Information security policy for service providers

Table of contents

Document history

Classification	Public
Next update	3rd quarter 2026

Version	Date	Processed by	Amendment
1.0	4.05.2022	Sven Meier	Creation of the document
1.1	27.7.2022	Tobias Vejda	Review and content update
1.2	25.08.2022	Sven Meier and Till Neßeler	Adaptation of section 3.1 Regulation due to special protection requirements
1.3	07.11.2022	Nico Lepel	Classification corrected
1.4	06.05.2024	Tobias Walter	Content update and CI adaptation

Examination

Checked by	Version	Date
Sven Rössig	1.4	14.11.2025

Release

Released by	Version	Date
Tobias Walter	1.4	17.11.2025

Preamble

(A) Gender-neutral wording

In the interest of better readability, the masculine and feminine forms are not used simultaneously. Irrespective of this, the formulations apply equally to the female, male and diverse genders.

(B) Scope of application

This security policy is mandatory for all service providers and their employees (simply referred to as "service providers") who access Avantgarde's IT systems and IT infrastructure in person or via remote maintenance. These guidelines are to be understood as a minimum requirement for the provision of services within Avantgarde.

If these minimum requirements cannot be met by service providers, Avantgarde will initiate suitable measures together with service providers in order to achieve the common goal.

(C) Current version

Avantgarde reserves the right to update this policy. The current version will always be published on the Avantgarde website https://avantgarde.net/en/

1 Objective

The potential risk can only be countered by implementing suitable safety standards. In order to do justice to this, the following overarching objectives must always be pursued:

- the protection of confidential information/data of both employees and business partners of Avantgarde and the associated confidential treatment of data
- the availability of data and applications and the technical and spatial IT infrastructure
- compliance with the integrity of data and IT systems
- the backup and recovery of data/IT infrastructure in the event of a failure or disaster
- Minimizing the downtime of IT systems
- ensuring the good reputation of the company in the public eye
- avoiding massive financial and immaterial consequences for the company and for employees due to breaches of contractual agreements or laws.

All information security measures must be economically justifiable in relation to the value of the information and IT systems worthy of protection.

2 Measures

Appropriate measures must be taken to achieve these objectives, which are as follows.

2.1 Regulation due to special protection requirements

All roles for which a service provider and / or freelancer etc. is responsible.

1. Access to the internal network is required (e.g. data access to on-premise share, printer access),
2. must process particularly sensitive employee data (e.g. accounting or HR),
3. Administrative access to IT systems required (e.g. admin in IT)

Conditionally, the service provider should use an Avantgarde laptop and is otherwise not allowed to connect to the internal network. Basically, it is a special case decision that is made by the project manager together with IT.

2.2 Structural and organizational measures

- Appointment of responsible persons to assist in determining the protection requirements and compliance with the protection of the respective IT infrastructure.
- To access the IT systems within Avantgarde, personal access data is required for each authorized employee of the service provider.

- Access data must be stored securely and protected against unauthorized access. Disclosure of these access data to other employees or insecure storage of the access data is prohibited.
- Accesses that are no longer required must be reported immediately to Avantgarde's commissioning office so that these accesses can be blocked.
- Protection through entry, access and access controls
- Security areas with a corresponding access authorization concept of the respective Avantgarde company must be observed.
- The use of data processing systems by unauthorized persons must be prevented. To this end, access regulations and access controls must be observed.
- Confidentiality and commitment agreements are part of the service contract. Employees of the service provider must be bound by these agreements, particularly with regard to personal data.
- Raising awareness and motivating employees to work in a safety-conscious manner.
- Induction of employees in line with their tasks and regular training, in particular for the applicable safety measures and correct compliance with them.
- Establishment of an emergency management system and/or at least preparation of an emergency plan in order to be able to react as quickly as possible in the event of a disaster.
- A deletion concept must be in place. The deletion and/or transmission of data after the end of the collaboration or on the instructions of the Avantgarde controller must be ensured at all times.

The aim must be to maintain critical business processes even in the event of a system failure and to restore the availability of the failed IT systems within a tolerable period of time. Cases of damage with high financial consequences must be prevented.

2.3 Technical measures

- Installing an antivirus program: To protect against viruses, worms and other malware (such as Trojans and spyware), an up-to-date antivirus program must be installed on all IT systems of the service provider and the group company. All protection programs are configured and administered in such a way that they provide effective protection and prevent manipulation.
- Operating systems and application software: Service providers must ensure that the IT systems they provide and use are equipped with a maintained operating system and application software.
- Firewall: Service providers must activate a local firewall on the IT systems operated in the company.
- Removable data carriers: The use of removable data carriers is prohibited. Removable data carriers within the meaning of this guideline are in particular
    - USB sticks
    - External hard disks
    - Non-company smartphones.

- Security gaps must be reported immediately to the respective process owners and system administrators and closed as soon as they become known.
- Data backup: Comprehensive and regular data backup, control and verification of the created backups for content, integrity and timing (emergency plan).
- Data loss can never be completely ruled out. Comprehensive data backup therefore ensures that IT operations can be restored at short notice if data is no longer available or is incorrect.
- Company data must generally be stored in such a way that if an employee is absent, their replacement or supervisor can access this data.
- Means of communication: The compliant use of means of communication such as e-mail, Internet, instant messaging, social media, video portals, etc. must be sensitized through guidelines, company agreements and training. Avantgarde data may not be published without authorization.
- Network segmentation through Virtual Local Area Networks (VLANs): A physical separation of sensitive areas or a separation of two companies at one location should always be checked; a possible logical separation via VLAN should also be checked if necessary and set up accordingly. Virtual network separation of individual areas depends on the protection requirements of the areas to be separated. Isolated operation of the IT systems should be possible by means of separation via VLAN. The installation of a VLAN is intended to prevent unauthorized access to the Avantgarde network.

2.4 Monitoring the improvement of security

Information security is regularly reviewed to ensure that it is up to date and effective. In addition, the measures are also regularly examined to ensure that the service provider's employees concerned are aware of them, that they have been implemented and that they are integrated into the operating procedures.

Avantgarde supports the continuous improvement of the security level. Service providers are required to report possible improvements or vulnerabilities to the respective process owner and the system administrator.

The desired level of security and data protection is ensured through continuous review of the regulations and compliance with them. Deviations are analyzed with the aim of improving the information security situation and keeping it constantly up to date with the latest information security technology.

2.5 License management

Only licensed software may be used on all IT systems. The owner of this license is responsible for ensuring that it is valid and up-to-date.

This regulation must be made known to all employees.

The process owners of the various IT systems must ensure that only licensed software is used. Without suitable version control and license control, experience has shown that a wide variety of software versions can quickly be used on an IT system or within an organizational unit, some of which may be used without a license.

The configuration of the installed IT systems must be adequately documented.

To prevent licenses from becoming invalid in the event of hardware defects, hardware-independent licenses should be used wherever possible. This way, an IT system can be replaced with less effort if the hardware fails.

If possible and economically viable, perpetual licenses should be preferred. This can prevent functional restrictions due to license expiry.

The following principles apply:

- Only licensed software may be used; possible test periods of the manufacturer must be observed.
- Only software and hardware that is under maintenance may be used.
- If service providers are manufacturers of this software and/or hardware, they are responsible for appropriate maintenance and must be able to guarantee this.
- Use of company-owned software on non-company computers only with a correspondingly valid license.
- No use of private software or private use of IT systems

The installed versions and the tracking of available licenses and their comparison with the installed number of products must be checked regularly.

3 Information security management system

3.1 Responsibilities and accountabilities

Service providers must ensure that the service is provided in accordance with this directive.

- Service providers must ensure at all times that their own actions and the actions of employees do not impair the availability, integrity or confidentiality of Avantgarde's IT systems and data.
- Copyright and patent regulations and license agreements must be complied with.
- The access data provided may not be passed on to third parties.
- In the case of order processing, a corresponding order processing contract must be concluded. As part of this, employees are encouraged and obliged to comply with legal regulations as well as contractual and internal company requirements for information processing and to report any violations immediately.

3.2 Roles

A role can be understood as a bundling of competencies that are required to perform tasks within an IT-supported business process. A role therefore describes who is responsible for which tasks, with which rights

and obligations. The specific assignment of roles and whether each role is required depends on the IT process in question.

Irrespective of the roles, the management is responsible for ensuring information security in the company, as well as the corresponding resources, in particular technical and personnel resources.

3.3 Behavior in the event of security incidents

Information security incidents must be reported immediately to the process owner. This person organizes the forwarding of information to the other roles mentioned above. In the event of a loss of network or system integrity, the system administrator must rectify these faults as quickly as possible.

Honesty and a willingness to cooperate are particularly important when dealing with security incidents. Reporting security incidents is therefore always viewed positively!

The causes of the security incidents must be analyzed together with the person responsible for the procedure and the system administrator on the basis of the logs created and improvements must be developed. The resulting necessary measures must be implemented. This must be documented accordingly.

The instructions of the person responsible for the procedure must be followed.

3.4 Emergency preparedness

To ensure that a system failure is detected in good time, the system resources and measured values for operational reliability (information on temperature, CPU utilization and free memory space, general availability) must always be monitored for critical values. If possible, a monitoring system with an automatic notification function should be installed and used for this purpose.

All insurance policies, purchase contracts and contracts with service providers are regularly reviewed with regard to the agreed SLAs.

The network, telecommunications and the necessary components must be designed, installed and configured in such a way that they meet the requirements for confidentiality, integrity and availability of the information to be transmitted.

Depending on the protection requirements, any necessary network separation, encrypted transmission and redundant installation of the critical infrastructure systems must be taken into account. The individual components should be selected, configured and documented in such a way that they correspond to the current "state of the art".

The cabling must be fully documented (physical topology, installation plans, labeling of the devices).

An emergency preparedness concept and emergency plan must be drawn up and reviewed at regular intervals and expanded if necessary. The following information should be included in the emergency concept/plan:

- Network and system documentation (including configurations).
- Licenses.
- Maintenance contracts, replacement of hardware in the event of a defect and regular review of the SLA contracts with the supplier/service provider.
- Behavior in an emergency (incl. shutdown and system start sequence).
- Alarm and escalation plan.

4 Workstation setup for remote maintenance

4.1 Remote maintenance / VPN

External access to Avantgarde's networks may only take place via a VPN tunnel or remote maintenance software approved by Avantgarde.

No freeware tools are to be installed for remote maintenance via remote connection. Only the standard software from Avantgarde is to be used for the remote connection. If no group standard is defined, the software described by the respective company must be used.

Service providers must ensure that their own network does not allow uncontrolled access by third parties to Avantgarde's network

- Protocol obligation
- Access via remote maintenance must be logged. As a minimum, the changes and activities carried out via remote access should be logged.
- At least upon request, service providers must be able to provide proof of the purpose for which certain accesses were made.
- Data may only be transferred after authorization
- Service Providers may only copy data to or extract data from Avantgarde's IT systems via access for which authorization has been granted. No unauthorized software may be installed and/or information may be extracted or removed from the IT systems.
- Changes to systems only after approval
- Service providers may only modify Avantgarde IT systems after consultation and approval.

4.2 Access protection / screen lock

Screens must be locked (manually or automatically) when leaving the workstation.

Service providers must properly log out of the system after completing maintenance.