Anlagen Informationssicherheit
Allgemeine Anforderungen

Version vom 09.05.2024

Internal - do not pass on to third parties

Im nachfolgenden Dokument sind die vier Anlagen zu den Anforderungen an Dienstleister und Lieferanten aufgeführt. Diese Anlagen sind ein wesentlicher Bestandteil unseres Informationssicherheitsmanagement-systems (ISMS) und definieren die notwendigen Sicherheitsmaßnahmen und -richtlinien, die von unseren Partnern eingehalten werden müssen.

Übersicht der Anlagen

ISMS - Anlage für Lieferanten und Dienstleister - IT-Sicherheit

Diese Anlage definiert die allgemeinen IT-Sicherheitsanforderungen, die alle Lieferanten und Dienstleister erfüllen müssen, um die Sicherheit unserer Systeme zu gewährleisten.

ISMS - Anlage für Lieferanten und Dienstleister - Wartung

Diese Anlage beschreibt die spezifischen Anforderungen und Verfahren für die Wartung von IT-Systemen und -Komponenten durch externe Dienstleister, um sicherzustellen, dass alle Wartungsarbeiten sicher und zuverlässig durchgeführt werden.

ISMS - Anlage für Lieferanten und Dienstleister - Software- und Produktentwicklung

Diese Anlage legt die Sicherheitsanforderungen für die Software- und Produktentwicklung fest. Sie beschreibt die notwendigen Maßnahmen, die Entwickler und Lieferanten ergreifen müssen, um die Sicherheit und Integrität der entwickelten Software und Produkte zu gewährleisten.

ISMS - Anlage für Lieferanten und Dienstleister - Third-Party-Softwarekomponenten

Diese Anlage befasst sich mit der Integration und Nutzung von Softwarekomponenten Dritter. Sie definiert die Sicherheitsanforderungen, die sicherstellen, dass alle Third-Party-Komponenten sicher und vertrauenswürdig sind.

BIZERBA

Anlage Informationssicherheit
Allgemeine Anforderungen an die IT-Sicherheit des Auftragnehmers

Version vom 04.02.2024

Internal - do not pass on to third parties

Inhaltsverzeichnis

1 Allgemeines

Für Fernwartung und externe Programmierer gelten weitere additive Anlagen.

2 Ansprechpartner

a) Der Auftragnehmer muss dem Auftraggeber einen qualifizierten Ansprechpartner benennen, der jederzeit Auskunft über Fragen zur IT-Sicherheit geben kann. Der Ansprechpartner muss folgende Informationen bereitstellen: Name, Funktion, Gesellschaft, Geschäftsadresse, Telefonnummer und E-Mail-Adresse.

b) Der Auftraggeber muss dem Auftragnehmer einen Ansprechpartner benennen, dem der Auftragnehmer Auskünfte erteilen und Informationen gemäß dieser Anlage mitteilen kann. Der Ansprechpartner des Auftraggebers ist:

Security Ansprechpartner, Auftragnehmer		Security Ansprechpartner, Auftraggeber	
Name:	_____	Name:	_____
Funktion:	_____	Funktion:	_____
Gesellschaft:	_____	Gesellschaft:	_____
Geschäftsadresse:	_____	Geschäftsadresse:	_____
Telefonnummer:	_____	Telefonnummer:	_____
E-Mail-Adresse:	_____	E-Mail-Adresse:	_____
		Allgemeine Information Security Office Anfragen: informationsecurityoffice@bizerba.com	

3 Allgemeine Anforderungen

a) Der Auftragnehmer ist verpflichtet, ein anerkanntes Informationssicherheits-Managementsystem (z.B. nach ISO 27001 oder BSI-Standard 200-2) zu implementieren und zu unterhalten, um einen angemessenen Schutz aller Informationen zu gewährleisten.

b) Der Auftragnehmer muss bei der Organisation seiner IT-Prozesse ein anerkanntes Rahmenwerk für das Management und die Steuerung der IT (IT-Governance) verwenden. Anerkannte IT-Governance-Rahmenwerke sind ITIL (IT Infrastructure Library) oder COBIT (Control Objectives for Information and Related Technology).

c) Wenn der Auftraggeber dies wünscht, muss der Auftragnehmer sicherstellen, dass bestimmte vom Auftraggeber genannte Daten innerhalb einer vorgegebenen Frist vollständig und zuverlässig gelöscht werden, vorbehaltlich gesetzlicher Aufbewahrungsfristen.

4 Sicherheit der IT des Auftragnehmers

a) Der Auftragnehmer muss einen angemessenen Virenschutz (für Server, Workstations und andere IT-Komponenten mit Zugriff auf Informationen oder Systeme mit Schutzbedarf) sowie weitere Sicherheitsmaßnahmen gegen Malware (wie Trojaner-Detektion, Spamschutz) implementieren und auf dem neuesten Stand der Technik halten.

b) Der Auftragnehmer muss für eine sichere Grundkonfiguration seiner IT Infrastruktur sorgen, z.B. durch den Einsatz gehärteter Betriebssysteme auf Server und Clients sowie die Deaktivierung nicht benötigter Funktionen und Netzwerk-Ports in seinen Systemen.

c) Der Auftragnehmer ist verpflichtet, alle Aktivitäten der Administratoren zur Erkennung von Angriffen oder Fehlbedienungen fortlaufend zu überwachen und zu protokollieren und die Logfiles für mindestens drei Monate sicher aufzubewahren.

d) Der Auftragnehmer muss regelmäßige Datensicherungen durchführen.

e) Der Auftragnehmer hat sicherzustellen, dass die Daten des Auftragnehmers nur von Personen gelesen, geändert und verarbeitet werden können, die innerhalb der zu erbringenden Dienstleistungen, des aktuellen Projektes oder Zusammenarbeit involviert sind.

f) Eventuelle portable Datenträger die für die Leistungserbringen genutzt werden, sind vor jeder Nutzung neu zu formatieren und die darauf gespeicherten Daten mit Microsoft BitLocker oder einer anderen Verschlüsselungstechnik nach Stand der Technik und einem mindestens 12 Zeichen langem Passwort zu verschlüsseln.

g) Der Auftragsnehmer muss ein Risikomanagement-System implementieren, um potenzielle Bedrohungen für die Informationssicherheit zu identifizieren und entsprechende Maßnahmen zu ergreifen.

h) Der Auftragsnehmer muss einen IT-Notfallplan erstellen, um im Falle eines Sicherheitsvorfalls schnell und effektiv reagieren zu können. Eine Kopie des Inhaltsverzeichnisses des IT-Notfallplanes ist auf Anfrage des Auftraggebers bereitzustellen.

i) Der Auftragnehmer muss dem Auftraggeber auf Anfrage sein IT-Sicherheitskonzept sowie alle relevanten Dokumente, Zertifikate, Nachweise oder Berichte zur Verfügung stellen, die die Einhaltung der IT-Sicherheitsanforderungen belegen.

j) Der Auftragnehmer trägt die Verantwortung dafür, dass seine Mitarbeiter, die über Administratorrechte verfügen, nur über eine Zwei-Faktor-Authentifizierung auf Systeme und Anwendungen zugreifen können, die im Auftrag des Auftraggebers betrieben werden. Dies stellt sicher, dass der Zugriff auf sensible Daten und Systeme durch eine zusätzliche Sicherheitsebene geschützt ist.

k) Der Auftragnehmer stellt sicher, dass alle Zugriffsrechte auf der Grundlage eines klaren, vordefinierten Rollenkonzepts vergeben werden. Dieses Rollenkonzept wird regelmäßig überprüft, um sicherzustellen, dass es den aktuellen Anforderungen entspricht. Der Auftraggeber ist dafür verantwortlich, dass im Falle von Änderungen des Rollenkonzepts oder bei Beendigung dieser Vereinbarung die Zugriffsrechte unverzüglich entzogen werden, um die Sicherheit der Daten und Systeme zu gewährleisten.

l) Der Auftragnehmer gewährleistet, dass Nutzer und Administratoren nur die Zugriffsrechte erhalten, die für die Erfüllung ihrer vertraglichen Pflichten erforderlich sind. Dies stellt sicher, dass der Zugriff auf sensible Daten und Systeme auf das notwendige Minimum beschränkt wird.

m) Der Auftragnehmer ist verpflichtet, bei der Aufgabenverteilung das Prinzip der Funktionstrennung einzuhalten. Dies bedeutet, dass insbesondere auf eine Verteilung der administrativen Tätigkeiten hingewirkt wird, um sicherzustellen, dass keine einzelne Person übermäßige Kontrolle über die Systeme und Daten hat. Dabei ist insbesondere auf eine Funktionstrennung zwischen operativen und kontrollierenden Funktionen sowie auf eine Funktionstrennung bei der Administration von Rollen, Genehmigung und Zuweisung von Zugriffsrechten zu achten. Dies trägt dazu bei, die Sicherheit der Daten und Systeme zu gewährleisten.

5 Anforderungen an das Personal des Auftragnehmers

a) Der Auftragnehmer ist verpflichtet, seine Mitarbeiter regelmäßig, mindestens jedoch einmal jährlich, in Bezug auf die Sicherstellung der Informationssicherheit auf eigene Kosten zu schulen und zu sensibilisieren. Der Auftragnehmer muss dem Auftraggeber auf Nachfrage den Nachweis erbringen, dass die Schulungen dem neuesten Stand der Erkenntnisse in der Informationssicherheit entsprechen und durchgeführt wurden.

b) Der Auftragnehmer ist verpflichtet, die Mitarbeiter, die er im Rahmen der Erfüllung seiner vertraglichen Pflichten gegenüber dem Auftraggeber einsetzt, vor ihrem Einsatz auf die besonderen Vertraulichkeitsanforderungen im Zusammenhang mit der Sicherstellung von Informationssicherheit und der vertraglichen Vertraulichkeitsverpflichtung im Hinblick auf den Umgang mit Daten und Systemen des Auftraggebers hinzuweisen. Der Auftragnehmer muss dies in geeigneter Form dokumentieren.

c) Sollte ein Mitarbeiter des Auftragnehmers die IT-Sicherheitsregeln des Auftragnehmers nicht einhalten, behält sich der Auftraggeber das Recht vor, diesen Mitarbeiter für weitere Leistungserbringungen abzulehnen. Der Auftragnehmer wird dann unverzüglich einen anderen Mitarbeiter bereitstellen, der die Anforderungen erfüllt.

6 Anlagen, Systeme und Gebäude des Auftragnehmers

a) Der Auftragnehmer muss sicherstellen, dass nur autorisierte Personen Zugang zu Bereichen mit Informationen oder Systemen mit hohem oder sehr hohem Schutzbedarf haben. Dies wird durch fortlaufende Überwachung und Zutrittsschutzmaßnahmen erreicht, wie zum Beispiel Einbruchsicherung, Zutrittskontrollsysteme, Videoüberwachung, Sicherheitspersonal und Alarmsysteme. Auf diese Weise wird die Integrität kritischer Bereiche gewährleistet.

7 Vorfälle beim Auftragnehmer

a) Der Auftragnehmer muss alle Vorfälle, die die Sicherheit, Verfügbarkeit, Integrität oder Vertraulichkeit der IT-Systeme, Daten oder Dienstleistungen des Auftraggebers beeinträchtigen oder gefährden könnten, unverzüglich dem Auftraggeber melden. Die Information zum Vorfall ist an informationsecurityoffice@bizerba.com in Deutscher oder Englischer Sprache zu senden.

b) Der Auftragnehmer muss dem Auftraggeber alle relevanten Informationen über die Ursache, den Umfang, die Auswirkungen und die ergriffenen oder geplanten Maßnahmen zur Behebung und Vermeidung des Vorfalls zur Verfügung stellen.

c) Der Auftragnehmer muss mit dem Auftraggeber bei der Untersuchung, Analyse, Bewertung und Beilegung des Vorfalls zusammenarbeiten und alle angemessenen Anweisungen des Auftraggebers befolgen.

d) Der Auftragnehmer muss dem Auftraggeber regelmäßig über den Status und den Fortschritt der Behebung des Vorfalls berichten und nach Abschluss des Vorfalls einen abschließenden Bericht erstellen.

8 Anforderungen an den Datenschutz

a) Datenminimierung und Zweckbindung:
Einführung eines Verfahrens zur Überprüfung und Sicherstellung, dass nur die für den jeweiligen Verarbeitungszweck notwendigen personenbezogenen Daten erhoben und verarbeitet werden. Dies beinhaltet auch eine regelmäßige Überprüfung der Datenverarbeitungsaktivitäten zur Identifizierung und Eliminierung unnötiger Datensammlungen.

b) Verschlüsselung personenbezogener Daten:
Neben der bereits erwähnten Verschlüsselung portabler Datenträger sollte spezifiziert werden, dass alle personenbezogenen Daten, die übertragen, gespeichert oder verarbeitet werden, mittels starker Verschlüsselungsverfahren geschützt werden müssen. Dazu gehört auch die Verschlüsselung von Daten bei der Übertragung über öffentliche Netzwerke.

c) Zugriffskontrollen und Berechtigungsmanagement:
Detaillierte Ausführung der Prozesse und Kontrollmechanismen zur Verwaltung von Zugriffsrechten auf personenbezogene Daten. Dies umfasst die Implementierung von Verfahren zur Vergabe, Überprüfung und Entziehung von Zugriffsrechten sowie die Nutzung von Least Privilege-Prinzip und Funktionstrennung, um sicherzustellen, dass Mitarbeiter nur Zugriff auf die Daten haben, die sie zur Erfüllung ihrer Aufgaben benötigen.

d) Protokollierung und Überwachung:
Ausführung der Protokollierungs- und Überwachungsmaßnahmen, um sicherzustellen, dass alle Zugriffe auf personenbezogene Daten und Systeme, die solche Daten verarbeiten, protokolliert und überwacht werden. Dies sollte auch die regelmäßige Überprüfung der Protokolle auf unbefugte Zugriffe oder verdächtige Aktivitäten umfassen.

e) Datenschutzbezogene Schulungen:
Spezifizierung der Anforderungen an Datenschutzschulungen für Mitarbeiter, die Zugang zu personenbezogenen Daten haben. Diese Schulungen sollten Aspekte des Datenschutzes, der Datensicherheit und der Verhaltensregeln im Umgang mit personenbezogenen Daten abdecken und regelmäßig aktualisiert werden, um den neuesten gesetzlichen Anforderungen und Best Practices zu entsprechen.

f) Verfahren bei Datenschutzverletzungen:
Einführung eines spezifischen Verfahrens für die Meldung und Handhabung von Datenschutzverletzungen, einschließlich der Benachrichtigung des Auftraggebers und der betroffenen Personen gemäß den Anforderungen der DSGVO.

g) Vertraulichkeitsvereinbarungen:
Einführung einer Regelung, die sicherstellt, dass alle Mitarbeiter, die im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten haben, eine Vertraulichkeitsvereinbarung unterzeichnen. Diese Vereinbarung sollte die Verpflichtung zur Wahrung der Vertraulichkeit dieser Daten klar festlegen und die Folgen bei Verstößen dagegen aufzeigen.

9 Allgemeine Anforderungen an Auftragnehmer und Unterauftragnehmer

a) Der Auftragnehmer muss sicherstellen, dass er und seine Unterauftragnehmer die geltenden gesetzlichen und vertraglichen Bestimmungen zum Schutz der IT-Sicherheit und der personenbezogenen Daten des Auftraggebers oder Dritter einhalten.

b) Der Auftraggeber hat das Recht, die IT-Dokumente sowie die IT-Infrastruktur des Auftragnehmers oder seiner Unterauftragnehmer jederzeit zu überprüfen, um die Einhaltung der IT-Sicherheitsanforderungen zu gewährleisten.

c) Der Auftraggeber kann dazu sowohl Fernaudits als auch Vor-Ort-Audits durchführen oder durchführen lassen. Der Auftraggeber kann dabei die Art, den Umfang, den Zeitpunkt und die Häufigkeit der Audits nach eigenem Ermessen festlegen.

10 Verwaltung und Rückgabe von Informationen sowie Unternehmenswerten des Auftraggebers

a) Wenn ein Mitarbeiter des Auftragnehmers nicht mehr für den Auftraggeber tätig ist oder das Projekt oder die Dienstleistung abgeschlossen ist, muss der Auftragnehmer sicherstellen, dass alle vom Auftraggeber erhaltenen Gegenstände, Informationen, Unterlagen oder ähnliche Vermögenswerte (zusammengefasst als “Unternehmenswerte”) ordnungsgemäß zurückgegeben werden.

   Dazu gehören unter anderem:

   - Firmenausweis und Zugangskarten
   - Geräte des Unternehmens wie z.B. Computer, Mobiltelefon, Tablet
   - Dokumente des Auftraggebers,
   - auf elektronischen Medien gespeicherte Informationen,
   - sonstige Informationen, für die kein Zurückbehaltungsrecht besteht,
   - sonstige übergebene Unternehmenswerte.

b) Der Auftragnehmer stellt sicher, dass alle Kenntnisse und Informationen, die für den laufenden Geschäftsbetrieb des Auftraggebers wichtig sind, dokumentiert und in einer mit dem Auftraggeber abgestimmten Form übergeben werden.

c) Informationen und Unterlagen, die auf Wunsch des Auftraggebers nicht gemäß Absatz (b) ausgehändigt werden, sind zu löschen oder zu vernichten. Eine schriftliche Bestätigung der Löschung oder Vernichtung ist dem Auftraggeber auf Anfrage auszuhändigen.

Anlage Wartung

Allgemeine Anforderungen an die Wartung

Version vom 04.02.2024

Internal - do not pass on to third parties

Inhaltsverzeichnis

1 Begriffsdefintion

Wartung

Wartung bezieht sich auf die regelmäßige Überprüfung, Aktualisierung und Reparatur von Computersystemen, Geräten und Netzwerken, um sicherzustellen, dass sie ordnungsgemäß funktionieren und auf dem neuesten Stand sind. Dies kann die Installation von Software-Updates, die Überprüfung der Sicherheitseinstellungen und die Behebung von Fehlern oder Problemen umfassen.

Fernwartung
Fernwartung ist ein Prozess, bei dem ein Techniker oder ein Dienstleister aus der Ferne auf ein Computersystem oder ein Netzwerk zugreift, um Wartungsarbeiten durchzuführen, Probleme zu diagnostizieren oder zu beheben. Dies ermöglicht es, ggf. schnell auf Probleme zu reagieren, ohne physisch anwesend sein zu müssen, und kann die Effizienz und Zuverlässigkeit von IT-Systemen verbessern. Es ist wichtig, dass Fernwartung nur von autorisierten Personen durchgeführt wird und dass alle Sicherheitsprotokolle eingehalten werden, um die Integrität und Vertraulichkeit von Daten zu gewährleisten

2 Allgemeines

Die Vereinbarung gilt additiv zum Dokument ISMS - Anlage für Lieferanten und Dienstleister - Allgemeine IT-Sicherheit.

3 Allgemeine Anforderungen an die Wartung

a) Jegliche Wartung muss vom Auftraggeber genehmigt oder initiiert werden, es sei denn es gelten andere Vertragliche Vereinbarungen. Dies stellt sicher, dass alle Wartungen ordnungsgemäß überwacht und genehmigt werden, um die Sicherheit und Integrität der Systeme des Auftraggebers zu gewährleisten.

b) Jeglicher Übertragung von Daten wie z.B. Datenbanktabellen oder Konfigurationseinstellungen vom Auftragsgeber zum Auftragsnehmer ist nur zur Fehlerdiagnose und jeweiliger schriftlicher Zustimmung des Auftraggebers erlaubt. Des weiteren dürfen etwaige personenbezogene nur anonymisiert übertragen werden.

c) Der Auftragnehmer muss für ein reibungsloses Patch- und Änderungsmanagement bei Wartungen sorgen, welches das zügige Einspielen von Patches, Updates und Service Packs ermöglicht. Daneben muss der Auftragnehmer ein Release Management etablieren und mit dem Auftraggeber abstimmen.

d) Um sicherzustellen, dass die Patches, Updates und Service Packs bei Wartungen im Wirkbetrieb rückwirkungsfrei funktionieren, muss der Auftragnehmer sie zuvor auf Testsystemen überprüfen. Der Auftragnehmer ist verpflichtet, Testberichte zu erstellen und dem Auftraggeber zur Verfügung zu stellen.

e) Wenn ein Mitarbeiter das Unternehmen des Auftragnehmers verlässt, müssen unverzüglich Maßnahmen ergriffen werden, um sicherzustellen, dass dieser Mitarbeiter keine Wartungsaufgaben mehr durchführen kann. Dazu gehört insbesondere die sofortige Entziehung aller Zugriffsrechte auf Systeme und Anwendungen, die im Auftrag des Auftraggebers betrieben werden. Der Auftragnehmer ist dafür verantwortlich, dass diese Maßnahmen schnell und effektiv umgesetzt werden, um die Sicherheit der Daten und Systeme des Auftraggebers zu gewährleisten.

f) Der Auftragnehmer hat sicherzustellen, dass die Bizerba ISMS-Richtlinie für Systemverantwortliche und Administratoren eingehalten wird. Dies bedeutet, dass bei Anpassungen der Konfiguration und anderen Wartungsaufgaben die Sicherheitsstandards der Bizerba eingehalten werden müssen. Der Auftragnehmer ist dafür verantwortlich, dass seine Mitarbeiter, die als Systemverantwortliche oder Administratoren tätig sind, diese Richtlinie kennen und befolgen, um die Integrität und Sicherheit der Systeme und Daten des Auftraggebers zu gewährleisten.

4 Zusätzliche Anforderungen an die Fernwartung

a) Der Auftraggeber bestimmt die Technologie sowie die Authentifizierungsmethoden für den Fernwartungszugriff.

b) Jegliche Fernwartungen müssen vom Auftraggeber genehmigt oder initiiert werden, es sei denn es gelten andere vertragliche Vereinbarungen. Dies stellt sicher, dass alle Fernwartungsaktivitäten ordnungsgemäß überwacht und genehmigt werden, um die Sicherheit und Integrität der Systeme des Auftraggebers zu gewährleisten.

c) Der Auftraggeber behält sich das Recht vor, die Fernwartung jederzeit zu beenden oder zu unterbrechen, wenn Bedenken hinsichtlich der Sicherheit oder des Datenschutzes bestehen.

d) In Bezug die Fernwartung ist es wichtig, dass alle Fernwartungssitzungen, hierzu zählen auch RDP Sessions, sofort nach Erbringung der jeweiligen Tätigkeit geschlossen werden. Dies gilt auch für kurze Pausen. Der Grund dafür ist, dass offene Fernwartungssitzungen ein Sicherheitsrisiko darstellen und unbefugten Zugriff auf Unternehmenssysteme und -daten ermöglichen können. Durch das sofortige Schließen von Fernwartungssitzungen wird die Sicherheit und Vertraulichkeit von Unternehmensdaten und -ressourcen gewährleistet und das Risiko von Sicherheitsverletzungen minimiert.

Anlage für Software- und Produktentwicklung

Version vom 04.02.2024

Internal - do not pass on to third parties

Inhaltsverzeichnis

1 Allgemeine Informationen

Dieser Anhang legt die allgemeinen organisatorischen Security-Anforderungen sowie -Mindeststandards fest, die Auftragnehmer erfüllen müssen, um sicherzustellen, dass ihre Produkte, Software und Dienstleistungen den geforderten Sicherheitsstandards entsprechen.

Die Vereinbarung gilt additiv zum Dokument ISMS - Anlage für Lieferanten und Dienstleister - Allgemeine IT-Sicherheit.

2 Allgemeine Organisatorische Anforderungen

1) Der Auftragnehmer verpflichtet sich, die Sicherheit des Software Development Life Cycle-Prozesses durch die Einhaltung allgemein anerkannter Securitystandards zu gewährleisten. Dies umfasst insbesondere Reviews, automatisierte Tests und Vulnerability Tests. Vor der Inbetriebnahme muss der Auftragnehmer alle Anwendungen für den Auftraggeber einer Überprüfung auf Anwendungsschwachstellen unterziehen und gegebenenfalls festgestellte Schwachstellen beseitigen.

2) Der Auftragnehmer gewährleistet den Stand der Technik der Informationssicherheit in allen seinen Produkten und Dienstleistungen. Der Auftragnehmer hat den Stand der Technik bei bestehenden Wartungsverträgen in angemessenen Wartungszyklen stets anzupassen und entsprechende technische Entwicklungen zu berücksichtigen.

3) Der Auftragnehmer ist dafür verantwortlich, ein effizientes Patch- und Änderungsmanagement sicherzustellen, das das schnelle Einspielen von Patches, Updates und Service Packs ermöglicht. Um sicherzustellen, dass die Patches, Updates und Service Packs im Produktivbetrieb ohne Rückwirkungen funktionieren, muss der Auftragnehmer diese zuvor auf Testsystemen überprüfen. Der Auftragnehmer ist verpflichtet, Testberichte zu erstellen und dem Auftraggeber auf Nachfrage zur Verfügung zu stellen.

4) Bei Bekanntwerden sehr kritischer Schwachstellen (entsprechend CVE Ratings) ist der Hersteller verpflichtet, zeitnah und auf seine Kosten zu überprüfen, ob sein Produkt davon betroffen ist und den Datenminimierung und Zweckbindung:
5) Einführung eines Verfahrens zur Überprüfung und Sicherstellung, dass nur die für den jeweiligen Verarbeitungszweck notwendigen personenbezogenen Daten erhoben und verarbeitet werden. Dies beinhaltet auch eine regelmäßige Überprüfung der Datenverarbeitungsaktivitäten zur Identifizierung und Eliminierung unnötiger Datensammlungen.
6)
7) Verschlüsselung personenbezogener Daten:
8) Neben der bereits erwähnten Verschlüsselung portabler Datenträger sollte spezifiziert werden, dass alle personenbezogenen Daten, die übertragen, gespeichert oder verarbeitet werden, mittels starker Verschlüsselungsverfahren geschützt werden müssen. Dazu gehört auch die Verschlüsselung von Daten bei der Übertragung über öffentliche Netzwerke.
9)
10) Zugriffskontrollen und Berechtigungsmanagement:
11) Detaillierte Ausführung der Prozesse und Kontrollmechanismen zur Verwaltung von Zugriffsrechten auf personenbezogene Daten. Dies umfasst die Implementierung von Verfahren zur Vergabe, Überprüfung und Entziehung von Zugriffsrechten sowie die Nutzung von Least Privilege-Prinzip und

Funktionstrennung, um sicherzustellen, dass Mitarbeiter nur Zugriff auf die Daten haben, die sie zur Erfüllung ihrer Aufgaben benötigen.

12)

13) Protokollierung und Überwachung:

14) Ausführung der Protokollierungs- und Überwachungsmaßnahmen, um sicherzustellen, dass alle Zugriffe auf personenbezogene Daten und Systeme, die solche Daten verarbeiten, protokolliert und überwacht werden. Dies sollte auch die regelmäßige Überprüfung der Protokolle auf unbefugte Zugriffe oder verdächtige Aktivitäten umfassen.

15)

16) Datenschutzbezogene Schulungen:

17) Spezifizierung der Anforderungen an Datenschutzschulungen für Mitarbeiter, die Zugang zu personenbezogenen Daten haben. Diese Schulungen sollten Aspekte des Datenschutzes, der Datensicherheit und der Verhaltensregeln im Umgang mit personenbezogenen Daten abdecken und regelmäßig aktualisiert werden, um den neuesten gesetzlichen Anforderungen und Best Practices zu entsprechen.

18)

19) Verfahren bei Datenschutzverletzungen:

20) Einführung eines spezifischen Verfahrens für die Meldung und Handhabung von Datenschutzverletzungen, einschließlich der Benachrichtigung des Auftraggebers und der betroffenen Personen gemäß den Anforderungen der DSGVO.

21)

22) Vertraulichkeitsvereinbarungen: Einführung einer Regelung, die sicherstellt, dass alle Mitarbeiter, die im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten haben, eine Vertraulichkeitsvereinbarung unterzeichnen. Diese Vereinbarung sollte die Verpflichtung zur Wahrung der Vertraulichkeit dieser Daten klar festlegen und die Folgen bei Verstößen dagegen aufzeigen.

23) entsprechend zu verständigen.

24) Der Auftragnehmer garantiert während des gesamten Betriebszeitraums, dass entdeckte Schwachstellen in den Lieferungen und Leistungen rasch und zeitnah und auf eigene Kosten (im Rahmen bestehender Wartungsverträge) behoben werden oder zumindest bis zur endgültigen Behebung eine brauchbare Umgehungsmaßnahme zur Mitigation der Bedrohung angeboten wird. Für nichtveröffentlichte Schwachstellen gilt eine Frist von maximal 60 Tagen, für öffentlich bekannte Schwachstellen eine Frist von maximal 3 Tagen zur Mitigation der Bedrohung.

25) Funktionsumfang und damit die Anzahl vorhandener Programme, Software-Module, Dienste und Netzwerkprotokolle auf Komponenten sind auf das für den Systembetrieb nötige Minimum reduziert. Alle nicht explizit benötigten Dienste sind standardmäßig deaktiviert. So ein System einem größeren Benutzerkreis zugänglich ist oder sehr kritische Funktionen innehat muss ein granulares Rollen- und Berechtigungssystem ermöglicht werden. Standardmäßig vorhandene Kombinationen aus Benutzernamen und Kennwörtern müssen während der initialen Konfiguration geändert werden bzw. änderbar sein. Jede Komponente und jeder Benutzer hat standardmäßig nur die Rechte, die für die Ausführung einer Aktion nötig sind. So werden z. B. Anwendungen und Netzwerk-Dienste nicht mit Administratorprivilegien, sondern nur mit den minimal nötigen Systemrechten betrieben (least privilege principle).

26) Anwendungen müssen eine personenspezifische Identifizierung und Authentifizierung vornehmen können. Ohne erfolgreiche Benutzer-Authentifizierung darf das System keinerlei Aktionen erlauben. Zugriffe auf Daten und Variablen dürfen nur nach einer erfolgreichen Authentisierungs- und Autorisierungsprüfung möglich sein. Bei Verwendung von Passwörtern muss das System Passwörter, mit vom Auftraggeber definierbarer Stärke und Gültigkeitsdauer erzwingen (Password-Policies). Es darf keine fest codierten Kombination aus Benutzernamen und Kennwörtern geben. Idealerweise bietet

die Lösung die Möglichkeit einer sicheren Multifaktorauthentifizierung. Für Lieferungen und Leistungen, die direkt über das Internet erreichbar sind und deren Zugriff nicht auf legitime Netzwerkverbindungen eingeschränkt ist, ist eine Zweifaktorauthentifizierung verpflichtend.

27) Der Auftragnehmer verpflichtet sich, seine Produkte und Dienstleistungen frei von Malware, Spyware, verstecktem Code, nicht-dokumentierten Hintertüren oder sonstigen verborgenen Funktionen (wie z.B. nicht-autorisierten Datenweiterleitungen) zu halten, die geeignet sind, die Informationssicherheit der Lieferungen und Leistungen zu kompromittieren. Für den Betrieb nicht unbedingt erforderliche Accounts werden entfernt oder zumindest deaktiviert.
Falls der Auftragnehmer in den Lieferungen und Leistungen eine Standardsoftware verwendet (z.B. Betriebssystem, Datenbank), so hat er die Installation von Sicherheitssoftware, die für diese Standardsoftware vom Betreiber gewählt und dafür lizensiert ist, zu erlauben und deren Integration zu ermöglichen ohne, dass der Auftraggeber Gewährleistungsansprüche auf die Lieferungen und Leistungen verliert. Übliche Sicherheitssoftware ist z.B. Software für Inventory, Malware Defense, Identity Management, SIEM, Intrusion Detection, DLP, Vulnerability Detection, etc.
Darüber hinaus müssen die Lieferungen und Leistungen Mechanismen bieten, die es erlauben (D)DoS Angriffe zu mitigieren oder zumindest den Netzwerkzugriff auf legitime Verbindungen einzuschränken (beispielsweise basierend auf Firewallregeln).

28) Der Auftragnehmer ist verpflichtet, durch geeignete Maßnahmen, wie zum Beispiel durch die Verwendung von Escrow (Hinterlegung des Sourcecodes und regelmäßig aktualisierter Daten/Informationen), unter Berücksichtigung der Vertraulichkeitsvereinbarungen und Datenschutzanforderungen sicherzustellen, dass der Betrieb des Auftraggebers im Falle einer Insolvenz des Auftragnehmers nicht wesentlich gestört wird und die vertragsgegenständlichen Leistungen durch den Auftraggeber selbst oder einen Dritten nahtlos weiter erbracht werden können.

29) Sofern der Auftragnehmer Testdaten für die Entwicklung von Anwendungen und Systemen verwendet, müssen diese sorgfältig und nachvollziehbar ausgewählt, geschützt und kontrolliert werden. Es sollen anonymisierte oder pseudonymisierte Daten verwendet werden. Die Verwendung von Echtdaten bedarf einer vorherigen Zustimmung des Auftraggebers. Ferner müssen die Testsysteme denselben Sicherheitsanforderungen genügen wie die Produktivsysteme.

30) Der Auftragnehmer muss eine schriftliche Richtlinie erstellen und implementieren, die die zulässigen Kryptographiealgorithmen definiert, um sicherzustellen, dass keine veralteten und unsicheren Kryptographielösungen in den vom Auftragnehmer bereitgestellten, verkauften oder beim Auftraggeber eingesetzten Produkten verwendet werden. Diese Richtlinie muss einem Industriestandard entsprechen (z.B. BSI TR-02102 in der jeweils aktuellen Version) und regelmäßig überprüft werden. Auf Anfrage muss sie dem Auftraggeber zur Verfügung gestellt werden.

31) Wenn eine angewandte Kryptographielösung als unsicher bekannt wird, müssen die Richtlinie und die Umsetzung angepasst werden. Wenn eine solche Kryptographielösung in einem bereits beim Auftraggeber eingesetzten Produkt oder einer Anwendung verwendet wird, muss der Auftragnehmer sie im Rahmen des Vulnerability-Management-Prozesses als Schwachstelle bewerten und melden. Der Auftragnehmer muss Vorschläge zur Umgehung der Schwachstelle unterbreiten.

32) Falls der Auftragnehmer Web-Anwendungen für den Auftraggeber entwickelt, verpflichtet sich der Auftragnehmer, die Entwicklungsprozesse gemäß den anerkannten Web-Standards für sichere Software-Entwicklung durchzuführen. Dazu gehören beispielsweise die Prinzipien des Open Web Application Security Project (OWASP). Der Auftragnehmer wird alle technisch möglichen und im

konkreten Fall zumutbaren Vorkehrungen treffen, um die vertragsgegenständliche Software gegen bekannte Angriffstechniken wie SQL-Injection, Cross-Site Scripting, Denial of Services Attacken, Brute-Force-Angriffe und Man-in-the-Middle-Attacken zu schützen.

33) Der Auftragnehmer hat sicherzustellen, dass nur mit der Entwicklung betraute Mitarbeiter des Auftragnehmers Zugriff zum Quellcode erhalten.

3 Anforderungen an die Programmierung

Der Auftragsnehmer verpflichtet sich, dass er bei der Entwicklung seiner Geräte, Anwendung und Cloudanwendungen mindestens folgende Security-Anforderungen einhält:

a) Alle Anwendungen und Systeme dürfen keine Backdoors und keine undokumentierten Interfaces enthalten
b) Alle Standard-Passwörter eines Systems müssen durch den Auftraggeber geändert werden können
c) Der clientseitige Sourcecode sollte frei von sensibler Geschäftslogik und muss frei von geheimen Schlüsseln sein.
d) Authentifizierungskontrollen müssen bei falschen Zugangsdaten immer fehlschlagen, um sicherzustellen, dass keine unbefugten Zugriffe möglich sind.
e) Eine “Passwort vergessen”-Funktion darf das aktuelle Passwort niemals preisgeben. Zudem müssen alle Funktionen zur Wiederherstellung des Kontozugriffs müssen mindestens genauso sicher sein wie der primäre Authentifizierungsmechanismus.
f) Neue Passwörter dürfen niemals im Klartext über unsichere Kanäle gesendet werden. Eventuelle Sicherheitsfragen müssen datenschutzkonform und stark genug sein, um Konten vor böswilliger Wiederherstellung zu schützen.
g) Admin-Oberflächen dürfen für nicht vertrauenswürdige Personen nicht zugänglich sein.
h) Bei Server / Client-Anwendungen müssen alte Sessions müssen bei neuer Abmeldung eines Benutzer ungültig werden und bei Login und Authentifizierung müssen immer neue Session-IDs generiert werden. Die Anwendung darf nur selbst generierte Session-IDs akzeptieren, die ausreichend lang, zufällig und eindeutig über die Menge der Sessions verteilt sind.
i) Der Zugang zu sensiblen und vertraulichen Daten muss geschützt sein und Directory Browsing und Listing müssen deaktiviert sein.
j) Die Anwendung muss gegen LDAP- und SQL-Injections geschützt sein.
k) Die Anwendung darf keine sensiblen Daten protokollieren, die einen Angreifer unterstützen könnten, einschließlich Sitzungsidentifikatoren, Passwörtern, Hashes oder API-Token.
l) Sensitive Daten dürfen nicht ungeschützt gespeichert werden. Auf dem Server und Client müssen alle gecachten oder temporären Kopien sensibler Daten vor unbefugtem Zugriff geschützt und spätestens nach der Beendigung der Session bereinigt werden.
m) Zwischen Client und Server muss das gleiche Encoding verwendet werden und alternative, weniger sichere Zugriffspfade sind nicht erlaubt.