ATOSS

CODE OF SUPPLIER INFORMATION SECURITY

Security information

Public version of 04-2024

As an international software company, ATOSS must comply with high information security requirements.

This Code of Supplier Information Security is a necessary component of our information security management to guarantee the highest possible information security for our end customers. In accordance with the ISO/IEC:27001 standard, we are also obliged to address our applicable information security standards in the contractual relationships with our business partners, temporary workers and suppliers (in short: **suppliers**).

The following security information is intended to inform you about our security standards and to ask you to observe these standards in your business relationship with ATOSS.

You can access the current Code of Supplier Information Security (CoSS) at any time on the ATOSS security website.

We kindly ask you to take note of and observe this information.

Thank you for your support!

Your ATOSS IT Compliance Team

A. Information security

The following security standards are a cornerstone of our supplier management based on the ISO/IEC 27001 certification.

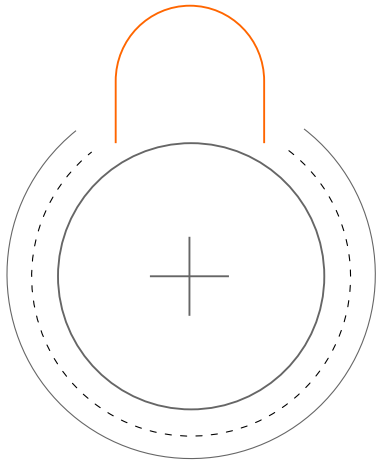
We provide an overview of our understanding of information security and our principles that we expect from our suppliers about the provision of information and communication technology (ICT) services. This applies if suppliers work at ATOSS locations or work via remote access at ATOSS or if they process sensitive information on behalf of ATOSS.

Our Code of Supplier Information Security is to be understood as a common orientation framework that helps to realize an appropriate information security strategy in projects and supplier relationships.

The responsibility for maintaining and monitoring our internal information security structures lies with the commissioning ATOSS department as business owner.

At the same time, we expect our suppliers to maintain close contact with us and to support us with the essential requirements in all project phases, including ongoing operations and during the entire contractual term of the supplier relationship in the mutual interest of a secure service relationship and to ensure compliance with the following security information.

ATOSS has the right to issue supplementary security instructions on the type, scope and procedures of the company's activities at any time.



When providing services, our suppliers shall comply with the following security principles:

State of the art: Considering the specific service provision, our suppliers shall take appropriate security measures in accordance with the current state of the art and continuously monitor their effectiveness. This requirement serves to ensure an appropriate level of security in favor of the confidentiality, integrity, availability and resilience of ATOSS systems and the sensitive information involved.

In order to meet this requirement in a comprehensible manner, the organizational and technical security measures should be based on established technical guidelines and best practices, such as the TeleTrust and BSI guidelines, applicable ISO standards or other relevant legal and industry-specific requirements (e.g. information security requirements for critical infrastructures, etc.).

Correct handling of sensitive data: Protection class concepts presented by ATOSS for the correct handling and classification of digital and physical data must be considered. In particular, the processing of sensitive documents is only permitted with the consent of the internal ATOSS contact person and within the framework of the confidentiality agreement.

Correct use of IT systems: Only hardware, networks and applications approved by ATOSS IT are to be connected to the company IT network. This also includes VPN connections approved by ATOSS IT or the use of the guest Wi-Fi. In case of doubt, the supplier bears the burden of proof for the approval granted.

As a rule, image, video and sound recordings (e.g., using smartphones, video cameras) are not permitted at ATOSS locations. Exceptions require documented permission. Taking screenshots or recording sessions via remote access is not permitted.

Data processing: If ATOSS data is hosted by suppliers or approved sub-suppliers, ATOSS data shall be stored, processed and transmitted separately from the data of other customers. If a supplier commissions a sub-supplier to carry out certain processing activities, this commission must be made by means of a contract that essentially imposes the same data protection and information security obligations on the sub-supplier as those that apply to the supplier.

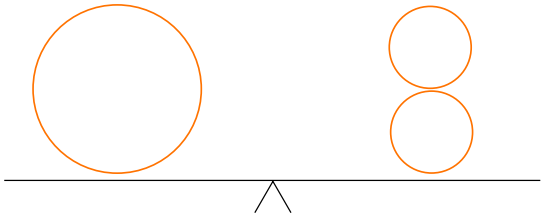
Reporting of security issues: An essential part of our information security management is the timely notification of security issues so that ATOSS can take appropriate measures. It is therefore crucial for ATOSS that security issues are reported to ATOSS immediately, stating the facts of the case. The online contact form can be found here.

B. Personal security requirements

When deploying personnel, our suppliers shall comply with the following security principles:

Contact point for information security: A contact point responsible for information security must be named to whom information security issues can be communicated via generally accessible sources (e.g., contact ID on website). If a contact point is not possible via generally accessible sources, the supplier shall provide other contact options and keep them up to date.

Qualification: Only trustworthy and qualified personnel shall be tasked with the provisioning of services (e.g., administration of IT systems, internal maintenance work). Personnel changes shall be reported.



Trainings: The supplier shall ensure through regular training on information security and data protection that the personnel provisioning services to ATOSS have been made aware of their responsibilities and obligations about information security and are familiar with the relevant provisions on information security, data secrecy and data protection.

Confidentiality: Any person working for the supplier to whom sensitive information from ATOSS must be disclosed in the course of service provision must be bound to confidentiality by the supplier. This confidentiality obligation shall continue to exist after the end of the contractual relationship and can be proven at any time upon request.

Disclosure: The supplier shall pass on this security information and the relevant data protection and information security requirements from the service contract with ATOSS to the personnel tasked with the service provision. The same applies if ATOSS issues supplementary security instructions on the type, scope and procedures of the company's activities.

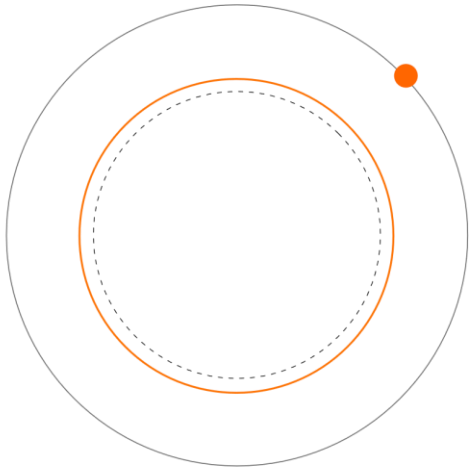
C. Security of IT systems and networks

Secure operating environments: Where suppliers' IT systems or networks are used for the generation, transmission or storage of ATOSS data, our suppliers shall take suitable appropriate security measures for their IT systems and network in accordance with the current state of the art and monitor these on an ongoing basis.

Our suppliers shall have the following minimum measures in place about ATOSS data:

- Patch, capacity and vulnerability management
- Data backups
- Access and authorization management
- Rights and role concepts
- Secure password management
- Communication security
- Use of cryptography
- Malware protection
- Active logging and monitoring
- Physical security precautions (e.g., protection against heat, fire and water for relevant information-processing IT systems)
- Emergency management

Security audits: Our suppliers can prove compliance with these minimum measures to ATOSS at any time. As a rule, proof can be provided by submitting a test certificate, an audit report from independent bodies (e.g., auditor, revision, data protection auditor, pen test report) or a certification - e.g., according to ISO/IEC:27001 or BSI standards. Upon request and in justified cases, ATOSS reserves the right to carry out independent security audits.



D. Secure software development

Suppliers who provide services in connection with our software development or license software programs to ATOSS should ensure compliance with the following software development principles:

Secure software development environment: Programs should be developed in a secure development environment (e.g., access concept to source code, version control). Secure repositories should be used.

Guidelines for secure software development: The developers of our suppliers should consider security guidelines and best practices for secure software development (e.g., security and privacy by design, principle of least privilege, segregation of duties).

Code reviews: Based on a defined software development methodology, our suppliers should ensure regular reviews (e.g., code reviews) of the software programs they license and address any weaknesses identified.

Software maintenance: Software maintenance and support may only be carried out via remote access authorized by ATOSS IT. All remote accesses must be logged.

Documentation obligations: Relevant documentation requirements should be contractually considered.

ATOSS.COM