ALLGEIER EXPERTS

INFORMATIONSSICHERHEITSRICHTLINIE FÜR EXTERNE DIENSTLEISTER UND GESCHÄFTSPARTNER

Richtlinie für externe Dienstleister und Geschäftspartner

Revision 2.7 | Stand: 22.02.2021

UNTERNEHMEN:

Allgeier Experts SE

Gustav-Stresemann-Ring 12-16

65189 Wiesbaden

INHALT

1. VORWORT (UNTERNEHMEN UND GESCHÄFTSZWECK)

Die Allgeier Experts SE bietet Personal- und Projektdienstleistungen für die Bereiche IT und Engineering an. Die Allgeier Experts verbinden ihre Kunden mit den besten IT- und Engineering-Experten. Als strategischer Partner lösen sie einfache Personalbedarfe ebenso wie komplexe Projektaufgaben durch ihre Technologie-, Methoden- und Prozesskompetenz, gepaart mit einem optimalen Mix aus eigenen Mitarbeitern, Freiberuflern und Experten auf Zeit.

Im Allgeier Experts Verbund steht die Allgeier Experts Go für die Vermittlung von freiberuflichen IT-Spezialisten und Ingenieuren, die Allgeier Experts Pro für die Überlassung von Personal nach dem Arbeitnehmerüberlassungsgesetz und Rekrutierungsdienstleistungen inkl. Direktvermittlung. Die Allgeier Experts Services GmbH bedient die Kunden mit IT-Management Consulting, die Übernahme von IT-Services und Projekten im gesamten IT-Bereich mit den Schwerpunkten: Managed Services, IT-Projekte und IT-Projektmanagement, IT-Personalservice, IT-Operation, IT-Service Desk, IT-Field Services und IT-Security. Die Allgeier Experts Services trägt hierbei besondere Verantwortung bei dem Umgang mit Kundendaten und -systemen, bei der sich Kunden vollends auf die Informationssicherheit verlassen müssen.

2. GELTUNGSBEREICH/ANWENDUNGSBEREICH

Diese Sicherheitsrichtlinie gilt für alle externen Dienstleister und Lieferanten, die für unser Unternehmen tätig sind und dabei Zugang zu unseren Datenverarbeitungssystemen haben. Sie gilt auch dann, wenn der externe Dienstleister informationssicherheitsrelevante Informationen und Daten von unserem Unternehmen erhalten.

3. EINHALTUNG VON RECHTSVORSCHRIFTEN

Bei Umgang mit Informationen in unserem Unternehmen sind von den externen Dienstleistern und Lieferanten die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie unsere Unternehmensregelungen einzuhalten. Sollten externen Dienstleister und Lieferanten unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren Ansprechpartner in unserem Unternehmen zur Klärung zu wenden.

4. ABWEICHEN VON VORGABEN

Jegliche Abweichung von den Informationssicherheitsvorgaben bedarf der vorherigen schriftlichen Freigabe durch den Informationssicherheits- oder den Datenschutzbeauftragten.

5. ARTEN VON INFORMATIONEN

Zur Gewährleistung des sicheren und sorgsamen Umgangs mit Informationen sind die folgenden 4 Kategorien für die Einstufung von Informationen hinsichtlich Vertraulichkeit festgelegt. Die Verantwortung für die richtige Klassifizierung und den Umgang mit den Informationen trägt der Informationseigner.

Wichtiger Hinweis zur Anwendung der Informationsklassifizierung bei elektronisch gespeicherten Daten: Die Klassifizierung nach den einzelnen Gruppen erfolgt bereits durch die restriktive Vergabe der Benutzerberechtigungen. Eine direkte Kennzeichnung der elektronischen Daten mit der Klassifizierung erfolgt bei der elektronischen Speicherung in den Business IT Systemen nicht. Hier muss im Rahmen einer etwaigen Weitergabe darauf geachtet werden, dass die Klassifizierung eindeutig vorgenommen wird.

Die Kennzeichnung ist verbindlich für alle seit Veröffentlichung der Richtlinie angelegten Dokumente. Nicht gekennzeichnete Dokumente werden gemäß der im Folgenden definierten Einstufung klassifiziert. Bei Unklarheiten hat der Fachbereich die Klassifizierung zu entscheiden.

5.1 VERTRAULICHKEIT

Informationen, die nicht zur allgemeinen Veröffentlichung bestimmt sind, sind nur den dafür Berechtigten zugänglich zu machen. Zur Gewährleistung des sicheren und sorgsamen Umgangs mit Informationen sind die folgenden 4 Kategorien für die Einstufung von Informationen hinsichtlich Vertraulichkeit festgelegt.

5.1.1 Geheime Informationen

Die Einstufung **geheim** bezeichnet die vertraulichsten aller Informationen gemäß Schutzklasse 3 der DIN 66399 und der Sicherheitsstufen 4, 5, 6 und 7. Hierbei handelt es sich um Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe und Verwendung das Unternehmen nachhaltig gefährden kann.

+ Die Weitergabe von geheimen Informationen muss auf einen sehr kleinen, namentlich bekannten Kreis von Personen beschränkt sein.
+ Halten Sie geheime Informationen immer unter Verschluss.
+ Papierunterlagen müssen Sie mit dem Wort „Geheim“ kennzeichnen, dies kann durch einen Stempel oder ähnliche Kennzeichnungen erfolgen.
+ Bei der Erstellung von vertraulichen Informationen müssen Sie die Kopf- oder Fußzeile mit „Geheim“ kennzeichnen.
+ Geheime Informationen dürfen Sie an externe Adressaten NUR VERSCHLÜSSELT per Email versenden, wenden Sie sich im Bedarfsfall an Ihren Ansprechpartner unseres Unternehmens.
+ Das Speichern von geheimen Informationen zum Transport darf NUR AUF VERSCHLÜSSELTEN mobilen Datenträgern (z.B. Notebookfestplatten) erfolgen.
+ Die Löschung und Vernichtung müssen in geeigneter Weise erfolgen (Aktenvernichter etc.).
+ Geheime Information dürfen nur auf individuellen und von Ihnen bewachten Druckern gedruckt werden.

Beispiele für **geheim** eingestufte Informationen sind:

- Unterlagen, die der Jahresabschlusserstellung dienen
- Strategische Entscheidungsgrundlagen
- Account-Passwörter (ausgenommen Initialpasswörter)

Eine Verletzung der Vertraulichkeit hat erhebliche Auswirkungen auf die Außenwirkung / das Erscheinungsbild des Unternehmens und/oder wirtschaftliche Konsequenzen, z.B.:

- Deutliche Einbrüche bei Verkaufszahlen / Umsatz
- Massive Schadensersatzansprüche durch zahlreiche Personen oder Organisationen
- Ausschluss aus bestimmten Märkten
- Nachteilige Auswirkungen auf das öffentliche Ansehen

5.1.2 Vertrauliche Informationen

Die Einstufung **vertraulich** bezeichnet Informationen mit dem zweithöchsten Vertraulichkeitsniveau gemäß Schutzklasse 2 der DIN 66399 und der Sicherheitsstufe 3. Hierbei handelt es sich um Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe und Verwendung das Erreichen von Zielen gefährden kann.

+ Die Weitergabe von vertraulichen Informationen muss auf einen Personenkreis beschränkt sein.
+ Halten Sie vertrauliche Informationen unter Verschluss zu halten.
+ Papierunterlagen müssen Sie mit dem Wort „Vertraulich“ zu kennzeichnen, dies kann durch einen Stempel oder ähnliche Kennzeichnungen erfolgen.
+ Bei der die Erstellung von vertraulichen Informationen müssen Sie die Kopf- oder Fußzeile mit „Vertraulich“ kennzeichnen.
+ Vertrauliche Informationen dürfen Sie per Email nur an Personen mit berechtigtem Interesse versenden werden. Sie sind als Absender verpflichtet, den Empfängerkreis vor Versand gründlich zu prüfen.
+ Das Speichern von vertraulichen Informationen erfolgt in Dateiverzeichnissen mit eingeschränktem Benutzerzugriff.
+ Drucke von vertraulichen Informationen müssen Sie sofort vom Drucker entfernen.

Beispiele für **vertraulich** eingestufte Informationen sind:

- Betriebswirtschaftliche Daten, Reportings
- Dokumentationen zu gravierenden Störfällen
- Kalkulationen
- Angebote
- Personaldaten
- Entgelt-Unterlagen
- Bewerberunterlagen
- Expertenprofile
- Vertragsunterlagen
- Entwicklungsdaten
- Projektdaten
- Besprechungsprotokolle
- Kundendatenbanken
- VS-NfD – Sicherheitsrelevante Dokumente

Konsequenzen beim Verlust der Vertraulichkeit sind wahrscheinlich und messbar z.B.:

- Verlust von Kunden
- Rückgang von Verkaufszahlen / Umsatz
- Schadenersatzansprüche einzelner Personen oder Organisationen

5.1.3 Interne Informationen

Intern ist die gebräuchlichste Einstufung von Informationen gemäß Schutzklasse 1 der DIN 66399 und der Sicherheitsstufen 1 und 2. Hierbei handelt es sich um Informationen, die nur für den internen Gebrauch und nicht für die Allgemeine Öffentlichkeit bestimmt sind.

+ Die Weitergabe von internen Informationen ist normalerweise auf größere Personengruppen beschränkt. Der Versand von Emails ist unverschlüsselt möglich.
+ Bei der Erstellung von internen Informationen verwenden Sie grundsätzlich „Intern“ als Kennzeichnung in der Kopf- oder Fußzeile.

Beispiele für intern eingestufte Informationen sind:

- Telefonverzeichnis der Mitarbeiter
- Organigramme
- Aufgabenbeschreibungen
- Prozessbeschreibungen
- Richtlinien
- Management System
- Referenzen ohne Kundenfreigabe
- Vorlagen

Konsequenzen beim Verlust der Vertraulichkeit sind denkbar, jedoch geringfügiger Natur, z.B.:

- Wenig wahrscheinliche Schadenersatzansprüche einzelner Personen oder Organisationen

5.1.4 Öffentliche Informationen

Als öffentlich eingestufte Informationen sind nicht vertraulich und für den allgemeinen Gebrauch innerhalb und außerhalb von Allgeier Experts bestimmt.

+ Unterliegen keinerlei Restriktionen und dürfen z.B. vom Unternehmen in Zeitungen oder im Internet veröffentlicht werden.
+ Die Verwendung von Unternehmensinformationen in der Öffentlichkeit bedarf der Zustimmung der zuständigen Stelle.
+ „öffentliche“ Informationen sind in der Kopf- oder Fußzeile der erstellten Dokumente zu kennzeichnen.

Beispiele für öffentlich eingestufte Informationen sind:

- Marketingunterlagen
- Vertriebspräsentationen
- Referenzlisten mit Kundenfreigabe

5.2 INTEGRITÄT

Zur Gewährleistung der fehlerfreien Verarbeitung der Informationen sowie der Schutz vor unberechtigter Veränderung, werden folgenden Stufen für zur Klassifizierung von Informationen hinsichtlich der Integrität festgelegt.

5.2.1 Integrität der Informationsverarbeitung: Sehr hoch

Eine Verletzung der Integrität der Informationsverarbeitung hat erhebliche Auswirkungen auf die Geschäftstätigkeit und/oder auf die Außenwirkung / das Erscheinungsbild des Unternehmens mit entsprechenden Konsequenzen, z.B.:

- Erheblicher Kundenverlust
- Deutliche Einbrüche bei Verkaufszahlen / Umsatz
- Massive Schadensersatzansprüche durch zahlreiche Personen oder Organisationen
- Ausschluss aus bestimmten Märkten
- Erhebliche Verzögerungen in Arbeitsabläufen
- Fehler/Störungen wirken sich massiv auf Arbeitsergebnisse aus bzw. Serviceprozesse fallen aus
- Entscheidungen werden stark beeinträchtigt / Fehlentscheidungen

Beispiel: Geheime Informationen, vertrauliche Unternehmensinformationen

5.2.2 Integrität der Informationsverarbeitung: Hoch

Eine Verletzung der Integrität der Informationsverarbeitung hat spürbare Auswirkungen auf die Geschäftstätigkeit und/oder auf die Außenwirkung / das Erscheinungsbild des Unternehmens. Konsequenzen sind wahrscheinlich und messbar, z.B.:

- Verlust von Kunden wahrscheinlich
- Rückgang von Verkaufszahlen / Umsatz
- Deutliche Verzögerungen in Arbeitsabläufen
- Fehler/Störungen wirken sich spürbar auf Arbeitsergebnisse aus bzw. wenige Serviceprozesse fallen aus
- Entscheidungen werden beeinträchtigt / Fehlentscheidungen sind wahrscheinlich

Beispiel: Vertrauliche Informationen

5.2.3 Integrität der Informationsverarbeitung: Mittel

Eine Verletzung der Integrität der Informationsverarbeitung hat nur geringe Auswirkungen auf die Geschäftstätigkeit und/oder nur geringe Außenwirkung / das Erscheinungsbild des Unternehmens. Konsequenzen sind denkbar, jedoch geringfügiger Natur, z.B.:

- Geringfügige Verzögerungen in Arbeitsabläufen
- Fehler/ Störungen wirken sich nicht auf Arbeitsergebnisse aus, keine Service Prozesse fallen aus
- Entscheidungen werden nicht beeinträchtigt
- Schadenersatzansprüche einzelner Personen oder Organisationen sind wenig wahrscheinlich

Beispiel: Interne Informationen

5.2.4 Integrität der Informationsverarbeitung: Gering

Eine Verletzung der Integrität der Informationsverarbeitung hat keine absehbaren Auswirkungen auf die Geschäftstätigkeit oder auf die Außenwirkung / das Erscheinungsbild des Unternehmens. Konsequenzen sind nicht zu erwarten.

Beispiel: Öffentliche Informationen

5.3 NACHWEISBARKEIT

Der Zugriff auf schützenswerte Informationen und die Durchführung von Transaktionen muss unbestreitbar sein. Folgende Stufen zur Klassifikation hinsichtlich der Nachweisbarkeit werden festgelegt.

5.3.1 Nachweisbarkeit: Sehr hoch

Für lesende und ändernde Zugriffe müssen Änderungen (inkl. Stand der Änderung) durchführende Personen und Zeitpunkte nachvollziehbar sein.

5.3.2 Nachweisbarkeit: hoch

Für ändernde Zugriffe müssen Änderungen (inkl. Stand der Änderung) durchführende Personen und Zeitpunkte nachvollziehbar sein.

5.3.3 Nachweisbarkeit: Mittel

Für ändernde Zugriffe müssen Art der Änderungen (Hinzufügen, Löschen, Ändern), durchführende Personen und Zeitpunkte nachvollziehbar sein.

5.3.4 Nachweisbarkeit: Gering

Es gibt keine Anforderungen an Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit.

5.4 VERFÜGBARKEIT

Für die Gewährleistung der Verfügbarkeit von Informationen innerhalb eines vereinbarten Zeitraums werden folgende Stufen zur Klassifikation von Informationen hinsichtlich der Verfügbarkeit festgelegt:

5.4.1 Verfügbarkeit: Sehr hoch

Das IT-System muss bezüglich Ausfalls oder unzureichender Antwortzeit zu 99% verfügbar sein, sonst droht ein signifikanter Schaden (finanziell oder für das Image des Unternehmens).

Ein signifikanter Schaden ist dabei z.B.:

- Verlust von Kunden
- Deutliche Einbrüche bei Verkaufszahlen / Umsatz
- Massive Schadensersatzansprüche durch zahlreiche Personen oder Organisationen
- Ausschluss aus bestimmten Märkten
- Fehler/ Störungen wirken sich massiv auf Arbeitsergebnisse aus bzw. mehrere Service Prozesse fallen aus

Beispiel: IT-Systeme, die in der Leistungserbringung eingesetzt werden, z.B. Telefonanlage im Service Desk

5.4.2 Verfügbarkeit: Hoch

Das IT-System muss bezüglich Ausfalls oder unzureichender Antwortzeit zu 98% verfügbar sein, sonst droht ein signifikanter Schaden (finanziell oder für das Image des Unternehmens).

Beispiel: IT-System, mit denen zeitlich verbindliche Zusagen eingehalten werden müssen, z.B. Zahlsysteme, Kommunikationsmittel Telefon/Mobilfunk

5.4.3 Verfügbarkeit: Mittel

Das IT-System muss bezüglich Ausfalls oder unzureichender Antwortzeit zu 95% verfügbar sein. Bei längeren Ausfällen droht ein signifikanter Schaden (finanziell oder für das Image des Unternehmens).

Beispiel: Bewerberportal, Angebotserstellung, O365

5.4.4 Verfügbarkeit: Gering

Das IT-System kann bezüglich Ausfalls oder unzureichender Antwortzeit weniger als 95% verfügbar sein, ohne dass ein signifikanter Schaden (finanziell oder für das Image des Unternehmens) entsteht.

Beispiel: Intranet

6. GRUNDSÄTZE BEIM UMGANG MIT PERSONENBEZOGENEN DATEN

Beim Umgang mit personenbezogenen Daten müssen die nachfolgenden Grundsätze zwingend eingehalten werden:

+ Die Verarbeitung personenbezogener Daten bedarf immer einer Rechtsgrundlage oder der nachweisbaren Einwilligung eines Betroffenen.
+ Die Betroffenen müssen bei Datenerhebung unverzüglich darüber informiert werden und der Zweck der Datenverarbeitung ist zu nennen.
+ Alle Datenverarbeitungsverfahren müssen transparent gestaltet werden.
+ Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie tatsächlich erhoben wurden.
+ Es dürfen nur die personenbezogenen Daten verarbeitet werden, die tatsächlich für die Durchführung der jeweiligen Aufgabe benötigt werden.
+ Bei der Erhebung personenbezogener Daten ist die Informationspflicht (gemäß Art. 12 + 14 DSGVO) zwingend zu erfüllen.
+ Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Bearbeitungstätigkeit notwendig ist. Die findet keine Anwendung bei Erfüllung einer rechtlichen Verpflichtung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, etc..
+ Die Möglichkeit der Anonymisierung oder Pseudonymisierung von personenbezogenen Daten ist zu berücksichtigen.
+ Personenbezogene Daten müssen immer zugriffsgeschützt gespeichert bzw. verwahrt werden.
+ Personenbezogene Daten müssen vor zufälligem bzw. ungewolltem Verlust geschützt werden.

7. RICHTIGES VERHALTEN IN UNSEREN GESCHÄFTSRÄUMEN

+ Zutritt zu den Büroräumen der Allgeier Experts ist nur mit Schlüssel/Zugangskarten möglich.
+ Externe Personen müssen am Empfang durch den besuchten Mitarbeiter registriert werden und dürfen sich nicht frei in den Büroräumen bewegen.
+ Vor dem Verlassen des Gebäudes müssen sich Besucher durch den besuchten Mitarbeiter am Empfang abmelden, dabei sind ggf. ausgegebene Zutrittskarten zurückzugeben.
+ Die standortbezogenen Sicherheitshinweise müssen eingehalten werden (z.B. Fotografierverbot, Schutzausrüstung usw.).
+ Fremdgeräte dürfen nicht an unsere Unternehmensnetzwerke angeschlossen werden.
+ Sie erhalten ggfs. einen Zugang zu unserem Gäste-WLAN.
+ Projektbezogene Regelungen und Vereinbarungen mit Kunden bezüglich der Arbeit in Sicherheitsbereichen werden separat geregelt.
+ Trinken und Essen in den Serverräumen ist nicht gestattet.

8. RICHTIGES VERHALTEN IN DER ÖFFENTLICHKEIT UND IM PRIVATEN UMFELD

Viele Geschäftsgeheimnisse werden durch Gedankenlosigkeit vor allem in Gesprächen mit Kollegen oder durch Telefongespräche in öffentlichem oder privatem Umfeld (z.B. Flugzeug, Biergarten, Restaurant) preisgegeben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

+ Seien Sie sich immer bewusst, worüber Sie wo kommunizieren. Achten Sie bei allen Gesprächen auf Vertraulichkeit.
+ Geben Sie Informationen und Daten unseres Unternehmens in Telefongesprächen nur an persönlich bekannte Geschäftspartner preis.
+ Prüfen Sie im Zweifelsfall durch einen Rückruf die Identität des Anrufers.
+ Achten Sie unterwegs darauf, dass niemand einsehen kann, an welchen Informationen und Daten unseres Unternehmens Sie arbeiten (z.B. Laptop, Dokumente, etc.) z.B. durch eine Polarisationsfolie oder entsprechende Stellung des Screens.
+ Geben Sie keine vertraulichen und geheimen Informationen und Daten unseres Unternehmens in privaten Gesprächen preis.
+ Führen Sie keine vertraulichen Gespräche über Informationen und Daten unseres Unternehmens in der Öffentlichkeit (z.B. in Flugzeugen, in Hotels, Restaurants) oder im Beisein von unbeteiligten und unberechtigten Dritten.
+ Übermitteln Sie keine vertraulichen und geheimen Informationen über unser Unternehmen an Dritte.
+ Lassen Sie mobile Geräte nie unbeaufsichtigt.
+ Geben Sie keine geheimen Informationen am Telefon preis.

- Hinterlassen Sie keine vertraulichen Informationen unseres Unternehmens auf Anrufbeantwortern.
- Geben Sie die Unternehmenshardware nicht an Familienangehörige und Dritte weiter und achten Sie darauf, dass Dritte keinen Zugriff auf Unternehmenshardware (insbesondere Notebook und Mobiltelefon) bekommen.
- Halten Sie die Unternehmenshardware nach Möglichkeit unter Verschluss, wenn Sie diese nicht nutzen.
- Mobile Endgeräte im Unternehmenseigentum dürfen zu betrieblichen Zwecken vom Standort entfernt werden (z.B. Dienstreise, Homeoffice). Andere Werte z.B. Dokumente dürfen außerhalb der Niederlassungen nur in elektronischer Form über Cloud und Terminalserver abgerufen werden. Das Entfernen von Papierdokumenten ohne Freigabe durch ihren Ansprechpartner ist außer zum Zwecke des Transports in andere Niederlassungen oder zum Zwecke der Aushändigung an Kunden unter Berücksichtigung der Vertraulichkeitsvorgaben nicht gestattet. Bei der Nutzung von Dokumenten außerhalb des Unternehmens ist von Ihnen sicherzustellen, dass sie keinem Dritten zugänglich sind weder in mündlicher noch in schriftlicher Form.
- Stellen Sie sicher, dass der Virenschutz und das Patch-Management aktuell ist bzw. für Unternehmenshardware durch die IT erfolgreich durchgeführt werden können.
- Speichern Sie Unternehmensinformationen ausschließlich auf Unternehmensgeräten bzw. unternehmenseigenen Ressourcen (Laufwerke, O365).
- Das Speichern von privaten Daten auf Unternehmensressourcen (PCs, Notebooks, Cloudspace, MDM gemanagter Bereich auf dem Smartphone) ist nicht gestattet.
- Der Zugriff auf Ihre Unternehmensdaten in Ihrem betrieblichen Account von außerhalb des Betriebs ist mit den vom Unternehmen bereitgestellten Mitteln gestattet, etwa einen webbasierten gesicherten Zugriff oder einem vom Auftraggeber realisierten gesicherten Zugang über einen Terminalserver. Das für den Zugang genutzte private Endgerät muss einen aktuellen Patchstand haben und mit einem aktuellen Virenscanner konfiguriert sein. Private mobile Endgeräte müssen eine 6-stellige PIN haben. Ein Verlust mobiler Geräte mit Zugriff ist sofort zu melden. Als Schutzmaßnahme zur Sicherstellung des Datenschutzes und der Datensicherheit wird im Verlustfall das Account-Passwort sofort geändert.

9. RICHTIGER UMGANG MIT SCHÜTZENSWERTEN INFORMATIONEN AUF REISEN UND IM MOBILEN ARBEITEN

Auf den mobilen Endgeräten, die im Eigentum des externen Dienstleisters oder Lieferanten stehen oder von unserem Unternehmen zur Verfügung gestellt werden (z.B. Laptops, Handys, Smartphones, Tablets, ...), sind ggf. unsere unternehmenseigenen Informationen und Daten gespeichert. Verlust oder Diebstahl der Geräte können schädliche Auswirkungen für das Unternehmen haben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Nehmen Sie grundsätzlich nur die Unterlagen, die Sie tatsächlich benötigen, auf Dienstreisen oder ins mobile Arbeiten mit.
- Bei Reisen in Drittländer (bspw. China, USA, Russland) kann nicht ausgeschlossen werden, dass Behörden bei Einreise Zugriff auf Daten von Endgeräten nehmen. Daher dürfen bei Reisen in solche Länder keine Informationen und Daten unseres Unternehmens auf den Geräten gespeichert sein und keine Unternehmensnotebooks mitgeführt werden.

- Speichern Sie nur die Informationen und Daten lokal verschlüsselt ab, die Sie tatsächlich unterwegs benötigen.
- Melden Sie jeden Verlust oder Diebstahl mobiler Endgeräte (Unternehmens- / Kunden- oder eigenes Eigentum) mit Daten oder Zutrittsmöglichkeit zu Unternehmensdaten/-accounts/Kundendaten, Daten oder Dokumenten unverzüglich Ihrem Ansprechpartner in unserem Unternehmen und benachrichtigen Sie den Informationssicherheitsbeauftragten (isb@allgeier-experts.com) und Datenschutzbeauftragten (datenschutz@allgeier-experts.com).
- Führen Sie keine mobilen Endgeräte ohne Passwortschutz mit sich, sofern Sie darauf Informationen und Daten unseres Unternehmens zugreifen.
- Smartphones unseres Unternehmens müssen im Mobile Device Management eingebunden sein.
- Geben Sie mobile Endgeräte bei Reisen nicht mit Ihrem Koffer auf.
- Lassen Sie mitgeführte Unterlagen und mobile Endgeräte nie unbeaufsichtigt (z.B. im Auto) liegen.
- Beim Arbeiten von zuhause aus (mobiles Arbeiten) ist ebenfalls darauf zu achten, dass Unterlagen nicht offen zugänglich liegen bleiben bzw. sind vor Einsicht durch Unbefugte zu schützen. Gleiches gilt für firmeneigene Laptops oder sonstige Hardware. Diese sind gegen Entwendung zu schützen bzw. sicher zu verwahren.
- Im Falle von längerfristigem mobilen Arbeiten (z.B. aufgrund der Corona Pandemie) ist darauf zu achten, dass verwendete Firmenhardware trotzdem regelmäßig einen Zugang zum Firmennetzwerk hat, um gegebenenfalls zu gewährleisten, dass Updates (insbesondere solche von Virenscannern und sonstigen sicherheitsrelevanten Softwareprodukten) durchgeführt werden können.

10. RICHTIGES VERHALTEN IM INTERNET UND BEI DER EMAIL-NUTZUNG

Viele Geschäftsgeheimnisse werden auch durch Gedankenlosigkeit und die unsachgemäße Nutzung von elektronischen Kommunikationsmitteln preisgegeben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Speichern Sie die Zugangsdaten zu unseren Unternehmenssystemen nicht in Ihrem Browser.
- Geben Sie keine Informationen und Daten unseres Unternehmens in sozialen Netzwerken (XING, Facebook oder ähnliche) oder in von Whatsapp und ähnlichen Messenger-Diensten (z.B. snapchat, threema, etc.) preis, die Sie im Rahmen Ihrer Tätigkeit in unserem Unternehmen zur Kenntnis bekommen haben.
- Besuchen Sie nur vertrauenswürdige Internetseiten.
- Klicken Sie nicht auf Links, die in SPAM-Mails oder „Kettenbriefen“ enthalten sind.
- Sofern Ihnen ein E-Mail-Account zur Verfügung gestellt wird, darf dieser ausschließlich für die geschäftliche Kommunikation der Allgeier Experts verwendet werden. Eine private Nutzung ist ausdrücklich verboten. Der Zugriff auf den E-Mail-Account ist mit den vom Unternehmen bereitgestellten Mitteln gestattet, etwa einem webbasierten gesicherten Zugriff auf Ihren E-Mail-Account oder einem vom Auftraggeber realisierten gesicherten Zugang auf den E-Mail-Account über einen Terminalserver.
- Beantworten Sie keine Emails, die persönliche Kennwörter oder PINs anfordern.
- Falls Sie am Absender der Email zweifeln – nicht antworten.

- Es ist nicht gestattet, Software und andere Dateien oder Daten im Internet, einer sog. „Tauschbörse“ oder dem Usenet hochzuladen, herunterzuladen, auf Unternehmenshardware zu installieren oder zu nutzen. Hierzu zählen insbesondere Bildschirmschoner, Spiele, Demo-Versionen oder andere Software, Fotos oder sonstige Bilder sowie Musik- und Videodateien. Als Hochladen gilt auch, wenn Software und andere Dateien oder Daten nicht zum Abruf für Dritte, sondern für eigene Zwecke hochgeladen werden, selbst wenn dies in einem durch Benutzername und Passwort oder sonst geschützten Bereich des Arbeitnehmers geschieht.
- Der Auftraggeber ist berechtigt, durch technische Maßnahmen den Zugriff auf einzelne oder eine bestimmte Gruppe von Internetseiten oder Diensten im Internet aus dem Unternehmensnetzwerk heraus zu unterbinden.

11. SICHERE AUFBEWAHRUNG UND AUSTAUSCH VON INFORMATIONEN (CLEAN DESK POLICY)

- Schließen Sie vertrauliche oder geheime Unterlagen, wenn möglich in Rollcontainern, Schränken bzw. Tresoren ein und lassen Sie sie nicht unbeaufsichtigt auf Ihrem Schreibtisch liegen.
- Sensible Unterlagen, wie z.B. Bewerberunterlagen, Personalakten oder Ausdrucke, dürfen nicht unbeaufsichtigt auf den Schreibtischen oder in Druckern liegen bleiben.
- Sollten Sie sensible Unterlagen ausdrucken ist stets darauf zu achten, dass diese unmittelbar aus dem Drucker entnommen werden.
- Sperren Sie Ihren Computer vor dem Verlassen des Arbeitsplatzes (Tasten "Strg+ALT+Entf" drücken und dann auf "Computer sperren" klicken), oder beenden Sie die Sitzung an Ihrem Computer immer durch "Herunterfahren" und nicht durch "Ruhezustand" oder "Standby".
- Lassen Sie keine Unterlagen (insbesondere Aufzeichnungen auf Flip-Charts oder Whiteboards etc.) in Besprechungszimmern liegen.
- Schließen Sie Türen und Fenster, wenn Sie ein sonst leeres Büro verlassen.
- Lassen Sie nie mobile Geräte unbeaufsichtigt auf Ihrem Schreibtisch liegen.
- Legen Sie alle Daten auf zentralen Systemen ab, da diese regelmäßig gesichert (Backup) werden.
- Auf Endgeräten (Rechner, Laptops, Mobiltelefonen, Mobile Speichermedien (Speicherkarten, etc.)) ist das exklusive Speichern von Daten ohne Synchronisation mit zentralen Systemen nicht erlaubt.
- Das führende System für die Ablage ist die zentrale Speicherablage. Dort ist immer die aktuellste Version abzulegen.
- Die Möglichkeiten der automatisierten Synchronisation (z.B. One Drive) sind zu verwenden.
- Daten müssen so gespeichert oder abgelegt werden, dass auf diese vom Auftraggeber jederzeit zugegriffen werden kann, insbesondere für den Fall der (überraschenden) Abwesenheit.

12. RICHTIGER UMGANG MIT SPEICHERMEDIEN, HARDWARE UND INFORMATIONEN

Auf elektronischen Speicher- und Kommunikationsmedien (z.B. Notebooks, USB-Sticks, CDs, DVDs, etc.) sind oft vertrauliche oder geheime Informationen unseres Unternehmens gespeichert. Um diese Informationen zu

schützen, ist ein sicherer Umgang mit diesen Medien zwingend notwendig. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Die Nutzung von USB Speichermedien in Unternehmenshardware ist grundsätzlich nicht gestattet.
- Vertrauliche Daten dürfen Sie auf mobilen Speichermedien (externe Datenträger) nur verschlüsselt speichern, wenden Sie sich im Bedarfsfall an ihren Ansprechpartner unseres Unternehmens.
- Verstauen Sie bei Flugreisen Ihre mobilen Endgeräte im Handgepäck.
- Verwahren Sie Laptops, Handys, Schlüssel etc. sicher auf, auch außerhalb der Arbeitszeiten.
- Lassen Sie nie mobile Endgeräte unbeaufsichtigt auf Ihrem Schreibtisch liegen.
- Lassen Sie niemanden unter Ihrem Account unbeaufsichtigt auf Ihren Endgeräten arbeiten.
- Private mobile Endgeräte/Speichermedien dürfen nicht an firmeneigene Endgeräte angeschlossen werden
- Verschicken von firmeneigenen Endgeräten ist nur mit vertrauenswürdigen Zustellungsdiensten erlaubt, wenden Sie sich im Bedarfsfall an ihren Ansprechpartner unseres Unternehmens. Der Versand erfolgt stets versichert

13. PASSWÖRTER

Zur Sicherstellung eines ausreichenden Zugangs- und Zugriffsschutzes ist es zwingend erforderlich, dass die Zugangsberechtigten mit Zugang zu den Datenverarbeitungssystemen sichere Passwörter verwenden. Jeder Zugangsberechtigte zu unseren Datenverarbeitungssystemen erhält einen ihm zugeordneten, eindeutigen Benutzernamen, mit dem der Benutzer eindeutig am jeweiligen Datenverarbeitungssystem identifiziert wird. Die nachfolgenden Passwort-Regelungen sind daher unbedingt von jedem Zugangsberechtigten einzuhalten:

- Startpasswörter, die die Zugangsberechtigten im Rahmen der ersten Anmeldung erhalten, sind umgehend durch eigene (individuelle) Passwörter zu ersetzen.
- Passwörter dürfen nicht aufgeschrieben oder am Arbeitsplatz hinterlegt werden.
- Passwörter dürfen nicht an Dritte (auch Kollegen der Abteilung) weitergegeben werden.
- Eine Anmeldung mit den Anmeldedaten eines anderen Benutzers ist verboten.
- Bei der Eingabe von Passwörtern ist darauf zu achten, dass Dritte Passwörter nicht zur Kenntnis nehmen.
- Passwörter müssen mindestens 12 Zeichen haben.
- Die letzten 10 Kennwörter dürfen nicht erneut verwendet werden.
- Passwörter müssen mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.
- Trivialpasswörter dürfen nicht verwendet werden (z.B. qwertz, 12345678, abcdefg).
- Das Geburtsdatum des Benutzers oder dessen Angehörigen darf nicht als Passwort verwendet werden.
- Passwörter müssen regelmäßig selbstständig vom Benutzer gewechselt werden, bzw. sind die Passwörter auf Verlangen des Informationssicherheitsbeauftragten sofort zu wechseln, wenn die Anweisung durch ihn explizit erfolgt.
- Passwörter müssen umgehend gewechselt werden, wenn der Verdacht besteht, dass diese kompromittiert wurden.
- Der Benutzername darf nicht Bestandteil des Passwortes sein.

+ Passwörter für Account Zugänge dürfen nicht gespeichert werden. Passwörter für Zugänge zu Datenverarbeitungssysteme dürfen auf firmeneigenen Endgeräten automatisch gespeichert werden.
+ Die innerhalb des Unternehmens (Netzwerk) verwendeten Passwörter dürfen nicht für Anwendungen im Internet oder im privaten Umfeld verwendet werden.

14. REGELN ZU NETZWERKEN UND NETZWERKDIENSTEN

Jeder Netzwerkzugriff auf unserer IT-System oder die der Kunden stellt ein Risiko dar, da durch diesen ein Kompromittieren des IT-Systems möglich sein kann.

+ Der Zugang zu Kundennetzwerken und Kundensystemen und der Umgang mit den Kundeninformationen im Rahmen der Dienstleistung für Kunden ist gemäß der vertraglichen Regelung mit dem Kunden zu handhaben.
+ Zugang zu firmeninternen Netzwerken ist nur mit firmeneigenen Endgeräten oder über die Terminalserverumgebung gestattet.
+ Firmenfremde Endgeräte dürfen nur mit dem Gäste WLAN verbunden werden.
+ Verbinden Sie Ihre firmeneigenen mobilen Endgeräte nur mit vertrauenswürdigen Netzwerken (z.B. mit Passwortschutz und Authentifizierung) und nutzen Sie für die Bearbeitung von Unternehmensinformationen den Terminalserver. Wenn Zweifel an der Sicherheit von Netzwerken bestehen, weichen Sie auf eine Internetverbindung mit dem Mobiltelefon aus (Tethering).
+ Ein Zugriff auf Unternehmensinformationen von unsicherer Hardware aus (z.B. Internetcafé) ist nicht gestattet.

15. RICHTIGER UMGANG MIT SOFTWARE

+ Die Installation von Software auf IT-Systemen des Unternehmens ohne vorherige Zustimmung des Auftraggebers ist untersagt.
+ Smartphones des Unternehmens unterliegen dem Mobile Device Management. Das MDM gewährleistet eine Trennung zwischen geschäftlichen und privaten Daten und erlaubt es der IT-Administration, das Gerät aus der Ferne zu verwalten und z.B. geschäftliche Daten bei einem iPhone-Verlust aus der Ferne zu löschen. Diese Software verhindert dann auch, dass ein Messenger, wie z.B. WhatsApp auf das geschäftliche Adressbuch zugreifen kann. Geschäftliche Aktivitäten und Ablage von Informationen sind ausschließlich in den durch das MDM verwalteten Bereichen gestattet. Installation von Apps außerhalb des MDM sind gestattet.
+ Die Installation von durch den Auftraggeber beschaffter oder sonst bereitgestellter Software auf privaten IT Systemen ist nur mit expliziter Freigabe gestattet.
+ Mit dem Beenden des Einsatzes eines Lieferanten beim Auftraggeber hat dieser unverzüglich etwaige bei ihm befindliche Kopien der ihm vom Auftraggeber überlassenen Software an den Auftraggeber herauszugegeben sowie Installationen oder Vervielfältigungen zu deinstallieren bzw. zu löschen.

16. VERHALTEN BEI SICHERHEITSVORFÄLLEN ODER SCHWACHSTELLEN

Sollte ein externer Dienstleister oder Lieferant feststellen oder den Verdacht haben, dass der Schutz oder die Sicherheit von Informationen oder Daten in irgendeiner Weise gefährdet sein könnte, z.B. bei Datenverlusten,

Befürchtungen, dass personenbezogene Daten oder sonstige geheime Informationen Dritten unrechtmäßig bekannt geworden sein könnten, oder beim Verdacht auf Einschleusung von Viren, Trojanern, Würmern oder anderen Schadprogrammen, hat dieser sich unverzüglich an seinen Ansprechpartner zu wenden. Alle Beweismaterialien sind unverzüglich zu sichern und bereitzustellen. Dies gilt insbesondere auch dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

Revisionsliste		Sicherheitsrichtlinie für externe Dienstleister	
Zugriffsberechtigung		Alle Mitarbeiter der Allgeier Experts SE mit Töchtern: Allgeier Experts Go, Allgeier Experts Pro und Allgeier Experts Services, externe Dienstleister und Geschäftspartner	
Anwendungsbereich		Externe Dienstleister und Geschäftspartner	
Klassifizierung		intern	
Dokumenteneigner		Processes, Quality & Projects (Informationssicherheitsbeauftragter)	
Freigabe		IS-Steuerkreis	
Version		2.7	
Datum		22.02.2021	
Status		freigegeben	
Version	am	von	Änderungen
0.1	11.03.2019	Brli	Ersterstellung
0.2	17.04.2019	Brli	Review und Anpassung an 27002 in Beratung durch Euroconsult
0.3	30.04.2019	Brli	Anpassung nach Steuerkreisbeschluss
1.0	03.05.2019	Brli+hosa	Finalisierung und Freigabe
1.1	15.05.2019	Brli+hosa	Aufnahme der Kennzeichnungsregeln für öffentliche Dokumente, Bearbeitung vertraulicher Daten in öffentlicher Umgebung, Regeln für die Klassifizierung
2.0	17.05.2019	Brli	Finalisierung nach Steuerkreisbeschluss und Freigabe
2.1	29.05.2019	Brli	Einarbeitung der Verbesserungsvorschläge aus dem Audit
2.2	02.08.2019	Brli	Anpassung an Änderungen in der internen Sicherheitsrichtlinie
2.3	15.08.2019	Brli	Anpassung an Finalisierung der internen Sicherheitsrichtlinie und Umstellung der Kapitelreihenfolge
2.4	21.08.2019	Brli	Umgang mit Drucken von geheimen und vertraulichen Informationen
2.5	22.08.2019 28.08.2019	Sawi+brli	Anpassung Grundzüge mit personenbezogenen Daten. Zusatz zum Schutz vor der Nutzung privater mobiler Geräte.
2.6	24.02.2020	Malb	Allgeier Engineering rausgenommen, da nicht mehr Experts Kern
2.7	22.02.2021	Malb+Niri	Ergänzung von Regelungen zu mobilem Arbeiten, Anpassung der Passwortrichtlinie, Ergänzung der „Clean Desk Policy“