Version: 1.0 | Responsible: Kevin Kaminski | Valid from: 10.12.2023 20:00:00 | Classification: Public | Status: Final

Statement of Applicability (SoA)

of the information security management system

Belfortstr. 5, 81667 München (HQ) | Kurfürstendamm 102, 10711 Berlin

27001:2022	Ref 27001:2013	Topic	Applicable	Reason	Implementation	Place of documentation
A.5.1	A.5.1.1, A.5.1.2	Policies for information security	Yes	Requirement of standard	Policies have been published in the intranet. Employees have access to the policies and were trained in dedicated workshops or recorded workshop sessions.	Information security guideline User policy Organisation policy Administration policy
A.5.2	A.6.1.1	Information security roles and responsibilities	Yes	Requirement of standard	Roles and authorization levels are defined including their responsibilities.	Organisation policy
A.5.3	A.6.1.2	Segregation of duties	Yes	Risk Reduction	Essential responsibilities are segregated through the organisation, e.g. access rights, planning of requirements, code reviews and software deployments, working on the infrastructure and more. The duties are documented throughout the documentation landscape of the organisation, such as policies, process descriptions or operation manuals.	Organisation policy User policy Internal working procedure
A.5.4	A.7.2.1	Management responsibilities	Yes	Requirement of standard	Management responssibilities are documented and have been approved by management.	Organisation policy
A.5.5	A.6.1.3	Contact with authorities	Yes	Requirement of standard	The Information Security Officer (ISO) is defined to be the contact person for authorities. The external Data Privacy Office (DPO) is the contact person for supervisory authorities.	Organisation policy
A.5.6	A.6.1.4	Contact with special interest groups	Yes	Requirement of standard	3Q is part of the "Alliance for Cybersecurity." Enabled CERT-Bund Newsletter. ISO checks IT news websites and BSIs offical "Warnhinweise" on a daily basis. ISO exchanges with other security experts on a reguar level.	Internal working procedure
A.5.7	New	Threat intelligence	Yes	Risk Reduction	Regular review of security news websites, newsletter that inform about potential threats (e.g. BSI or Cyber Alliance). Regular vulnerability scans of infrastructure to detect threats. EDR solution enrolled on all end user devices prevent threats to be present.	Administration policy
A.5.8	A.6.1.5, A.14.1.1	Information security in project management	Yes	Risk Reduction	Identifiying and analysing potential risks of a feature or an implementation are discussed in the refinement meetings of the development team. Complex new features are previously discussed on a high level on Tech Lead level to already identify potential risks early.	Internal working procedure
A.5.9	A.8.1.1, A.8.1.2	Inventory of information and other associated assets	Yes	Risk Reduction	Inventory of information is collected in the Business Impact Analysis document. An internal policy describes the procedure of the evaluation of primary assets and the assignment to owners, services and secondary assets.	Administration policy
A.5.10	A.8.1.3, A.8.2.3	Acceptable use of information and other associated assets	Yes	Risk Reduction	Classification and handling of information is documented in a policy. Documents are labelled so employees know how to handle the asset accordingly. Handling and administration of laptops is described in a dedicated working procedure.	User policy Internal working procedure
A.5.11	A.8.1.4	Return of assets	Yes	Risk Reduction	The return of assets follows a documented procedure (e.g. handover, signing protocol, functionality check, secure storage).	Internal working procedure
A.5.12	A.8.2.1	Classification of information	Yes	Risk Reduction	Information are classified according to their protection level and potential damage. A classification scheme for all information used within the company, has been defined in a policy.	User policy
A.5.13	A.8.2.2	Labeling of information	Yes	Risk Reduction	The different forms of labels, rules and label exceptions have been defined in a policy.	Organisation policy
A.5.14	A.13.2.1; A.13.2.2 A.13.3	Information transfer	Yes	Risk Reduction	The handling of information and a detailled categorization of allowed procedures for each classified information has been defined in a policy. Further it contains the definition and work in protection zones and rules for mobile working.	User policy
A.5.15	A.9.1.1, A.9.1.2	Access control	Yes	Risk Reduction	Handling of access control of physical means of identification and access right to IT services is described in a policy. Internal working instructions are in place that describe more detailed description of particular processes (e.g. acces request workflow, handling of physical means of identification).	User policy Internal working procedure
A.5.16	A.9.2.1	Identity management	Yes	Risk Reduction	Each user access is assigned to a unique user ID. Shared user accounts are possible if dedicated users can't be set up. The target state of all accesses is documented in a dedicated list.	User policy
A.5.17	A.9.2.4, A.9.3.1, A.9.4.3	Authentication information	Yes	Risk Reduction	There is a policy that defines the handling of login information, rules for passwords and the usage of 2FA.	User policy
A.5.18	A.9.2.2, A.9.2.5, A.9.2.6	Access rights	Yes	Risk Reduction	There is an access rights management with approval workflow in place. Regular review of acces rights.	User policy Internal working procedure
A.5.19	A.15.1.1	Information security in supplier relationships	Yes	Risk Reduction	General requirements for cooperating with suppliers and partners and exchaning of information is described in a policy. There is a documented process for the evaluation of external services/suppliers.	Organisation policy Internal working procedure
A.5.20	A.15.1.2	Addressing information security within supplier agreements	Yes	Risk Reduction	The evaluation of suppliers follow a standardized evaluation questionaire. It is required to make sure that relevant terms are considered for the inclusion in a suppliers agreement.	Administration policy
A.5.21	A.15.1.3	Managing information security in the ICT supply chain	Yes	Risk Reduction	ICT supply chain procurement follows the existing process of supplier or external services evaluation. The usage of software librariers in development follow a documented software dependency workflow.	Administration policy Internal working procedure
A.5.22	A.15.2.1, A.15.2.2	Monitoring, review and change management of supplier services	Yes	Risk Reduction	Supplier reviews are performed by checking if information security requirements have changed and if a re-evaluiation or additional measures are necessary.	Organisation policy Internal working procedure
A.5.23	New	Information security for use of cloud services	Yes	Risk Reduction	This control follows the existing evaluation of IT services which are described in a apolicy. In addition to that, a dedicated working procedure exists with details and best practices.	Administration policy Internal working procedure
A.5.24	A.16.1.1	Information security incident management planning and preparation	Yes	Risk Reduction	Incident management process for employees is described in a policy. Incidents can be reported via a request form. A policy describes the procedures on the administration level, e.g. definition, roles, classification and communication in case of an security or incident event.	User policy Administration policy
A.5.25	A.16.1.4	Assessment and decision on information security events	Yes	Risk Reduction	A categorization of security events is existent and the communication hierarchy is defined in a policy.	Administration policy
A.5.26	A.16.1.5	Response to information security incidents	Yes	Risk Reduction	The response procedures in cases of security or incident events are described in a policy. Documentation of detailed steps on how to internally handle a security incident by the ISO.	Administration policy Internal working procedure
A.5.27	A.16.1.6	Learning from information security incidents	Yes	Risk Reduction	Security or incident events are analyzed in each case and retroactively reviewed in management review. Incident management plan will be adjusted if necessary.	Internal working procedure
A.5.28	A.16.1.7	Collection of evidence	Yes	Risk Reduction	General rules when evidences are necessary and advices for the process of taking and storing evidences has been described in a policy. We defined specific procedures for evidence collection in a dedicated process for the development team.	User policy Internal working procedure
A.5.29	A.17.1.1, A.17.1.2, A.17.1.3	Information security during disruption	Yes	Risk Reduction	An emergency plan lists different emergency scenarios and instruction of actions. Certain scenarios can be described in more detailed process descriptions or operation manuals.	Emergency plan Internal working procedure

A.5.30	New	ICT readiness for business continuity	Yes	Risk Reduction	Essential customer data gets replicated on a daily basis. Recovery scenarios for sensitive customer data are in place. Customer media files are stored redundantly in separated data center. Essential infrastructure components are set up redundently to assure business continuance in case of failure.	Internal working procedures Operation manual
A.5.31	A.18.1.1, A.18.1.5	Legal, statutory, regulatory and contractual requirements	Yes	Risk Reduction	We have rules for contracts and laws in place. Internal index of statutory and regulatory requirements exist and is adjusted if necessary. In addition we collect important contractual customer requirements in a separate overview document.	Organisation policy
A.5.32	A.18.1.2	Intellectual property rights	Yes	Risk Reduction	Software and external software components are only used following a defined review processes.	User policy Developer policy Internal working procedure
A.5.33	A.18.1.3	Protection of records	Yes	Risk Reduction	Physical records are stored in dedicated locked rooms or locked cabinets. Record folders are clearly labeled with information regarding area of responsibility and protection level according to to classicifcation scheme.	User policy
A.5.34	A.18.1.4	Privacy and protection of PII	Yes	Risk Reduction	Customer media data and customer information are deleted after there is no purpose of use. Data is permanetly deleted from the storage after user deletion or after contract has been expired following an automatic deletion process. A register exists that summarizes all personal data collected through our service.	Internal working procedure
A.5.35	A.18.2.1	Independent review of information security	Yes	Requirement of standard	General rules and procedures for the verification of effectiveness are described in a policy which states that external audits are performed by an independet organisation that is specified on ISO 27001 audits. Internal audits can be performed by ISO or indipendet external agency.	Organisation policy
A.5.36	A.18.2.2, A.18.2.3	Compliance with policies, rules and standards for information security	Yes	Requirement of standard	Internal audits are planned throughout the year for all main processes to ensure that information secuity is implemented according to policies, rules and standards.	Organisation policy Internal working procedure
A.5.36	A.12.1.1	Documented operating procedures	Yes	Requirement of standard	Internal documentation must follow documentation rules. Important operating systems or processes are internally documented so that specialized employees can understand and and use the system accordingly.	Organisation policy
A.6.1	A.7.1.1	Screening	Yes	Risk Reduction	Rules for hiring employees and verification checks according to the positions are implemented.	Organisation policy
A.6.2	A.7.1.2	Terms and conditions of employment	Yes	Risk Reduction	During recruiting process potential candidates are informed about information security procedures and responsibilities. Employees contract contains a non-disclosure agreement and commitment to comply with data protection regulations.	Employee contract Internal working procedure
A.6.3	A.7.2.2	Information security awareness, education and training	Yes	Risk Reduction	New employees are obliged to read company policies and watch policy workshops. Information security officer schedules dedicated appointment with new emploeeyes to make sure information security rules are understood. ISO uses measures (e.g. mails, workshops) to raise awareness for information security throughout the whole company.	Organisation policy
A.6.4	A.7.2.3	Disciplinary process	Yes	Risk Reduction	We created an overview for the commitment to information security and a disciplinary catalogue which is a step-by-step plan on how to procede in case of information security violation.	Organisation policy
A.6.5	A.7.3.1	Responsibilities after termination or change of employment	Yes	Risk Reduction	An offboarding process and offboarding checklist is in place that covers different actions that needs to be taken care of when it comes to an employee termination.	Internal working procedure
A.6.6	A.13.2.4	Confidentiality or non-disclosure agreements	Yes	Risk Reduction	Confidentiality clauses exist in all employee contracts. In addition to that, NDAs are existent and will be used in necessary situations.	Employee contract
A.6.7	A.6.2.2	Remote working	Yes	Risk Reduction	A policy describes risks and behaviour when working outside the protection zones (e.g. from home or in transfer).	User policy
A.6.8	A.16.1.2, A.16.1.3	Information security event reporting	Yes	Risk Reduction	Employees are made aware of their responsibility to report information security events. Security events can be reported via a centrally available request form accessible for every employee.	User policy
A.7.1	A.11.1.1	Physical security perimeters	Yes	Risk Reduction	Roofs, walls, ceilings and flooring of office premises are of solid construction and all external doors are suitably protected against unauthorized access. There are rules for behaviour within premises (e.g. close window, lock door when out). Further security instructions are existent per office location.	User policy Internal working procedure
A.7.2	A.11.1.2, A.11.1.6	Physical entry	Yes	Risk Reduction	There is a process in place for the administration of physical means of identification for both office premises. Electronic acces is logged. Visitors have to be registered. Physical access needs to be approved via request workflow.	User policy Internal working procedure
A.7.3	A.11.1.3	Securing offices, rooms and facilities	Yes	Risk Reduction	Both offices are part of premises that are secured with physical means of identification. The existence of information with high confidentiality level is not visble from the outside or within the premises. Protection zone map only accessible via user login.	User policy
A.7.4	New	Physical security monitoring	Yes	Risk Reduction	Premises are video monitored on entrance, exit and windows. Both premises have electronic door mechansim at main entrance that logs every access to the premise.	Internal working procedure
A.7.5	A.11.1.4	Protecting against physical and environmental threats	Yes	Risk Reduction	An emergency plan covers scenarios for physical and environmental threats that is available for all employees digitally and physically. Data center has extensive general and fire protection measures in place (e.g. 24/7 monitoring, fire alarm, constant power supply, etc.).	Emergency plan
A.7.6	A.11.1.5	Working in secure areas	Yes	Risk Reduction	Protection zones have been established in the premises. There is a set of rules in regards to the protection zones that apply accordingly.	User policy
A.7.7	A.11.2.9	Clear desk and clear screen	Yes	Risk Reduction	Employees are made aware about rules and bevhaviour when working in protection zones.	User policy
A.7.8	A.11.2.1	Equipment siting and protection	Yes	Risk Reduction	Internal network hardware and sensitive documents in premises are placed in locked rooms with restricted and documented access. Premises are equipped with smoke detectors and fire extinguisher. Smoking is prohibited in all premises. Data center has extensive general and fire protection measures in place (e.g. 24/7 monitoring, fire alarm, constant power supply, etc.).	User policy Internal working procedure
A.7.9	A.11.2.6	Security of assets off-premises	Yes	Risk Reduction	The are rules for working with mobile devices outside the protection zones. Mobile devices are centrally managed and administrated. Each device is only handed out after signed protocol and labour supply contract that contains further responsibilities of employee.	User policy Internal working procedure
A.7.10	A.8.3.1, A.8.3.2, A.8.3.3.A.11.2.5	Storage media lifecycle	Yes	Risk Reduction	The usage of removeable storage media on employee end devices is generally prohibited. The removal of general hardware devices (e.g. notebooks) and infrastructure storage media follows a documented procedures which includes the previous deletion of data.	User policy Internal working procedure
A.7.11	A.11.2.2	Supporting utilities	Yes	Risk Reduction	Supporting utilities of office premises are in responsibility of landlord. However, working procedures with contact information and important advices in case of supporting utilities fail, do exists. Data center is equipped with emergency power (diesel generator) that can be re-filled during service.	Internal working procedures
A.7.12	A.11.2.3	Cabling security	Yes	Risk Reduction	Data cables are properly installed in walls or floors in both office facilities. Cable to power or connect equipment is properly and securely mounted at workstations.	User policy
A.7.13	A.11.2.4	Equipment maintenance	Yes	Risk Reduction	Office equipment for premises in Berlin and Munich is listed in an overview which contains the responsibility and next maintenance dates. Equipment in data centers are managed by data center provider and follows contractural agreement and service description.	Internal working procedures Service contract

A.7.14	A.11.2.7	Secure disposal or re-use of equipment	Yes	Risk Reduction	A policy describes procedures in the handling of assets and the disposal (e.g. means of identification). Dedicated working procedures for general devices (e.g. notebooks) and infrastructure hardware are exsitent.	Administration policy Internal working procedure
A.8.1	A.6.2.1, A.11.2.8	User endpoint devices protection	Yes	Risk Reduction	There are rules and procedures in regards to the configuration and handling of user endpoint devices. (e.g. use of mobile devices, installation if software). Users are also informed about the handling of equipment in protection zones or during mobile work.	User policy
A.8.2	A.9.2.3	Privileged access rights restriction and management	Yes	Risk Reduction	Privileged access rights are managed through a dedicated access management process. Access to systems must be requested first, evaluated and configured before actually usable.	User policy
A.8.3	A.9.4.1	Information access restriction	Yes	Risk Reduction	The access to information is handled via a dediated access management process. System or information accesses are documented in an access control list.	User policy
A.8.4	A.9.4.5	Access to source code	Yes	Risk Reduction	Access to source code via version control system and repositories is managed through the access management process. The handling of source code and usage of program source libraries is described in a dedicated policy and working procedures.	User policy Developer policy Internal working procedure
A.8.5	A.9.4.2	Secure authentication	Yes	Risk Reduction	Every software at 3Q requires a user name and password authentication. Selected and sensitive systems require 2FA or are additionally protected via network filtering. Several infrastructure services require additional authentication mechanisms. Access to VPN network require appproval first.	User policy
A.8.6	12.1.3	Capacity management	Yes	Risk Reduction	Capacity of infrastructure ressources is continously monitored via central monitoring system. Capcity of particular customer production processes (e.g. encoding) is publicly monitored incl. internal alerting to a selected group of employees.	Operation manual
A.8.7	12.2.1.	Protection against malware	Yes	Risk Reduction	Installation of software on end user device only possible if software is on the list of approved services. Infrastructure gets scanned for vulnaribilities on a regular basis. User end devices are protected with help of EDR solution.	User policy Administration policy
A.8.8	12.6.1, 18.2.3	Management of technical vulnerabilities	Yes	Risk Reduction	ISO checks in daily routine for technical vulnarabilities and security situation in market via BSI website, security newsletter and major security information websites. Infrastructure components, such as networks, servers and virtual machines are regularly scanned via an internal vulnerability tool. Results of reports will be analysed immediately and measures taken to reduce risk in case of reported vulnaribilities. Software, libraries and components of development processes are manually checked on a weekly basis if updates are available and installed as soon as possible. User endpoint devices will receive automatic updates of OS and software installed by MDM solution.	Administration policy Internal working procedure
A.8.9	New	Configuration management	Yes	Risk Reduction	Important or sensitive systems require a sophisticated documentation in form of operation manuals that contains configuration details of a particular system. Changing configurations in a particular documentation follow rules defined in the organization policy.	Organisation policy Operation manual
A.8.10	New	Information deletion	Yes	Risk Reduction	Customer media data and customer information are deleted after there is no purpose of use according to license agreement. Both end user devices (laptop, mobile phone) and infrastructure hardware are following a working procedure that contains a deletion of data of the hardware.	Internal working procedures
A.8.11	New	Data masking	Yes	Risk Reduction	Data in transit is encrypted. IP addresses in webserver logs ar unanonymised, however archived with encryption after 30 days with restricted acccess.	Administration policy Internal working procedure
A.8.12	New	Data leakage prevention	Yes	Risk Reduction	Data leakage prevention measures in place such as policy for secure document management and access control for systems and information. Employees hardware devices are centrally managed and can be accessed by administrators. Hard drive of devices are encrypted. Transfer to portable storage device is not possible.	User policy Organisation policy
A.8.13	A.12.3.1	Information backup	Yes	Risk Reduction	General back up procedures have been described in a policy. Detailed backup processes have been described in according operation manual documentation of a particular systems.	Administration policy Operation manual
A.8.14	A.17.2.1	Redundancy of information processing facilities	Yes	Risk Reduction	Customer media data is stored redundantly in separate data center locations. Delivery and data base services have automated failover in place. Code repository back ups are replicated redundentaly.	Operation manual
A.8.15	A.12.4.1, A.12.4.2, A.12.4.3	Logging	Yes	Risk Reduction	Actions on important systems are constantly logged. Logs of infrastructure are only accessible by administrators or priviliged employees. Unusual events of infrastructure are logged and connected via alerting mechanism. Admin activities are logged.	Administration policy
A.8.16	New	Monitoring activities	Yes	Risk Reduction	Central monitoring service in place that monitors infrastructure services, data base back ups, errors and warnings. Selected metrics such as file encoding queue notifies customer success team. Operation manual of infrastructure monitoring service is in place.	Operation manual
A.8.17	A.12.4.4	Clock synchronization	Yes	Risk Reduction	This display of time is configured for all important systems and especially the server infrastructure in UTC.	Administration policy
A.8.18	A.9.4.4	Use of privileged utility programs	Yes	Risk Reduction	Privileged access rights are managed through an access management process. This applies especially for priviliged utility programs. Priviliged user rights are monitored on a regular basis.	Administration policy
A.8.19	A.12.5.1, A.12.6.2	Installation of software on operational systems	Yes	Risk Reduction	Deployment of software on user devices is restricted and can be only performed via a self service solution. Every new software runs through an evaluation process before release. Deployment of code on the operational system follows a strict process documented in a policy. There are documented procedures in place for usage of new software libraries and updates.	User policy Developer policy Internal working procedure
A.8.20	A.13.1.1	Networks security	Yes	Risk Reduction	The office premises in Berlin and Munich are equipped with protected wifi services. Mobile work requires the usage of a VPN all the time. Office networks and infrastructure networks in the data center are managed and controlled by an internal Infrastructure team.	Administration policy
A.8.21	A.13.1.2	Security of network services	Yes	Risk Reduction	Access to management and documentation of infrastructure network services is restricted and requires a request and approval first. Additionally access to the infrastructure is securred with multiple encrypted authentication mechanisms. Network connection of data center provider follows contractural agreement and service description.	Administration policy

A.8.22	A.13.1.3	Segregation of networks	Yes	Risk Reduction	Office wifi networks are configured for employee and guest access separately. During mobile working the usage of a VPN is mandatory for every employee. Access to specific infrastructure and development services is segregated by different networks. The access to a specific VPN requires a request and approval.	Administration policy
A.8.23	New	Web filtering	No	Explanation on the right	Web filtering is currently not active, since we manage all of our devices via centralized MDM solution. Device can be disabled and deleted at any time remotely. In addition, an EDR solution on every device protects each device from malware.	
A.8.24	A.10.1.1, A.10.1.2	Use of cryptography	Yes	Risk Reduction	Customer video content is encrypted in transit. Administrative tasks on the infrastructure are performed via multiple encrypted authentication mechanisms.	Administration policy
A.8.25	A.14.2.1	Secure development life cycle	Yes	Risk Reduction	Secure development of software is ensured by separation of environments, implementation of a developer policy which includes coding guidlines, security requirements in design phase, system and security testing, authorisation process for repositories and a version control system.	Developer policy Internal working procedures
A.8.26	A.14.1.2, A.14.1.3	Application security requirements	Yes	Risk Reduction	New applications that are acquired needs to run through an approval process in the first place. A new application will be evaluated according to a set of different security requirements. Only after this risk assessment a new application can be applied.	Administration policy Internal working procedure
A.8.27	A.14.2.5	Secure system architecture and engineering principles	Yes	Risk Reduction	Required principles are followed and described in a policy and different working procedures for topics, such as workflow for bugs and security events, requirements workflow with different stages of requirement evaluations (roadmap planning, refinement meeting, etc.), enabling secure coding practics for development.	Developer policy Internal working procedures
A.8.28	New	Secure coding	Yes	Risk Reduction	Secure coding principles are documented in a policy. Requirements are discussed in refinement meetings prior to the actual coding. Coding practics and design techniques are described in a policy. We use different environments for testing new code before production deployment. Topic specific process documentation describe procedures in detail.	Developer policy Internal working procedures
A.8.29	A.14.2.8, A.14.2.9	Security testing in development and acceptance	Yes	Risk Reduction	Testing procedures are documented in a policy and working procedures. Tests are always performed on dedicated test environment. Code will be always reviewed before testing.	Developer policy Internal working procedures
A.8.30	A.14.2.7	Outsourced development	No	We don't have outsourced development.		
A.8.31	A.12.1.4, A.14.2.6	Separation of development, test and production environments	Yes	Risk Reduction	Development, test and production environments are adequatly separated operating on different domains. Code changes are always tested on one of the testing environments before production deployment. Multiple test environments for different requirements (application, file upload) are in place.	Developer policy Internal working procedures
A.8.32	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4	Change management	Yes	Risk Reduction	A general company wide change management process is in place and documented in a policy. There are topic specific standard change procedures, e.g. procurements of new infrastructure hardware or new employee devices. Changes of major versions are always discussed in an experts round and planned according to existing processes.	Administration policy Internal working procedure
A.8.33	A.14.3.1	Test information	Yes	Risk Reduction	General rules of how to handle internal test data and customer test data are described in a policy.	Administration policy
A.8.34	A.12.7.1	Protection of information systems during audit testing	Yes	Risk Reduction	Activities are in place and documented in a policy that assure protection during audit testing and minimizes risk during operational business hours.	Organisation policy