# Tilaa B.V. ISO 27001:2022 Statement of Applicability

### Document status

| | |
|---|---|
| **Owner** | Security officer |
| **Classification** | C-4 Public |
| **Status** | Approved |
| **Approved on** | Nov 17, 2025 |
| **Approved by** | Pieter Krul |

| | |
|---|---|
| **Organization** | Tilaa B.V. |
| **Date** | Nov 17, 2025 |
| **Control set(s)** | • ISO/IEC 27001:2022 |

### ISO/IEC 27001:2022

| Control | Requirement | Applicable | Reason | Status |
|---|---|---|---|---|
| A.5.1 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 assessment | Implemented |
| A.5.2 Information security roles and responsibilities | Information security roles and responsibilities shall be defined and allocated according to the organization needs. | YES | Roles and responsibilities | Implemented |
| A.5.3 Segregation of duties | Conflicting duties and areas of responsibility shall be segregated. | YES | Risk assessment<br>Roles & responsibilities | Implemented |
| A.5.4 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 assessment<br>Objectives<br>Continuous Improvement | Implemented |
| A.5.5 Contact with authorities | The organization shall establish and maintain contact with relevant authorities. | YES | Best practice | Implemented |
| A.5.6 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 assessment<br>Legislation | Implemented |
| A.5.7 Threat intelligence | Information relating to information security threats shall be collected and analysed to produce threat intelligence. | YES | Risk assessment<br>Continuous Improvement | Implemented |
| A.5.8 Information security in project management | Information security shall be integrated into project management. | YES | Risk assessment<br>Best Practice | Implemented |
| A.5.9 Inventory of information and other associated assets | An inventory of information and other associated assets, including owners, shall be developed and maintained. | YES | Risk assessment | Implemented |
| A.5.10 Acceptable use of information and other associated assets | Rules for the acceptable use and procedures for the handling of information and other associated assets shall be identified, documented and implemented. | YES | Risk assessment<br>Best Practice | Implemented |

| | | | | |
|---|---|---|---|---|
| A.5.11 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 assessment<br>Asset management | Implemented |
| A.5.12 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 assessment | Implemented |
| A.5.13 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 assessment<br>Asset Management | Implemented |
| A.5.14 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 assessment<br>Communication | Implemented |
| A.5.15 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 assessment<br>Roles and responsibilities | Implemented |
| A.5.16 Identity management | The full life cycle of identities shall be managed. | YES | Risk assessment | Implemented |
| A.5.17 Authentication information | Allocation and management of authentication information shall be controlled by a management process, including advising personnel of appropriate handling of authentication information. | YES | Risk assessment | Implemented |
| A.5.18 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 assessment | Implemented |
| A.5.19 Information | Processes and procedures shall be | YES | Risk assessment | Implemented |

| | | | | |
|---|---|---|---|---|
| security in supplier relationships | defined and implemented to manage the information security risks associated with the use of supplier’s products or services. | | Supplier policy | |
| A.5.20 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 assessment<br>Supplier policy | Implemented |
| A.5.21 Managing information security in the ICT supply chain | Processes and procedures shall be defined and implemented to manage information security risks associated with the ICT products and services supply chain. | YES | Risk assessment<br>Supplier policy | Implemented |
| A.5.22 Monitoring, review and change management of supplier services | The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. | YES | Risk assessment<br>Supplier policy | Implemented |
| A.5.23 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 assessment | Implemented |
| A.5.24 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 assessment<br>Incident management | Implemented |
| A.5.25 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 assessment<br>Incident management | Implemented |
| A.5.26 Response to information security incidents | Information security incidents shall be responded to in accordance with the documented procedures. | YES | Risk assessment<br>Incident management | Implemented |
| A.5.27 Learning from information security incidents | Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. | YES | Risk assessment<br>Incident management | Implemented |
| A.5.28 Collection of evidence | The organization shall establish and implement procedures for the identification, collection, acquisition | YES | Risk assessment<br>Continuous improvement | Implemented |

| | | | | |
|---|---|---|---|---|
| | and preservation of evidence related to information security events. | | | |
| A.5.29 Information security during disruption | The organization shall plan how to maintain information security at an appropriate level during disruption. | YES | Business continuity | Implemented |
| A.5.30 ICT readiness for business continuity | ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. | YES | Business continuity | Implemented |
| A.5.31 Identification of 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 assessment Legislation | Implemented |
| A.5.32 Intellectual property rights | The organization shall implement appropriate procedures to protect intellectual property rights. | YES | Legislation | Implemented |
| A.5.33 Protection of records | Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release. | YES | Risk assessment | Implemented |
| A.5.34 Privacy and protection of PII | The organization shall identify and meet the requirements regarding preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. | YES | Risk assessment GDPR | Implemented |
| A.5.35 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 assessment Best practice | Implemented |
| A.5.36 Compliance with policies and standards for information security | Compliance with the organization’s information security policy, topic-specific policies and standards shall be regularly reviewed. | YES | Risk assessment | Implemented |
| A.5.37 Documented operating procedures | Operating procedures for information processing facilities shall be documented and made available to | YES | Compliance | Implemented |

| | | | | |
|---|---|---|---|---|
| | personnel who need them. | | | |
| A.6.1 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 assessment<br>Resources<br>Competences | Implemented |
| A.6.2 Terms and conditions of employment | The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security. | YES | Risk assessment | Implemented |
| A.6.3 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 assessment | Implemented |
| A.6.4 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 assessment | Implemented |
| A.6.5 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 assessment | Implemented |
| A.6.6 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 assessment | Implemented |
| A.6.7 Remote working | Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or | YES | Risk assessment | Implemented |

| | | | | |
|---|---|---|---|---|
| | stored outside the organization's premises. | | | |
| A.6.8 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 assessment | Implemented |
| A.7.1 Physical security perimeter | Security perimeters shall be defined and used to protect areas that contain information and other associated assets. | YES | Risk assessment | Implemented |
| A.7.2 Physical entry controls | Secure areas shall be protected by appropriate entry controls and access points. | YES | Risk assessment | Implemented |
| A.7.3 Securing offices, rooms and facilities | Physical security for offices, rooms and facilities shall be designed and implemented. | YES | Risk assessment | Implemented |
| A.7.4 Physical security monitoring | Premises shall be continuously monitored for unauthorized physical access. | YES | Risk assessment | Implemented |
| A.7.5 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 assessment | Implemented |
| A.7.6 Working in secure areas | Security measures for working in secure areas shall be designed and implemented. | YES | Risk assessment | Implemented |
| A.7.7 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 assessment | Implemented |
| A.7.8 Equipment siting and protection | Equipment shall be sited securely and protected. | YES | Risk assessment | Implemented |
| A.7.9 Security of assets off-premises | Off-site assets shall be protected. | YES | Risk assessment<br>Asset management | Implemented |
| A.7.10 Storage media | Storage media shall be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization’s | YES | Risk assessment | Implemented |

| | | | | |
|---|---|---|---|---|
| | classification scheme and handling requirements. | | | |
| A.7.11 Supporting utilities | Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. | YES | Risk assessment<br>Business continuity | Implemented |
| A.7.12 Cabling security | Cables carrying power, data or supporting information services shall be protected from interception, interference or damage. | YES | Risk assessment<br>Business continuity | Implemented |
| A.7.13 Equipment maintenance | Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. | YES | Risk assessment<br>Business continuity | Implemented |
| A.7.14 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 assessment | Implemented |
| A.8.1 User endpoint devices | Information stored on, processed by or accessible via user endpoint devices shall be protected. | YES | Risk assessment | Implemented |
| A.8.2 Privileged access rights | The allocation and use of privileged access rights shall be restricted and managed. | YES | Risk assessment | Implemented |
| A.8.3 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 assessment | Implemented |
| A.8.4 Access to source code | Read and write access to source code, development tools and software libraries shall be appropriately managed. | YES | Risk assessment | Implemented |
| A.8.5 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 assessment | Implemented |
| A.8.6 Capacity management | The use of resources shall be monitored and adjusted in line with | YES | Risk assessment<br>Resource management | Implemented |

| | | | | |
|---|---|---|---|---|
| | current and expected capacity requirements. | | | |
| A.8.7 Protection against malware | Protection against malware shall be implemented and supported by appropriate user awareness. | YES | Risk assessment | Implemented |
| A.8.8 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 assessment | Implemented |
| A.8.9 Configuration management | Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. | YES | Risk assessment | Implemented |
| A.8.10 Information deletion | Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. | YES | Risk assessment | Implemented |
| A.8.11 Data masking | Data masking shall be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific, and business requirements, taking applicable legislation into consideration. | YES | Risk assessment<br>Privacy & protection of PII | Implemented |
| A.8.12 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 assessment | Implemented |
| A.8.13 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 assessment | Implemented |
| A.8.14 Redundancy of information processing facilities | Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. | YES | Risk assessment | Implemented |
| A.8.15 Logging | Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, | YES | Risk assessment<br>Incident management | Implemented |

| | | | | |
|---|---|---|---|---|
| | protected and analysed. | | | |
| A.8.16 Monitoring activities | Networks, systems, and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. | YES | Risk assessment | Implemented |
| A.8.17 Clock synchronization | The clocks of information processing systems used by the organization shall be synchronized to approved time sources. | YES | Risk assessment | Implemented |
| A.8.18 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 assessment<br>Penetration testing | Implemented |
| A.8.19 Installation of software on operational systems | Procedures and measures shall be implemented to securely manage software installation on operational systems. | YES | Risk assessment | Implemented |
| A.8.20 Network controls | Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. | YES | Risk assessment | Implemented |
| A.8.21 Security of network services | Security mechanisms, service levels, and service requirements of network services shall be identified, implemented and monitored. | YES | Risk assessment | Implemented |
| A.8.22 Segregation in networks | Groups of information services, users, and information systems shall be segregated in the organization's networks. | YES | Risk assessment | Implemented |
| A.8.23 Web filtering | Access to external websites shall be managed to reduce exposure to malicious content. | YES | Risk assessment | Implemented |
| A.8.24 Use of cryptography | Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. | YES | Risk assessment | Implemented |
| A.8.25 Secure development life cycle | Rules for the secure development of software and systems shall be established and applied. | YES | Risk assessment<br>Best practice | Implemented |
| A.8.26 Application | Information security requirements | YES | Risk assessment | Implemented |

| | | | | |
|---|---|---|---|---|
| security requirements | shall be identified, specified and approved when developing or acquiring applications. | | | |
| A.8.27 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 assessment | Implemented |
| A.8.28 Secure coding | Secure coding principles shall be applied to software development. | YES | Risk assessment | Implemented |
| A.8.29 Security testing in development and acceptance | Security testing processes shall be defined and implemented in the development life cycle. | YES | Risk assessment<br>Quality management | Implemented |
| A.8.30 Outsourced development | The organization shall direct, monitor and review the activities related to outsourced system development. | YES | Risk assessment<br>Secure development<br>Quality management | Implemented |
| A.8.31 Separation of development, test and production environments | Development, testing, and production environments shall be separated and secured. | YES | Risk assessment | Implemented |
| A.8.32 Change management | Changes to information processing facilities and information systems shall be subject to change management procedures. | YES | Risk assessment | Implemented |
| A.8.33 Test information | Test information shall be appropriately selected, protected and managed. | YES | Risk assessment | Implemented |
| A.8.34 Protection of information systems during audit and 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 assessment | Implemented |