INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Reference number
ISO/IEC 27701:2019(E)

© ISO/IEC 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **vi**
Introduction ..... **vii**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviations **1**
4 General **2**
4.1 Structure of this document 2
4.2 Application of ISO/IEC 27001:2013 requirements 2
4.3 Application of ISO/IEC 27002:2013 guidelines 3
4.4 Customer 4
5 PIMS-specific requirements related to ISO/IEC 27001 ..... **4**
5.1 General 4
5.2 Context of the organization 4
5.2.1 Understanding the organization and its context 4
5.2.2 Understanding the needs and expectations of interested parties 5
5.2.3 Determining the scope of the information security management system 5
5.2.4 Information security management system 5
5.3 Leadership 5
5.3.1 Leadership and commitment 5
5.3.2 Policy 5
5.3.3 Organizational roles, responsibilities and authorities 5
5.4 Planning 6
5.4.1 Actions to address risks and opportunities 6
5.4.2 Information security objectives and planning to achieve them 7
5.5 Support 7
5.5.1 Resources 7
5.5.2 Competence 7
5.5.3 Awareness 7
5.5.4 Communication 7
5.5.5 Documented information 7
5.6 Operation 7
5.6.1 Operational planning and control 7
5.6.2 Information security risk assessment 7
5.6.3 Information security risk treatment 7
5.7 Performance evaluation 8
5.7.1 Monitoring, measurement, analysis and evaluation 8
5.7.2 Internal audit 8
5.7.3 Management review 8
5.8 Improvement 8
5.8.1 Nonconformity and corrective action 8
5.8.2 Continual improvement 8
6 PIMS-specific guidance related to ISO/IEC 27002 ..... **8**
6.1 General 8
6.2 Information security policies 8
6.2.1 Management direction for information security 8
6.3 Organization of information security 9
6.3.1 Internal organization 9
6.3.2 Mobile devices and teleworking 10
6.4 Human resource security 10
6.4.1 Prior to employment 10
6.4.2 During employment 10
6.4.3 Termination and change of employment 11

© ISO/IEC 2019 – All rights reserved

6.5 Asset management ... 11
6.5.1 Responsibility for assets ... 11
6.5.2 Information classification ... 11
6.5.3 Media handling ... 12
6.6 Access control ... 13
6.6.1 Business requirements of access control ... 13
6.6.2 User access management ... 13
6.6.3 User responsibilities ... 14
6.6.4 System and application access control ... 14
6.7 Cryptography ... 15
6.7.1 Cryptographic controls ... 15
6.8 Physical and environmental security ... 15
6.8.1 Secure areas ... 15
6.8.2 Equipment ... 16
6.9 Operations security ... 17
6.9.1 Operational procedures and responsibilities ... 17
6.9.2 Protection from malware ... 18
6.9.3 Backup ... 18
6.9.4 Logging and monitoring ... 18
6.9.5 Control of operational software ... 19
6.9.6 Technical vulnerability management ... 20
6.9.7 Information systems audit considerations ... 20
6.10 Communications security ... 20
6.10.1 Network security management ... 20
6.10.2 Information transfer ... 20
6.11 Systems acquisition, development and maintenance ... 21
6.11.1 Security requirements of information systems ... 21
6.11.2 Security in development and support processes ... 21
6.11.3 Test data ... 23
6.12 Supplier relationships ... 23
6.12.1 Information security in supplier relationships ... 23
6.12.2 Supplier service delivery management ... 24
6.13 Information security incident management ... 24
6.13.1 Management of information security incidents and improvements ... 24
6.14 Information security aspects of business continuity management ... 27
6.14.1 Information security continuity ... 27
6.14.2 Redundancies ... 27
6.15 Compliance ... 27
6.15.1 Compliance with legal and contractual requirements ... 27
6.15.2 Information security reviews ... 28

7 Additional ISO/IEC 27002 guidance for PII controllers ... 29
7.1 General ... 29
7.2 Conditions for collection and processing ... 29
7.2.1 Identify and document purpose ... 29
7.2.2 Identify lawful basis ... 29
7.2.3 Determine when and how consent is to be obtained ... 30
7.2.4 Obtain and record consent ... 30
7.2.5 Privacy impact assessment ... 31
7.2.6 Contracts with PII processors ... 31
7.2.7 Joint PII controller ... 32
7.2.8 Records related to processing PII ... 32
7.3 Obligations to PII principals ... 33
7.3.1 Determining and fulfilling obligations to PII principals ... 33
7.3.2 Determining information for PII principals ... 33
7.3.3 Providing information to PII principals ... 34
7.3.4 Providing mechanism to modify or withdraw consent ... 34
7.3.5 Providing mechanism to object to PII processing ... 35
7.3.6 Access, correction and/or erasure ... 35

© ISO/IEC 2019 – All rights reserved

7.3.7 PII controllers' obligations to inform third parties 36
7.3.8 Providing copy of PII processed 36
7.3.9 Handling requests 37
7.3.10 Automated decision making 37
7.4 Privacy by design and privacy by default 38
7.4.1 Limit collection 38
7.4.2 Limit processing 38
7.4.3 Accuracy and quality 38
7.4.4 PII minimization objectives 39
7.4.5 PII de-identification and deletion at the end of processing 39
7.4.6 Temporary files 39
7.4.7 Retention 40
7.4.8 Disposal 40
7.4.9 PII transmission controls 40
7.5 PII sharing, transfer, and disclosure 41
7.5.1 Identify basis for PII transfer between jurisdictions 41
7.5.2 Countries and international organizations to which PII can be transferred 41
7.5.3 Records of transfer of PII 41
7.5.4 Records of PII disclosure to third parties 42
8 Additional ISO/IEC 27002 guidance for PII processors 42
8.1 General 42
8.2 Conditions for collection and processing 42
8.2.1 Customer agreement 42
8.2.2 Organization's purposes 43
8.2.3 Marketing and advertising use 43
8.2.4 Infringing instruction 43
8.2.5 Customer obligations 43
8.2.6 Records related to processing PII 44
8.3 Obligations to PII principals 44
8.3.1 Obligations to PII principals 44
8.4 Privacy by design and privacy by default 44
8.4.1 Temporary files 44
8.4.2 Return, transfer or disposal of PII 45
8.4.3 PII transmission controls 45
8.5 PII sharing, transfer, and disclosure 46
8.5.1 Basis for PII transfer between jurisdictions 46
8.5.2 Countries and international organizations to which PII can be transferred 46
8.5.3 Records of PII disclosure to third parties 47
8.5.4 Notification of PII disclosure requests 47
8.5.5 Legally binding PII disclosures 47
8.5.6 Disclosure of subcontractors used to process PII 47
8.5.7 Engagement of a subcontractor to process PII 48
8.5.8 Change of subcontractor to process PII 48
Annex A (normative) **PIMS-specific reference control objectives and controls (PII Controllers) 49**
Annex B (normative) **PIMS-specific reference control objectives and controls (PII Processors) 53**
Annex C (informative) **Mapping to ISO/IEC 29100 ..... 56**
Annex D (informative) **Mapping to the General Data Protection Regulation 58**
Annex E (informative) **Mapping to ISO/IEC 27018 and ISO/IEC 29151 ..... 61**
Annex F (informative) **How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002 ..... 64**
Bibliography 66

© ISO/IEC 2019 – All rights reserved

ISO/IEC 27701
第一版
2019-08

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

Security techniques - Extension to

ISO/IEC 27001 and ISO/IEC 27002 for

privacy information management - Requirements and guidelines



（ISO/IEC 27701:2019）

本文由中交远航认证有限公司翻译内部使用

目录

目录.....I
前言.....VII
引言.....VIII
0.1 总则.....VIII
0.2 与其他管理体系标准的兼容性.....VIII
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.....61
附录 F.....64
参考文献.....66

如需查阅全文，可联系公司获取

联系电话:010-63260528

邮　　箱:isooffer0211@sina.com