SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
5	**Organizational Controls**		**Applicable**	**Implemented**	**Reason Applicable: IRA**	**Reason Applicable: law/contract and regulations**	**Reason of exlution**
5.1	Policies for information security	**Control:** Information security policy and topic-specific policies shall be de fined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes	Yes	integrated risk analysis	N/A	N/A
5.2	Information security roles and responsibilities	**Control:** Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes	Yes	integrated risk analysis	N/A	N/A
5.3	Segregation of duties	**Control:** Conflicting duties and conflicting areas of responsibility shall be seg regated.	Yes	Yes	integrated risk analysis	N/A	N/A
5.4	Management responsibilities	**Control:** Management shall require all personnel to apply information security in accordance with the established information security policy, top ic-specific policies and procedures of the organization.	Yes	Yes	integrated risk analysis	N/A	N/A
5.5	Contact with authorities	**Control:** The organization shall establish and maintain contact with relevant authorities.	Yes	Yes	integrated risk analysis	N/A	N/A
5.6	Contact with special interest groups	**Control:** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	Yes	integrated risk analysis	N/A	N/A
5.7	Threat intelligence	**Control:** Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes	Yes	integrated risk analysis	N/A	N/A
5.8	Information security in project management	**Control:** Information security shall be integrated into project management.	Yes	Yes	integrated risk analysis	N/A	N/A
5.9	Inventory of information and other associated assets	**Control:** An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes	Yes	integrated risk analysis	N/A	N/A
5.10	Acceptable use of information and other associated assets	**Control:** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Yes	Yes	integrated risk analysis	N/A	N/A
5.11	Return of assets	**Control:** Personnel and other interested parties as appropriate shall return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement.	Yes	Yes	integrated risk analysis	N/A	N/A

SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
5.12	Classification of information	**Control:** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Yes	Yes	integrated risk analysis	N/A	N/A
5.13	Labelling of information	**Control:** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information clas sification scheme adopted by the organization.	Yes	Yes	integrated risk analysis	N/A	N/A
5.14	Information transfer	**Control:** Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes	Yes	integrated risk analysis	N/A	N/A
5.15	Access Control:	**Control:** Rules to Control: physical and logical access to information and other associated assets shall be established and implemented based on busi ness and information security requirements.	Yes	Yes	integrated risk analysis	N/A	N/A
5.16	Identity management	**Control:** The full life cycle of identities shall be managed.	Yes	Yes	integrated risk analysis	N/A	N/A
5.17	Authentication information	**Control:** Allocation and management of authentication information shall be Control:led by a management process, including advising personnel on appropriate handling of authentication information.	Yes	Yes	integrated risk analysis	N/A	N/A
5.18	Access rights	**Control:** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access Control:.	Yes	Yes	integrated risk analysis	N/A	N/A
5.19	Information security in supplier relationships	**Control:** Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier’s products or services.	Yes	Yes	integrated risk analysis	N/A	N/A
5.20	Addressing information security within supplier agreements	**Control:** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Yes	Yes	integrated risk analysis	N/A	N/A
5.21	Managing information security in the information and commu nication technology (ICT) supply chain	**Control:** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	Yes	integrated risk analysis	N/A	N/A

SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
5.22	Monitoring, review and change management of supplier services	**Control:** The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	Yes	integrated risk analysis	N/A	N/A
5.23	Information security for use of cloud services	**Control:** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Yes	Yes	integrated risk analysis	N/A	N/A
5.24	Information security incident management planning and prepa ration	**Control:** The organization shall plan and prepare for managing information secu rity incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes	Yes	integrated risk analysis	N/A	N/A
5.25	Assessment and decision on in formation security events	**Control:** The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Yes	Yes	integrated risk analysis	N/A	N/A
5.26	Response to information security incidents	**Control:** Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Yes	integrated risk analysis	N/A	N/A
5.27	Learning from information se curity incidents	**Control:** Knowledge gained from information security incidents shall be used to strengthen and improve the information security Control:s.	Yes	Yes	integrated risk analysis	N/A	N/A
5.28	Collection of evidence	**Control:** The organization shall establish and implement procedures for the iden tification, collection, acquisition and preservation of evidence related to information security events.	Yes	Yes	integrated risk analysis	N/A	N/A
5.29	Information security during disruption	**Control:** The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes	Yes	integrated risk analysis	N/A	N/A
5.30	ICT readiness for business con tinuity	**Control:** ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	Yes	integrated risk analysis	N/A	N/A
5.31	Legal, statutory, regulatory and contractual requirements	**Control:** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes	Yes	integrated risk analysis	N/A	N/A
5.32	Intellectual property rights	**Control:** The organization shall implement appropriate procedures to protect intellectual property rights.	Yes	Yes	integrated risk analysis	N/A	N/A

SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
5.33	Protection of records	**Control:** Records shall be protected from loss, destruction, falsification, unau thorized access and unauthorized release.	Yes	Yes	integrated risk analysis	N/A	N/A
5.34	Privacy and protection of person al identifiable information (PII)	**Control:** The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	Yes	integrated risk analysis	Law and regulations	N/A
5.35	Independent review of informa tion security	**Control:** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Yes	Yes	integrated risk analysis	N/A	N/A
5.36	Compliance with policies, rules and standards for information security	**Control:** Compliance with the organization's information security policy, top ic-specific policies, rules and standards shall be regularly reviewed.	Yes	Yes	integrated risk analysis	N/A	N/A
5.37	Documented operating proce dures	**Control:** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes	Yes	integrated risk analysis	N/A	N/A
6	**People Control:s**		**Applicable**	**Implemented**	**Reason Applicable: IRA**	**Reason Applicable: law/contract and regulations**	**Reason of exlution**
6.1	Screening	**Control:** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Partially	Partially	integrated risk analysis	Law and regulations	Therapieland has identified no risk in not repeating the screening. The following part of the control is therefore deemed not applicable: 'and on an ongoing basis'.
6.2	Terms and conditions of em ployment	**Control:** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes	Yes	integrated risk analysis	N/A	N/A
6.3	Information security awareness, education and training	**Control:** Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Yes	Yes	integrated risk analysis	N/A	N/A
6.4	Disciplinary process	**Control:** A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes	Yes	integrated risk analysis	N/A	N/A

SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
6.5	Responsibilities after termination or change of employment	**Control:** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Yes	Yes	integrated risk analysis	N/A	N/A
6.6	Confidentiality or non-disclosure agreements	**Control:** Confidentiality or non-disclosure agreements reflecting the organ ization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	Yes	integrated risk analysis	N/A	N/A
6.7	Remote working	**Control:** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes	Yes	integrated risk analysis	N/A	N/A
6.8	Information security event re porting	**Control:** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	Yes	integrated risk analysis	N/A	N/A
7	**Physical Control:s**		**Applicable**	**Implemented**	**Reason Applicable: IRA**	**Reason Applicable: law/contract and regulations**	**Reason of exlution**
7.1	Physical security perimeters	**Control:** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Yes	Yes	integrated risk analysis	N/A	N/A
7.2	Physical entry	**Control:** Secure areas shall be protected by appropriate entry Control:s and access points.	Yes	Yes	integrated risk analysis	N/A	N/A
7.3	Securing offices, rooms and fa cilities	**Control:** Physical security for offices, rooms and facilities shall be designed and implemented.	Yes	Yes	integrated risk analysis	N/A	N/A
7.4	Physical security monitoring	**Control:** Premises shall be continuously monitored for unauthorized physical access.	No	No	N/A	N/A	Therapieland's office premises contain no business or client data and no storage media. All data and systems are hosted in the data center, which is managed by the supplier under an outsourced service. On this basis, this control is excluded
7.5	Protecting against physical and environmental threats	**Control:** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Yes	Yes	integrated risk analysis	N/A	N/A
7.6	Working in secure areas	**Control:** Security measures for working in secure areas shall be designed and implemented.	Yes	Yes	integrated risk analysis	N/A	N/A

SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
7.7	Clear desk and clear screen	**Control:** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Yes	Yes	integrated risk analysis	N/A	N/A
7.8	Equipment siting and protection	**Control:** Equipment shall be sited securely and protected.	Yes	Yes	integrated risk analysis	N/A	N/A
7.9	Security of assets off-premises	**Control:** Off-site assets shall be protected.	Yes	Yes	integrated risk analysis	N/A	N/A
7.10	Storage media	**Control:** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	Yes	integrated risk analysis	N/A	N/A
7.11	Supporting utilities	**Control:** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Yes	integrated risk analysis	N/A	N/A
7.12	Cabling security	**Control:** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Yes	Yes	integrated risk analysis	N/A	N/A
7.13	Equipment maintenance	**Control:** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	Yes	integrated risk analysis	N/A	N/A
7.14	Secure disposal or re-use of equipment	**Control:** Items of equipment containing storage media shall be verified to en sure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	Yes	integrated risk analysis	N/A	N/A
8	**Technological Control:**		**Applicable**	**Implemented**	**Reason Applicable: IRA**	**Reason Applicable: law/contract and regulations**	**Reason of exlution**
8.1	User end point devices	**Control:** Information stored on, processed by or accessible via user end point devices shall be protected.	Yes	Yes	integrated risk analysis	N/A	N/A
8.2	Privileged access rights	**Control:** The allocation and use of privileged access rights shall be restricted and managed.	Yes	Yes	integrated risk analysis	N/A	N/A
8.3	Information access restriction	**Control:** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access Control:.	Yes	Yes	integrated risk analysis	N/A	N/A
8.4	Access to source code	**Control:** Read and write access to source code, development tools and software libraries shall be appropriately managed.	Yes	Yes	integrated risk analysis	N/A	N/A

SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
8.5	Secure authentication	**Control:** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access Control:.	Yes	Yes	integrated risk analysis	N/A	N/A
8.6	Capacity management	**Control:** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes	Yes	integrated risk analysis	N/A	N/A
8.7	Protection against malware	**Control:** Protection against malware shall be implemented and supported by appropriate user awareness.	Yes	Yes	integrated risk analysis	N/A	N/A
8.8	Management of technical vul nerabilities	**Control:** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Yes	Yes	integrated risk analysis	N/A	N/A
8.9	Configuration management	**Control:** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes	Yes	integrated risk analysis	N/A	N/A
8.10	Information deletion	**Control:** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Yes	Yes	integrated risk analysis	N/A	N/A
8.11	Data masking	**Control:** Data masking shall be used in accordance with the organization's topic-specific policy on access Control: and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes	Yes	integrated risk analysis	N/A	N/A
8.12	Data leakage prevention	**Control:** Data leakage prevention measures shall be applied to systems, net works and any other devices that process, store or transmit sensitive information.	Yes	Yes	integrated risk analysis	N/A	N/A
8.13	Information backup	**Control:** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	Yes	integrated risk analysis	N/A	N/A
8.14	Redundancy of information pro cessing facilities	**Control:** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Yes	integrated risk analysis	N/A	N/A
8.15	Logging	**Control:** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Yes	Yes	integrated risk analysis	N/A	N/A

SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
8.16	Monitoring activities	**Control:** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential infor mation security incidents.	Yes	Yes	integrated risk analysis	N/A	N/A
8.17	Clock synchronization	**Control:** The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes	Yes	integrated risk analysis	N/A	N/A
8.18	Use of privileged utility programs	**Control:** The use of utility programs that can be capable of overriding system and application Control:s shall be restricted and tightly Control:led.	Yes	Yes	integrated risk analysis	N/A	N/A
8.19	Installation of software on op erational systems	**Control:** Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes	Yes	integrated risk analysis	N/A	N/A
8.20	Networks security	**Control:** Networks and network devices shall be secured, managed and Control:led to protect information in systems and applications.	Yes	Yes	integrated risk analysis	N/A	N/A
8.21	Security of network services	**Control:** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Yes	Yes	integrated risk analysis	N/A	N/A
8.22	Segregation of networks	**Control:** Groups of information services, users and information systems shall be segregated in the organization’s networks.	Yes	Yes	integrated risk analysis	N/A	N/A
8.23	Web filtering	**Control:** Access to external websites shall be managed to reduce exposure to malicious content.	No	No	N/A	N/A	Therapieland does not apply web filtering. The risk of accessing malicious websites is mitigated through other means: employees are made aware of the associated risks via the staff regulations (personeelsreglement), and endpoint protection is implemented as a technical control against malware and other threats arising from internet use.
8.24	Use of cryptography	**Control**: Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Yes	Yes	integrated risk analysis	N/A	N/A
8.25	Secure development life cycle	**Control:** Rules for the secure development of software and systems shall be established and applied.	Yes	Yes	integrated risk analysis	N/A	N/A
8.26	Application security require ments	**Control:** Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Yes	Yes	integrated risk analysis	N/A	N/A

SoA ISO 27001: 2023 Organisation: Therapieland B.V. Name: K. Klijn. Date: 9 september 2026 version 1.0 [1]							
8.27	Secure system architecture and engineering principles	**Control:** Principles for engineering secure systems shall be established, docu mented, maintained and applied to any information system development activities.	Yes	Yes	integrated risk analysis	N/A	N/A
8.28	Secure coding	**Control:** Secure coding principles shall be applied to software development.	Yes	Yes	integrated risk analysis	N/A	N/A
8.29	Security testing in development and acceptance	**Control:** Security testing processes shall be defined and implemented in the development life cycle.	Yes	Yes	integrated risk analysis	N/A	N/A
8.30	Outsourced development	**Control:** The organization shall direct, monitor and review the activities related to outsourced system development.	No	No	N/A	N/A	Therapieland does not outsource software development to third parties; software development is carried out internally. This control is therefore not applicable.
8.31	Separation of development, test and production environments	**Control:** Development, testing and production environments shall be separated and secured.	Yes	Yes	integrated risk analysis	N/A	N/A
8.32	Change management	**Control:** Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes	Yes	integrated risk analysis	N/A	N/A
8.33	Test information	**Control:** Test information shall be appropriately selected, protected and managed.	Yes	Yes	integrated risk analysis	N/A	N/A
8.34	Protection of information systems during audit testing	**Control:** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Yes	Yes	integrated risk analysis	N/A	N/A

[1] Verklaring van Toepasselijkheid