1. Ziele

- Verständnis der Wichtigkeit der Informationssicherheit
- Verpflichtung auf das Informationssicherheitsmanagement für alle Mitarbeitenden

2. Geltungsbereich und Gültigkeit

Diese Richtlinie zur Informationssicherheit inklusive des intern veröffentlichten zugehörigen Regelwerks zur Informationssicherheit gilt verbindlich für alle Bereiche und Beschäftigte der Argon & Co Deutschland GmbH. Die Bestimmungen dieser Richtlinie sind – neben den gesetzlichen und tariflichen Bestimmungen – wesentlicher Bestandteil jedes Arbeitsvertrages und sind verbindlich einzuhalten.

3. Zielgruppe

Zielgruppe dieser Richtlinie sind alle festen Mitarbeiterinnen und Mitarbeiter der Argon & Co Deutschland GmbH.

4. Allgemeine Bestimmungen

4.1. Änderungen

Das Unternehmen ist jederzeit berechtigt, Regelungen aus dieser Richtlinie durch anderweitige Regelungen zu ersetzen, ergänzen oder vollständig aufzuheben. Die Mitarbeiterinnen und Mitarbeiter werden darüber schriftlich informiert.

4.2. Verstöße

Verstöße gegen diese Richtlinie stellen Verletzungen von arbeitsvertraglichen Pflichten dar, die im Rahmen der gesetzlichen Möglichkeiten geahndet werden können. Zudem können Verletzung von Regelungen aus dieser Informationssicherheitsrichtlinie zivilrechtliche, wettbewerbsrechtliche und strafrechtliche Folgen haben.

Da das Verhalten eines und einer jeden Einzelnen zur Gewährleistung von Informationssicherheit und Datenschutz beiträgt, sind nachfolgend die wichtigsten Vorgaben, deren Einhaltung verbindlich ist, zusammengefasst. Die dazugehörigen detaillierten Regelungen können in den entsprechenden Dokumentationen, die auf SharePoint in IT & Sicherheit - Richtlinien abgelegt sind, nachgelesen werden.

5. Umgang mit Betriebsmitteln und Datenträgern

- Vertrauliche Dokumente dürfen niemals unbeaufsichtigt liegengelassen werden, um die Einsichtnahme durch Unbefugte zu verhindern.
- Ausgedruckte Dokumente mit personenbezogenen, vertraulichen oder geheimen Daten müssen mit einem Dokumentenschredder ab Sicherheitsstufe P4 geschreddert oder über eine Datentonne entsorgt werden.
- Es werden ausschließlich unternehmenseigene Datenträger für den Austausch von Daten genutzt. Der Gebrauch von privaten USB-Sticks, Speicherkarten o. Ä. ist untersagt.

- Die bereitgestellten Betriebsmittel dürfen nur für den entsprechenden Verwendungszweck eingesetzt werden.

6. Klassifizierung von Informationen und Sicherheitszonen

Die Klassifizierung von Informationen wird durch die Gesetzgebung (personenbezogene Daten), vertragliche Anforderungen oder interne Regelungen bestimmt. Verantwortlich dafür ist die Projektleitung, die im Austausch mit den Auftraggebenden steht. Diese legt auch zu Beginn eines jeden Projekts die Klassifizierung fest, sowohl für die Informationen, die von Kund:innen kommen, als auch die Informationen, die im Auftrag erstellt werden, und kommuniziert diese an alle Beteiligten.

Wir unterscheiden zwischen den folgenden Schutzklassen und entsprechenden Sicherheitszonen, um einen unberechtigten Zutritt zu verhindern:

	Öffentlich	Intern	Vertraulich
Definition	Alle Informationen, die öffentlich verfügbar sind, unterliegen keinem besonderen Schutz.	Implizite Kennzeichnung genügt à Die Informationen bzw. der Informationsträger (z. B. Papierdokument, E-Mail) müssen selbst nicht gekennzeichnet werden, da der Nutzer die Vertraulichkeitsstufe anhand der Informationen erkennt	Implizite Kennzeichnung genügt, solange die Information nicht den Kreis der Kernnutzer verlässt Andernfalls ist eine explizite Kennzeichnung notwendig à Kennzeichnung mit „vertraulich“ und Seitenangabe entsprechend der unternehmensinternen Vorgabe („Richtlinie Dokumentenlenkung“)
Das sind grund-sätzlich Informati onen wie:	- Veröffentlichte Presse-mitteilungen - Informationen, die auf der Unternehmens-Website veröffentlicht wurden	- Diese Richtlinie - Urlaubsantrag - Reisekostenabrechn ung	- Alle personenbezogenen Daten - Personalakten - Vom Kunden als “Vertraulich” ausgegebene Informationen
Sicherhei ts-zonen	Der öffentliche Bereich ist frei zugänglich für alle. Ein Zutritt ist ohne Schlüssel möglich.	In der kontrollierten / internen Zone haben nur Mitarbeitende oder Besucher:innen in Begleitung Zutritt.	In der eingeschränkten/ Vertraulichen Zone dürfen nur Mitarbeitende, freie Mitarbeitende oder Dienstleistungen mit Vertraulichkeitsvereinbaru ng.

7. Weitergabe von Informationen

- Bei jeglicher Verarbeitung von Informationen ist der jeweilige Schutzbedarf/Klassifizierung zu beachten.
- Die Klassifizierung wird von der zuständigen Projektleitung in Zusammenarbeit mit den Kund:innen festgelegt.
- Alle vom Unternehmen freigegebenen Dienste, um sensible Informationen zu verarbeiten, sind im Dokument “Leitfaden zur Klassifizierung” aufgelistet. Nicht freigegebene Software und Cloud-Dienste müssen zunächst bei IT unter isms-team@advyce.com angefragt werden

8. No Local Data

- Sämtliche Dokumente dürfen nur als Zwischenablage auf dem lokalen Computer gespeichert werden.
- Jede Mitarbeiterin und jeder Mitarbeiter muss sicherstellen, dass sämtliche Daten auf dem Datenserver abgelegt sind. Die Synchronisation muss einmal täglich stattfinden.

9. Clean Desk

- Beim Verlassen des Arbeitsplatzes haben die Mitarbeitenden dafür Sorge zu tragen, dass Unberechtigte keinen Einblick auf Informationen erlangen können.
- Die Schreibtische (sowie der Computer-Desktop) sind deshalb möglichst leer zu lassen. Spätestens am Abend werden sensible Daten weggeräumt.
- Es ist dafür Sorge zu tragen, dass Informationen auf Papier oder anderen Medien abgedeckt werden, wenn sich Kunden im Haus befinden.

10. Mobiles Arbeiten und Homeoffice

- Dienstliche Unterlagen sollten in einem abschließbaren Schrank aufbewahrt werden.
- Dienstliche Hardware darf nicht von anderen Personen genutzt werden.
- Bei der Verwendung von Smartphone, Tablet und Laptop muss der Bildschirm vor Einsicht geschützt werden (insbesondere bei der Nutzung im Flugzeug, Zug, Café etc.).
- Bei der Entsorgung von dienstlichen Unterlagen muss ein Aktenvernichter ab der Sicherheitsstufe P4 verwendet werden.
- Wenn Eheleute/Kinder oder Dritte (beispielsweise in einer Wohngemeinschaft) mit unter einem Dach wohnen, muss der Computer auch bei kurzzeitigem Verlassen gesperrt werden.
- Vertrauliche Gespräche, Telefonate und Videokonferenzen sollten nicht in öffentlichen Räumen, sondern nur an geschützten Plätzen geführt werden, wo kein Dritter zuhören kann.
- Hardware, Datenträger und geschäftliche Unterlagen von der Argon & Co Deutschland GmbH dürfen nie unbeaufsichtigt gelassen werden und sollten immer persönlich mitgeführt oder sicher versperrt werden.
- Ein sicherer Zugriff auf das Firmennetzwerk außerhalb der Geschäftsräume ist, sofern möglich, über eine VPN-Verbindung (Virtual Private Network) herzustellen.

11. Schutz von personenbezogenen Daten

- Nach der EU-Datenschutz-Grundverordnung (EU-DSGVO) ist es untersagt, personenbezogene Daten zu einem anderen als dem zugewiesenen zur jeweiligen regelmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen.
- Die EU-DSGVO schützt alle Daten natürlicher Personen, die aufgezeichnet oder verarbeitet werden. Hierzu zählen auch Aufzeichnungen auf mobilen, personenbezogenen Speicher- und Verarbeitungsmedien sowie Angaben auf Formularen. Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

12. Sicherheitsereignisse

- Bei Bekanntwerden von Ereignissen, die zu einer Verletzung der Informationssicherheit oder des Datenschutzes führen können, sind Mitarbeiterin und Mitarbeiter zur Meldung an isms-team@advyce.com verpflichtet.

12.1. Leitfaden bei Verlust oder Diebstahl

Bei Verlust oder Diebstahl von mobilen Endgeräten oder Datenträgern ist unverzüglich eine E-Mail an Advyce & Company zu schreiben. Die IT sperrt bzw. löscht dann das Gerät aus der Ferne.

13. Nutzung mobiler Endgeräte

- Mit mobilen Endgeräten ist sorgsam umzugehen. Es ist zu verhindern, Geräte offen herumliegen und unbeaufsichtigt zu lassen.
- Der Einblick in den Bildschirm verschiedener Geräte ist in Anwesenheit betriebsferner Personen bestmöglich zu verhindern. (Fensterplatz im Flugzeug/ Zug etc.)
- Mobile Endgeräte mit eingerichteten Firmen-Accounts (E-Mail, Kalender, etc.) dürfen ausschließlich Mitarbeitende verwenden. Auch Familienmitgliedern ist die Benutzung verboten.
- Das Koppeln oder Verbinden mit anderen Geräten z.B. via „AirDrop“ ist verboten (keine Protokollierung).
- Die Entsorgung von mobilen Endgeräten und Datenträgern erfolgt durch die IT-Abteilung. Eine eigenständige Entsorgung durch den die Mitarbeiterin oder den Mitarbeiter ist verboten.

14. Persönliche Logins und Passwörter

- Ein persönliches Passwort darf ausschließlich der jeweiligen Benutzerin oder dem jeweiligen Benutzer bekannt sein.
- Persönliche Passwörter dürfen nicht handschriftlich notiert oder anderen Personen mitgeteilt werden.
- Ein betrieblich genutztes Passwort darf nicht auf externen oder privaten Diensten genutzt werden.
- Passwörter müssen aus mindestens 12 Zeichen bestehen und sich aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen zusammensetzen.

- Die Geräte müssen vor der Nutzung durch unbefugte Personen mit einem passwortgeschützten Bildschirmschoner ausgestattet sein. Dieser muss sich spätestens nach fünf Minuten automatisch aktivieren und über die Funktion „aktive Ecken“ (oder Shortcut) jedes Mal beim Verlassen des Arbeitsplatzes aktiviert werden.
- Bei iPhones und iPads müssen Zugangscodes aktiviert sein, die aus mindestens sechs Ziffern bestehen. Es dürfen keine trivialen Kombinationen wie z. B. „111111“ und keine Zugangscodes mit persönlichem Bezug (z. B. Geburtsdatum) verwendet werden. Die Funktion „Code anfordern“ muss auf „sofort“ eingestellt sein.
- Die Benutzung von Finger- oder Gesichtserkennung ist erlaubt.

15. Speicherung der Verbindungsdaten

- Sämtliche Verbindungsdaten werden von einem EDV-System erfasst und gespeichert. Eine andere Form der Verarbeitung oder Nutzung findet zunächst nicht statt.
- Das Unternehmen weist darauf hin, dass der Zugriff auf bestimmte Seiten im Internet durch Einsatz einer Filtersoftware gesperrt werden kann. Ebenso können die Zugriffe auf diese bestimmten Seiten untersucht werden.

16. Private Nutzung

16.1. Telefon und Internet

- Internet und Telefondienste dürfen nur für betriebliche Zwecke genutzt werden.
- Eine private Nutzung ist dann erlaubt, wenn der optionalen Einwilligung am Ende dieses Dokumentes zugestimmt wird.

16.2. E-Mail-Accounts

- E-Mail-Accounts dürfen nur für betriebliche Zwecke genutzt werden. Die private Nutzung ist verboten.
- E-Mails können in Einzelfällen bei Abwesenheit der Mitarbeitenden (z. B. bei Urlaub oder Krankheit) zur Aufrechterhaltung des Dienstbetriebs an die zuständige Vertretung weitergeleitet werden.

17. Schutz vor Schadsoftware

- Beim Herunterladen sowie Speichern von Programmen und jeder anderen Form ausführbarer oder selbstausführender Dateien - einschließlich Makros - auf dem betrieblichen Endgerät ist darauf zu achten, dass diese aus einer vertrauenswürdigen Quelle stammen.
- Das Herunterladen von offensichtlich rechtswidrigen Angeboten oder Plattformen ist unzulässig.
- Der Mitarbeiter oder die Mitarbeiterin muss sich vor dem Download über etwaige Nutzungs- und Lizenzbedingungen des Contents informieren.
- Jeder Verdacht auf Computerviren muss der IT sofort gemeldet werden.

18. Netzwerkschutz

- Betriebsfremde Rechner dürfen nur in von der IT genehmigungspflichtigen Ausnahmefällen an das betriebliche Computernetz (LAN und/oder internes WLAN) angeschlossen werden.
- Gäste müssen das Gäste WLAN benutzen.

19. Verpflichtung

Über die notwendigen Pflichten und Verhaltensweisen zur Informationssicherheit und zum Datenschutz wurde ich aufgeklärt. Ich bin mir meiner Verantwortung bewusst und werde mich an diese Richtlinien halten. Mir ist weiter bewusst, dass die Verletzung von Regelungen aus dieser Betriebsrichtlinie zivilrechtliche, wettbewerbsrechtliche und strafrechtliche Folgen haben kann. Zudem kann eine Verletzung zu arbeitsrechtlichen Konsequenzen (Abmahnung, Kündigung) führen.

_____, den _____

Ort Datum

_____ _____

Name Mitarbeiter:in Unterschrift des/der Verpflichteten

20. OPTIONAL: Private Nutzung

Ich willige ein, dass auch meine privaten Internetzugriffe und meine private Telefonnutzung verarbeitet und protokolliert sowie personenbezogen ausgewertet werden. Mir ist bewusst, dass ich hierdurch auf den Schutz des Fernmeldegeheimnisses gem. § 3 TDDDG verzichte. Mir ist bewusst, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, mit der Folge, dass ich ab dem Zeitpunkt des Widerrufs Internet und Telefon nicht mehr privat nutzen darf.

_____, den _____

Ort Datum

_____ _____

Name Mitarbeiter:in Unterschrift des/der Verpflichteten