

DIN EN ISO/IEC 27701:2021-07 (E)

Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines (ISO/IEC 27701:2019)

Contents		Page
European foreword		6
Foreword		7
Introduction		8
1	Scope	9
2	Normative references	9
3	Terms, definitions and abbreviations	9
4	General	10
4.1	Structure of this document	10
4.2	Application of ISO/IEC 27001:2013 requirements	10
4.3	Application of ISO/IEC 27002:2013 guidelines	11
4.4	Customer	12
5	PIMS-specific requirements related to ISO/IEC 27001	12
5.1	General	12
5.2	Context of the organization	12
5.2.1	Understanding the organization and its context	12
5.2.2	Understanding the needs and expectations of interested parties	13
5.2.3	Determining the scope of the information security management system	13
5.2.4	Information security management system	13
5.3	Leadership	13
5.3.1	Leadership and commitment	13
5.3.2	Policy	13
5.3.3	Organizational roles, responsibilities and authorities	13
5.4	Planning	14
5.4.1	Actions to address risks and opportunities	14
5.4.2	Information security objectives and planning to achieve them	15
5.5	Support	15
5.5.1	Resources	15
5.5.2	Competence	15
5.5.3	Awareness	15
5.5.4	Communication	15
5.5.5	Documented information	15
5.6	Operation	15
5.6.1	Operational planning and control	15
5.6.2	Information security risk assessment	15
5.6.3	Information security risk treatment	15
5.7	Performance evaluation	16
5.7.1	Monitoring, measurement, analysis and evaluation	16
5.7.2	Internal audit	16
5.7.3	Management review	16
5.8	Improvement	16
5.8.1	Nonconformity and corrective action	16
5.8.2	Continual improvement	16
6	PIMS-specific guidance related to ISO/IEC 27002	16

6.1	General	16
6.2	Information security policies	16
6.2.1	Management direction for information security	16
6.3	Organization of information security	17
6.3.1	Internal organization	17
6.3.2	Mobile devices and teleworking	18
6.4	Human resource security	18
6.4.1	Prior to employment	18
6.4.2	During employment	18
6.4.3	Termination and change of employment	19
6.5	Asset management	19
6.5.1	Responsibility for assets	19
6.5.2	Information classification	19
6.5.3	Media handling	20
6.6	Access control	21
6.6.1	Business requirements of access control	21
6.6.2	User access management	21
6.6.3	User responsibilities	22
6.6.4	System and application access control	22
6.7	Cryptography	23
6.7.1	Cryptographic controls	23
6.8	Physical and environmental security	23
6.8.1	Secure areas	23
6.8.2	Equipment	24
6.9	Operations security	25
6.9.1	Operational procedures and responsibilities	25
6.9.2	Protection from malware	26
6.9.3	Backup	26
6.9.4	Logging and monitoring	26
6.9.5	Control of operational software	27
6.9.6	Technical vulnerability management	28
6.9.7	Information systems audit considerations	28
6.10	Communications security	28
6.10.1	Network security management	28
6.10.2	Information transfer	28
6.11	Systems acquisition, development and maintenance	29
6.11.1	Security requirements of information systems	29
6.11.2	Security in development and support processes	29
6.11.3	Test data	31
6.12	Supplier relationships	31
6.12.1	Information security in supplier relationships	31
6.12.2	Supplier service delivery management	32
6.13	Information security incident management	32
6.13.1	Management of information security incidents and improvements	32
6.14	Information security aspects of business continuity management	35
6.14.1	Information security continuity	35
6.14.2	Redundancies	35
6.15	Compliance	35
6.15.1	Compliance with legal and contractual requirements	35
6.15.2	Information security reviews	36
7	Additional ISO/IEC 27002 guidance for PII controllers	37
7.1	General	37
7.2	Conditions for collection and processing	37
7.2.1	Identify and document purpose	37
7.2.2	Identify lawful basis	37
7.2.3	Determine when and how consent is to be obtained	38
7.2.4	Obtain and record consent	39
7.2.5	Privacy impact assessment	39
7.2.6	Contracts with PII processors	39
7.2.7	Joint PII controller	40
7.2.8	Records related to processing PII	40
7.3	Obligations to PII principals	41

7.3.1	Determining and fulfilling obligations to PII principals	41
7.3.2	Determining information for PII principals	41
7.3.3	Providing information to PII principals	42
7.3.4	Providing mechanism to modify or withdraw consent	42
7.3.5	Providing mechanism to object to PII processing	43
7.3.6	Access, correction and/or erasure	43
7.3.7	PII controllers' obligations to inform third parties	44
7.3.8	Providing copy of PII processed	44
7.3.9	Handling requests	45
7.3.10	Automated decision making	45
7.4	Privacy by design and privacy by default	45
7.4.1	Limit collection	46
7.4.2	Limit processing	46
7.4.3	Accuracy and quality	46
7.4.4	PII minimization objectives	47
7.4.5	PII de-identification and deletion at the end of processing	47
7.4.6	Temporary files	47
7.4.7	Retention	48
7.4.8	Disposal	48
7.4.9	PII transmission controls	48
7.5	PII sharing, transfer, and disclosure	49
7.5.1	Identify basis for PII transfer between jurisdictions	49
7.5.2	Countries and international organizations to which PII can be transferred	49
7.5.3	Records of transfer of PII	49
7.5.4	Records of PII disclosure to third parties	50
8	Additional ISO/IEC 27002 guidance for PII processors	50
8.1	General	50
8.2	Conditions for collection and processing	50
8.2.1	Customer agreement	50
8.2.2	Organization's purposes	51
8.2.3	Marketing and advertising use	51
8.2.4	Infringing instruction	51
8.2.5	Customer obligations	51
8.2.6	Records related to processing PII	52
8.3	Obligations to PII principals	52
8.3.1	Obligations to PII principals	52
8.4	Privacy by design and privacy by default	52
8.4.1	Temporary files	53
8.4.2	Return, transfer or disposal of PII	53
8.4.3	PII transmission controls	53
8.5	PII sharing, transfer, and disclosure	54
8.5.1	Basis for PII transfer between jurisdictions	54
8.5.2	Countries and international organizations to which PII can be transferred	54
8.5.3	Records of PII disclosure to third parties	55
8.5.4	Notification of PII disclosure requests	55
8.5.5	Legally binding PII disclosures	55
8.5.6	Disclosure of subcontractors used to process PII	55
8.5.7	Engagement of a subcontractor to process PII	56
8.5.8	Change of subcontractor to process PII	56
Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers)		57
Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors)		61
Annex C (informative) Mapping to ISO/IEC 29100		64
Annex D (informative) Mapping to the General Data Protection Regulation		66
Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151		69
Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002		72
Bibliography		74