



ANTEO
mobility innovations

INFORMATIONSSICHERHEITS-
LEITLINIE

anteo GmbH
Hafenstr. 7
38442 Wolfsburg

1 Verbindlichkeitserklärung

Hiermit wird folgende Leitlinie zur Informationssicherheit, durch die Geschäftsführung der anteo GmbH, als Bestandteil der Unternehmensstrategie verabschiedet. Aufgrund der permanenten Weiterentwicklung in der Informationstechnologie unterliegt diese Informationssicherheitsleitlinie und alle darauf aufbauenden Richtlinien sowie mitgeltende Unterlagen der fortlaufenden Anpassung und Weiterentwicklung. Die Informationssicherheitsleitlinie ist für alle Beschäftigten der anteo GmbH intern und extern (Homepage) einsehbar und wird auf Wunsch allen interessierten Partnern des Unternehmens zur Verfügung gestellt.

2 Anwendungsbereich

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheitsmanagementsystems (ISMS) der anteo GmbH. Die Anwender/-innen dieses Dokuments sind alle Mitarbeiter/-innen im Anwendungsbereich der anteo GmbH.

3 Informationssicherheitsmanagementsystem

Zur Sicherstellung einer dauerhaften Wirksamkeit der Informationssicherheit führt die anteo GmbH ein Informationssicherheitsmanagementsystem (ISMS) nach den Anforderungen des VDA-Kataloges auf Basis der international anerkannten Norm ISO/IEC 27001 ein und stellt eine geeignete Sicherheitsorganisation auf.

Zur Erreichung der Sicherheitsziele benennt die Geschäftsführung einen Informationssicherheitsbeauftragten (ISB), der die Geschäftsführung bei der Planung und Umsetzung der Informationssicherheit im Unternehmen berät und unterstützt. Er berichtet in seiner Funktion anlassbezogen, mindestens jedoch jährlich direkt an die Geschäftsführung.

Die Aufgaben aller Beteiligten, Richtlinien und erforderliche Maßnahmen im Rahmen des ISMS, sind detailliert in der Informationssicherheitsrichtlinie der anteo GmbH beschrieben.

4 Informationen und Sicherheit

4.1 Stellenwert der Informationssicherheit

Heute sind Informationen ein grundlegender Faktor für den Geschäftsbetrieb und stellen für uns als Konstruktions-, Fehler- und Projektmanagementdienstleister eine wesentliche Grundlage zur Erreichung unserer Unternehmensziele dar. Durch informationsverarbeitende Systeme werden alle wesentlichen, strategischen und operativen Funktionen und Aufgaben der anteo GmbH unterstützt. Die Definition und Umsetzung der Ziele und Grundsätze der Informationssicherheit erfolgt auf Grundlage der strategischen Ausrichtung der anteo GmbH.

Alle Kunden, Geschäftspartner und Beschäftigte müssen sich darauf verlassen können, dass die anteo GmbH die Sicherheitsverantwortung, für die von ihr verarbeiteten Informationen gewissenhaft wahrnimmt und Informationen vor missbräuchlicher Verwendung schützt. Die Geschäftsführung trägt die Verantwortung für die Informationssicherheit und ist sich dessen bewusst. Sie stellt ausreichend Ressourcen bereit, um in einem wirtschaftlich vertretbaren Maß das Informationssicherheitsniveau auf einem hohen Niveau zu etablieren und stetig weiterzuentwickeln.

4.2 Zielsetzung der Informationssicherheit

Der Informationsverarbeitung kommt, bei der anteo GmbH, eine Schlüsselrolle bei der Erfüllung extern und intern zu realisierenden Aufgaben zu. Informationen kommen in verschiedenster Form (elektronische Daten, Papierform, mündliche Informationen, etc.) vor. Die Verarbeitenden dieser Informationen sind auf die Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität dieser Informationen angewiesen.

Durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden die Schutzziele Authentizität und Integrität, da sie in der Praxis nur schwer voneinander zu trennen sind, in dem Schutzziel Integrität zusammengefasst.

Zur Wahrung der Informationssicherheit dienen daher die folgenden Schutzziele:

- **Vertraulichkeit**
Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen.
- **Integrität**
Integrität bedeutet Schutz vor Veränderung von Informationen durch nicht berechnete Personen und stellt die Richtigkeit, Konsistenz und Vollständigkeit von Informationen dar.
- **Verfügbarkeit**
Verfügbarkeit bedeutet, dass Informationen, IT-Systeme, IT-Netzwerke und informationsverarbeitende Systeme immer dann verfügbar sind, wenn diese bearbeitet bzw. in Anspruch genommen werden müssen.

Der anteo GmbH ist bewusst, dass Sicherheit nur in einem ausgewogenen Verhältnis der vorgenannten Schutzziele sinnvoll möglich ist, da z.B. die Vertraulichkeit ohne Integrität zu keiner ernstzunehmenden Wahrung der Informationssicherheit führt. Daher werden die Schutzziele für jedes Asset festgelegt, um geeignete Maßnahmen zu ihrer Umsetzung ergreifen zu können. Da wir als Entwicklungsdienstleister oft mit sensiblen Informationen unserer Kunden in Berührung kommen, sind für uns die Schutzziele Vertraulichkeit und Integrität von höchster Priorität. Jedoch muss auch das Schutzziel Verfügbarkeit in den jeweiligen Geschäftsprozessen analysiert werden und hinreichend Berücksichtigung finden.

Alle wesentlichen operativen und strategischen Aufgaben und Funktionen werden durch Informations- und Kommunikationstechnik, in unterschiedlichem Umfang, unterstützt. Ein Ausfall dieser Systeme und Technik muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen legen wir Wert darauf, dass unsere Systeme und Prozesse durchgängig zur Verfügung stehen und funktionieren. Da unsere Kernprozesse auf die sichere Verarbeitung von Informationen angewiesen sind, ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von existenzieller Bedeutung.

4.3 Grundsätze der Informationssicherheit

Verspätete oder fehlerhafte Entscheidungen des Managements können weitreichende Folgen nach sich ziehen. Daher ist für das Management bei wichtigen Entscheidungen ein Zugriff auf einen aktuellen Stand an Informationen wichtig. Für diese Informationen ist ein hohes Schutzniveau, in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität, sicher zu stellen.

Für die anteo GmbH ist die Aufrechterhaltung der Kommunikation nach außen, zu unseren Kunden und Geschäftspartnern, von elementarer Bedeutung. Es darf zu keiner Verzögerung oder Gefährdung der Abwicklung von Aufträgen kommen. Wenn vertraglich festgelegte Leistung nicht erbracht oder gar Liefertermine nicht eingehalten werden können, kann dies erhebliche negative Folgen haben. Für uns ist daher die ständige Verfügbarkeit unserer Informations- und Kommunikationstechnik sowie die durchgängige Gewährleistung des Zugriffs auf korrekte Daten für unsere Beschäftigten von höchster Bedeutung, woraus wir einen hohen Schutzbedarf für diese Unternehmenswerte ableiten.

Durch die anteo GmbH werden innerhalb einiger Prozesse und Bereiche Informationen verarbeitet, welche sehr hohe Anforderungen an die Vertraulichkeit stellen. Durch entsprechende technische und organisatorische Maßnahmen und die hohe Aufmerksamkeit der Mitarbeiter/Mitarbeiterinnen, sichergestellt durch jährliche Sensibilisierungsmaßnahmen im Bereich der Informationssicherheit, wird das hohe Niveau der Informationssicherheit in der Organisation sichergestellt.

Die Nutzung von Internet und E-Mail zur Beschaffung von Informationen und zur Kommunikation ist für uns selbstverständlich. Durch entsprechende Maßnahmen wird sichergestellt, dass mit der Nutzung dieser Technologien verbundene Risiken möglichst gering bleiben.

Bei der Verarbeitung personenbezogener Daten unserer Kunden und Beschäftigten legen wir größten Wert auf die Einhaltung gesetzlicher Vorschriften und Regelungen. Die mit der Verarbeitung beauftragten Beschäftigten gehen vertraulich mit diesen Daten um.

4.4 Ziele der Informationssicherheit

Nachfolgende Grundsätze bilden die Basis dieser Informationssicherheitsleitlinie an denen sich alle Sicherheitsmaßnahmen und -vorgaben ausrichten und die für alle im Geltungsbereich tätigen Personen verbindlich sind.

1. In der Zusammenarbeit mit Kooperationspartnern und Auftragnehmern ist ein angemessenes Informationssicherheitsniveau etabliert. So kommt es zu keiner Gefährdung der Abwicklung von Aufträgen.
2. Alle Unternehmenswerte (Assets) sind identifiziert und entsprechend ihrem Schutzbedarf klassifiziert. Mögliche Risiken werden frühzeitig identifiziert und auf ein akzeptierbares Restrisiko minimiert.
3. Kosten für Maßnahmen zur Informationssicherheit stehen in einem angemessenen Verhältnis zur Größe und Wirtschaftlichkeit des Unternehmens.
4. Vertragliche und rechtliche Vorgaben für die Informationssicherheit werden stets eingehalten.
5. Für die Wiederherstellung des Betriebes der wesentlichen Informationssysteme ist ein Notfallkonzept etabliert.
6. Die Beschäftigten werden hinsichtlich des sicheren Umgangs mit Informationswerten geschult und sensibilisiert und sind sich ihrer Verantwortung bewusst.

5 Verantwortung als Dienstleister

Die Auftraggeber und Geschäftspartner der anteo GmbH erwarten einen vertrauenswürdigen Umgang mit den im Rahmen bestehender Vertragsverhältnisse ausgetauschten oder bekanntgewordenen Informationen.

Wir stellen uns dieser Verantwortung, indem wir alle notwendigen Maßnahmen zum Schutz der Informationen und ihrer Verfügbarkeit in einem wirtschaftlichen Verhältnis umsetzen.

Unsere Unternehmenswerte bzw. Assets sind:

- Unsere Beschäftigten, mit ihren Qualifikationen, Erfahrungen und Fähigkeiten
- Compliance
- Informationen als Ergebnisse unserer Prozesse
- Hard- und Software
- Reputation und Ansehen

6 Verbesserung der Sicherheit

Die Informationssicherheitsleitlinie und die Informationssicherheitsrichtlinie sowie alle mitgeltenden Unterlagen werden regelmäßig, mindestens jedoch jährlich, hinsichtlich der Aktualität und Wirksamkeit, geprüft.

Werden Schwachstellen in der Informationssicherheit identifiziert, so werden neue geeignete Maßnahmen entwickelt, auf ihre Integrationsfähigkeit in die Geschäftsabläufe untersucht und nach erfolgter Verifizierung in die Informationssicherheitsrichtlinie eingearbeitet.

Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus.

Alle Beschäftigten der anteo GmbH sind dazu verpflichtet, an der kontinuierlichen Verbesserung des Sicherheitsniveaus mitzuwirken und mögliche Schwachstellen oder Verbesserungen, z.B. durch Hinweise oder Verbesserungsvorschläge, an die entsprechenden Stellen weiterzuleiten.

7 Inkraftsetzung durch Unterzeichnung der Leitlinie

Mit Unterzeichnung dieser Informationssicherheitsleitlinie durch die Geschäftsführung, ist diese ab dem Tag der Unterzeichnung gültig und anzuwenden.

Wolfsburg, den 20.09.2022



Stefan Wagner
Geschäftsführer