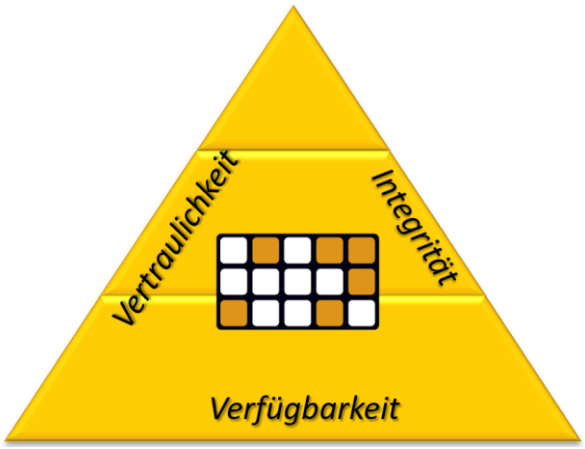
Richtlinie für Partnerfirmen

Richtlinie der e.solutions Informationssicherheit



Version: 2.4
Status: RELEASED
Gültig ab: 02.07.2024

Zielgruppe

Diese Richtlinie *muss* von **Personen** in Partnerfirmen[1] gelesen und beachtet werden, die auf Basis von vertraglichen Regelungen **Leistungen für die e.solutions GmbH erbringen**. Weiterhin *muss* die Richtlinie von **Personen** in der e.solutions GmbH gelesen werden, die in Ihrem Verantwortungs- und/oder Aufgabenbereich **für die Zusammenarbeit mit Partnerfirmen verantwortlich oder betroffen sind.**

Kernaussage

Die Richtlinie für Partnerfirmen definiert die Informationssicherheits-Vorschriften, die von Partnerfirmen in ihrem Verantwortungsbereich für von Ihnen bereitgestellte und genutzte IT-Systeme & -Anwendungen und Infrastruktur zu beachten sind.
Partnerfirmen müssen geltende Vorschriften identifizieren und einhalten.
In dieser Richtlinie werden die Regeln für Informationssicherheit definiert, die von Partnerfirmen beim Umgang mit Informationen und IT-Geräten (z. B. PCs, Arbeitsplätze, Laptops, Smartphones oder Tablet-PCs) zu befolgen sind.
Partnerfirmen sind in dieser Richtlinie definiert als jeder Dritte, der Dienstleistungen für e.solutions auf Basis vertraglicher Beziehungen erbringt. e.solutions tritt hier als „Auftraggeber“ der Partnerfirmen auf. Diese Handlungsrichtlinie richtet sich an die Leitung der Partnerfirmen, deren Mitarbeiter, Erfüllungs-/Verrichtungshilfen und Affiliates (im Folgenden zusammengefasst als „Auftragnehmer“ benannt).
Zweck der Informationssicherheitsrichtlinie ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen des Auftraggebers und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit dem Auftraggeber eingehen und/oder Tätigkeiten für diesen ausführen.

[1] Definition Partnerfirma in Kapitel 4

Inhaltsverzeichnis

1 Dokumentinformationen

1.1 Zuständige Stellen im Sinne der Richtlinie

1.1.1 Organisation und Compliance

- Namentlich benannte Ansprechpartner in den Beauftragungen
- Rechtsabteilung der e.solutions
- Datenschutzbeauftragter der e.solutions
- Informationssicherheit der e.solutions

1.1.2 Technik und Issues

- B2B-Support[2] der e.solutions
- e.solutions CERT[3]

2 Mitgeltende Unterlagen

Nach innen auf e.solutions gerichtet gelten alle weiteren Dokumente der Informationssicherheits-Organisation der e.solutions GmbH.
Auf die Partnerfirmen gerichtet gelten neben dieser Richtlinie die geschlossenen Verträge. Sollte die Partnerfirma Zugriff auf Informationssysteme des Auftraggebers erlangen, gelten zusätzlich die besonderen Regelungen zu diesen Systemen.

2.1 Initiale Bereitstellung der Unterlagen an Partnerfirmen

Im Rahmen der Vertragsanbahnung erhält die zukünftige Partnerfirma die Unterlagen

- vom B2B-Portal[4] der e.solutions
- oder durch die Rechtsabteilung der e.solutions GmbH

2.2 Bereitstellung aktualisierter Unterlagen an Partnerfirmen

Partnerfirmen sind verpflichtet, sich regelmäßig darüber zu informieren, ob es aktualisierte Unterlagen gibt. Die Partnerfirma kann die aktuellen Versionen der für sie geltenden Unterlagen immer über das B2B-Portal[5] einsehen bzw. herunterladen.

Regeln aus aktualisierten Unterlagen, sind durch die Partnerfirma umgehend umzusetzen.

3 Allgemeine Anforderungen

Die folgenden Anforderungen müssen von allen Partnerfirmen, unabhängig von ihrem konkreten Auftrag und unabhängig von der konkreten Zusammenarbeitsform eingehalten werden.
Anforderungen an den Auftraggeber sind nicht Bestandteil dieses Dokuments.

---

[2] https://b2b.esolutions.de/support.html

[3] eso.Group.CERT@esolutions.de

[4] https://b2b.esolutions.de

[5] https://b2b.esolutions.de/informationsecurity.html

3.1 Organisatorische Anforderungen

Bezüglich des Mitbringens von IT-Geräten auf das Firmengelände oder in Sicherheitsbereiche des Auftraggebers, die nicht vom Auftraggeber gestellt sind, gelten die Regelungen des Auftraggebers.
Die private Verwendung vom Auftraggeber bereitgestellter Arbeitsmittel (z. B. ePN.Client) ist verboten.
Das Verwenden von Daten oder Software, die zum Auftraggeber gehören, auf IT-Systemen oder Speichergeräten die weder durch den Auftraggeber noch vom Auftragnehmer bereitgestellt oder freigegeben sind, ist nicht zulässig.
Die Weitergabe von Daten an Dritte ist nur mit schriftlicher Freigabe durch den Dateneigentümer des Auftraggebers gestattet.
Regelungen des Auftraggebers zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten müssen eingehalten werden.
Mitarbeiter des Auftragnehmers müssen von ihrer Leitung auf die Geheimhaltung im Sinne der bestehenden Geheimhaltungsvereinbarung (NDA) 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.
Vor Auslandsreisen sind die länderspezifischen Regelungen zum Einsatz von Sicherheitstechniken (z. B. Verschlüsselung) zu beachten.
Nach Vertragsende müssen alle Daten des Auftraggebers an den Auftraggeber übergeben werden und sind auf allen Geräten und Speichermedien des Auftragnehmers nachweislich zu löschen. Rechtliche Anforderungen (z. B. Aufbewahrungspflichten) sind zu beachten.

3.2 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 Auftrag gebenden Stellen (z. B. zuständiger Benutzeradministrator des Auftraggebers) zu melden, damit die entsprechende Sperrung/ Löschung erfolgen kann. Handelt es sich um eine Benutzerkennung im e.PN[6], so hat der Partnerfirmenadministrator diese umgehend im B2B-Portal zu löschen.
Nicht mehr benötigte Medien zur Identifizierung (z. B. Smartcards, SecurID-Karten) 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 des Auftragnehmers übergebenen IT-Geräten sowie von Medien zum Zwecke der Authentifizierung sind durch den Benutzer umgehend der zuständigen Stelle des Auftraggebers zu melden.

[6] e.solutions Partnerfirmen Netzwerk

3.3 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 streng vertrauliche Dokumente dürfen niemals unbeaufsichtigt liegen gelassen werden, um Einsichtnahme durch Unberechtigte zu verhindern.

3.4 Management von organisationseigenen Werten

3.4.1 Regelungen für die Klassifikation

Eine Klassifikation findet anhand der drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit statt und muss für alle Informationen und alle informationsverarbeitenden IT-Systeme durchgeführt werden.
Der Auftragnehmer muss die Klassifikation nach Vertraulichkeit, Integrität und Verfügbarkeit (im Rahmen des Geltungsbereiches der Verträge) vom Auftraggeber anfordern.
Informationen sind über ihre gesamte Lebensdauer hinweg gemäß den Maßnahmen, die ihrer Vertraulichkeitseinstufung entsprechen, vor unbefugtem Zugriff zu schützen.
Vertraulichkeitseinstufungen können mit einem Ablaufdatum versehen werden.
Falls erforderlich, ist bei der Verarbeitung von Daten die Klassifikation in Bezug auf Integrität, Nachweisbarkeit und Verfügbarkeit durch den jeweiligen Prozesseigentümer zu überprüfen und zu bestimmen. Diese Klassifikation ist regelmäßig, unter Einbeziehung des Informationseigentümers, zu evaluieren und gegebenenfalls anzupassen.
Die korrekte Klassifizierung muss vom Informationseigentümer bestätigt werden.

3.4.1.1 Vertraulichkeit

Informationen, die nicht für die Allgemeinheit bestimmt sind, dürfen nur den Personen zugänglich gemacht werden, die dazu berechtigt sind (Grundsatz „need-to-know“).

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

Klassifikation	Definition
öffentlich	Informationen, die keinen Einschränkungen unterliegen und beispielsweise in der Presse oder im Internet veröffentlicht werden können. Die Verwendung von Unternehmensinformationen in der Öffentlichkeit bedarf der Zustimmung der zuständigen Stellen. Beispiele: Homepage, Social Media, Firmenpräsentationen
intern	Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe oder Verwendung nur geringen Einfluss auf das Erreichen von Produkt- und Projektzielen haben und daher einem berechtigten Personenkreis zugänglich gemacht werden dürfen. Vertraulichkeitsverstöße können negative Folgen haben, wenn auch eher geringfügiger Natur. Beispiel: Schadenersatzforderungen durch Einzelpersonen oder Organisationen sind unwahrscheinlich

Klassifikation	Definition
	Beispiele: Kunden/Lieferantenadressen, Lieferscheine, Rechnungen, Protokolle, Mitteilungen, Notizen, Prozessbeschreibungen, Telefonliste Mitarbeiter, Layout, Richtlinien, Arbeitsordnung, Arbeitsschutzunterlagen, Projekt/Prozessdaten
vertraulich	Informationen, deren Bekanntgabe oder Offenlegung an unbefugte Personen das Erreichen von Produkt- und Projektzielen gefährden kann und die daher ausschließlich einer begrenzten Gruppe von Berechtigten zugänglich gemacht werden dürfen. Vertraulichkeitsverstöße führen voraussichtlich zu messbaren negativen Folgen, wie z. B.: ▪ Verlust von Kunden ▪ Rückgang von Verkaufs-/Umsatzzahlen ▪ Schadenersatzforderungen durch Einzelpersonen oder Organisationen Beispiele: Arbeitsverträge, Abmahnungen, Kündigungen, Personaldaten, personenbezogene Daten, Preislisten, Kalkulationen, Angebote, Verträge, Aufträge, betriebswirtschaftliche Auswertungen, Bankverbindungsdaten, Zeitwirtschaft, Lohnabrechnung, Spezifikationen des Kunden, Quelltexte, Software, Targets (Vorserien- und Serienteile), Designbilder (z. B. 3D Modelle von Autos, bei Kundenanforderung), Projekt- und Prozessdaten (bei Kundenanforderung)
streng vertraulich	Informationen, deren Bekanntgabe oder Offenlegung an unbefugte Personen das Erreichen von Unternehmenszielen in hohem Maße gefährden kann und die daher nur einer äußerst restriktiven Verteilerliste zugänglich gemacht werden dürfen und strengen Kontrollen unterliegen müssen. Vertraulichkeitsverstöße haben erhebliche negative Auswirkungen auf das Image bzw. Erscheinungsbild des Unternehmens sowie wirtschaftliche Folgen, wie z. B.: ▪ erheblicher Verlust von Kunden ▪ starker Rückgang von Verkaufs-/Umsatzzahlen ▪ Schadenersatzforderungen durch diverse Einzelpersonen oder Organisationen ▪ Ausschluss aus bestimmten Marktgebieten ▪ negative Effekte in der öffentlichen Wahrnehmung Beispiele: Entwurfszeichnungen von Prototypen

3.4.1.2 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	Eine Verletzung der Integrität hat keine vorhersehbaren Auswirkungen auf die geschäftlichen Tätigkeiten oder das Image bzw. Erscheinungsbild des Unternehmens.
mittel	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

Klassifikation	Definition
	▪ Fehler ohne Auswirkungen auf die Arbeitsergebnisse (keine produktiven Ausfallzeiten) ▪ Entscheidungen werden nicht beeinträchtigt ▪ Schadenersatzforderungen durch Einzelpersonen oder Organisationen sind unwahrscheinlich Beispiele: Standortpläne, Organigramme, einzelne interne Telefonnummern
hoch	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 ▪ Rückgang von Verkaufs-/Umsatzzahlen 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 Beispiele: JIT-Aufträge, Pressemeldungen, Inhalte des Internetauftritts, Produktionssteuerungsdaten
sehr hoch	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 ▪ starker Rückgang von Verkaufs-/Umsatzzahlen ▪ 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 Beispiele: Bilanzierung (z. B. Jahresabschluss), kryptographische Schlüssel, Gehalt

3.4.1.3 Verfügbarkeit

Informationen müssen innerhalb eines vereinbarten Zeitraums verfügbar sein.

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

Klassifikation	Definition
gering	Die Verfügbarkeit des IT-Systems darf in Bezug auf Ausfall oder inakzeptable Antwortzeiten weniger als 95 % betragen, ohne dass es zu nennenswerten Beeinträchtigungen (finanzieller Art oder am Image des Unternehmens) kommt. Beispiel: Intranet-Anwendung mit allgemeinen Mitarbeiterinformationen

Klassifikation	Definition
mittel	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 95 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (finanzieller Art oder am Image des Unternehmens). Beispiel: Bewerberportal; Internetauftritt
hoch	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 98 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (finanzieller Art oder am Image des Unternehmens). Beispiele: Gehaltsabrechnung, Buchhaltung
sehr hoch	Die Verfügbarkeit des IT-Systems muss in Bezug auf Ausfall oder inakzeptable Antwortzeiten mindestens 99 % betragen. Eine niedrigere Verfügbarkeit führt zu nennenswerten Beeinträchtigungen (finanzieller Art oder am Image des Unternehmens). Beispiel: IT-System, dessen Ausfall einen unmittelbaren Stopp der Arbeitsprozesse zur Folge hat Bei nennenswerten Beeinträchtigungen kann es sich z. B. handeln um: ▪ Verlust von Kunden ▪ Schadenersatzforderungen durch diverse Einzelpersonen, Organisationen oder Verbände ▪ starker Rückgang von Verkaufs-/Umsatzzahlen ▪ Ausschluss aus bestimmten Marktgebieten ▪ Fehler/Fehlfunktionen mit schwerwiegenden Auswirkungen auf die Arbeitsergebnisse und/oder Ausfall mehrerer Serviceprozesse (sehr hohe produktive Ausfallzeiten)

3.4.2 Regelung zur Kennzeichnung

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, vertrauliche und streng vertrauliche 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.

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 „need-to-know“ 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	▪ Kennzeichnung: keine/optional (z.B. Vermerk im Impressum) Vervielfältigung und Verteilung: keine Einschränkungen ▪ Speicherung: keine Einschränkungen ▪ Löschung: keine Einschränkungen ▪ Entsorgung: keine Einschränkungen
intern	▪ Kennzeichnung: auf allen Seiten des Dokumentes in der Fußzeile mit „intern“ bzw. „internal“ ▪ Vervielfältigung und Verteilung: nur an berechtigte Mitarbeiter der e.solutions GmbH und berechtigte Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereichs ▪ Speicherung: Schutz vor unbefugtem Zugriff ▪ Löschung: Nicht mehr benötigte Daten sind zu löschen ▪ Entsorgung: ordnungsgemäße Entsorgung
vertraulich	▪ Kennzeichnung: auf allen Seiten des Dokumentes in der Fußzeile mit „vertraulich“ oder „confidential“ . ▪ Vervielfältigung und Verteilung: nur an eine beschränkte Gruppe von berechtigten Mitarbeitern der e.solutions GmbH 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 e.solutions und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs (z. B. durch geschlossene Nutzergruppen). Es sind geeignete Speicherorte und/oder Speichermedien zu verwenden. ▪ Vertrauliche Dokumente müssen in versperrten Stahlmöbeln oder in versperrten Räumen, die nur von einer dafür berechtigten Personengruppe geöffnet werden können, aufbewahrt werden, wenn sie nicht benötigt werden. ▪ Löschung: Nicht mehr benötigte Daten sind zu löschen. ▪ Entsorgung: ordnungsgemäße Entsorgung ▪ Authentifizierung: Starke Authentifizierung ▪ Transport: Vertrauliche Dokumente und Speichermedien müssen in verschlossenen, neutralen Umschlägen versendet 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	▪ Kennzeichnung: auf allen Seiten des Dokumentes in der Fußzeile mit „streng vertraulich“ oder „high confidential“ 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 e.solutions GmbH und berechtigte Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereichs

Klassifikation	Anforderungen
	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 e.solutions 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. ▪ Streng vertrauliche Dokumente müssen in versperrten Stahlmöbeln aufbewahrt werden. Es sind dabei separate Schließungen zu verwenden. Mobile Datenträger mit streng vertraulichen Informationen müssen in geeigneten Datensafes aufbewahrt werden. ▪ Löschung: Nicht mehr benötigte Daten sind zu löschen. ▪ Entsorgung: ordnungsgemäße Entsorgung ▪ Authentifizierung: starke Authentifizierung ▪ Transport: streng vertrauliche Dokumente und Speichermedien müssen in neutralen, verschlossenen Außenumschlägen (ohne Zusätze wie “persönlich, streng vertraulich, etc.“) versendet werden. In diesen ist ein zweiter innerer Umschlag zu platzieren, welcher mit der Klassifikation “streng vertraulich” gekennzeichnet ist und die streng vertraulichen Dokumente enthält.

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

3.4.3 Austausch von Informationen

Bei allen Gesprächen (einschließlich Telefonaten, Video- und Webkonferenzen), die vertrauliche oder streng vertrauliche 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 Transport von IT-Geräten und Datenträgern außerhalb der Gebäude- bzw. Geländegrenzen des Auftraggebers sind die Regelungen und Betriebsvereinbarungen des Auftraggebers bindend.

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

Die Erstellung und der Versand von Ketten-E-Mails sind unzulässig.

3.4.4 Handhabung von Speicher- und Aufzeichnungsmedien

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.

3.5 Umgang mit Informationssicherheitsvorfällen

Informationssicherheitsereignisse (z. B. auftretende Störungen, Verstöße gegen das Informationssicherheitsregelwerk), welche Daten oder Systeme des Auftraggebers betreffen sind unverzüglich der zuständigen Stelle zu melden.
Vermutete Verwundbarkeiten und Schwachstellen von IT-Systemen sind unverzüglich der zuständigen Stelle zu melden. Die Prüfung von Verwundbarkeiten und Schwachstellen (z.B. Penetration Testing) darf nur durch die zuständige Stelle erfolgen.
Beim Verdacht auf Verlust von vertraulichen oder streng vertraulichen Informationen muss dies sofort an die zuständige Stelle (siehe Kap. 1.1) gemeldet werden.

3.6 Vermittlung von Wissen

Der Auftragnehmer muss in geeigneter Weise, regelmäßig sicherstellen, dass die Inhalte dieser Leitlinie den Personen innerhalb seiner Organisation, die für den Auftraggeber tätig sind, vermittelt wird. Dies ist bestenfalls mit Nachweisen zu belegen.

3.7 Compliance und Einhaltung gesetzlicher Verpflichtungen

Durch die Partnerfirma ist ein Compliance Management unter Beachtung rechtlicher und betrieblicher Anforderungen (inklusive Ressourcen-Management, internes Kontrollsystem, IT Continuity Management und Schutz von Informationen) einzurichten. Dies muss alle Informationen, Hard- und Software des Auftraggebers umfassen.
Das Compliance Management muss die folgenden Punkte beinhalten.

3.7.1 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.

3.7.2 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.

3.7.3 Datenschutz

Die jeweiligen landesspezifischen Gesetze und Vorschriften zum Datenschutz sind einzuhalten. Auftragnehmer[7] müssen von der Geschäftsführung der jeweiligen Partnerfirma auf die Einhaltung der gesetzlichen Datenschutzvorgaben verpflichtet werden.

3.7.4 Vertragliche Compliance

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

3.7.5 Internes Regelwerk

Partnerfirmen 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.

3.8 Verstöße und Durchsetzung

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

4 Zusätzliche Anforderungen für Auftragnehmer mit direktem Zugang zu Informationssystemen des Auftraggebers

Die folgenden Anforderungen müssen von allen Partnerfirmen eingehalten werden, die Zugriff auf Informationssysteme und damit Informationen haben, die beim Auftraggeber verwaltet werden. Dabei spielt es keine Rolle auf welchem technologischen Weg oder mit welchem System dieser Zugriff hergestellt wird.

4.1 Anforderungen

4.1.1 Interne Organisation

Partnerfirmen dürfen die Bereitstellung oder Installation von Hardware und Software nur über den für sie zuständigen Fachbereich des Auftraggebers durchführen oder initiieren.
Bezüglich der Nutzung der zur Verfügung gestellten Hard- und Software gelten die Regelungen und Betriebsvereinbarungen des Auftraggebers.

[7] Sub-Unternehmer-Regelung zur Weitergabe der Verpflichtung auf die Einhaltung des Datenschutzes.

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 den zuständigen Stellen gestattet.
Der Einsatz oder das nachträgliche Verändern von Programmen des Auftraggebers ist nur zulässig, wenn diese von den zuständigen Stellen genehmigt wird.
Auf den zur Verfügung gestellten IT-Geräten sind ausschließlich Daten zur Verarbeitung zugelassen, die im Rahmen der Beauftragung notwendig sind.
Die bereitgestellten Systeme dürfen nicht für andere Auftraggeber verwendet werden.
Das Verwenden von IT-Geräten oder Daten des Auftraggebers durch Mitarbeiter der Partnerfirma erfordert die ausdrückliche Zustimmung des Auftraggebers. Der Auftraggeber ist ermächtigt, jederzeit den Zugriff oder die Benutzung zu untersagen (z. B. bei Missbrauch).
Daten des Auftraggebers müssen von Daten Dritter und besonders von den Daten anderer Kunden der Partnerfirma (z. B. über ein Rechtemanagement) getrennt sein. Daten dürfen nicht für Dritte zugreifbar sein (z. B. durch Verschlüsselung).
Die e.solutions Klassifikation muss auf das Klassifikationsschema der Partnerfirma abgebildet werden um sicherzustellen, dass alle erforderlichen Sicherheitsmaßnahmen umgesetzt werden.
Partnerfirmen 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 der Partnerfirma nur nach dem Need-to-know-Prinzip gewährt werden.

4.1.2 Physische und umgebungsbezogene Sicherheit

Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen.
Die Vorschriften des Herstellers zum Schutz der Geräte sind einzuhalten.

4.1.3 Schutz vor Schadsoftware und mobilem Programmcode

Bei Verdacht auf Befall durch Schadsoftware dürfen betroffene IT-Geräte und Datenträger nicht weiter benutzt werden. Die zuständigen Stellen sind sofort zu benachrichtigen.

4.1.4 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) oder Systemen mit vergleichbarer Funktionalität, ist die e.solutions IT nicht verantwortlich.
Backupdaten und Medien zur Sicherung sind so zu behandeln, wie die originalen Daten.

4.1.5 Zugangskontrolle

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. Smart Cards oder SecurID-Karten) ist nicht gestattet.
- Passwörter oder PINs einer Benutzerkennung, die zur persönlichen Verwendung bestimmt ist (bezeichnet als „persönliche Benutzerkennung“, sind streng vertraulich zu halten und dürfen nicht weitergegeben werden.
- Das Speichern oder das Aufschreiben von Passwörtern (z. B. auf Papier, über Mobilgeräte oder in Dateien) ist nicht zulässig, sofern dies nicht als sichere Methode festgelegt ist.
- Sobald der Verdacht der Kompromittierung oder des Bekanntwerdens eines Passworts oder einer PIN besteht, ist dieses bzw. 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 einem Jahr (Letzteres gilt nur für Passwörter).
- Das Ausspähen von Passwörtern ist nicht gestattet.
- Passwörter sind mindestens als vertraulich zu klassifizieren.
- Wenn Passwörter schriftlich aufbewahrt werden müssen, sind sie durch den Mitarbeiter 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 Mitarbeiter zu berichten. Nach jeder Öffnung muss der Mitarbeiter 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.
- Anwender, die ihren Multifunktionsausweis zur Anmeldung an IT-Systemen benutzen, haben beim Verlassen des Systems den Ausweis aus dem Lesegerät zu entfernen.

4.1.5.1 Generierung von Passwörtern

Bei der Generierung eines Passworts müssen folgende Mindestanforderungen erfüllt werden:

- 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 vom Auftraggeber bereitgestellt werden, und Systeme, die von Dritten bereitgestellt werden (z. B. Anwendungen, Registrierungsdienste im Internet), zu verwenden.

- Die von Systemen erzwungene Mindestlänge für Passwörter ist einzuhalten. Sie richtet sich nach den Vorgaben der entsprechenden Regelung.

- Triviale Passwörter (z.B. „Test123456“) oder Passwörter mit persönlichem Bezug (z. B. Namen, Geburtsdatum) sind nicht zulässig.
- Erfordern bestimmte Systeme oder Anwendungen komplexere Passwörter (gemäß Definition in der Passwort-Regelung), dann sind diese Vorgaben zu erfüllen.
- Hinweis: Für ein sicheres Passwort können Sie Eselsbrücken oder Abkürzungen sowie Verfälschungen verwenden (Beispiel: „Jeden Tag gehe ich ins Bad und wasche mich gründlich“ wird zum Passwort „JTg11B&wmg“).
- Alternativ erzeugt eine Kombination aus vier Wörtern (z.B. „SonneHolzTeeZeit“) ein sehr starkes Passwort, das leicht zu merken ist. Die hier aufgeführten Beispiele dürfen nicht als tatsächliche Passwörter verwendet werden.

4.1.5.2 PINs zum Entsperren von Smartphones und Tablets

Es gelten die in Kapitel 4.1.5.1 beschriebenen Anforderungen.

4.1.5.3 PINs für Authentifizierungs-Smartcards

Es gelten die in Kapitel 4.1.5.1 beschriebenen Anforderungen.

4.1.5.4 Gruppenkennungen

Gruppenkennungen sind nicht zulässig.

4.1.6 Zugangskontrolle für Netze

Ein vom Auftraggeber bereitgestelltes IT-Gerät darf nur dann und nur so lange mit unternehmensfremden Netzwerken (z. B. Hot Spot, privates WLAN; ausgenommen Mobilfunknetze) verbunden werden, wenn dies zum Verbindungsaufbau mit dem e.solutions-Netzwerk geschieht. Direktes “Surfen” usw. ist nicht zulässig (ausgenommen mit Mobilfunknetzen verbundene Smartphones und Tablets).
Wird die Verbindung nicht mehr benötigt, ist diese zu trennen.
Uneingeschränkte Verbindungen von Kommunikationsgeräten (z.B. ohne Firewalls) an das interne Netz (Intranet) sind nur gestattet, wenn diese vom Auftraggeber gestellt sind.

5 Umgang mit schutzbedürftigem Material

Im Rahmen der Beauftragung kann der Partnerfirma Material/Komponenten/Muster durch den Auftraggeber übergeben werden, welches einem erhöhten Schutzbedarf unterliegt. Für dieses Material gelten sinngemäß die Regeln aus Kapitel 3.4.
Zusätzlich dazu können mit dem Material weitere Richtlinien übergeben werden, die durch die Partnerfirma zusätzlich zu erfüllen sind.

6 Abschlussbestimmungen

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, sind nur temporär und nach Rücksprache mit den zuständigen Stellen und dem Auftraggeber zulässig.

Anhang

Dokumentenhistorie

Datum	Version	Bearbeiter	Beschreibung	Geänderte Seiten/ Kapitel
01.11.2018	0.9	J. Pfannenstein	Initiale Version des Dokuments	
15.11.2018	1.0	J. Pfannenstein	Vorbereitung Review	
29.01.2019	2.0	J. Pfannenstein	Update	Policy Pyramide und IS
09.07.2019	2.1	P. Walhekar	Anpassung an Verweise Hinzufügen von keine private Nutzung von e.solutions Arbeitsmittel	Kap. 7 Kap. 8.1
12.11.2019	2.2	P. Walhekar	Anpassung der Backup Regelung	Kap. 9.1.4
03.02.2021	2.3	C. Ostermeier	Anpassung an neues Layout und Update	
13.07.2021	2.4	B. Brauns	Autorenänderung Hinzufügen Kapitel, Zielgruppe, Wissensvermittlung u. Anhang Inhaltliche Korrekturen Abgleich der Vorgaben mit ISMS Handbuch	Kap. 2, 9.6 und 13
11.03.2022	2.4	C. Ostermeier	Aktualisierung Links	Gesamtes Dokument
02.04.2024	2.4	C. Ostermeier	Anpassung Fußzeile; Rainer Lange bei Geschäftsleitung Entfernt	Fußzeile
02.07.2024	2.4	C. Ostermeier	Internes Review ohne inhaltliche Veränderung; Anpassung Fußzeile; Timo Schreiber bei Geschäftsleitung hinzugefügt	Gesamtes Dokument
28.08.2024	2.4	C. Ostermeier	Anpassung an das neue Layout; Leitlinie durch Richtlinie ersetzt	Gesamtes Dokument

Verweise auf Anforderungskataloge[8]

Control VDA ISA: 1.1.1 Vorhandensein von Richtlinien zur Informationssicherheit

6.1.1 Sicherstellung der Informationssicherheit bei Auftragnehmern und Kooperationspartnern

[8] Das Dokument gibt Antwort auf Controls des VDA ISA Katalogs in seiner zum Zeitpunkt des Entstehens des Dokumentes gültigen Fassung.