GAMS

ISO27001:2013 Statement of Applicability

Revision 1

Date: January 19, 2024

ID	Control	Applicable	Reason for application or exclusion	Status
A.5.1.1	Policies for information security	Yes	Management approved policies foster effective interaction between all employees and external parties involved in ensuring information security and demonstrate management committment.	Implemented
A.5.1.2	Review of the policies for information security	Yes	Regular updates to the guides ensure that the latest developments and tasks are included and that the guides remain effective and appropriate.	Implemented
A.6.1.1	Information security roles and responsibilities	Yes	Role assignments help us determine who has what responsibilities regarding information security measures in which situations.	Implemented
A.6.1.2	Segregation of duties	Yes	We implement segregation of duties as far as possible to ensure that a system of mutual assurance is created for security-critical tasks. However, it ends where it leads to inflexibility and cannot be achieved with the existing staffing levels of a small company.	Implemented
A.6.1.3	Contact with authorities	Yes	Contacts with relevant authorities provide us with early information on vulnerabilities, threats and legislative developments that could be relevant to information security.	Implemented
A.6.1.4	Contact with special interest groups	Yes	Contacts with relevant interest groups provide us with early information on vulnerabilities, threats, and other developments that could be relevant to information security.	Implemented
A.6.1.5	Information security in project management	Yes	By looking at planned information security requirements in our projects, we can control and implement them in a targeted manner and at an early stage.	Implemented
A.6.2.1	Mobile device policy	Yes	Mobile devices can be a gateway for attacks and security vulnerabilities. That's why we regulate how they can and cannot be used.	Implemented
A.6.2.2	Teleworking	Yes	Like mobile devices, teleworkplaces are not fully "controllable" and can be a gateway for attacks and security breaches. Therefore, we regulate how to work in telework to create security.	Implemented
A.7.1.1	Screening	Yes	We rely on only hiring people who can meet our security requirements. Therefore, we carefully review who we hire (or have work for us as freelancers).	Implemented
A.7.1.2	Terms and conditions of employment	Yes	Agreements on information security that employees must adhere to can only be reliably adhered to if all parties have insight into what has been agreed upon. That's why we rely on contractual arrangements here.	Implemented
A.7.2.1	Management responsibilities	Yes	Information security is only taken seriously if the management stands behind it and demands compliance on a sustained basis. That's why we hold management accountable.	Implemented
A.7.2.2	Information security awareness, education and training	Yes	To ensure that our employees are able to implement information security, we provide training in this area and develop each employee so that he or she can securely perform the tasks assigned to him or her with regard to information security.	Implemented
A.7.2.3	Disciplinary process	Yes	If employees do not fulfill their information security duties, we care. We talk about it and point it out. This ensures that the importance of the issue is recognized.	Implemented
A.7.3.1	Termination or change of employment responsibilities	Yes	Since we know that information security does not simply stop at the end of an employee's employment, we ensure that we also regulate the obligations that exist beyond the end of working hours.	Implemented
A.8.1.1	Inventory of assets	Yes	Devices (and other assets) can only be operated securely if they are known and controlled.	Implemented
A.8.1.2	Ownership of assets	Yes	Securing devices (and other assets) is only possible if someone feels responsible for each asset. Therefore, we ensure this.	Implemented
A.8.1.3	Acceptable use of assets	Yes	Securing devices (and other assets) is only possible if it is clear for each device which use is permissible – i.e., “secure”. Therefore, we ensure that assets are only used securely.	Implemented
A.8.1.4	Return of assets	Yes	To ensure that equipment is not left unattended when the employee responsible for it leaves the company, there is an obligation to return it in a regulated manner.	Implemented
A.8.2.1	Classification of information	Yes	Different types of information are critical in different ways. Therefore, we have classified the types of information that require protection in our company.	Implemented
A.8.2.2	Labelling of information	Yes	So that it is quickly clear to everyone which information is classified in which way, these are marked.	Implemented
A.8.2.3	Handling of assets	Yes	To ensure that devices (and other assets) are handled as intended (and that improper use does not inadvertently compromise information security), there are rules for how all important devices may be used.	Implemented
A.8.3.1	Management of removable media	Yes	Removable storage media can quickly get lost. We have therefore regulated how and under what conditions they may be used.	Implemented
A.8.3.2	Disposal of media	Yes	When data media are disposed of, critical information may still be stored on them. We have therefore regulated how to dispose of them securely.	Implemented
A.8.3.3	Physical media transfer	Yes	When critical information is stored on transportable data carriers, the risk of it being compromised is higher than on non-transportable data carriers. That is why we have strictly regulated transport.	Implemented
A.9.1.1	Access control policy	Yes	We have an access control policy that regulates who can access which devices and information and for what reason. This ensures that access to devices and information is not arbitrary.	Implemented

GAMS

ISO27001:2013 Statement of Applicability

Revision 1

Date: January 19, 2024

ID	Control	Applicable	Reason for application or exclusion	Status
A.9.1.2	Access to networks and network services	Yes	We secure access to our networks so that information flowing in them is not compromised.	Implemented
A.9.2.1	User registration and deregistration	Yes	To ensure that users are created and deleted correctly and cleanly, we have a process by which we register or deregister users.	Implemented
A.9.2.2	User access provisioning	Yes	To ensure that registered users are granted rights correctly and cleanly, we have a process by which we grant and revoke rights to users.	Implemented
A.9.2.3	Management of privileged access rights	Yes	To ensure that privileged access (admin accounts) does not intentionally or unintentionally compromise information security, we regulate their use.	Implemented
A.9.2.4	Management of secret authentication information of users	Yes	We allocate secret authentication information (passwords, etc.) via a regulated process to ensure that it remains secret during allocation.	Implemented
A.9.2.5	Review of user access rights	Yes	All employees who are responsible for devices (and other assets) at our company regularly check whether the access rights granted are still required. This is how we ensure that unauthorized persons no longer have access.	Implemented
A.9.2.6	Removal of access rights	Yes	When employees (or freelancers who work for us) change their job responsibilities or leave us, we adjust or delete their access rights so that they do not have unauthorized access to information worthy of protection.	Implemented
A.9.3.1	Use of secret authentication information	Yes	We oblige all users to keep their access data secret so that unauthorized persons cannot use it and thus gain access to information worthy of protection.	Implemented
A.9.4.1	Information access restriction	Yes	In accordance with the need-to-know principle, we restrict access to information to those employees who need to have access to this information in order to perform their duties - all others are denied access. In this way, we ensure as far as possible that no one who does not actually need access to sensitive information unintentionally or intentionally handles it in an insecure manner.	Implemented
A.9.4.2	Secure logon procedures	Yes	To ensure that secret authentication information is not compromised after it is entered into information systems, we use only secure logon procedures in which the authentication information is transported securely.	Implemented
A.9.4.3	Password management system	Yes	To prevent passwords from being guessed or spied out via brute force, we ensure that they are secure (long enough, complex enough) via system-side and organizational guidelines.	Implemented
A.9.4.4	Use of privileged utility programs	Yes	We restrict the use of privileged utilities (“Run as…”, “sudo”), especially on production systems, because these programs can lead to accidental system changes or be a gateway for attacks by malware.	Implemented
A.9.4.5	Access control to program source code	Yes	Our source code repository is also a system to which we only grant access in accordance with our access control policy, so that no unauthorized persons can misuse or modify source code.	Implemented
A.10.1.1	Policy on the use of cryptographic controls	Yes	We have a policy to encrypt information – both when it is stored and when it is sent. This ensures that we protect critical information appropriately against spying.	Implemented
A.10.1.2	Key management	Yes	We have a policy for the use of cryptographic keys, because encrypted and authenticated information is only as secure as the custody and use of its keys.	Implemented
A.11.1.1	Physical security perimeter	Yes	We have defined physical security zones in which specific information security rules apply. This ensures that security-critical information cannot be compromised on our premises.	Implemented
A.11.1.2	Physical entry controls	Yes	We make sure that our security zones are protected in an appropriate way. In this way, we improve the security of the information and devices in the zones.	Implemented
A.11.1.3	Securing offices, rooms and facilities	Yes	We protect our offices, rooms and facilities so that no information worth protecting can be compromised here.	Implemented
A.11.1.4	Protecting against external and environmental threats	Yes	We take care of adequate protection against natural disasters and malicious attacks, so that we do not lose valuable information due to these incidents.	Implemented
A.11.1.5	Working in secure areas	Yes	We have established procedures that apply to work in secure areas so that we do not unintentionally compromise the security of sensitive information here.	Implemented
A.11.1.6	Delivery and loading areas	Yes	We have defined access points to our premises and monitor them to ensure that no unauthorized persons can enter at these points and compromise information security.	Implemented
A.11.2.1	Equipment siting and protection	Yes	To ensure that important equipment and other resources do not fail, we make sure that they are securely installed.	Implemented
A.11.2.2	Supporting utilities	Yes	We design and protect supply lines (electricity, water, etc.) in such a way that failures and leaks do not occur or, if they do, that they do not compromise the security of the information requiring protection.	Implemented
A.11.2.3	Cabling security	Yes	We protect data transmission lines to ensure that they are not interrupted or tapped, and that sensitive information is not compromised.	Implemented
A.11.2.4	Equipment maintenance	Yes	In order to prevent the failure of devices that are important for the security of information, we ensure that they are professionally maintained in accordance with the specified intervals.	Implemented
A.11.2.5	Removal of assets	Yes	Anyone who wants to remove devices or other assets from their intended locations must arrange this in advance. This ensures that we always know where important devices are and detect their loss early so that we can react.	Implemented

GAMS

GAMS

ISO27001:2013 Statement of Applicability

Revision 1

Date: January 19, 2024

ID	Control	Applicable	Reason for application or exclusion	Status
A.11.2.6	Security of equipment and assets off-premises	Yes	When devices are removed (and operated away from their actual location), we have rules that specify how they must be secured so that sensitive information processed with them is not compromised.	Implemented
A.11.2.7	Secure disposal and re-use of equipment	Yes	We erase devices that contain storage media before we dispose of or recycle them. In this way, we ensure that no information requiring protection (including copyright protection) is stored on them.	Implemented
A.11.2.8	Unattended user equipment	Yes	To prevent unauthorized persons from accessing unattended devices that are important for information security, we protect such devices in an appropriate manner when they are not being monitored by employees: By locking them away, by locking them up, and by other appropriate measures.	Implemented
A.11.2.9	Clear desk and clear screen policy	Yes	To ensure that sensitive information cannot be compromised among employees, we have a "clean desk policy".	Implemented
A.12.1.1	Documented operating procedures	Yes	If information security depends on operating procedures on devices or systems being followed precisely, then we document these operating procedures.	Implemented
A.12.1.2	Change management	Yes	We ensure that important processes, information systems and the like are not changed "just like that", because this can jeopardize information security.	Implemented
A.12.1.3	Capacity management	Yes	If the utilization of certain resources (systems, employees) is important for information security, we monitor them to identify trends towards overload at an early stage and to be able to counteract them.	Implemented
A.12.1.4	Separation of development, testing and operational environments	Yes	We deliberately separate development, staging and production systems so that changes to one cannot have unexpected consequences on the information security of the other.	Implemented
A.12.2.1	Controls against malware	Yes	We implement anti-malware measures on all systems where this is reasonably possible, so that the systems are hardened against malicious attacks and can maintain information security.	Implemented
A.12.3.1	Information backup	Yes	To ensure that important information is not lost, we have a backup policy for all information whose availability requires protection.	Implemented
A.12.4.1	Event logging	Yes	To be able to evaluate, either in advance or forensically, which events affect our systems, we log important events on production systems.	Implemented
A.12.4.2	Protection of log information	Yes	The log information is in turn secured so that it cannot be falsified, deleted, or disclosed, either consciously or unconsciously.	Implemented
A.12.4.3	Administrator and operator logs	Yes	Logging of user and administrator activities ensures that activities can be traced and assigned later if required.	Implemented
A.12.4.4	Clock synchronization	Yes	To correctly use log information for analysis, we synchronize the clocks of all systems that generate log information.	Implemented
A.12.5.1	Installation of software on operational systems	Yes	To prevent critical information systems from failing unexpectedly or not working as required, we ensure that new or modified software is not simply installed on them.	Implemented
A.12.6.1	Management of technical vulnerabilities	Yes	We obtain information about technical vulnerabilities in the systems we use so that we can remedy them quickly and prevent sensitive information from being compromised.	Implemented
A.12.6.2	Restrictions on software installation	Yes	An installation policy implemented in the organization ensures that the risk of unknowingly installing malware is reduced.	Implemented
A.12.7.1	Information systems audit controls	Yes	If our production systems are to be audited, we will ensure that this does not happen during peak business hours so that we can ensure the availability of our systems for our customers even during the audit.	Implemented
A.13.1.1	Network controls	Yes	We design and manage the networks used by our production systems so that they do not fail abruptly or cannot handle the expected traffic.	Implemented
A.13.1.2	Security of network services	Yes	We consider what network services we need (both internal and external) and ensure that they are available so as not to be taken by surprise.	Implemented
A.13.1.3	Segregation in networks	Yes	Where necessary, we separate the networks in which our employees work and the networks in which our productive systems operate so that they cannot interfere with each other.	Implemented
A.13.2.1	Information transfer policies and procedures	Yes	To ensure that employees know how to protect which information when it is transferred, we have established transfer guidelines that can be referred to at any time.	Implemented
A.13.2.2	Agreements on information transfer	Yes	We reach agreements with our partners on how critical business information is transferred so that it is adequately protected during the transfer.	Implemented
A.13.2.3	Electronic messaging	Yes	We also protect sensitive information when we send it in electronic messages. We do this because the rapid exchange of information via messages/chats is important to us and is used frequently – which is precisely why it needs to be secure.	Implemented
A.13.2.4	Confidentiality or non-disclosure agreements	Yes	We use non-disclosure agreements to ensure that we always keep secret what is important to us or our customers.	Implemented
A.14.1.1	Information security requirements analysis and specification	Yes	We analyze what information security requirements we have for the systems we develop (or buy in) so that we can implement them.	Implemented
A.14.1.2	Securing application services on public networks	Yes	We protect our online systems so that they are secure from fraudulent attacks that cause us to be unable to meet our contracts with our customers.	Implemented
A.14.1.3	Protecting application services transactions	Yes	We protect all transactions that our customers perform with our applications so that they remain complete, unaltered, authentic, and confidential.	Implemented

GAMS

GAMS

ISO27001:2013 Statement of Applicability

Revision 1

Date: January 19, 2024

ID	Control	Applicable	Reason for application or exclusion	Status
A.14.2.1	Secure development policy	Yes	We have a software development policy and require everyone who develops software for us to apply it so that software is developed securely.	Implemented
A.14.2.2	System change control procedures	Yes	We don't change the systems we use to develop software or the software products we develop “just like that”, but only after thorough testing of what we change - because we know that changes can also mean information security leaks. And we want to avoid that.	Implemented
A.14.2.3	Technical review of applications after operating platform changes	Yes	When we update the operating systems used in development, we check that our development systems still function without errors - because we know that failure to behave correctly can lead to information security leaks.	Implemented
A.14.2.4	Restrictions on changes to software packages	Yes	We do not update software packages “because we can”, but because we see the need. We have tested the new packages in advance.	Implemented
A.14.2.5	Secure system engineering principles	Yes	We have principles for the development of secure systems. We apply these to ensure that the systems we develop are also secure.	Implemented
A.14.2.6	Secure development environment	Yes	We secure the development environments we use as much as possible to prevent introducing security risks.	Implemented
A.14.2.7	Outsourced development	Yes	We outsource development activities to partners. We monitor them because we want to ensure that the systems they develop are as secure as we need them to be.	Implemented
A.14.2.8	System security testing	Yes	We test all the security functions of the systems we develop so that we can be sure they work as intended.	Implemented
A.14.2.9	System acceptance testing	Yes	An acceptance test on a representative infrastructure ensures that the production system is more likely to be available after the update.	Implemented
A.14.3.1	Protection of test data	Yes	We make sure that test data does not contain any confidential data stemming from a production environment.	Implemented
A.15.1.1	Information security policy for supplier relationships	Yes	If our service providers need to access our organization's assets, we regulate this in advance to ensure that no security gaps occur.	Implemented
A.15.1.2	Addressing security within supplier agreements	Yes	We conclude contracts with all service providers relevant to information security that contain the obligations of the service providers regarding information security.	Implemented
A.15.1.3	Information and communication technology supply chain	Yes	In the contracts, we include provisions relating to information security risks that occur or may occur at service providers, because we also want to avoid information security risks when they occur at our service providers.	Implemented
A.15.2.1	Monitoring and review of supplier services	Yes	We continuously check whether our service providers adhere to the information security regulations agreed with them, so that we can be sure of this.	Implemented
A.15.2.2	Managing changes to supplier services	Yes	Services provided by our suppliers may change: we keep this in mind so that we can adapt the information security arrangements in the case with our service providers.	Implemented
A.16.1.1	Responsibilities and procedures	Yes	We have established a procedure that enables us to respond quickly and reliably to information security incidents. This is important to us to be able to resolve information security incidents quickly.	Implemented
A.16.1.2	Reporting information security events	Yes	We ensure that information security events and incidents are reported and handled as quickly as possible through the above procedures, because this ensures that we restore security as quickly as possible if it does become compromised.	Implemented
A.16.1.3	Reporting information security weaknesses	Yes	We encourage our employees and service providers to report information security incidents and events promptly so that we can address them quickly and effectively.	Implemented
A.16.1.4	Assessment of and decision on information security events	Yes	We evaluate each information security event (i.e., any suspicion that the information security goals have been compromised) to determine whether it is an incident (i.e., information security has been demonstrably compromised) to respond adequately.	Implemented
A.16.1.5	Response to information security incidents	Yes	We ensure that we respond adequately to identified information security incidents so that they are remedied as quickly as possible.	Implemented
A.16.1.6	Learning from information security incidents	Yes	We ensure that we specifically learn from previous information security incidents so that they do not occur again in the future if possible.	Implemented
A.16.1.7	Collection of evidence	Yes	In the event of an acute information security incident, all employees and service providers are required to collect evidence to simplify the assessment of the incident or to be able to reconstruct it later.	Implemented
A.17.1.1	Planning information security continuity	Yes	We have determined in which exceptional situations we want to maintain which level of information security, so that we can communicate this to our interested parties and in particular contractual partners and focus on maintaining the defined information security.	Implemented
A.17.1.2	Implementing information security continuity	Yes	We establish procedures to ensure information security in the defined exceptional situations so that we can respond when necessary.	Implemented
A.17.1.3	Verify, review and evaluate information security continuity	Yes	We test the above procedures to make sure they work when we need them.	Implemented
A.17.2.1	Availability of information processing facilities	Yes	We plan the infrastructure we need in such a redundant way that the risks arising from failure can be reduced to an acceptable level.	Implemented
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes	We collect all the legal, contractual and regulatory requirements that apply to us with regard to information security so that we know which requirements we have to meet from this perspective.	Implemented

ISO27001:2013 Statement of Applicability

Revision 1

Date: January 19, 2024

ID	Control	Applicable	Reason for application or exclusion	Status
A.18.1.2	Intellectual property rights	Yes	We have procedures in place to ensure that we use copyrighted works as intended or in accordance with the contract.	Implemented
A.18.1.3	Protection of records	Yes	We store documents as required by applicable laws, contracts and other regulatory requirements to ensure information security in this area.	Implemented
A.18.1.4	Privacy and protection of personally identifiable information	Yes	We adhere to the GDPR regarding personal data.	Implemented
A.18.1.5	Regulation of cryptographic controls	Yes	We adhere to all applicable cryptography regulations – both minimum and maximum permitted cryptography – to ensure the compliant operation of our software products throughout.	Implemented
A.18.2.1	Independent review of information security	Yes	We have our information security policies reviewed by independent external bodies (e.g., certification organizations) to ensure that we do not overlook anything important.	Implemented
A.18.2.2	Compliance with security policies and standards	Yes	We check internally whether all our employees adhere to the specified rules on information security so that they do not just pay lip service to them.	Implemented
A.18.2.3	Technical compliance review	Yes	We also review the information systems we use to ensure that they comply with all security policies to prevent unintentional information security leaks.	Implemented