SAG

Progress in Aluminium

Guideline

Information security requirements for external IT partners

January 2025

GUIDELINES

Modification History

Version	Creation Date	Valid From	Change
1.0	15.01.2025	31.03.2025	Initial Version

1. Introduction and scope of application

The SAG Group (hereinafter referred to as SAG) is one of the most reputable manufacturers of aluminium tanks, lightweight components for vehicle construction and cryogenic tank systems for LNG. With more than 950 employees at various locations in Europe, Mexico and the USA. SAG is established worldwide as a reliable partner of the major OEMs in many industries and, as a technology leader and innovator, is an important contributor to sustainable mobility with its products and services.

The Information Security Requirements guideline ensures that external IT partners working for SAG maintain the integrity and security of our information resources. It describes the measures and requirements for external IT partners to ensure the confidentiality, integrity and availability of sensitive information.

This document regulates SAG's procedure for selecting, monitoring and working with external IT partners to ensure information security. It contains measures for the procurement of systems. The aim is to establish sustainable and mutually acceptable relationships with external IT partners without jeopardizing the security of SAG information.

The guideline applies to all external IT partners who receive access to sensitive information or provide services that may have an impact on our company's information security. This includes both short-term and long-term partnerships and projects.

2. General requirements

The following requirements apply to all external IT partners.

2.1 Contact person for information security

Designate a contact person for information security and provide SAG with their contact details. This person has the necessary technical knowledge of information security issues and is responsible for implementing security measures and requirements. This person is available for SAG‘s inquiries about information security. Questions regarding information security may be addressed to our Information Security Officer at iso@sag.at or to your contact person in supplier management.

2.2 Security Management

Implement and maintain security practices that meet the established standards for your business environment and industry. Integrate these practices into a mature information security program and continuously improve them. For example:

- Ensuring confidentiality and integrity when processing SAG data and information.
- Ensuring the availability of systems, information and your services by implementing mechanisms such as failover, redundancy and resilience.
- Compliance with all applicable data protection regulations, e.g. when exporting, exchanging or processing data or in the case of data retention or deletion requirements.

2.3 Personnel

You are responsible for ensuring that each person you employ (e.g. management, employees, subcontractors) complies with this guideline and:

- understands their responsibilities and is suitable for their assigned role,
- maintains the confidentiality of shared information (on-site and off-site, while traveling),
- keeps their physical workstation free of confidential documents and locks their device when it is unattended to prevent unauthorized access (“Clean Desk/Clean Screen”),
- devices that store or process SAG information are used securely to prevent unauthorized persons from viewing or accessing the information. Special care must be taken when using mobile devices.
- understands the importance of information security practices, data protection and the specific requirements of this guideline. To this end, you will conduct regular training and awareness programs.
- takes appropriate corrective action in the event of misuse or disclosure of SAG information and informs SAG immediately within 24 hours of becoming aware of it

- promotes a culture of responsibility for information security and data protection.

2.4 Information management

This section describes the requirements for the transfer, transportation, storage and handling of information.

2.4.1 Transfer & transport of information

- Consider the criticality of information and systems when transporting information.
- In general, only use secure methods to transfer information. If you have access, preferably use the SAG services (e.g. OneDrive, email from SAG, etc.) und send links instead of the files themselves.
- Make sure that sensitive information is only transmitted in encrypted form.
- Ensure that receiving capabilities are available for information that is transmitted with encryption. The technical requirements are coordinated with SAG.
- Inform yourself about country-specific regulations on the use of security technologies (e.g. encryption) before traveling abroad.

2.4.2 Storage & handling of information

- Do not move, modify, process or delete any information stored on SAG systems, without prior approval from SAG
- Do not pass on any information received from SAG to third parties without prior written approval from SAG.
- Save or process SAG information only on systems managed by SAG IT.
- Only save or process SAG information on data services that have been authorized by SAG.
- Keep access permissions for files shared on file services up to date and restrict access to those who need it.
- Separate SAG information from other customer and third-party information.
- Protect storage media (e.g. USB sticks, hard drives) against loss, destruction, mix-ups and unauthorized access.
- Dispose of storage media that are no longer required in a safe manner.
- At the end of the collaboration, return the information you have received from SAG and delete it from your own IT systems or storage media if necessary. Observe all legal and, if applicable, contractual requirements (e.g. retention periods).

2.5 Security incidents

Security incidents can occur. Therefore, in addition to preventive measures, you must establish suitable detection and response processes to deal with security incidents.

- Have an emergency plan ready for dealing with IT security incidents.
- Collect, store and analyze log data to ensure that security incidents and reportable events are identified and processed. Reportable events include in particular:
    - Unusual/suspicious system behavior (unexpected restart, data deletion, etc.)
    - Uncontrolled user behavior (unusual / unintended account activity / account takeover)
    - Extensive malware attack
    - Loss of storage media or end devices
    - Loss of information
    - Disclosure of information to unauthorized third parties
    - Break-in into the company building.
- Report security incidents or incidents involving information from SAG to your contact person in the supplier management and to iso@sag.at immediately. Even if you are unsure about the type, scope or other aspects, inform SAG within 24 hours after becoming aware of the incident so that we can take appropriate measures together.
- After you have reported the incidents to SAG, SAG will determine appropriate corrective measures.
- Work with SAG at all times when an investigation is required and implement remedial action promptly to minimize the impact of the information leakage.

2.6 Vulnerability- & patch-management

Consider this guideline when procuring systems and ensure that they are properly maintained and kept up to date. Appropriate controls identify and mitigate vulnerabilities in your network, system and software.

- Create a patch management schedule and controls to identify, test and deploy all required patches.
- Maintain transparency in your technical environment and stay informed about vulnerabilities.
- Scan for vulnerabilities regularly and consider penetration testing, red-teaming, bug bounty and other tests to identify vulnerabilities early on.
- Plan patching and remediation based on the criticality (potential impact and likelihood of exploitation) of all identified vulnerabilities.

- Consider testing changes in development and quality environments before rolling out to production systems.

- Apply security patches as soon as they are available, unless you can rule out negative effects. Track all non-remediable vulnerabilities, maintain a list of compensating controls that mitigate the vulnerabilities, and regularly review the status.

- Aim to distribute patches or updates automatically and centrally.

2.7 Compliance-Management

Consider legal, organizational and contractual requirements (including resource management, internal control system, IT continuity management and information protection) to cover all SAG information, hardware and software e.g:

- Respect intellectual property rights, such as copyrights for software, texts, images, trademarks, patents and source code.

- Properly license any software you use to perform services for SAG before entering into an agreement with SAG.

- Comply with applicable laws and regulations on data protection (if necessary, conclude a data processing agreement wit SAG).

- Regularly review and update your own organizational policies and regulations to comply with contractual requirements.

3. Additional requirements – IT partners with direct access

The additional requirements in this section apply to you if you fall into one or more of the following categories:

- You receive an end device (Windows/Mac/Smartphone), owned and managed by SAG.

- You are connected to a SAG network via remote access/VPN, a physical connection or a SAG WLAN (except the guest WLAN).

- You access SAG data and SAG services at system or database level.

3.1 Security of end device

To ensure security of SAG data, it is important that all end devices meet the specified minimum requirements.

3.1.1 Use

- If provided, only use the SAG end device.
- Use it exclusively for contractually agreed purposes.

- Process data only to the extent necessary for fulfillment of SAG's orders. Any other processing of our data is prohibited..
- Protect the device against loss or unauthorized use (always keep the device with you or in a safe place).
- - Private use is prohibited.

3.1.2 Changes, updates und patches

- Do not open the end device.
- - Hardware changes are not permitted.
- - Software changes can only be made via SAG IT.
- Apply updates and patches offered by SAG IT without delay.

3.1.3 Backup

- Save SAG information on the assigned storage systems and not on a local, unsynchronized hard drive/folder. In this way, we can guarantee a centralized and automatic backup.

3.1.4 Encryption

- The hard disk on the device is fully encrypted.

3.1.5 Malware-Schutz

- Do not make any changes to the security software installed on the end device.
- Do not use the end device if you suspect that it is infected with malware. Inform SAG immediately.

3.2 Return of the device/Loss of the device

Return the assigned devices immediately to SAG if they are no longer required or at the end of the order. Report the loss of devices immediately to the IT support of SAG.

3.3 Access Control

3.3.1 Access to SAG-systems

- Access to SAG systems and SAG data is based on access controls and authorization mechanisms and follows the principle of necessity.

- Only use your personal access data and do not share it.

- Only access SAG systems and SAG information when necessary and in accordance with our instructions. Access to unauthorized areas is prohibited.

- Only access systems via approved technical solutions or connections provided by SAG.

- Inform SAG immediately about any changes such as change of role, responsibilities or changes in personnel (e.g. termination of employment relationships).
- If possible, use biometric authentication (fingerprint, facial recognition, etc.) to prevent unauthorized access to passwords by third parties.
- To avoid unforeseeable consequences, bypassing security mechanisms on SAG systems is prohibited.

3.3.2 Password requirements

To prevent unauthorized access to SAG information, protect all devices that process information by using state-of-the-art passwords.

3.3.2.1 Password creation

- The password contains at least sixteen characters.
- The password is a combination of upper and lower case letters, numbers and special characters.
- - The password does not correspond to a dictionary word or name.

3.3.2.2 Protection of passwords

- Never share passwords for user accounts and keep them confidential.
- Save passwords for SAG systems only in special environments (e.g. Privileged Access Management (PAM) for administrator accounts) if this has been expressly agreed. Do not save these in a browser or a file.
- Only use unique and individual passwords. Do not reuse the same password for private or business purposes.
- Do not use passwords that contain personal references (e.g. name or position, date of birth, etc.).
- Always use a second factor if the system allows this. Keep the second factor confidential and secure. The same requirements apply as for the password itself.
- If you suspect that a password has been compromised, please inform SAG and change the password immediately.

Depending on the type of data processing or service, SAG may impose stricter requirements for the assignment of passwords. You are responsible for informing yourself about these requirements in advance and implementing them.

3.4 Network security & firewall

If you are accessing SAG systems or SAG data from your network, please note the following:

- Use suitable firewall protection and ensure that routing through the device is not possible. Check the configuration regularly.
- Consider the criticality of the underlying systems and information when configuring and using the firewall.
- Monitor your network for unusual activity and anomalies and take appropriate action.

3.5 Access to SAG Premises

If you are working on SAG premises, you must comply with the relevant local SAG regulations on bringing your own end devices onto SAG premises or into secured areas.

Some general rules:

- - Keep our premises clean and act responsibly.
- - Do not share your access token/key.
- If you lose your access token/key, inform SAG immediately.
- Do not bring visitors or other external personnel to our premises.

4. Consequences of violation

Non-compliance with statutory or internal company regulations can not only cause considerable damage to our entire Group, but also have serious **consequences** for each individual.

We therefore do not hesitate to take action in the event of such violations and to act appropriately to clarify the facts. In the event of a violation, remedies provided by national applicable laws, and contractual agreements may be taken. SAG also reserves the right to claim damages and civil action.

Exceptions to these guidelines must be documented and communicated to the Information Security Officer.

5. Contact information

In the event of suspicion or knowledge of violations of statutory or internal regulations, each individual is required to report this to the contact persons named.

In addition, our Integrity Line offers an additional channel for reporting perceived violations and misconduct confidentially or anonymously. The **Integrity Line** can be accessed via our corporate website.

We assure special protection and support to all persons who make a report in good faith. This also applies if a report proves to be incorrect in terms of content but was made in good faith.

Questions regarding this guideline, please contact:

Viktor Kanizsai

Information Security Officer

SAG Group | Austria

SAG New Technologies GmbH, Lend 25, 5651 Lend

Kontakt ISO: iso@sag.at