ISO/IEC 27701:2019 (E)

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

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms, definitions and abbreviations

4 General

- 4.1 Structure of this document
- 4.2 Application of ISO/IEC 27001:2013 requirements
- 4.3 Application of ISO/IEC 27002:2013 guidelines
- 4.4 Customer

5 PIMS-specific requirements related to ISO/IEC 27001

- 5.1 General
- 5.2 Context of the organization
- 5.2.1 Understanding the organization and its context
- 5.2.2 Understanding the needs and expectations of interested parties
- 5.2.3 Determining the scope of the information security management system
- 5.2.4 Information security management system
- 5.3 Leadership
- 5.3.1 Leadership and commitment
- 5.3.2 Policy
- 5.3.3 Organizational roles, responsibilities and authorities
- 5.4 Planning
- 5.4.1 Actions to address risks and opportunities
- 5.4.1.1 General
- 5.4.1.2 Information security risk assessment
- 5.4.1.3 Information security risk treatment
- 5.4.2 Information security objectives and planning to achieve them
- 5.5 Support
- 5.5.1 Resources
- 5.5.2 Competence
- 5.5.3 Awareness
- 5.5.4 Communication
- 5.5.5 Documented information
- 5.5.5.1 General
- 5.5.5.2 Creating and updating
- 5.5.5.3 Control of documented information
- 5.6 Operation
- 5.6.1 Operational planning and control
- 5.6.2 Information security risk assessment
- 5.6.3 Information security risk treatment
- 5.7 Performance evaluation
- 5.7.1 Monitoring, measurement, analysis and evaluation
- 5.7.2 Internal audit
- 5.7.3 Management review
- 5.8 Improvement
- 5.8.1 Nonconformity and corrective action
- 5.8.2 Continual improvement

6 PIMS-specific guidance related to ISO/IEC 27002
- **6.1 General**
- **6.2 Information security policies**
- **6.2.1 Management direction for information security**
- **6.2.1.1 Policies for information security**
- **6.2.1.2 Review of the policies for information security**
- **6.3 Organization of information security**
- **6.3.1 Internal organization**
- **6.3.1.1 Information security roles and responsibilities**
- **6.3.1.2 Segregation of duties**
- **6.3.1.3 Contact with authorities**
- **6.3.1.4 Contact with special interest groups**
- **6.3.1.5 Information security in project management**
- **6.3.2 Mobile devices and teleworking**
- **6.3.2.1 Mobile device policy**
- **6.3.2.2 Teleworking**
- **6.4 Human resource security**
- **6.4.1 Prior to employment**
- **6.4.1.1 Screening**
- **6.4.1.2 Terms and conditions of employment**
- **6.4.2 During employment**
- **6.4.2.1 Management responsibilities**
- **6.4.2.2 Information security awareness, education and training**
- **6.4.2.3 Disciplinary procedures**
- **6.4.3 Termination and change of employment**
- **6.4.3.1 Termination or change of employment responsibilities**
- **6.5 Asset management**
- **6.5.1 Responsibility for assets**
- **6.5.1.1 Inventory of assets**
- **6.5.1.2 Ownership of assets**
- **6.5.1.3 Acceptable use of assets**
- **6.5.1.4 Return of assets**
- **6.5.2 Information classification**
- **6.5.2.1 Classification of information**
- **6.5.2.2 Labelling of information**
- **6.5.2.3 Handling of assets**
- **6.5.3 Media handling**
- **6.5.3.1 Management of removable media**
- **6.5.3.2 Disposal of media**
- **6.5.3.3 Physical media transfer**
- **6.6 Access control**
- **6.6.1 Business requirements of access control**
- **6.6.1.1 Access control policy**
- **6.6.1.2 Access to networks and network services**
- **6.6.2 User access management**
- **6.6.2.1 User registration and de-registration**
- **6.6.2.2 User access provisioning**
- **6.6.2.3 Management of privileged access rights**
- **6.6.2.4 Management of secret authentication information of users**
- **6.6.2.5 Review of user access rights**
- **6.6.2.6 Removal or adjustment of access rights**
- **6.6.3 User responsibilities**
- **6.6.3.1 Use of secret authentication information**
- **6.6.4 System and application access control**
- **6.6.4.1 Information access restriction**
- **6.6.4.2 Secure log-on procedures**
- **6.6.4.3 Password management system**
- **6.6.4.4 Use of privileged utility programs**
- **6.6.4.5 Access control to program source code**
- **6.7 Cryptography**
- **6.7.1 Cryptographic controls**
- **6.7.1.1 Policy on the use of cryptographic controls**
- **6.7.1.2 Key management**

6.8 Physical and environmental security
6.8.1 Secure areas
6.8.1.1 Physical security perimeter
6.8.1.2 Physical entry controls
6.8.1.3 Securing offices, rooms and facilities
6.8.1.4 Protecting against external and environmental threats
6.8.1.5 Working in secure areas
6.8.1.6 Delivery and loading areas
6.8.2 Equipment
6.8.2.1 Equipment siting and protection
6.8.2.2 Supporting utilities
6.8.2.3 Cabling security
6.8.2.4 Equipment maintenance
6.8.2.5 Removal of assets
6.8.2.6 Security of equipment and assets off-premises
6.8.2.7 Secure disposal or re-use of equipment
6.8.2.8 Unattended user equipment
6.8.2.9 Clear desk and clear screen policy
6.9 Operations security
6.9.1 Operational procedures and responsibilities
6.9.1.1 Documenting operating procedures
6.9.1.2 Change management
6.9.1.3 Capacity management
6.9.1.4 Separation of development, testing and operational environments
6.9.2 Protection from malware
6.9.2.1 Controls against malware
6.9.3 Backup
6.9.3.1 Information backup
6.9.4 Logging and monitoring
6.9.4.1 Event logging
6.9.4.2 Protection of log information
6.9.4.3 Administrator and operator logs
6.9.4.4 Clock synchronization
6.9.5 Control of operational software
6.9.5.1 Installation of software on operational systems
6.9.6 Technical vulnerability management
6.9.6.1 Management of technical vulnerabilities
6.9.6.2 Restriction on software installation
6.9.7 Information systems audit considerations
6.9.7.1 Information systems audit controls
6.10 Communications security
6.10.1 Network security management
6.10.1.1 Network controls
6.10.1.2 Security in network services
6.10.1.3 Segregation in networks
6.10.2 Information transfer
6.10.2.1 Information transfer policies and procedures
6.10.2.2 Agreements for information transfer
6.10.2.3 Electronic messaging
6.10.2.4 Confidentiality or non-disclosure agreements
6.11 Systems acquisition, development and maintenance
6.11.1 Security requirements of information systems
6.11.1.1 Information security requirements analysis and specification
6.11.1.2 Securing application services on public networks
6.11.1.3 Protecting application services transactions
6.11.2 Security in development and support processes
6.11.2.1 Secure development policy
6.11.2.2 System change control procedures
6.11.2.3 Technical review of applications after operating platform changes
6.11.2.4 Restrictions of changes to software packages
6.11.2.5 Secure systems engineering principles
6.11.2.6 Secure development environment
6.11.2.7 Outsourced development
6.11.2.8 System security testing

6.11.2.9 System acceptance testing
6.11.3 Test data
6.11.3.1 Protection of test data
6.12 Supplier relationships
6.12.1 Information security in supplier relationships
6.12.1.1 Information security policy for supplier relationships
6.12.1.2 Addressing security within supplier agreements
6.12.1.3 Information and communication technology supply chain
6.12.2 Supplier service delivery management
6.12.2.1 Monitoring and review of supplier services
6.12.2.2 Managing changes to supplier services
6.13 Information security incident management
6.13.1 Management of information security incidents and improvements
6.13.1.1 Responsibilities and procedures
6.13.1.2 Reporting information security events
6.13.1.3 Reporting information security weaknesses
6.13.1.4 Assessment of and decisions on information security events
6.13.1.5 Response to information security incidents
6.13.1.6 Learning from information security incidents
6.13.1.7 Collection of evidence
6.14 Information security aspects of business continuity management
6.14.1 Information security continuity
6.14.1.1 Planning information security continuity
6.14.1.2 Implementing information security continuity
6.14.1.3 Verify, renew and evaluate information security continuity
6.14.2 Redundancies
6.14.2.1 Availability of information processing facilities
6.15 Compliance
6.15.1 Compliance with legal and contractual requirements
6.15.1.1 Identification of applicable legislation and contractual requirements
6.15.1.2 Intellectual property rights
6.15.1.3 Protection of records
6.15.1.4 Privacy and protection of personally identifiable information
6.15.1.5 Regulation of cryptographic controls
6.15.2 Information security reviews
6.15.2.1 Independent review of information security
6.15.2.2 Compliance with security policies and standards
6.15.2.3 Technical compliance review

7 Additional ISO/IEC 27002 guidance for PII controllers

7.1 General
7.2 Conditions for collection and processing
7.2.1 Identify and document purpose
7.2.2 Identify lawful basis
7.2.3 Determine when and how consent is to be obtained
7.2.4 Obtain and record consent
7.2.5 Privacy impact assessment
7.2.6 Contracts with PII processors
7.2.7 Joint PII controller
7.2.8 Records related to processing PII
7.3 Obligations to PII principals
7.3.1 Determining and fulfilling obligations to PII principals
7.3.2 Determining information for PII principals
7.3.3 Providing information to PII principals
7.3.4 Providing mechanism to modify or withdraw consent
7.3.5 Providing mechanism to object to PII processing
7.3.6 Access, correction and/or erasure
7.3.7 PII controllers' obligations to inform third parties
7.3.8 Providing copy of PII processed
7.3.9 Handling requests
7.3.10 Automated decision making
7.4 Privacy by design and privacy by default
7.4.1 Limit collection
7.4.2 Limit processing

7.4.3 Accuracy and quality
7.4.4 PII minimization objectives
7.4.5 PII de-identification and deletion at the end of processing
7.4.6 Temporary files
7.4.7 Retention
7.4.8 Disposal
7.4.9 PII transmission controls
7.5 PII sharing, transfer, and disclosure
7.5.1 Identify basis for PII transfer between jurisdictions
7.5.2 Countries and international organizations to which PII can be transferred
7.5.3 Records of transfer of PII
7.5.4 Records of PII disclosure to third parties

8 Additional ISO/IEC 27002 guidance for PII processors

8.1 General
8.2 Conditions for collection and processing
8.2.1 Customer agreement
8.2.2 Organization’s purposes
8.2.3 Marketing and advertising use
8.2.4 Infringing instruction
8.2.5 Customer obligations
8.2.6 Records related to processing PII
8.3 Obligations to PII principals
8.3.1 Obligations to PII principals
8.4 Privacy by design and privacy by default
8.4.1 Temporary files
8.4.2 Return, transfer or disposal of PII
8.4.3 PII transmission controls
8.5 PII sharing, transfer, and disclosure
8.5.1 Basis for PII transfer between jurisdictions
8.5.2 Countries and international organizations to which PII can be transferred
8.5.3 Records of PII disclosure to third parties
8.5.4 Notification of PII disclosure requests
8.5.5 Legally binding PII disclosures
8.5.6 Disclosure of subcontractors used to process PII
8.5.7 Engagement of a subcontractor to process PII
8.5.8 Change of subcontractor to process PII

Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers)

Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors)

Annex C (informative) Mapping to ISO/IEC 29100

Annex D (informative) Mapping to the General Data Protection Regulation

Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151

Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

F.1 How to apply this document
F.2 Example of refinement of security standards

Page count: 67