Sicherheitsleitlinie für Partner - InfoSec General

1. Zielsetzung

Diese Richtlinie regelt die Tätigkeiten und Verantwortlichkeiten hinsichtlich der Regeln, die von Dienstleistern beim Umgang mit Informationen und IT-Geräten für die Informationssicherheit durchgeführt werden.

2. Anwendungsbereich

Diese Richtlinie ist von allen Mitarbeitern, die mit der Durchführung und Betreuung von Sicherheitsleitlinien für Partner betraut sind, zwingend anzuwenden. Die Nennung der männlichen Form in diesem Dokument erfolgt ausschließlich aus Gründen der besseren Lesbarkeit. Mit der männlichen Person sind zugleich sämtliche Personen gleichwelchen Geschlechtes gemeint.

Verbindlich für:
ALTEN GmbH und verbundene Unternehmen

3. Verantwortlichkeiten

Die Gesamtverantwortung für diese Richtlinie liegt bei dem Prozessverantwortlichen. Dieser gibt das Dokument zur Veröffentlichung frei.

4. Definitionen

Begriff	Beschreibung
n.z	n.z.

5. Allgemeine Anforderungen

Die folgenden Anforderungen müssen von allen Dienstleistern, entsprechend der Definition in diesem Dokument, eingehalten werden.

Anforderungen an den Auftraggeber sind nicht Bestandteil dieses Dokuments.

5.1. Organisatorische Anforderungen

Regelungen des Auftraggebers bezüglich des Mitbringens von nicht dem Auftraggeber gehörenden IT-Geräten auf das Firmengelände oder in Sicherheitsbereiche (Projektbüros) müssen eingehalten werden.

Die Weitergabe von Daten an Dritte ist nur mit schriftlicher Freigabe vom Dateneigentümer des Auftraggebers gestattet.

Regelungen des Auftraggebers zur Verwendung, Speicherung und jedweder Verarbeitung von personenbezogenen Daten (siehe auch Anhang, A.1.2) müssen eingehalten werden.

Mitarbeiter des Dienstleisters müssen von ihrer Geschäftsleitung auf die Geheimhaltung im Sinne der bestehenden Vertraulichkeitsvereinbarung zwischen Auftraggeber und Auftragnehmer verpflichtet werden. Dem Auftraggeber ist jederzeit Einsicht in diese Vereinbarungen zu gewähren.

Falls Daten des Auftraggebers auf mobilen Systemen oder IT-Geräten gespeichert werden, sind diese mit dem aktuellen Stand der Technik entsprechender Hardware oder Software zu verschlüsseln.

Nach Vertragsende müssen Daten des Auftraggebers an den Auftraggeber übergeben werden und sind auf Geräten und Speichermedien des Dienstleisters zu löschen. Die Vorgaben des Auftraggebers und rechtliche Anforderungen (z.B. Geheimhaltungsvereinbarung, Rahmenvertrag, Aufbewahrungspflichten) sind zu beachten.

5.2. Personalsicherheit

Eine nicht mehr benötigte Benutzerkennung oder ein nicht mehr benötigtes Zugriffsrecht auf Daten des Auftraggebers, ist von dem jeweiligen Nutzer unverzüglich bei den jeweiligen auftraggebenden Stellen (z.B. zuständiger Benutzeradministrator bzw. IT-Support des Auftraggebers, siehe A.1.4) zu melden, damit die entsprechende Sperrung/ Löschung erfolgen kann.

Nicht mehr benötigte Medien zur Identifizierung (z.B. RSA-Token) sind unverzüglich an die auftraggebende Stelle zurückzugeben.

Überlassene Geräte (z.B. Laptops) und Datenträger bzw. Speichermedien müssen nach Ablauf des Vertrags, oder wenn diese nicht mehr benötigt werden, an den Auftraggeber zurückgegeben werden.

Der Verlust von, an den Benutzer übergebenen, IT-Geräten sowie von Medien zum Zwecke der Authentifizierung, sind durch den Benutzer umgehend der zuständigen Stelle des Auftraggebers (siehe Anhang, A.1.4) zu melden.

5.3. Physische und umgebungsbezogene Sicherheit

IT-Geräte, die Daten des Auftraggebers speichern oder verarbeiten sind so zu verwenden, dass keine Unbefugten diese Daten einsehen oder darauf zugreifen können. Besondere Vorsicht ist bei der Verwendung mobiler Systeme geboten.

Vertrauliche und geheime Dokumente dürfen niemals unbeaufsichtigt liegengelassen werden, um Einsichtnahme durch Unberechtigte zu verhindern.

5.4. Management von organisationseigenen Werten

5.4.1. Regelungen für die Klassifikation

Eine Klassifikation findet anhand der drei Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit statt und muss für alle Informationen und alle informationsverarbeitenden IT-Systeme durchgeführt werden.

Die Klassifikation hat den Zweck, Informationen abhängig von deren Schutzbedürftigkeit in Stufen einzuordnen. Abhängig von der Einordung sind unterschiedliche Schutzmaßnahmen erforderlich.

Informationen (Schutzziel Vertraulichkeit) sind über ihre gesamte Lebensdauer hinweg gemäß den Maßnahmen, die ihrer Vertraulichkeitseinstufung entsprechen, vor unbefugtem Zugriff zu schützen. Falls erforderlich, ist bei der Verarbeitung von Daten die Klassifikation in Bezug auf Integrität und Verfügbarkeit durch den jeweiligen Prozesseigentümer zu überprüfen und zu bestimmen. Diese Klassifikation ist regelmäßig, unter Einbeziehung des Informationseigentümers, zu evaluieren und gegebenenfalls anzupassen.

5.4.1.1. Vertraulichkeit

Informationen, die nicht für die Allgemeinheit bestimmt sind, dürfen nur den Personen zugänglich gemacht werden, die dazu berechtigt sind (Grundsatz „Kenntnis nur, wenn nötig“).

Vorgaben für Ersteller und Eigentümer von Informationen:

- Neu erstellte Informationen und Daten sind durch den Ersteller zu kennzeichnen.
- Der Informationseigentümer ist verantwortlich für die Klassifikation.
- Der Ersteller muss die korrekte Klassifikation über den Informationseigentümer anfordern.
- Vertraulichkeitseinstufungen müssen für alle IT-Systeme erfolgen.
- Wenn eine Klassifikation noch nicht eindeutig ist, beispielsweise bei neu angelegten Dokumenten/IT-Systemen, ist die Einstufung „vertraulich“ zu wählen.
- Der Informationseigentümer muss (spätestens bei der nächsten Überprüfung oder Aktualisierung) für interne (C1), vertrauliche (C2) und streng vertrauliche (C3) Informationen prüfen, ob deren Vertraulichkeitseinstufung noch korrekt ist, und sie entsprechend kennzeichnen.

Vorgaben für den Empfänger:

- Nicht gekennzeichnete Informationen und Daten gelten als vertraulich.

- Im Falle von Zweifeln an der Klassifikation ist der Informationseigentümer zu kontaktieren.

Folgende Klassifikationsstufen sind in Bezug auf die Vertraulichkeit von Informationen definiert:

Klassifikation	Definition
Öffentlich (C0)	Dies betrifft alle Informationen, welche von ALTEN veröffentlicht wurden und somit frei verfügbar sind, wie z.B.: • Werbemitteln (Flyer etc.) • alle öffentlichen Teile der Webseite Bei Werbemitteln (Flyer etc.) kann auf eine Kennzeichnung der Informationen verzichtet werden.
Intern (C1)	Dies betrifft alle Informationen, deren unerwünschte Offenlegung oder Weitergabe an Dritte einen Schaden für die Firma nach sich ziehen kann. Dies sind in der Regel Informationen, die einem größeren Mitarbeiterkreis zugänglich, jedoch nicht für Außenstehende bestimmt sind, wie z.B.: • Interne Kommunikation (Schriftverkehr per E-Mail, virtuelle Teams), • interne Regelungen (Richtlinien, Rundschreiben, Anweisungen, Organisationspläne), • interne Informationen (Arbeitsergebnisse, Planungen und Vorhaben), • Veröffentlichungen im Intranet
Vertraulich (C2)	Dies betrifft alle Informationen, deren unerwünschte Offenlegung oder Weitergabe an Dritte einen erheblichen finanziellen Schaden, rechtliche Konsequenzen oder eine Schädigung des Ansehens von ALTEN nach sich ziehen können. Diese sind immer mit den Vermerk „vertraulich“ zu versehen. Hier werden in der Regel alle Informationen eingeordnet, die für den technischen oder finanziellen Erfolg einzelner Unternehmensbereiche von Bedeutung sind. Insbesondere sind dies alle Informationen, welche für Mitbewerber von Wert sein könnten, so z.B.: • vertrauliche Kommunikation (Kunden Schriftverkehr per E-Mail, Video Conferencing & Collaboration), • Sicherung der Wettbewerbsfähigkeit (Marketingdaten, Kunden- und Lieferantendaten, Kundenanfragen) • personenbezogene Daten, • Reisekosten- und Lohnabrechnung, • Forschungsdaten, • Projektinformationen (kaufmännisch, technisch), • techn. Daten (Baupläne sensibler Räume, Netzwerkpläne)
Streng vertraulich (C3)	Die betrifft firmenvertrauliche Informationen, deren unerwünschte Offenlegung oder Weitergabe an Dritte einen sehr schweren Schaden für die Geschäftszwecke und Ziele von ALTEN, gravierende rechtliche Konsequenzen oder eine schwere Schädigung des Ansehens nach sich ziehen kann. Diese Informationen sind immer die Schutzklasse „streng vertraulich“ zu vermerken. Dies sind üblicherweise Informationen, die für den Erfolg und das Weiterbestehen der ganzen Firma von größter Bedeutung sind, z.B.: • Firmenstrategien, • technologische und strategische Planungen, • Informationen über geplante Firmenübernahmen oder Firmenverkäufe, • Wirtschafts- und Budgetpläne von Unternehmensbereichen, • Informationen gleicher Vertraulichkeit von Geschäftspartnern, • Informationen über Krisensituationen, • Kopien streng vertraulicher Informationen

5.4.1.2. Integrität

Die fehlerfreie Verarbeitung von Informationen und der Schutz vor unbefugten Änderungen müssen sichergestellt werden.

Folgende Klassifikationsstufen sind in Bezug auf die Integrität von Informationen definiert:

Klassifikation	Definition
Gering **(I0)**	Eine Verletzung der Integrität hat keine vorhersehbaren Auswirkungen auf die geschäftlichen Tätigkeiten oder das Image bzw. Erscheinungsbild des Unternehmens.
Mittel **(I1)**	Eine Verletzung der Integrität hat nur geringe Auswirkungen auf die geschäftlichen Tätigkeiten und/oder das Image bzw. Erscheinungsbild des Unternehmens. Es kann zu negativen Folgen kommen, wenn auch in geringem Umfang. Beispiele: • leichte Verzögerungen bei Arbeitsabläufen • Fehler ohne Auswirkungen auf die Arbeitsergebnisse (keine produktiven Ausfallzeiten) • Entscheidungen werden nicht beeinträchtigt • Schadenersatzforderungen durch Einzelpersonen oder Organisationen sind unwahrscheinlich
Hoch **(I2)**	Eine Verletzung der Integrität hat spürbare Auswirkungen auf die geschäftlichen Tätigkeiten und/oder das Image bzw. Erscheinungsbild des Unternehmens. Es kommt voraussichtlich zu messbaren negativen Folgen, wie z. B.: • Verlust von Kunden ist wahrscheinlich • deutliche Verzögerungen bei Arbeitsabläufen • Fehler/Fehlfunktionen mit wahrnehmbaren Auswirkungen auf die Arbeitsergebnisse (hohe Produktionsausfälle) und/oder Ausfall einiger Serviceprozesse • Entscheidungen werden beeinträchtigt / Fehlentscheidungen sind wahrscheinlich • Schadenersatzforderungen durch Einzelpersonen oder Organisationen sind wahrscheinlich
Sehr hoch **(I3)**	Eine Verletzung der Integrität hat erhebliche Auswirkungen auf die geschäftlichen Tätigkeiten und/oder das Image bzw. Erscheinungsbild des Unternehmens sowie entsprechende Konsequenzen, wie z. B.: • erheblicher Verlust von Kunden • Schadenersatzforderungen durch diverse Einzelpersonen oder Organisationen • Ausschluss aus bestimmten Marktgebieten • deutliche Verzögerungen bei Arbeitsabläufen • Fehler/Fehlfunktionen mit schwerwiegenden Auswirkungen auf die Arbeitsergebnisse und/oder Ausfall mehrerer Serviceprozesse (sehr hohe produktive Ausfallzeiten) • Entscheidungen werden stark beeinträchtigt / falsche Entscheidungen getroffen Beispiele: Bilanzierung (z.B. Jahresabschluss), Patente, kryptographische Schlüssel, Lohnabrechnung

5.4.1.3. Verfügbarkeit

Informationen müssen innerhalb eines vereinbarten Zeitraums verfügbar sein.

Folgende Klassifikationsstufen sind in Bezug auf die Verfügbarkeit von Informationen definiert:

Klassifikation	Definition
Gering (A0)	Die Verfügbarkeit des IT-Systems darf in Bezug auf Ausfall oder inakzeptable Antwortzeiten weniger als 95 % betragen, ohne dass es zu nennenswerten Beeinträchtigungen (z.B. finanzieller Art oder am Image des Unternehmens) kommt.
Mittel (A1)	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 95 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (z.B. finanzieller Art oder am Image des Unternehmens).
Hoch (A2)	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 98 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (z.B. finanzieller Art oder am Image des Unternehmens).
Sehr hoch (A3)	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 99 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (z.B. finanzieller Art oder am Image des Unternehmens). Beispiel: IT-System, dessen Ausfall einen unmittelbaren Produktionsstopp zur Folge hat Bei nennenswerten Beeinträchtigungen kann es sich z. B. handeln um: • Verlust von Kunden • Schadenersatzforderungen durch diverse Einzelpersonen, Organisationen oder Verbände Fehler/Fehlfunktionen mit schwerwiegenden Auswirkungen auf die Arbeitsergebnisse und/oder Ausfall mehrerer Serviceprozesse (sehr hohe produktive Ausfallzeiten)

5.4.2. Kennzeichnung von Informationen und Umgang mit Informationen

Informationen dürfen nur einer berechtigten Gruppe von Personen zum Zwecke der vereinbarten Tätigkeiten und unter Einhaltung der entsprechenden Regelungen zugänglich gemacht werden. Dabei ist der Grundsatz „Kenntnis nur, wenn nötig“ zu befolgen.

Informationen müssen während des gesamten Lebenszyklus entsprechend ihrer aktuellen Vertraulichkeitseinstufung vor einem Zugriff durch Unberechtigte geschützt werden. Es gelten folgende Regelungen:

Klassifikation	Anforderungen
Öffentlich	Es gelten die unternehmensinternen Vorgaben zur Positionierung der Kennzeichnung der Klassifikation: • **Kennzeichnung**: „öffentlich“ (Verzicht auf Kennzeichnung bei Flyern oder anderen Marketing-Maßnahmen möglich) • **Vervielfältigung und Verteilung:** keine Einschränkungen • **Speicherung:** keine Einschränkungen • **Löschung**: keine Einschränkungen • **Entsorgung**: keine Einschränkungen

Intern (C1)	Es gelten die unternehmensinternen Vorgaben zur Positionierung der Kennzeichnung der Klassifikation: • **Kennzeichnung:** Angabe der Vertraulichkeitsstufe in Landessprache/ „Intern“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form • **Vervielfältigung und Verteilung:** nur an berechtigte Mitarbeiter der Firma und berechtigte Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereichs • **Speicherung:** Schutz vor unbefugtem Zugriff • **Löschung:** Nicht mehr benötigte Daten sind zu löschen (siehe Anhang, A.1.2, A.1.3) • **Entsorgung:** ordnungsgemäße Entsorgung (siehe Anhang, A.1.2, A.1.3)
Vertraulich (C2)	Es gelten die unternehmensinternen Vorgaben zur Positionierung der Kennzeichnung der Klassifikation: • **Kennzeichnung:** Angabe der Vertraulichkeitsstufe in Landessprache/ „Vertraulich“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form • **Vervielfältigung und Verteilung:** nur an eine beschränkte Gruppe von berechtigten Mitarbeitern der Firma und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs. Die Person, die die Informationen verteilt, ist für angemessene Verteilwege verantwortlich, um die Informationen und Daten vor unbefugtem Zugriff und/oder unbefugtem Mithören zu schützen (z. B. mithilfe von Verschlüsselung). • **Speicherung:** Zugriff nur für eine beschränkte Gruppe von berechtigten Mitarbeitern der Firma und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs (z. B. durch geschlossene Nutzergruppen). Es sind geeignete Speicherorte und/oder Speichermedien zu verwenden. • **Löschung:** Nicht mehr benötigte Daten sind zu löschen (siehe Anhang, A.1.2, A.1.3)) • **Entsorgung:** ordnungsgemäße Entsorgung (siehe Anhang, A.1.2, A.1.3)) • **Authentifizierung:** Starke Authentifizierung (2. Faktor) • **Transport:** Vertrauliche Dokumente und Speichermedien müssen in verschlossenen, neutralen Umschlägen verendet werden; bei Bedarf kann der Zusatz “persönlich” hinzugefügt werden. Dies bedeutet, dass der Umschlag nur direkt an den genannten Empfänger übergeben werden darf.
Streng vertraulich (C3)	Es gelten die unternehmensinternen Vorgaben zur Positionierung der Kennzeichnung der Klassifikation: • **Kennzeichnung:** Angabe der Vertraulichkeitsstufe in Landessprache / „Streng vertraulich“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form. Darüber hinaus sind alle Seiten mit „Seite x von y“ zu kennzeichnen. • **Vervielfältigung und Verteilung:** nur an eine äußerst begrenzte Gruppe (z.B. namentliche Liste) von berechtigten Mitarbeitern der Firma und berechtigte Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereichs und nach vorheriger Genehmigung durch den Informationseigentümer. Soweit technisch möglich, sind alle Daten nach aktuellem Stand der Technik zu verschlüsseln. Falls dies nicht möglich ist, sind vergleichbar starke Sicherheitslösungen zu verwenden. Je nach Anwendungsfall sind weitere technische bzw. organisatorische Schutzmaßnahmen zu verwenden (z.B. Verbot von Weiterleiten und Ausdrucken, Wasserzeichen). • **Zur Kommunikation:** sind geeignete Medien zu verwenden, die ein Mithören verhindern (z.B. verschlüsselte Videokonferenzen). • **Speicherung:** Zugriff nur für eine äußerst begrenzte Gruppe (z.B. namentliche Liste) von berechtigten Mitarbeitern der Firma und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs (z.B. durch geschlossene Nutzergruppen). Soweit technisch möglich, sind alle Daten nach aktuellem Stand der Technik zu verschlüsseln. Falls dies nicht möglich ist, sind vergleichbar starke Sicherheitslösungen zu verwenden. • **Löschung:** Nicht mehr benötigte Daten sind zu löschen (siehe Anhang, A.1.2,

	A.1.3). • **Entsorgung:** ordnungsgemäße Entsorgung (siehe Anhang, A.1.2, A.1.3) • **Authentifizierung:** Starke Authentifizierung (2. Faktor) • **Transport:** Streng vertrauliche Dokumente und Speichermedien müssen in neutralen, verschlossenen Umschlägen (ohne Zusätze wie „persönlich, geheim, etc.“) versendet werden. In diesen ist ein zweiter innerer Umschlag zu platzieren, welcher mit der Klassifikation „geheim” oder „streng vertraulich“ gekennzeichnet ist.

Nicht gekennzeichnete Informationen, welche offensichtlich nicht „öffentlich“ sind, sind als „Vertraulich” einzustufen.

Die Vorgaben zum Umgang mit Informationen (Kennzeichnung, Vervielfältigung, Verteilung, Speicherung, Löschung und Entsorgung) gelten ebenfalls für IT-Systeme (z.B. Datenbanken und Sicherungsmedien).

5.4.3. Umgang mit Speichermedien

Datenträger (wie z.B. CDs, DVDs, USB-Sticks und Festplatten) sind vor Verlust, Zerstörung und Verwechslung sowie vor unbefugtem Zugriff zu schützen.

Nicht mehr benötigte Datenträger sind auf sichere Weise zu entsorgen (siehe Anhang, A.1.3).

5.4.3.1. Informationsaustausch

Bei allen Gesprächen (einschließlich Telefonaten, Video- und Webkonferenzen), die vertrauliche oder geheime Informationen betreffen oder enthalten, ist sicherzustellen, dass diese nicht unberechtigt mitgehört werden können.

Faxnummern und E-Mail-Adressen sind aktuellen Verzeichnissen zu entnehmen oder beim Empfänger zu erfragen, um fehlerhafte Übertragungen zu vermeiden.

Für den Inhalt und die Verteilung einer E-Mail ist der Absender verantwortlich. Für die weitere Verarbeitung und Verteilung der Empfänger.

5.5. Umgang mit Informationssicherheitsvorfällen

Informationssicherheitsereignisse (z.B. auftretende Störungen, Verstöße gegen das Informationssicherheits-Regelwerk), welche Daten oder Systeme des Auftraggebers betreffen sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang, A.1.5).

Vermutete Verwundbarkeiten und Schwachstellen von IT-Systemen sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang, A.1.4)

Beim Verdacht auf Verlust von vertraulichen oder geheimen Informationen muss dies sofort an die zuständige Stelle gemeldet werden (siehe Anhang, A.1.7).

5.6. Compliance und Einhaltung gesetzlicher Verpflichtungen

Durch den Dienstleister ist ein Compliance Management unter Beachtung rechtlicher und betrieblicher Anforderungen (inklusive Ressourcenmanagement, internes Kontrollsystem, IT Continuity Management und Schutz von Informationen) einzurichten. Dies muss alle Informationen, Hard- und Software des Auftraggebers umfassen.

Die zuständige Stelle (siehe Anhang, A.1.7) ist für Anfragen und Hilfestellungen zu kontaktieren. Das

Compliance Management muss die folgenden Punkte beinhalten.

5.6.1. Risikofrüherkennung

Ein Prozess zur frühen Erkennung von Risiken und potenziellen Bedrohungen für IT-Systeme und Daten muss implementiert sein.

Vorbeugende Tätigkeiten und Maßnahmen müssen getroffen werden, um erkannte Risiken zu behandeln.

5.6.2. Geistiges Eigentum / Lizenzmanagement

Alle Rechte geistigen Eigentums (z.B. Urheberrechte an Software, Dokumenten und Grafiken, Entwurfsrechte, Handelsmarken, Patente und Quellcode-Lizenzen) sind zu beachten und einzuhalten.

Die Verwendung nicht lizenzierter Software (Raubkopien) ist nicht zulässig.

Für lizenzierte Software gelten die gesetzlichen Bestimmungen hinsichtlich Urheberrechte (z.B. verstößt das Anfertigen von Kopien, ausgenommen zu Sicherungs- und Archivierungszwecken, gegen die Urheberrechte). Verstöße gegen diese Bestimmungen können eine strafrechtliche Verfolgung nach sich ziehen und einstweilige Verfügungen oder Schadenersatzforderungen zur Folge haben.

Lizenzierte Software darf nur zum vereinbarten Zweck unter Einhaltung geltender Vorschriften und Lizenzvereinbarungen mit dem Hersteller verwendet werden.

5.6.3. Datenschutz

Die jeweiligen landesspezifischen Gesetze und Vorschriften zum Datenschutz (siehe Anhang, A.1.8) sind einzuhalten.

Auftragnehmer müssen von der Geschäftsführung des jeweiligen Dienstleisters auf die Einhaltung der gesetzlichen Datenschutzvorgaben verpflichtet werden.

5.6.4. Vertragliche Compliance

Die IT-Organisation des Dienstleisters muss die vertraglichen Anforderungen des Auftraggebers erfüllen. Es müssen Maßnahmen implementiert sein um sicherzustellen, dass die eigenen organisatorischen Regelungen des Dienstleisters überprüft und aktuell gehalten werden, so dass die aktuellen vertraglichen Anforderungen abgebildet sind.

5.6.5. Interne Anweisungen

Dienstleister müssen ihren Mitarbeitern Regelungen und Verhaltensgrundsätze vorgeben, um die Einhaltung der Anforderungen und den angemessenen Umgang mit Informationen sowie Hard- und Software des Auftraggebers sicherzustellen.

5.7. Verstöße und Durchsetzung

Verstöße gegen die Informationssicherheits-Handlungsleitlinien müssen individuell entsprechend der geltenden betrieblichen, vertraglichen und rechtlichen Vorschriften und Vereinbarungen geprüft und geahndet werden.

5.7.1. Kategorien von Ereignissen und Beobachtungen

Wir unterscheiden vier meldepflichtige Hauptkategorien.

Ereignisse und Beobachtungen in Bezug auf Personal

(z. B. Verfehlung/Fehlverhalten)
Hier geht es um menschliches Verhalten, das die Informationssicherheit beeinträchtigen könnte.

Beispiele:

- Ein Mitarbeiter lässt vertrauliche Unterlagen offen liegen.
- Ein Mitarbeiter teilt sein Passwort.
- Ein Mitarbeiter nutzt private Geräte für dienstliche Daten, obwohl das untersagt ist.
- Ein Mitarbeiter sendet eine E-Mail an den falschen Empfänger
- Ein Mitarbeiter verwendet eine nicht freigegebene KI-Software zur Arbeit

Ereignisse und Beobachtungen in Bezug auf die physische Sicherheit

(z. B. Einbruch, Diebstahl, unbefugter Zugang zu Sicherheitszonen, Schwachstellen in den Sicherheitszonen)
Physische Sicherheit schützt unsere Gebäude, Geräte und Informationen.

Beispiele:

- Eine Tür zu einem gesicherten Bereich schließt nicht richtig.
- Sie sehen eine fremde Person ohne Ausweis im Büro.
- Ihr Laptop wird gestohlen.
- Besuchende bewegen sich unbeaufsichtigt durch Sicherheitszonen.
- Jemand blockiert den automatischen Türschließer.

Ereignisse und Beobachtungen in Bezug auf IT und Cybersicherheit

(z. B. anfällige IT-Systeme, erkannte erfolgreiche oder nicht erfolgreiche Angriffe)
Hier geht es um digitale Risiken und technische Schwachstellen.

Beispiele:

- Sie bekommen eine verdächtige E-Mail (Phishing).
- Ihr Computer verhält sich merkwürdig oder ist ungewöhnlich langsam.
- Sie entdecken ein unbekanntes Programm auf Ihrem Gerät.
- Sie bemerken, dass jemand unbefugt auf ein System zugreift.

Ereignisse und Beobachtungen in Bezug auf Lieferanten und andere Geschäftspartner

(z. B. alle Vorfälle, die sich negativ auf die Sicherheit der eigenen Organisation auswirken können)
Auch externe Partner beeinflussen unsere Informationssicherheit.

Beispiele:

- Sie erfahren, dass ein Lieferant Opfer eines Cyberangriffs wurde.
- Ein externer Dienstleister sendet Daten unverschlüsselt.
- Ein Partnerunternehmen verliert Kundendaten.
- Dienstleister verstoßen gegen geltende Regeln im Büro, in dem sie zum Beispiel Fotos machen.

5.8. Wie melde ich einen Informationssicherheitsvorfall?

Allen Mitarbeitern steht das interne Meldeformular für Vorfälle im Intranet bzw. MySupport zur Verfügung. Hier können Informationssicherheits-, Datenschutz- und IT-Sicherheitsvorfälle gemeldet werden.

Oder melden Sie ihren Vorfall direkt an ALG-Informationssicherheit@alten.com

Externe Partner, Kunden und Lieferanten können Vorfälle jederzeit melden, unter: ALG-Informationssicherheit@alten.com .

6. Zusätzliche Anforderungen (Netzwerkzugriff auf das interne Firmennetzwerk)

6.1. Definition

Die folgenden Anforderungen müssen von allen Dienstleistern eingehalten werden, die zu einer der folgenden Kategorien gehören:

- Clients (Endgeräte) werden von ALTEN zur Verfügung gestellt
- Die Anbindung erfolgt z.B. über VPN-Lösungen mit direktem Zugriff auf das ALTEN Netzwerk und/oder die des Kunden.
- Die Anbindung erfolgt direkt über das ALTEN Netzwerk und/oder des Kunden

Diese Dienstleister können sich sowohl auf dem Gelände der eigenen Firma, als auch auf dem Gelände einer ALTEN Niederlassung oder des Kunden befinden.

6.2. Anforderungen

6.2.1. Interne Organisation

Bezüglich der Nutzung der zur Verfügung gestellten Hard- und Software gelten die Regelungen und Betriebsvereinbarungen der jeweiligen Firmengesellschaft.

Das Öffnen des IT-Gerätes und das Durchführen von Veränderungen an der Hardware (z.B. Ein-/Ausbau von Festplatten, Speicherbausteinen) sowie manuelle Veränderungen der Sicherheitseinstellungen (z.B. Browsereinstellungen) ist nur der zuständigen Stelle (siehe Anhang, A.1.4) gestattet.

Der Einsatz oder das nachträgliche Verändern von Programmen des Auftraggebers ist nur zulässig, wenn diese von der zuständigen Stelle (siehe Anhang, A.1.4) genehmigt wird.

Auf den zur Verfügung gestellten IT-Geräten sind keine Daten von weiteren Kunden zu verarbeiten.

Das Verwenden von Software oder Daten des Auftraggebers auf IT- oder Speichergeräten, die nicht vom Auftraggeber bereitgestellt werden oder dessen Eigentum sind, ist nicht zulässig.

Das Verwenden von IT-Geräten oder Daten des Auftraggebers durch Mitarbeiter des Dienstleisters, erfordert die ausdrückliche Zustimmung des Auftraggebers. Der Auftraggeber ist ermächtigt, jederzeit den Zugriff oder die Benutzung zu untersagen (z.B. bei Missbrauch).

6.2.2. Physische und umgebungsbezogene Sicherheit

Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen.

Durch den Auftraggeber zur Verfügung gestellte Geräte (z.B. Laptops, Mobiltelefone) dürfen nur nach erfolgter Genehmigung vom Auftraggebers mitgenommen werden.

6.2.3. Schutz vor Schadsoftware und mobilen Programmcode

Bei Verdacht auf Befall durch Schadsoftware dürfen betroffene IT-Geräte und Datenträger nicht weiter benutzt werden. Die zuständige Stelle (siehe Anhang, A.1.4) ist sofort zu benachrichtigen.

6.2.4. Backup

Daten sollten auf den zugeordneten Netzlaufwerken gespeichert werden und nicht auf der lokalen Festplatte, da nur im Netzwerk eine zentrale und automatische Datensicherung gewährleistet ist.

Für die Sicherung der Daten, die nicht auf zentralen Netzlaufwerken gespeichert sind (z.B. lokale Festplatte, mobile Datenträger), ist der Anwender selbst verantwortlich.

Backupdaten und Medien zur Sicherung sind so zu behandeln, wie die originalen Daten.

6.2.5. Zugriffskontrolle

6.2.5.1. Benutzerverantwortung

Folgende Vorgaben sind durch alle Nutzer zu befolgen:

- Die Verwendung der Benutzerkennung oder des Kontos einer anderen Person ist nicht gestattet.
- Die Weitergabe von Identifikationsmitteln (z.B. SmartCards, RSA-Token) ist nicht gestattet.

- Passwort oder PIN einer Benutzerkennung, die zur persönlichen Verwendung bestimmt ist (bezeichnet als „persönliche Benutzerkennung“, sind geheim zu halten und dürfen nicht weitergegeben werden.
- Sobald der Verdacht der Kompromittierung oder des Bekanntwerdens eines Passwortes oder einer PIN besteht, ist diese unverzüglich zu ändern.
- Temporäre Passwörter (z.B. für neue Konten) sind bei der ersten Anmeldung zu ändern.
- Alle Passwörter oder PINs sind bei der ersten Verwendung zu ändern sowie spätestens nach 90 Tagen.
- Das Ausspähen von Passwörtern ist nicht gestattet.
- Passwörter sind mindestens als vertraulich zu klassifizieren.

Wenn Passwörter schriftlich aufbewahrt werden müssen, sind sie durch den Verantwortlichen in einem versiegelten Umschlag an einem geeigneten Ort zu verwahren, der vor unrechtmäßigem Zugriff geschützt ist (z.B. einem Tresor).

Bei jeder Änderung ist das verwahrte Passwort entsprechend zu aktualisieren. Der versiegelte Umschlag ist durch den jeweiligen Mitarbeiter abzuzeichnen.

Die Personen, die berechtigt sind, den Umschlag zu öffnen, müssen namentlich benannt werden, da es in Ausnahmefällen (z.B. bei Krankheit) nötig sein kann, das verwahrte Passwort zu verwenden. Dabei ist die sogenannte „Zwei-Personen-Regel“ zu befolgen.

Jede Öffnung ist zu dokumentieren und dem Verantwortlichen zu berichten. Nach jeder Öffnung muss der Verantwortliche das Passwort umgehend ändern und wieder sicher verwahren.

Als Alternative sind IT-Systeme zulässig, die eine entsprechende Funktionalität gewährleisten (z.B. elektronische Passwort-Tresore).

Bei Verlassen des Systems im laufenden Betrieb (z.B. Pause, Besprechung) muss der Anwender eine Systemsperre (z.B. passwortgeschützter Bildschirmschoner) aktivieren.

6.2.5.2. Generierung von Passwörtern

Bei der Generierung eines Passworts müssen folgende Mindestanforderungen erfüllt werden:

- Das Passwort muss aus mindestens 10 Zeichen bestehen und mindestens 3 der folgenden 4 Zeichenarten enthalten:
  - Großbuchstaben
  - Kleinbuchstaben
  - Ziffern
  - Sonderzeichen
- Erfordern bestimmte Systeme oder Anwendungen komplexere Passwörter, dann sind diese Vorgaben zu erfüllen.
- Insbesondere sind keine trivialen Passwörter zulässig (z.B. „Test1234“) oder Passwörter mit persönlichem Bezug (z.B. Namen, Geburtsdatum).
- Es ist Mitarbeitern (des Auftragnehmers) nicht gestattet, zum Zugriff auf Systeme des Auftraggebers, ein identisches Passwort für berufliche und private Zwecke zu verwenden.
- Es ist Mitarbeitern (des Auftragnehmers) nicht gestattet, ein identisches Passwort für Systeme, die von ALTEN bereitgestellt werden, und Systeme, die von Dritten bereitgestellt werden (z.B. Anwendungen, Registrierungsdienste im Internet), zu verwenden.

6.2.6. Zugangskontrolle für Netze

6.2.6.1. Regelwerk zur Nutzung von Netzdiensten

Ein vom Auftraggeber bereitgestelltes IT-Gerät darf nur dann und nur solange mit unternehmensfremden Netzwerken (z.B. Hot Spot, privates WLAN) verbunden werden, wenn dies zum Verbindungsaufbau mit dem Firmennetzwerk (über Remote-Zugriff/VPN) geschieht.

Wird die Verbindung nicht mehr benötigt, ist diese zu trennen.

6.2.6.2. Geräteidentifikation in Netzen

Uneingeschränkte Verbindungen von Kommunikationsgeräten (z.B. ohne Firewalls) an das interne Netz (Intranet) sind nur gestattet, wenn diese vom Auftraggeber gestellt sind.

7. Zusätzliche Anforderungen (ohne direkten Zugriff auf internes Firmennetzwerk)

7.1. Definition

Die in Kapitel 3 enthaltenen Anforderungen müssen von allen Dienstleistern eingehalten werden, die zu einer der folgenden Kategorien gehören:

- Dienstleister, die keinen direkten Zugang zum Netzwerk einer Firmengesellschaft haben
- Dienstleister, die keine Endgeräte zur Verfügung gestellt bekommen, die einer ALTEN Gesellschaft gehören und lediglich Endgeräte verwenden, die der Firma des Dienstleisters gehören.
- Dienstleister, die nicht über remote access oder eine andere VPN Lösung angebunden sind.

Diese Dienstleister befinden sich am Standort ihres Unternehmens und sind an die Regularien ihres Unternehmens gebunden.

7.2. Anforderungen

7.2.1. Interne Organisation

Daten von Firmengesellschaften müssen von Daten Dritter und besonders von den Daten anderer Kunden des Dienstleisters (z.B. über ein Rechtemanagement) getrennt sein. Daten dürfen nicht für Dritte zugreifbar sein (z.B. durch Verschlüsselung umzusetzen).

Die ALTEN Informationsklassifikation muss auf das Klassifikationsschema des Dienstleisters abgebildet werden um sicherzustellen, dass alle erforderlichen Sicherheitsmaßnahmen umgesetzt werden.

Dienstleister müssen die Informationssicherheits-Anforderungen aus dem ihnen zur Erfüllung der Aufgabe übergebenem Regelwerk durch angemessene Sicherheitsmaßnahmen in ihrem eigenen Unternehmen abbilden.

Zugriff auf Daten des Auftraggebers darf Mitarbeitern des Dienstleisters nur nach dem Need-to-know-Prinzip (Kenntnis nur bei Bedarf) gewährt werden.

8. Verpflichtung zur Einhaltung

Diese Regelung ist von allen Dienstleistern, entsprechend der Definition in diesem Dokument, einzuhalten.

Sollte in Ausnahmefällen von diesen Handlungsleitlinien, dann ist dies nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang A.1.5 - A.1.7) und dem Auftraggeber zulässig.

9. Mitgeltende Dokumente

– n.z.

Anhang A

In diesem Kapitel werden spezifische Eigenschaften aufgeführt, die für eine Gesellschaft gelten.

A.1.1 Jeder Auftragnehmer ist dafür verantwortlich, dass Informationen, Programme und IT-Geräte nur für Unternehmenszwecke und im Rahmen der jeweiligen Aufgabenstellung ordnungsgemäß eingesetzt und genutzt werden.

Das Versenden von Daten mit nicht dienstlichem Inhalt ist unzulässig.

Die Nutzung des Internets zu privaten Zwecken ist nur im Rahmen von im Unternehmen bestehenden Regelungen zugelassen.

Der Einsatz privater Software und Daten auf den von der Gesellschaft gestellten IT-Geräten ist verboten.

A.1.2 Es gelten folgende Regelungen für die Datensicherheit bzw. den Schutz von personenbezogenen Daten:

- Personenbezogene Daten, die über dienstliche Kommunikationsdaten hinausgehen, sind bezogen auf die Datenklassifizierung mindestens vertraulich und erfordern eine technische Verschlüsselung und eine starke Authentifizierung (z.B. PKI-Zertifikat). Abweichungen sind mit dem Datenschutz von ALTEN abzustimmen.
- Die Löschung und/oder die Entsorgung von Beschäftigtendaten sind gemäß nachfolgendem Punkt A 1.3 entsprechend ihrer Einstufung zu behandeln.

A.1.3 Es gelten folgende Regelungen für die Löschung bzw. die Entsorgung:

- Streng vertrauliche Papierdokumente sind mittels eines Shredders der Sicherheitsstufe P5 oder höher zu entsorgen
- Vertrauliche Papierdokumente sind gemäß der Sicherheitsstufe P4 oder höher zu entsorgen (Datentonnen oder Shredder)
- Datenträger müssen vor Wiederverwendung oder bei Entsorgung durch physikalisches und damit vollständiges Löschen der Information (z.B. unwiderrufliches Formatieren) bzw. durch geeignete Entsorgung (z.B. mechanische Zerstörung) gelöscht werden
- Die Datenträger sollten, wenn möglich, entsprechend dem Datenlösch-Verfahren BSI 2011 oder mindestens nach dem Standard 5220.22-M des DoD (Department of Defense) gelöscht werden.
- Wenn es sich bei dem Datenträger um eine SSD-Festplatte oder generell um ein Flash-Speicher Medium handelt ist die Gutmann-Methode zwingend zu verwenden.
- Nicht mehr benötigte Datenträger sind zuverlässig durch Überschreiben zu löschen oder physikalisch zu zerstören.
- Die Vernichtung von Festplatten und anderen Speichermedien ist zu protokollieren und von einem geprüften Entsorgungsunternehmen durchführen zu lassen
- Optische Datenträger (CD, DVD, Blu-Ray etc.) und Magnetbänder müssen ebenfalls physikalisch zerstört werden, um sichere Unkenntlichmachung der gespeicherten Informationen zu gewährleisten

A.1.4 Help Desk: IT-Support: Mail: ALG-Support@alten.com

A.1.5 ALTEN InfoSec-Team: Mail: ALG-Informationssicherheit@alten.com

A.1.6 ALTEN Datenschutz DE: Mail: ALG-Datenschutzvorfall@alten.com
ALTEN Datenschutz AT: Mail: datenschutz@alten.at

A.1.7 Verantwortlichkeit: Zentraler Ansprechpartner für Einhaltung gesetzlicher Verpflichtungen ist die Rechtsabteilung von ALTEN (Mail: ALG-legal@alten.com)

A.1.8 In der Bundesrepublik Deutschland gelten die jeweils aktuell gültigen Fassungen von BDSG-neu und EU-DSGVO
In der Republik Österreich gelten die jeweils aktuell gültigen Fassungen von DSG und EU-DSGVO