ISO/IEC 27701:2019 (E)

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

Contents

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

Page count: 67