5.6 处理 PII 分包商的披露 ..... 47
8.5.7 分包商参与处理 PII ..... 48
8.5.8 处理 PII 分包商的变更 ..... 48
附录 A ..... 49
附录 B ..... 52
附录 C ..... 54
附录 D ..... 56
附录 E ..... 62
附录 F ..... 65
参考文献 ..... 67

# 前言

ISO（国际标准化组织）和 IEC（国际电工委员会）是为国际标准化制定专门体制的国际组织。国家机构是 ISO 或 IEC 的成员，他们通过各自的组织建立技术委员会通过处理特定领域的技术活动来参与国际标准的制定。ISO 和 IEC 技术委员会在共同感兴趣的领域合作。其他国际组织、政府和非政府等机构，通过联络 ISO 和 IEC 参与这项工作。

ISO/IEC 导则第 1 部分中描述了用于开发本标准的过程以及进一步维护的过程。特别是，应注意不同类型的 ISO 文档依据不同的批准标准。本国际标准遵照 ISO/IEC 导则第 2 部分的规则起草。（参见 www.iso.org /directives）。

本标准中的某些内容有可能涉及一些专利权问题，这一点应该引起注意。ISO 和 IEC 不负责识别任何这样的专利权问题。在标准制定过程中确定的任何专利权的细节将被列在引言中和/或在收到的 ISO 专利声明中（见 www.iso.org/patents）或收到的 IEC 的专利声明清单中（见 http://patents.iec.ch）。

本标准中使用的任何商标名称是为方便用户而提供的信息，并不构成认可。

有关标准的自愿性的解释，与符合性评估相关的 ISO 特定术语和表达的含义，以及 ISO 在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，请参阅 www.iso.org/iso/foreword.html.

本标准由联合技术委员会 ISO/IEC JTC1（信息技术）分委员会 SC27（安全技术）起草。

有关本标准的任何反馈或问题，请直接与本国家的标准组织联系。有关这些机构的完整列表，请访问：www.iso.org/members.html.

# 引言

## 0.1 总则

几乎每个组织都会处理个人身份信息（PII）。此外，处理的 PII 的数量和种类以及组织需要与其他组织合作处理 PII 的情况均在增加。在处理 PII 的时候，保护隐私是一项社会需求， 也是成为全世界立法和/或法规的主题。

信息安全管理体系（ISMS）ISO/IEC 27001被设计成为容许追加特定领域的要求，而无需开发新的管理体系。ISO 管理体系标准，包括行业特定标准，旨在单独实施或作为综合管理体系实施。

PII 保护的要求和指南取决于组织的背景，特别是所在国的国家有立法和/或法规要求的情况。ISO/ IEC 27001 要求理解并考虑该背景 。本标准包括映射到：

-ISO/IEC 29100 中定义的隐私框架和原则；

-ISO/IEC 27018；

-ISO/IEC 29151；和

-欧盟通用数据保护条例。

但是，这些可能需要解释为考虑到当地立法和/或法规。

本标准可供 PII 控制者（包括 PII 联合控制者）和 PII 处理者（包括使用分包的 PII 处理者和作为分包商处理 PII 的处理者） 使用 。符合本标准要求的组织将生成有关如何处理 PII 的书面证据。这些证据可用于促进与业务伙伴达成的协议，其中 PII 的处理是相互关联的。这也可以帮助与其他利益相关者建立关系。如果需要，可以将本标准与 ISO/IEC 27001 结合使用，对该证据进行独立验证。

本标准最初是作为 ISO/IEC 27552 开发的。

## 0.2 与其他管理体系标准的兼容性

本标准应用ISO 开发的框架，以改善与其管理体系之间的一致性。

本标准使组织能够将其 PIMS 与其他管理体系的要求相协调或整合。

**安全技术 - 针对 ISO/IEC 27001 和 ISO/IEC 27002 在隐私信息管理的扩展 - 要求和指南**

# 1 范围

本标准规定了要求，并以 ISO/IEC 27001 和 ISO/IEC 27002 扩展的形式为建立，实施，维护和持续改进隐私信息管理体系（PIMS）提供了指南，以便在组织环境内实施隐私管理。

本标准规定了与 PIMS 相关的要求，并为 PII 控制者和 PII 处理者提供了 PII 处理的责任提供了问责的指导。

本标准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，它们是在 ISMS 中处理 PII 的 PII 控制者和/或 PII 处理者。

# 2 规范性引用文件

下列文件全部或部分通过引用而成为本标准的条款。凡是注明日期的引用文件，只有指定版本用于本标准。凡是不注明日期的引用文件，其最新版本（包括对其的任何修订）都适用于本标准。

ISO/IEC 27000，信息技术 - 安全技术 - 信息安全管理体系 - 总则和词汇

ISO/IEC 27001:2013，信息技术 - 安全技术 - 信息安全管理体系 - 要求

ISO/IEC 27002:2013，信息技术 - 安全技术 - 信息安全控制实用规则

ISO/IEC 29100，信息技术 - 安全技术 - 隐私框架

# 3 术语，定义和缩写

就本标准而言，ISO/IEC 27000 和 ISO/IEC 29100 中给出的术语和定义同样适用。

ISO/IEC 在以下地址维护用于标准化的术语数据库：

— ISO 在线浏览平台：可从 https://www.iso.org/obp 获得

— IEC Electropedia：可在 http://www.electropedia.org/获得

## 3.1PII 联合控制者

与一个或多个 PII 控制者共同决定处理 PII 的目的和方法的 PII 控制者。

如有需要，请通过如下方式联系本机构索取相关认证依据（标准）全文。

电话：0571-85067843

邮箱：wangxin@gac.org.cn