
**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*



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

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

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