Statement of Applicability Relatics B.V.

Ridderpoort 32
2984 BG Ridderkerk
Scope: Development, hosting and support of the Relatics software.

C-ID	Source	Name	Description	Applicable	Justification	Risks	Goals	Requirements	Implemented?
A.05.01	ISO27001:2022	Policies for information security	Information security policy and topic-specific policies shall be defined, 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	Risk mitigation and achievement of goals	04.02; 06.01; 06.02	2		Yes
A.05.02	ISO27001:2022	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	yes	Risk mitigation and achievement of goals	06.02	2		Yes
A.05.03	ISO27001:2022	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	yes	Risk mitigation	06.02			Yes
A.05.04	ISO27001:2022	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	yes	Risk mitigation	06.02			Yes
A.05.05	ISO27001:2022	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	yes	Risk mitigation and meeting external requirements	06.02; 06.07			Yes
A.05.06	ISO27001:2022	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	yes	Risk mitigation	02.01; 02.10			Yes
A.05.07	ISO27001:2022	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	yes	Risk mitigation	02.01; 03.02; 06.07			Yes
A.05.08	ISO27001:2022	Information security in project management	Information security shall be integrated into project management.	yes	Risk mitigation	06.03			Yes
A.05.09	ISO27001:2022	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	yes	Risk mitigation	01.01; 01.04; 06.09			Yes
A.05.10	ISO27001:2022	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	yes	Risk mitigation	01.02; 01.06			Yes
A.05.11	ISO27001:2022	Return of assets	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	Risk mitigation	01.04			Yes
A.05.12	ISO27001:2022	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	yes	Risk mitigation	06.09; 06.10			Yes
A.05.13	ISO27001:2022	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	yes	Risk mitigation	01.03; 06.09; 06.10			Yes
A.05.14	ISO27001:2022	Information transfer	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	Risk mitigation	03.01; 04.05			Yes
A.05.15	ISO27001:2022	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	yes	Risk mitigation	02.02; 02.04; 02.05; 05.02; 06.13			Yes
A.05.16	ISO27001:2022	Identity management	The full life cycle of identities shall be managed.	yes	Risk mitigation	06.11			Yes
A.05.17	ISO27001:2022	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	yes	Risk mitigation	06.12			Yes
A.05.18	ISO27001:2022	Access rights	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	Risk mitigation	02.04; 02.05; 04.03; 06.11; 06.13			Yes
A.05.19	ISO27001:2022	Information security in supplier relationships	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	Risk mitigation and meeting external requirements	06.06; 06.16; 06.17		EW.05	Yes
A.05.20	ISO27001:2022	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	yes	Risk mitigation and meeting external requirements	06.06; 06.16; 06.17		EW.05	Yes
A.05.21	ISO27001:2022	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	yes	Risk mitigation	06.16; 06.17			Yes
A.05.22	ISO27001:2022	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	Risk mitigation	06.06; 06.16; 06.17			Yes

A.05.23	ISO27001:2022	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	yes	Risk mitigation and meeting external requirements	02.01; 02.04; 02.05; 06.16; 06.17		EK.02	Yes
A.05.24	ISO27001:2022	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	yes	Risk mitigation	06.07			Yes
A.05.25	ISO27001:2022	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	yes	Risk mitigation	02.09; 06.07			Yes
A.05.26	ISO27001:2022	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	yes	Risk mitigation	06.07			Yes
A.05.27	ISO27001:2022	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	yes	Risk mitigation	6.07			Yes
A.05.28	ISO27001:2022	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	yes	Risk mitigation	06.18			Yes
A.05.29	ISO27001:2022	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	yes	Risk mitigation and meeting external requirements	06.08		EW.05	Yes
A.05.30	ISO27001:2022	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	yes	Risk mitigation and meeting external requirements	06.08		EW.05	Yes
A.05.31	ISO27001:2022	Legal, statutory, regulatory and contractual requirements	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	Risk mitigation and meeting external requirements	06.05; 06.06		EW.01; EW.02; EW.03; EW.04; EW.05	Yes
A.05.32	ISO27001:2022	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	yes	Risk mitigation	06.05			Yes
A.05.33	ISO27001:2022	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	yes	Risk mitigation and meeting external requirements	01.08; 06.05		EW.02	Yes
A.05.34	ISO27001:2022	Privacy and protection of personal identifiable information (PII)	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	Risk mitigation and meeting external requirements	06.04; 06.05		EW.01	Yes
A.05.35	ISO27001:2022	Independent review of information security	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	Risk mitigation and achievement of goals	06.04	1		Yes
A.05.36	ISO27001:2022	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	yes	Risk mitigation and achievement of goals	06.01; 06.04	1		Yes
A.05.37	ISO27001:2022	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	yes	Risk mitigation	02.01; 02.03			Yes
A.06.01	ISO27001:2022	Screening	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.	yes	Risk mitigation and meeting external requirements	04.04; 04.06; 06.05		EK.01	Yes
A.06.02	ISO27001:2022	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	yes	Risk mitigation	04.06; 04.07			Yes
A.06.03	ISO27001:2022	Information security awareness, education and training	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	Risk mitigation and achievement of goals	04.01; 04.02; 04.05; 06.03	3		Yes
A.06.04	ISO27001:2022	Disciplinary process	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	Risk mitigation	04.04; 04.06; 04.07; 06.06			Yes
A.06.05	ISO27001:2022	Responsibilities after termination or change of employment	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	Risk mitigation	04.06; 06.13			Yes
A.06.06	ISO27001:2022	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	yes	Risk mitigation	04.06; 04.07			Yes
A.06.07	ISO27001:2022	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	yes	Risk mitigation	01.02; 03.01			Yes

A.06.08	ISO27001:2022	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	yes	Risk mitigation and meeting external requirements	06.07		EW.05	Yes
A.07.01	ISO27001:2022	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	yes	Risk mitigation	05.01; 05.02			Yes
A.07.02	ISO27001:2022	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	yes	Risk mitigation	05.01; 05.02			Yes
A.07.03	ISO27001:2022	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	yes	Risk mitigation	01.03; 05.01; 05.02			Yes
A.07.04	ISO27001:2022	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	yes	Risk mitigation	01.03; 05.01; 05.02			Yes
A.07.05	ISO27001:2022	Protecting against physical and environmental threats	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	Risk mitigation	01.05; 01.06; 05.02			Yes
A.07.06	ISO27001:2022	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	yes	Risk mitigation	01.03; 05.02			Yes
A.07.07	ISO27001:2022	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	yes	Risk mitigation	01.02; 01.03; 05.01			Yes
A.07.08	ISO27001:2022	Equipment siting and protection	Equipment shall be sited securely and protected.	yes	Risk mitigation	01.07; 05.01; 05.02			Yes
A.07.09	ISO27001:2022	Security of assets off-premises	Off-site assets shall be protected.	yes	Risk mitigation	01.01; 01.02			Yes
A.07.10	ISO27001:2022	Storage media	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	Risk mitigation	01.04			Yes
A.07.11	ISO27001:2022	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	yes	Risk mitigation	05.02			Yes
A.07.12	ISO27001:2022	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	yes	Risk mitigation	05.02			Yes
A.07.13	ISO27001:2022	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	yes	Risk mitigation	01.07			Yes
A.07.14	ISO27001:2022	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	yes	Risk mitigation	01.04			Yes
A.08.01	ISO27001:2022	User end point devices	Information stored on, processed by or accessible via user endpoint devices shall be protected.	yes	Risk mitigation	01.01; 02.07; 03.02			Yes
A.08.02	ISO27001:2022	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	yes	Risk mitigation	04.03; 06.13; 06.14			Yes
A.08.03	ISO27001:2022	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	yes	Risk mitigation	01.02; 01.03; 02.02; 04.03			Yes
A.08.04	ISO27001:2022	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	yes	Risk mitigation	06.13			Yes
A.08.05	ISO27001:2022	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	yes	Risk mitigation	06.12			Yes
A.08.06	ISO27001:2022	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	yes	Risk mitigation	01.08			Yes
A.08.07	ISO27001:2022	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	yes	Risk mitigation	02.07			Yes
A.08.08	ISO27001:2022	Management of technical vulnerabilities	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	Risk mitigation	02.06; 02.07; 02.10			Yes
A.08.09	ISO27001:2022	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	yes	Risk mitigation	02.01; 02.06; 03.02			Yes
A.08.10	ISO27001:2022	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	yes	Risk mitigation and meeting external requirements	06.05		EW.05	Yes
A.08.11	ISO27001:2022	Data masking	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	Risk mitigation	02.04; 02.05; 06.05			Yes
A.08.12	ISO27001:2022	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	yes	Risk mitigation	04.05; 04.06; 06.10			Yes

A.08.13	ISO27001:2022	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	yes	Risk mitigation	01.01; 02.08; 04.03; 04.04			Yes
A.08.14	ISO27001:2022	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	yes	Risk mitigation	01.07; 01.08			Yes
A.08.15	ISO27001:2022	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	yes	Risk mitigation	03.02; 04.03; 04.04; 06.07; 06.18			Yes
A.08.16	ISO27001:2022	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	yes	Risk mitigation	04.04; 06.07; 06.14			Yes
A.08.17	ISO27001:2022	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	yes	Risk mitigation	06.18			Yes
A.08.18	ISO27001:2022	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	yes	Risk mitigation	02.02			Yes
A.08.19	ISO27001:2022	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	yes	Risk mitigation	02.03; 02.06			Yes
A.08.20	ISO27001:2022	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	yes	Risk mitigation	03.02			Yes
A.08.21	ISO27001:2022	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	yes	Risk mitigation	03.02			Yes
A.08.22	ISO27001:2022	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization’s networks.	yes	Risk mitigation	03.01			Yes
A.08.23	ISO27001:2022	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	yes	Risk mitigation	02.07			Yes
A.08.24	ISO27001:2022	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	yes	Risk mitigation	02.04; 02.05; 03.01			Yes
A.08.25	ISO27001:2022	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	yes	Risk mitigation	02.06; 02.08; 02.10			Yes
A.08.26	ISO27001:2022	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	yes	Risk mitigation	02.08; 02.09; 02.10			Yes
A.08.27	ISO27001:2022	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	yes	Risk mitigation	02.08; 02.09; 02.10			Yes
A.08.28	ISO27001:2022	Secure coding	Secure coding principles shall be applied to software development.	yes	Risk mitigation	02.08; 02.09; 02.10			Yes
A.08.29	ISO27001:2022	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	yes	Risk mitigation	02.10			Yes
A.08.30	ISO27001:2022	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	N/A	There is no outsourced software development within Relatics	N/A	N/A	N/A	N/A
A.08.31	ISO27001:2022	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	yes	Risk mitigation	02.03			Yes
A.08.32	ISO27001:2022	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	yes	Risk mitigation	02.03			Yes
A.08.33	ISO27001:2022	Test information	Test information shall be appropriately selected, protected and managed.	yes	Risk mitigation	02.05			Yes
A.08.34	ISO27001:2022	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	yes	Risk mitigation	06.15			Yes

Version	Date	Name	Change	Approved by
1.0	11/13/2023	I. Kroeze	First version	I. Vollebregt
1.1	11/30/2023	I. Kroeze	Change in requirements	
1.2	18/11/2025	I. Kroeze	Update + addition of scope	