



Progress in Aluminium

Guideline

Information Security Requirements for External Consultants

January 2025

COMPLIANCE
The Power of Integrity

GUIDELINES

Modification History	2
1. Introduction and scope of application	3
2. Security Awareness at SAG	4
3. Responsibility.....	4
4. Email-security	4
5. Reporting of suspicious incidents.....	4
6. Accounts, passwords, access.....	4
7. End device	5
8. Consequences of violation	5
9. Contact information	5

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 aluminum 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 consultants working for SAG maintain the integrity and security of our information resources. It describes the measures and requirements for external consultants to ensure the confidentiality, integrity and availability of sensitive information.

This document describes how we ensure information security when selecting, monitoring and working with external consultants. The aim is to establish sustainable and mutually acceptable relationships with external consultants without jeopardizing the security of our information. The guideline applies to all external consultants who have access to sensitive information or provide services that may affect the information security of our company. This includes both temporary and permanent consultancy contracts.

We have clear standards regarding ethics, morals and respect, which we also expect from our business partners. Compliance with applicable laws and internal rules is a prerequisite for doing business with SAG-Group.

2. Security Awareness at SAG

SAG has granted you access to its premises, systems, networks and information. We expect absolute discretion. We expect comprehensive responsibility. By this we mean:

3. Responsibility

- Protect the confidentiality of SAG. Only use documents for the purposes permitted by contract and do not pass on internal information to third parties.
- Protect your screen and documents from prying eyes. Only speak in protected areas, especially when you are outside SAG premises
- Act only in the name of SAG, if explicitly instructed to do so.
- If SAG Security Mechanisms are circumvented, we will terminate business relationship immediately and draw the legal consequences.
- Store SAG data exclusively on the business applications and platforms provided by SAG IT.

4. Email security

- Email messages may contain links to criminal websites. Attachments may contain viruses. Be careful when opening attachments and links. Hover your mouse over a link to check the destination address before clicking on it. Do not enter login data carelessly if you are asked to log in after clicking on an email link.
- Do not reply or react to spam emails. Such emails must be deleted immediately. Many spam emails contain an “unsubscribe” link. Unfortunately, this link is often used maliciously to confirm that your email address exists and that you have received the message. This can lead to receiving even more spam. It is therefore important to only unsubscribe if you are sure that the sender is trustworthy.
- Get in touch with your contact person at SAG Group, if you need dedicated email encryption.

5. Reporting of suspicious incidents

If you note something suspicious, contact your contact person at SAG Group and the local SAG IT Support immediately.

6. Accounts, passwords, access

- Register your SAG account for multi-factor authentication (MFA) and only confirm login requests you have initiated.
- Never share your SAG account or password.
- Use strong and different passwords for SAG, your own undertaking and personal/private accounts.
- Change your SAG password immediately, if there are signs of sharing or misuse.
- Use the approved VPN mechanism for remote access to certain internal SAG services (development and maintenance tasks for apps, IT infrastructure, etc.)

7. End device

- If you receive a device managed by SAG, use it exclusively for work on SAG agenda. Your personal or business smartphone is accepted for MFA.
- Lock your computer, tablet or smartphone when you leave your seat to protect it from unauthorized access.
- Keep your devices with you or in a safe place.
- There is no backup of local data on your device. Always save files to OneDrive, SharePoint, etc.
- Report lost or stolen SAG access tokens/keys, laptops etc. and inform immediately your contact person at SAG Group.

8. 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.

9. 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 person named below.

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 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