Clause	Title	Control objective	Why is the control applicable?				Implementation method	Excluded	Motivation for exclusion
			Business requirement	Legal requirement	Contractual requirement	Used in Risk treatment			
5		**Organizaional Controls**							
5.1	**Policies for information security**	Information security policy and topic-specific policies should 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	No	Yes	No	Set of ISMS policies are created, approved and published on SharePoint. Policy owners review the policies at least yearly.	**No**	
5.2	**Information security roles and responsibilities**	Information security roles and responsibilities should be defined and allocated according to the organization needs	Yes	No	No	No	Operational security is managed by the IT Manage.CISO manages the ISMS and supports the Managers in maintaining and improving the ISMS.	**No**	
5.3	**Segregation of duties**	Conflicting duties and conflicting areas of responsibility should be segregated.	Yes	No	Yes	Yes	IT manages the internal IT infrastructure. Users have limited rights based on the need within their function.	**No**	
5.4	**Management Responsibilities**	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes	No	No	Yes	Management team ensures that their team members adhere to the ISMS policies and that information security is embedded in the design of our solutions.	**No**	
5.5	**Contact with Authorities**	The organization should establish and maintain contact with relevant authorities.	Yes	No	No	No	MD supported by external legal counsel maintain the appropriate contacts with the authorities.	**No**	
5.6	**Contact with special interest groups**	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	No	No	No	As part of our threath intelligence monitoring technical and functional employees maintain contacts with vendors, technology partners, cloud providers, hackernews forums and other relevant information sources. An overview is maintained.	**No**	
5.7	**Threat intelligence**	Information relating to information security threats should be collected and analysed to produce threat intelligence.	Yes	No	No	No	To prevent hackers to penetrate our systems we pro-actively collect information on known threats to analyse if they can impact us.	**No**	
5.8	**Information security in project management**	Information security should be integrated into project management.	Yes	Yes	No	No	Information security is embedded in each type of project at Tein Technology. In some cases it can be a contractual requirement by the customers.	**No**	
5.9	**Inventory of information and other associated assets**	An inventory of information and other associated assets, including owners, should be developed and maintained.	Yes	No	No	No	IT manages the internal IT infrastructure and maintains an asset inventory.	**No**	
5.10	**Acceptable use of information and other associated assets**	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Yes	No	No	Yes	Acceptable use policy created, published and explained to the staff.	**No**	
5.11	**Return of Assets**	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Yes	Yes	Yes	No	All assets need to be returned at temination of a contract both by staff as third parties.	**No**	
5.12	**Classification Of Information**	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Yes	No	No	Yes	Information classification created and implemented.	**No**	

5.13	**Labelling of Information**	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	No	No	Yes	Information classification created and implemented.	**No**	
5.14	**Information Transfer**	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Yes	No	No	No	Information classification created and implemented including the information transfer rules.	**No**	
5.15	**Access Control**	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Yes	No	No	Yes	Access control policy created and implemented. Least priviliged principle adhered.	**No**	
5.16	**Identity Management**	The full life cycle of identities should be managed.	Yes	No	No	Yes	Access control policy created and implemented. Least priviliged principle adhered.	**No**	
5.17	**Authentication information**	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Yes	No	No	Yes	Included in the onboarding process and Acceptable use policy.	**No**	
5.18	**Access rights**	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes	No	No	Yes	Acces rights provisioning in place. Managed by IT.	**No**	
5.19	**Information security in supplier relationships**	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes	No	No	Yes	Secure supplier policy created and implemented	**No**	
5.20	**Addressing information security within supplier agreements**	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Yes	No	No	Yes	Agreements in place including requirements on information security with all relevant suppliers.	**No**	
5.21	**Managing information security in the ICT supply chain**	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	No	No	Yes	Included in the supplier contracts.	**No**	
5.22	**Monitoring, review and change management of supplier services**	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	No	No	Yes	Critical suppliers are monitored and reviewed on a yearly basis	**No**	
5.23	**Information security for use of cloud services**	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	Yes	No	No	No	Cloud services policy created and implemented	**No**	
5.24	**Information security incident management planning and preparation**	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities	Yes	No	No	No	Incident management policy created and implemented. IT incidents are managed through security tickets and handled by the CISO.	**No**	
5.25	**Assessment and decision on information security events**	The organization should assess information security events and decide if they are to be categorized as information security incidents.	Yes	No	No	No	Incident management policy created and implemented. IT incidents are managed through security tickets and handled by the CISO.	**No**	
5.26	**Response to information security incidents**	Information security incidents should be responded to in accordance with the documented procedures.	Yes	No	No	No	Incident management policy created and implemented. IT incidents are managed through security tickets and handled by the CISO.	**No**	
5.27	**Learning from information security incidents**	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Yes	No	No	No	Incident management policy created and implemented. IT incidents are managed through security tickets and handled by the CISO.	**No**	

5.28	**Collection of evidence**	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	No	No	No	Incident management policy created and implemented. IT incidents are managed through security tickets and handled by the CISO.	**No**	
5.29	**Information security during disruption**	The organization should plan how to maintain information security at an appropriate level during disruption.	Yes	No	No	No	Managed by IT and regularly tested.	**No**	
5.30	**ICT readiness for business continuity**	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	No	No	No	Managed by IT and regularly tested.	**No**	
5.31	**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 should be identified, documented and kept up to date.	Yes	No	No	No	Overview of applicable legislation and contractual requirements created and maintained.	**No**	
5.32	**Intellectual property rights**	The organization should implement appropriate procedures to protect intellectual property rights.	Yes	No	No	No	Included in the acceptable use policy	**No**	
5.33	**Protection of records**	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	No	No	No	Managed by IT and the cloud service providers.	**No**	
5.34	**Privacy and protection of PII**	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	No	No	No	Privacy by design implemented as baseline for new applications and customer developments.	**No**	
5.35	**Independent review of information security**	The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Yes	No	No	No	Internal audits are performed by external consultants. Certification audits ISO 9001 and 27001 by DQS.	**No**	
5.36	**Compliance with policies, rules and standards for information security**	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Yes	No	No	No	Managers check at least yearly if the policies still compliant.	**No**	
5.37	**Documented operating procedures**	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Yes	No	No	No	Available onSharePoint.	**No**	
6	**People controls**		**Business requirement**	**Legal requirement**	**Contractual requirement**	**Used in Risk treatment**	**Implementation method**	**Excluded**	**Motivation for exclusion**
6.1	**Screening**	Background verification checks on all candidates to become personnel should 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	No	No	Yes	Managed by HR in cooperation with the hiring manager.	**No**	
6.2	**Terms and conditions of employment**	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	Yes	No	No	Yes	Standard labour contracts including confidentiality statements.	**No**	
6.3	**Information security awareness, education and training**	Personnel of the organization and relevant interested parties should 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	No	No	Yes	Employees get a set of manadatory trainings as well as a specific ISMS awareness training from the CISO.	**No**	

6.4	**Disciplinary process**	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes	No	No	Yes	Managed through our labour rules.	**No**	
6.5	**Responsibilities after termination or change of employment**	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	Yes	No	No	Yes	Standard labour contracts including confidentiality statements remain in affect after termination of contract.	**No**	
6.6	**Confidentiality or non-disclosure agreements**	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	No	No	Yes	Signed whenever confidential information is exchanged.	**No**	
6.7	**Remote working**	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes	No	No	No	Included in the acceptable use policy	**No**	
6.8	**Information security event reporting**	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	No	No	No	Staff can log information security incidents by sending an e-mail to a dedicated mailbox.	**No**	
7	**Physical controls**		**Business requirement**	**Legal requirement**	**Contractual requirement**	**Used in Risk treatment**	**Implementation method**	**Excluded**	**Motivation for exclusion**
7.1	**Physical security perimeters**	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Yes	No	No	Yes	Office is considered as one security area.	**No**	
7.2	**Physical entry**	Secure areas should be protected by appropriate entry controls and access points.	Yes	No	No	Yes	Entry through badge access. CCTV in place	**No**	
7.3	**Securing offices, rooms and facilities**	Physical security for offices, rooms and facilities should be designed and implemented.	Yes	No	No	Yes	Badge controlled entrance to the building	**No**	
7.4	**Physical security monitoring**	Premises should be continuously monitored for unauthorized physical access.	Yes	No	No	No	CCTV in place	**No**	
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 should be designed and implemented.	Yes	No	No	Yes	No critical systems running on-site. Main business applications are cloud based. Server room equiped with UPS.	**No**	
7.6	**Working in secure areas**	Security measures for working in secure areas should be designed and implemented.	Yes	No	No	Yes	ISMS policies include the security measures for working at the office.	**No**	
7.7	**Clear desk and clear screen**	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Yes	No	No	No	Included in the Acceptable use policy	**No**	
7.8	**Equipment siting and protection**	Equipment should be sited securely and protected.	Yes	No	No	Yes	Server room – demo room – staging room	**No**	
7.9	**Security of assets off-premises**	Off-site assets should be protected.	Yes	No	No	No	All laptops are encrypted	**No**	
7.10	**Storage media**	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	No	No	Yes	Limited use of external storage media. Storage media is always wiped after use.	**No**	
7.11	**Supporting utilities**	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	No	No	Yes	Managed by IT for the IT Infrastructure.	**No**	
7.12	**Cabling security**	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Yes	No	No	No	Managed by IT for the IT Infrastructure.	**No**	

7.13	**Equipment maintenance**	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	No	No	Yes	Managed by IT for the IT Infrastructure and by facilities for the HVAC systems.	**No**	
7.14	**Secure disposal or re-use of equipment**	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	No	No	No	Equipment is returned to IT. They securely wipe the data.	**No**	
8	**Technological controls**		**Business requirement**	**Legal requirement**	**Contractual requirement**	**Used in Risk treatment**	**Implementation method**	**Excluded**	**Motivation for exclusion**
8.1	**User endpoint devices**	Information stored on, processed by or accessible via user endpoint devices should be protected.	Yes	No	No	Yes	Managed by IT and controlled through an global policies	**No**	
8.2	**Privileged access rights**	The allocation and use of privileged access rights should be restricted and managed.	Yes	No	No	Yes	Managed by IT. Only limited number of authorized staff have priveliged access.	**No**	
8.3	**Information access restriction**	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Yes	No	No	Yes	Policy created and implemented	**No**	
8.4	**Access to source code**	Read and write access to source code, development tools and software libraries should be appropriately managed.	Yes	No	No	Yes	Access to source code is limited to the Software team.	**No**	
8.5	**Secure authentication**	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	No	No	Yes	Secure login managed by IT.	**No**	
8.6	**Capacity management**	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Yes	No	No	No	Managed by IT and controlled through PRTG monitoring.	**No**	
8.7	**Protection against malware**	Protection against malware should be implemented and supported by appropriate user awareness.					Antimalware installed on endpoints and servers.		
8.8	**Management of technical vulnerabilities**	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Yes	No	No	No	Managed by IT.	**No**	
8.9	**Configuration management**	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Yes	No	No	Yes	Managed by IT.	**No**	
8.10	**Information deletion**	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.					Data retention policy in place		
8.11	**Data masking**	Data masking should 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	No	No	No	Managed by IT and controlled through access right provisioning and encryption.	**No**	
8.12	**Data leakage prevention**	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.					Data Leakage prevention policy in place		
8.13	**Information backup**	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	No	No	Yes	Data is kept according to the legal and contractual retention times	**No**	
8.14	**Redundancy of information processing facilities**	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Yes	No	No	No	Critical business applications are cloud based solution with guaranteed redundancy.	**No**	
8.15	**Logging**	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Yes	No	No	Yes	Managed by IT, secure log storage.	**No**	

8.16	**Monitoring activities**	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	No	No	Yes	Monitoring through PRTG.	**No**	
8.17	**Clock synchronization**	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Yes	No	No	No	NTP	**No**	
8.18	**Use of privileged utility programs**	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Yes	No	No	Yes	Only IT admins use priviliged utility programs	**No**	
8.19	**Installation of software on operational systems**	Procedures and measures should be implemented to securely manage software installation on operational systems.	Yes	No	No	No	Only IT admins can install software on operational systems	**No**	
8.20	**Networks security**	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Yes	No	No	Yes	Secure networjs installed with outside security through firewall.	**No**	
8.21	**Security of network services**	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Yes	No	No	Yes	Secure networjs installed with outside security through firewall.	**No**	
8.22	**Segregation of networks**	Groups of information services, users and information systems should be segregated in the organization's networks.	Yes	No	No	No	Segregation through VLANS in place.	**No**	
8.23	**Web filtering**	Access to external websites should be managed to reduce exposure to malicious content.	Yes	No	No	No	Managed by IT through the firewall settings.	**No**	
8.24	**Use of cryptography**	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Yes	No	No	No	Encryption policy in place	**No**	
8.25	**Secure development life cycle**	Rules for the secure development of software and systems should be established and applied.	Yes	No	No	No	Secure development policy and development guidelines in place	**No**	
8.26	**Application security requirements**	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Yes	No	No	No	Set of security requirements is defined before the acquisition of new applications	**No**	
8.27	**Secure system architecture and engineering principles**	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Yes	No	No	No	Secure development policy and development guidelines in place	**No**	
8.28	**Secure coding**	Secure coding principles should be applied to software development.	Yes	No	No	No	Secure coding guidelines in place.	**No**	
8.29	**Security testing in development and acceptance**	Security testing processes should be defined and implemented in the development life cycle.	Yes	No	No	No	Secure development policy and development guidelines in place	**No**	
8.30	**Outsourced development**	The organization should direct, monitor and review the activities related to outsourced system development.	Yes	No	No	No	Secure development policy and development guidelines in place	**No**	
8.31	**Separation of development, test and production environments**	Development, testing and production environments should be separated and secured.	Yes	No	No	No	Segregation in place accoriding to the project requirements	**No**	
8.32	**Change management**	Changes to information processing facilities and information systems should be subject to change management procedures.	Yes	No	No	No	Changes are managed with the projects by the I&D team.	**No**	
8.33	**Test information**	Test information should be appropriately selected, protected and managed.	Yes	No	No	No	Testing is managed with the projects by the I&D team.	**No**	
8.34	**Protection of information systems during audit testing**	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Yes	No	No	No	Testing is managed with the projects by the I&D team.	**No**	