Informationssicherheitsrichtlinie für Dienstleister

Inhaltsverzeichnis

Dokumentenhistorie

Klassifizierung	Öffentlich
Nächste Aktualisierung	3. Quartal 2026

Version	Datum	Bearbeitet durch	Änderung
1.0	4.05.2022	Sven Meier	Erstellung des Dokuments
1.1	27.7.2022	Tobias Vejda	Review und inhaltliche Aktualisierung
1.2	25.08.2022	Sven Meier und Till Neßeler	Anpassung Abschnitt 3.1 Regelung aufgrund besonderem Schutzbedarf
1.3	07.11.2022	Nico Lepel	Klassifizierung korrigiert
1.4	06.05.2024	Tobias Walter	Inhaltliche Aktualisierung und CI-Anpassung

Prüfung

Geprüft durch	Version	Datum
Sven Rössig	1.4	14.11.2025

Freigabe

Freigegeben durch	Version	Datum
Nico Lepel	1.4	17.11.2025

Präambel

(A) Geschlechtsneutrale Formulierung

Im Interesse einer besseren Lesbarkeit wird auf die gleichzeitige Verwendung der männlichen und weiblichen Form verzichtet. Ungeachtet dessen, gelten die Formulierungen gleichberechtigt für das weibliche, männliche sowie diverse Geschlecht.

(B) Geltungsbereich

Diese Sicherheitsrichtlinie ist für alle Dienstleistenden und seine Mitarbeitenden (einfachhalber nur „Dienstleistende“ genannt) verpflichtend, die persönlich oder per Fernwartung auf die IT-Systeme und IT-Infrastruktur von Avantgarde zugreifen. Diese Vorgaben sind als Mindestanforderung für die Dienstleistungserbringung innerhalb von Avantgarde zu verstehen.

Sofern diese Mindestanforderungen durch Dienstleistende nicht erfüllt werden können, wird Avantgarde gemeinsam mit Dienstleistenden geeignete Maßnahmen initiieren, um das gemeinsame Ziel zu erreichen.

(C) Aktuelle Version

Avantgarde behält sich das Recht vor, diese Richtlinie zu aktualisieren. Die aktuelle Version wird jeweils auf der Internetseite der Avantgarde https://avantgarde.net/de/ veröffentlicht.

1 Zielsetzung

Dem Gefährdungspotential kann nur durch die Implementierung geeigneter Sicherheitsstandards begegnet werden. Um diesem gerecht zu werden, sind nachfolgende übergreifende Ziele stets zu verfolgen:

- der Schutz vertraulicher Informationen/Daten sowohl von den Mitarbeitenden als auch von Geschäftspartnern von Avantgarde und damit verbunden auch die vertrauliche Behandlung von Daten
- die Verfügbarkeit von Daten und Anwendungen und der technischen und räumlichen IT-Infrastruktur
- die Einhaltung der Integrität von Daten und IT-Systemen
- die Sicherung und Wiederherstellung von Daten/IT-Infrastruktur im Falle eines Ausfalls oder einer Katastrophe
- die Minimierung der Stillstandzeiten von IT-Systemen
- die Gewährleistung des guten Rufs des Unternehmens in der Öffentlichkeit
- die Vermeidung massiver finanzieller und immaterieller Folgen für das Unternehmen und für Mitarbeitende durch Verstöße gegen vertragliche Vereinbarungen oder Gesetze.

Alle Informationssicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen.

2 Maßnahmen

Um die genannten Ziele zu erreichen, müssen geeignete Maßnahmen ergriffen werden, welche sich folgend darstellen.

2.1 Regelung aufgrund besonderem Schutzbedarf

Alle Rollen für die ein Dienstleister und / oder Freelancer etc.

1. Zugriff auf das interne Netzwerk benötigt (z.B. Datenzugriff auf On-Premise Share, Druckerzugriff),
2. Besonders sensible Mitarbeitenden-Daten verarbeiten muss (z.B. Buchhaltung oder HR),
3. Administrative Zugänge zu IT-Systemen benötigt (z.B. Admin in der IT)

Bedingt, dass der Dienstleister ein Avantgarde Laptop verwenden sollte und es ihr / ihm sonst nicht erlaubt ist sich in das interne Netzwerk einzuklinken. Grundsätzlich ist es eine Sonderfallentscheidung die durch den/ die Projektverantwortliche/n gemeinsam mit der IT getroffen wird.

2.2 Strukturelle und organisatorische Maßnahmen

- Benennung von verantwortlichen Personen zur Mitwirkung bei der Bestimmung des Schutzbedarfes und der Einhaltung des Schutzes der jeweiligen IT-Infrastruktur.

- Für den Zugriff auf die IT-Systeme innerhalb von Avantgarde werden persönliche Zugangsdaten für jeden zugriffsberechtigten Mitarbeitenden des Dienstleistenden benötigt.
- Die Zugangsdaten sind sicher zu verwahren und gegen unberechtigte Zugriffe zu schützen. Eine Weitergabe dieser Zugangsdaten an andere Mitarbeitende oder eine unsichere Verwahrung der Zugangsdaten ist untersagt.
- Nicht mehr benötigte Zugänge oder Zugriffe sind unverzüglich der auftraggebenden Stelle von Avantgarde zu melden, damit die Sperrung dieser Zugänge erfolgen kann.
- Schutz durch Zutritts-, Zugangs- und Zugriffskontrollen
- Es sind Sicherheitsbereiche mit einem entsprechenden Zutrittsberechtigungskonzept des jeweiligen Unternehmens von Avantgarde zu beachten.
- Die Nutzung von Datenverarbeitungssystemen durch Unbefugte muss verhindert werden. Dazu sind die Zugangsregelungen und Zugriffskontrollen zu beachten.
- Vertraulichkeits- und Verpflichtungserklärungen sind Bestandteil des Dienstleistungsvertrages. Mitarbeitende des Dienstleistenden müssen auf diese Vereinbarungen, insbesondere in Bezug auf personenbezogene Daten, verpflichtet werden.
- Sensibilisierung und Motivation der Mitarbeitenden zur sicherheitsbewussten Arbeitsweise.
- Ihren Aufgaben entsprechende Einarbeitung der Mitarbeitenden und regelmäßige Schulungen, insbesondere auch für die geltenden Sicherheitsmaßnahmen und deren korrekter Einhaltung.
- Einrichtung eines Notfallmanagements und/oder mindestens Erstellung eines Notfallplans, um im Katastrophenfall schnellstmöglich reagieren zu können.
- Ein Löschkonzept muss vorhanden sein. Die Löschung und/oder Übermittlung von Daten nach Beendigung der Zusammenarbeit, bzw. auf Weisung durch Avantgarde Verantwortliche muss durchgängig sichergestellt sein.

Das Ziel muss sein, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen IT-Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

2.3 Technische Maßnahmen

- Installieren eines Antiviren Programms: Zum Schutz vor Viren, Würmern und sonstigen Schadprogrammen (wie z.B. Trojanern und Spyware) ist auf allen IT-Systemen des Dienstleistenden sowie des Unternehmen-Gruppenunternehmens ein aktuelles Antivirenprogramm zu installieren. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindern.
- Betriebssysteme und Anwendungssoftware: Dienstleistende haben dafür Sorge zu tragen, dass die von ihnen zur Verfügung gestellten und genutzten IT-Systeme mit einem sich in Wartung befindenden Betriebssystem und Anwendungssoftware ausgestattet sind.

- Firewall: Dienstleistenden haben auf den im Unternehmen-betriebenen IT-Systemen eine lokale Firewall zu aktivieren.
- Wechseldatenträger: Das Verwenden von Wechseldatenträgern ist untersagt. Wechseldatenträger im Sinne dieser Richtlinie sind insbesondere
    - USB-Sticks
    - Externe Festplatten
    - Firmenfremde Smartphones.
- Sicherheitslücken sind bei Bekanntwerden umgehend jeweiligen Verfahrensverantwortlichen und Systemadministrierenden zu melden und zu schließen.
- Datensicherung: Umfassende und regelmäßige Datensicherung, Kontrolle und Überprüfung der erstellten Backups auf Inhalt, Integrität und zeitliche Vorgaben (Notfallplan).
- Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederhergestellt werden kann, wenn Datenbestände nicht mehr verfügbar oder fehlerhaft sind.
- Betriebsdaten müssen generell so gespeichert werden, dass bei Ausfall eines Mitarbeitenden dessen Vertretung oder der Vorgesetzte auf diese Daten zugreifen kann.
- Kommunikationsmittel: Die regelkonforme Nutzung der Kommunikationsmittel wie E-Mail, Internet, Instant Messaging, Social Media, Video-Portale, etc. muss durch Richtlinien, Betriebsvereinbarungen und Schulungen sensibilisiert werden. Daten von Avantgarde dürfen ohne Genehmigung grundsätzlich nicht veröffentlicht werden.
- Netzwerksegmentierung durch Virtual Local Area Networks (VLANs): Eine physikalische Trennung von sensiblen Bereichen oder eine Trennung zweier Unternehmen an einem Standort ist grundsätzlich zu prüfen, dabei ist auch eine mögliche logische Trennung über VLAN gegebenenfalls zu prüfen und ggf. entsprechend einzurichten. Eine virtuelle Netzwerktrennung einzelner Bereiche ist vom Schutzbedarf der zu trennenden Bereiche abhängig. Mittels der Trennung über VLAN soll ein isoliertes Betreiben der IT-Systeme möglich sein. Die Installation eines VLAN soll den unerlaubten Zugriff auf das Netz von Avantgarde verhindern.

2.4 Kontrolle der Verbesserung der Sicherheit

Die Informationssicherheit wird regelmäßig auf Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitenden des Dienstleistenden bekannt, umgesetzt und in den Betriebsablauf integriert sind.

Avantgarde unterstützt die ständige Verbesserung des Sicherheitsniveaus. Dienstleistende sind angehalten, mögliche Verbesserungen oder Schwachstellen an den jeweiligen Verfahrensverantwortlichen und dem Systemadministrator weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der Informationssicherheitstechnik zu halten.

2.5 Lizenzmanagement

Auf allen IT-Systemen darf ausschließlich lizenzierte Software eingesetzt werden. Der Eigentümer dieser Lizenz ist für die Gültigkeit und Aktualität verantwortlich.

Diese Regelung muss allen Mitarbeitenden bekanntgemacht werden.

Die Verfahrensverantwortlichen der verschiedenen IT-Systeme müssen sicherstellen, dass nur lizenzierte Software eingesetzt wird. Ohne eine geeignete Versionskontrolle und Lizenzkontrolle kommt es erfahrungsgemäß schnell zur Verwendung verschiedenster Software-Versionen auf einem IT-System oder innerhalb einer Organisationseinheit, von denen eventuell einige ohne Lizenz benutzt werden.

Die Konfiguration der installierten IT-Systeme ist hinreichend zu dokumentieren.

Damit Lizenzen bei Hardware-Defekten nicht ungültig werden, sollten möglichst Hardware-unabhängige Lizenzen eingesetzt werden. So kann ein IT-System mit weniger Aufwand ersetzt werden, wenn die Hardware ausfällt.

Wenn es möglich und wirtschaftlich sinnvoll ist, sollten unbefristete Lizenzen bevorzugt werden. Damit kann eine Funktionseinschränkung durch den Ablauf der Lizenz verhindert werden.

Es gelten folgende Grundsätze:

- Es darf nur lizenzierte Software genutzt werden, mögliche Testzeiträume der Hersteller sind zu beachten.
- Es darf ausschließlich sich in Wartung befindende Soft- und Hardware verwendet werden.
- Sofern Dienstleistende Herstellende dieser Soft- und/oder Hardware sind, so ist er für eine entsprechende Wartung verantwortlich und muss diese garantieren können.
- Einsatz firmeneigener Software auf firmenfremden Rechnern nur mit entsprechend gültiger Lizenzierung.
- Kein Einsatz von privater Software oder privater Nutzung der IT-Systeme

Die Kontrolle der installierten Versionen und die Nachverfolgung der verfügbaren Lizenzen und deren Abgleich mit der installierten Anzahl der Produkte muss regelmäßig erfolgen.

3 Informationssicherheitsmanagementsystem

3.1 Zuständigkeiten und Verantwortungen

Dienstleistende haben dafür Sorge zu tragen, dass die Dienstleistungserbringung im Rahmen der hier vorliegenden Richtlinie erfolgt.

- Dienstleistende haben jederzeit sicher zu stellen, dass das eigene Handeln und das Handeln von Mitarbeitenden nicht die Verfügbarkeit, Integrität oder Vertraulichkeit der IT-Systeme und Daten von Avantgarde beeinträchtigt.
- Urheberrechtliche und patentrechtliche Bestimmungen sowie Lizenzvereinbarungen sind einzuhalten.
- Die bereitgestellten Zugangsdaten dürfen nicht an Dritte weitergegeben werden.
- Im Falle einer Auftragsverarbeitung ist ein entsprechender Auftragsverarbeitungsvertrag abzuschließen. Im Rahmen dessen werden die Mitarbeitenden dazu angehalten und verpflichtet, gesetzliche Regelungen sowie vertragliche und unternehmensinterne Vorgaben an die Informationsverarbeitung zu erfüllen und Zuwiderhandlungen umgehend zu melden.

3.2 Rollen

Eine Rolle kann als Bündelung von Kompetenzen aufgefasst werden, die zur Bearbeitung von Aufgaben innerhalb eines IT-gestützten Geschäftsprozesses benötigt werden. Eine Rolle beschreibt somit, wer für welche Aufgaben, mit welchen Rechten und Pflichten zuständig ist. Die konkrete Zuordnung der Rollen bzw. ob jede Rolle benötigt wird, hängt von dem jeweiligen IT-Verfahren ab.

Unabhängig von den Rollen, ist die Geschäftsführung für die Gewährleistung der Informationssicherheit im Unternehmen, sowie den entsprechenden Ressourcen, insbesondere den technischen und personellen, verantwortlich.

3.3 Verhalten bei Sicherheitsvorfällen

Informationssicherheitsvorfälle sind umgehend dem Verfahrensverantwortlichen zu melden. Dieser organisiert die Informationsweitergabe an die anderen obengenannten Rollen. Der Systemadministrator hat bei Verlust der Netz- oder Systemintegrität schnellstmöglich diese Störungen zu beseitigen.

Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Die Meldung von Sicherheitsvorfällen wird daher immer positiv gewertet!

Die Ursachen der Sicherheitsvorfälle sind anhand der erstellten Protokolle mit dem Verfahrensverantwortlichen und dem Systemadministrator gemeinsam zu analysieren und Verbesserungen zu erarbeiten. Daraus resultierende erforderliche Maßnahmen sind umzusetzen. Dies ist entsprechend zu dokumentieren.

Die Anweisungen der Verfahrensverantwortlichen sind zu befolgen.

3.4 Notfallvorsorge

Damit ein Ausfall der Systeme rechtzeitig erkannt wird, sind die Systemressourcen und Messwerte zur Betriebssicherheit (Informationen über die Temperatur, die CPU-Auslastung und den freien Speicherplatz, allgemein die Verfügbarkeit) immer auf kritische Werte hin zu überwachen. Wenn möglich sollte dazu ein Monitoring-System mit automatischer Benachrichtigungsfunktion installiert und genutzt werden.

Die Prüfung aller Versicherungen, der Kaufverträge und Verträge mit Dienstleistenden hinsichtlich der vereinbarten SLAs wird regelmäßig durchgeführt.

Das Netzwerk, die Telekommunikation und die dafür notwendigen Komponenten sind so auszulegen, zu installieren und zu konfigurieren, dass sie den Ansprüchen an Vertraulichkeit, Integrität und Verfügbarkeit der zu übermittelnden Informationen genügen.

Dabei ist je nach Schutzbedarf eine eventuell erforderliche Netztrennung, verschlüsselte Übermittlung und eine redundante Installation der kritischen Infrastruktursysteme zu berücksichtigen. Die einzelnen Komponenten sollten so ausgewählt, konfiguriert und dokumentiert werden, dass sie dem aktuellen „Stand der Technik“ entsprechen.

Die Verkabelung muss vollständig dokumentiert sein (physikalische Topologie, Verlegungspläne, Beschriftung der Geräte).

Ein Notfallvorsorgekonzept und Notfallplan sind zu erstellen und in regelmäßigen Abständen zu prüfen und ggfs. zu erweitern. Die folgenden Informationen sollen im Notfallkonzept/-plan hinterlegt werden:

- Netzwerk- und Systemdokumentation (einschließlich Konfigurationen).
- Lizenzen.
- Wartungsverträge, Austausch der Hardware bei Defekt und regelmäßige Prüfung der SLA-Verträge mit dem Lieferanten/Dienstleister.
- Verhalten im Notfall (incl. Reihenfolge Herunterfahren und Start der Systeme).
- Alarm- und Eskalationsplan.

4 Arbeitsplatzeinrichtung bei Fernwartung

4.1 Fernwartung / VPN

Ein Zugriff von extern auf die Netzwerke von Avantgarde darf ausschließlich mittels eines VPN-Tunnels oder einer von Avantgarde freigegebenen Fernwartung-Software erfolgen.

Zur Fernwartung via Remote-Verbindung sind keine Freeware-Tools zu installieren. Es ist ausschließlich die Standardsoftware von Avantgarde zur Remote-Verbindung zu verwenden. Sollte kein Gruppenstandard definiert sein, ist die vom jeweiligen Unternehmen beschriebene Software zu nutzen.

Dienstleistende haben sicherzustellen, dass das eigene Netzwerk keine unkontrollierten Zugriffe Dritter auf das Netzwerk von Avantgarde ermöglicht

- Protokollpflicht
- Die Zugriffe mittels Fernwartung müssen protokolliert werden. Protokolliert werden sollen mindestens die Veränderungen und Tätigkeiten, die mittels des Fernzugriffs erfolgen.
- Zumindest auf Nachfrage müssen Dienstleistende einen Nachweis erbringen können, zu welchem Zweck bestimmte Zugriffe erfolgt sind.
- Datentransfer darf nur nach Genehmigung erfolgen
- Dienstleistende dürfen über den Zugang nur solche Daten auf IT-Systeme von Avantgarde kopieren oder von diesen extrahieren, für die eine Genehmigung vorliegt. Es darf keine nicht genehmigte Software installiert werden und/oder Informationen aus den IT-Systemen extrahiert, bzw. abgezogen werden.
- Änderungen an Systemen nur nach Genehmigung
- Dienstleistende dürfen IT-Systeme von Avantgarde nur nach Absprache und Genehmigung verändern.

4.2 Zugangsschutz / Bildschirmsperre

Bildschirme sind bei Verlassen des Arbeitsplatzes (manuell bzw. automatisch) zu sperren.

Dienstleistende haben sich nach Beendigung der Wartung vom System ordnungsgemäß abzumelden.