Vertragsanlage IT Sicherheitsanforderungen für Lieferanten und Dienstleister

Vertragsparteien	Eintrag
Auftraggeber	Knappschaft Kliniken Solution GmbH, In der Schornau 23-25, 44892 Bochum
Auftragnehmer	[Name und Anschrift]
Hauptvertrag und Datum	[Bezeichnung und Datum]

1 Geltungsbereich und Begriffe

1.1 Diese Anlage ist Bestandteil des oben bezeichneten Hauptvertrags und gilt für alle Produkte, Systeme, Softwarekomponenten und Dienstleistungen des Auftragnehmers, die für die vereinbarte Leistung eingesetzt, geliefert, entwickelt, gewartet oder betrieben werden oder Zugang zu Informationen oder Systemen des Auftraggebers ermöglichen, soweit dies für die jeweilige Leistung einschlägig ist. Sie gilt während Planung, Integration, produktiver Nutzung und Außerbetriebnahme. Die Pflichten zu Softwareentwicklung gelten, soweit der Auftragnehmer Software entwickelt oder verändert; die zusätzlichen Pflichten zum IT-Betrieb gelten, soweit er Betriebsleistungen erbringt.

1.2 Der Auftragnehmer erfüllt die nachstehenden Anforderungen auch durch eingesetzte Beschäftigte und Unterauftragnehmer. Er setzt angemessene Sicherheitsmaßnahmen nach dem Stand der Technik und entsprechend dem Schutzbedarf, der Art, dem Umfang und den konkreten Risiken der betroffenen Leistungen um. Dabei sind die jeweils einschlägigen gesetzlichen und regulatorischen Anforderungen an die Informations- und Cybersicherheit zu beachten. Abweichungen bedürfen vor ihrer Umsetzung einer dokumentierten Vereinbarung mit dem Auftraggeber. Eine bloße Anzeige einer Abweichung ersetzt diese nicht.

1.3 „Sicherheitsvorfall“ ist ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit der vertragsbezogenen Systeme, Leistungen oder Informationen beeinträchtigt oder beeinträchtigen kann. „Schwachstelle“ ist eine technische oder organisatorische Schwäche, deren Ausnutzung eine solche Beeinträchtigung ermöglichen kann. „Neutralisierung“ bedeutet die wirksame Beseitigung oder vorläufige Kompensation der Auswirkungen einer Schwachstelle.

2 Sicherheitsorganisation und Ansprechpartner

2.1 Der Auftragnehmer dokumentiert Zuständigkeiten, Sicherheitsrichtlinien und Prozesse für die vertragsbezogene Leistung, macht sie seinem eingesetzten Personal bekannt und überprüft sie regelmäßig. Soweit er Betriebsleistungen erbringt, unterhält er dafür Informationssicherheitsmanagementprozesse nach einem anerkannten und für die jeweilige Leistung geeigneten Informationssicherheitsstandard, insbesondere ISO/IEC 27001 oder einem gleichwertigen Standard.

2.2 Der Auftragnehmer benennt einen erreichbaren Sicherheitskontakt und einen Eskalationskontakt einschließlich Vertretung und hält deren Kontaktdaten aktuell. Er stellt für Sicherheitsvorfälle und hochkritische Schwachstellen einen jederzeit erreichbaren Meldeweg bereit. Er eskaliert Verletzungen dieser Anlage und offene Sicherheitsfragen unverzüglich an die benannten Stellen.

2.3 Der Auftragnehmer verfolgt sicherheitsrelevante technische und organisatorische Entwicklungen, bewertet deren Auswirkungen auf die vertragsbezogene Leistung und passt die Maßnahmen bei Bedarf an. Er stellt die für die Erfüllung dieser Anlage erforderlichen personellen und technischen Ressourcen bereit.

3 Unterauftragnehmer und Lieferkette

3.1 Der Auftragnehmer legt vor ihrem Einsatz die an der Leistung beteiligten Unterauftragnehmer, deren Aufgaben und die weitere wesentliche Leistungskette offen. Er informiert vor einer beabsichtigten Auslagerung oder wesentlichen Änderung der Leistungskette in Textform über Art und Umfang der Änderung.

3.2 Der Auftragnehmer verpflichtet seine Unterauftragnehmer schriftlich mindestens auf die jeweils einschlägigen Sicherheitsanforderungen dieser Anlage, überwacht deren Einhaltung und bleibt für die Erfüllung gegenüber dem Auftraggeber verantwortlich. Er gewährleistet die erforderliche Nachweisbarkeit und Prüfungsrechte auch entlang der Leistungskette.

4 Schwachstellenmanagement

4.1 Der Auftragnehmer prüft seine Produkte und die für die Leistung eingesetzten Komponenten kontinuierlich auf Schwachstellen. Dies umfasst insbesondere Betriebssysteme, Datenbanken, Server, Middleware, Anwendungen, Bibliotheken und weitere abhängige Komponenten. Er sichtet einschlägige Sicherheitshinweise, bewertet die Betroffenheit

und dokumentiert Kritikalität, mögliche Auswirkungen auf Verfügbarkeit, Integrität und Vertraulichkeit sowie den geplanten Umgang.

4.2 Der Auftragnehmer informiert den Auftraggeber aktiv über relevante Schwachstellen und Produktfehler, die sich auf die Leistung oder den Betrieb des Auftraggebers auswirken können. Die Mitteilung enthält, soweit bekannt, betroffene Versionen, Ausnutzbarkeit, Auswirkungen, Schutzmaßnahmen, Behebungsplan und voraussichtliche Termine. Neue Erkenntnisse und Verzögerungen teilt er nach.

4.3 Für betroffene Komponenten neutralisiert der Auftragnehmer Schwachstellen spätestens innerhalb der in der nachstehenden Tabelle genannten Fristen. Die Frist beginnt mit Kenntniserlangung des Auftragnehmers von der Schwachstelle, spätestens mit deren Mitteilung durch den Auftraggeber. Eine vorläufige Maßnahme ist nur ausreichend, solange sie die Auswirkungen wirksam kompensiert. Der Auftragnehmer betreibt die endgültige Behebung weiter und nennt hierfür einen verbindlichen Termin. Kann die Schwachstelle innerhalb der genannten Frist nicht vollständig behoben werden, setzt der Auftragnehmer innerhalb dieser Frist eine wirksame vorläufige Schutzmaßnahme um und legt dem Auftraggeber unverzüglich eine begründete Risikobewertung sowie einen Maßnahmen- und Zeitplan für die endgültige Behebung vor.

Priorität	CVSS Grundwert	Frist bis zur Neutralisierung
Kritisch	9,0 bis 10,0	3 Tage
Hoch	7,0 bis 8,9	7 Tage
Mittel	4,0 bis 6,9	1 Monat
Niedrig	0,1 bis 3,9	3 Monate

4.4 Der Auftragnehmer berücksichtigt bei der Priorisierung zusätzlich die konkrete Ausnutzbarkeit, Exposition und Auswirkungen in der Einsatzumgebung. Er dokumentiert jede Abweichung von der öffentlichen CVSS Einstufung nachvollziehbar. Ist innerhalb der Frist kein wirksamer Workaround verfügbar, meldet er dies unverzüglich mit einer Risikobewertung und einem Maßnahmenplan. Sicherheitsbezogene Mitteilungen und Dokumente übermittelt er über geschützte Kanäle.

5 Patchmanagement und Lebenszyklus

5.1 Der Auftragnehmer bezieht alle in seinem Leistungsumfang enthaltenen Komponenten in das Patchmanagement ein, insbesondere Betriebssystem, Systemsoftware, Wartungswerkzeuge, Zielanwendung, Middleware und Datenbanken. Vor Übergabe oder Abnahme weist er den aktuellen Patchstand und die Installation freigegebener sicherheitsrelevanter Patches nach. Bei standardisierten Clouddiensten kann der Nachweis durch einen dokumentierten und unabhängig geprüften Patchprozess erfolgen.

5.2 Der Auftragnehmer stellt während der Vertragslaufzeit mindestens zweimal jährlich sowie bei sicherheitsrelevantem Bedarf unverzüglich Updates und Patches bereit oder installiert sie, soweit der Betrieb zu seinem Leistungsumfang gehört. Für Schwachstellen gelten zusätzlich die Fristen nach Ziffer 4.3. Er informiert über adressierte Schwachstellen, deren Kritikalität, betroffene Schutzziele und verbleibende Risiken.

5.3 Der Auftragnehmer informiert rechtzeitig über das absehbare Ende der Unterstützung für eingesetzte Komponenten, bietet eine sichere Nachfolgelösung an und beschreibt erforderliche Übergangsmaßnahmen. Soweit der Auftragnehmer nur eine Anwendung liefert, prüft und erhält er deren Funktionsfähigkeit bei sicherheitsrelevanten Aktualisierungen der von ihm spezifizierten Systemplattform.

6 Sichere Konfiguration und Härtung

6.1 Der Auftragnehmer härtet gelieferte und betriebene Systeme vor Übergabe oder Inbetriebnahme und hält die Härtung aufrecht. Er installiert nur für Funktion, Integration, Betrieb und Wartung erforderliche Komponenten. Nicht benötigte Dienste, Schnittstellen und TCP oder UDP Ports deaktiviert er; erforderliche Zugänge und deren Zweck dokumentiert er.

6.2 Der Auftragnehmer setzt vereinbarte Konfigurationsstandards um, ermöglicht die Änderung aller Passwörter einschließlich voreingestellter Initialpasswörter und ersetzt Standardzugangsdaten vor Produktivsetzung. Er stellt sicher, dass seine Lösung keine ihm bekannten Hintertüren enthält, die Sicherheitsmechanismen umgehen. Die Umsetzung weist er durch geeignete Prüfprotokolle nach.

7 Fernzugriff und Berechtigungen

7.1 Der Auftragnehmer nutzt Fernzugänge ausschließlich für den vereinbarten Zweck, über die freigegebenen Zugangswege und nur für die erforderliche Dauer. Er verwendet für Zugriffe auf geschützte Zonen Sprungserver oder gleichwertige Sicherheitsfunktionen, mindestens Multi-Faktor-Authentisierung (MFA) und eine zeitliche Begrenzung oder automatische Schließung. Er richtet keine eigenständigen, unautorisierten Fernzugänge ein.

7.2 Er verwendet personenbezogene Nutzerkonten. Ausnahmen für gemeinsam genutzte Konten bedürfen vorab einer dokumentierten Vereinbarung; in diesem Fall gewährleistet er die lückenlose Zuordnung jeder Nutzung zu einer Person und stellt die Nachweise mindestens jährlich sowie auf Verlangen bereit. Er prüft Fernzugangsberechtigungen mindestens alle sechs Monate, meldet entfallene Berechtigungen unverzüglich und schützt Zugangsdaten und Schlüssel nach dem Need to know Prinzip.

7.3 Der Auftragnehmer sorgt für dokumentierte Freigaben von Berechtigungen, deren zeitnahe Entziehung bei Rollenwechsel oder Ausscheiden, angemessene Authentisierungsregeln und automatische Bildschirmsperren. Handlungen über seine Konten sind nachvollziehbar zu protokollieren.

8 Sichere Softwareentwicklung

8.1 Soweit der Auftragnehmer Software entwickelt oder verändert, integriert er Sicherheit in Architektur, Entwicklung, Test und Wartung. Er dokumentiert und schult Regeln für sichere Programmierung und überprüft Quellcode sicherheitsbezogen. Für aus nicht geschützten Netzen erreichbare Webanwendungen führt er Prüfungen anhand anerkannter Verfahren wie OWASP oder gleichwertiger Methoden durch.

8.2 Der Auftragnehmer erfasst eingesetzte Fremd und Open Source Komponenten, konfiguriert und wartet sie sicher und prüft regelmäßig veraltete Protokolle und Bibliotheken sowie zusätzliche Funktionen neuer Bibliotheken. Tests schließen Verschlüsselung, Authentisierung, Zugriffskontrolle und weitere Sicherheitsfunktionen ausdrücklich ein. Er stellt die zum sicheren Funktionsnachweis erforderlichen Testfälle sowie die Ergebnisse wesentlicher Codeprüfungen und Penetrationstests für die ausgelieferte Fassung zur Verfügung. Exponierte Systeme lässt er risikogerecht unabhängig prüfen.

9 Kryptografie

Der Auftragnehmer dokumentiert zulässige kryptografische Verfahren, überprüft sie regelmäßig anhand anerkannter Empfehlungen, etwa BSI TR 02102, und ersetzt unsichere Verfahren. Eingesetzte, als unsicher erkannte Verfahren behandelt er als Schwachstelle nach Ziffer 4. Er verschlüsselt Kommunikation und Speicherung dort, wo dies zum Schutz der Informationen erforderlich ist, insbesondere bei Daten mit hohem Schutzbedarf über öffentliche oder nicht ausreichend sichere Netze. Schlüssel verwaltet und schützt er mit geeigneten Verfahren.

10 Zusätzliche Anforderungen an Betriebsleistungen

10.1 Soweit der Auftragnehmer IT Betriebsleistungen erbringt, führt er ein Inventar der hierfür eingesetzten Assets, benennt Verantwortliche und löscht Daten beziehungsweise vernichtet Datenträger nach Schutzbedarf sicher. Er schützt Betriebsstätten gegen unbefugten Zutritt, Einbruch, Feuer, Wasser, extreme Temperaturen und Stromausfall; Zutritte zu Schutzbereichen beschränkt und protokolliert er.

10.2 Er trennt Netzsegmente nach Schutzbedarf, schützt Perimeter, lässt Firewallregeln dokumentiert freigeben und sichert administrative Zugänge angemessen ab. Authentisierungsmerkmale werden nur verschlüsselt übertragen. Er protokolliert Netzverbindungen, Systemzugriffe und administrative Tätigkeiten in einem Umfang, der die Aufklärung von Angriffen und Fehlbedienungen ermöglicht, und schützt sowie bewahrt Protokolle nach den vereinbarten Vorgaben auf.

10.3 Er betreibt aktuellen Schadsoftwareschutz, Datensicherungs und Wiederherstellungsverfahren mit regelmäßigen Wiederherstellungstests, sichere Transporte von Speichermedien, dokumentierte Änderungen an Produktivsystemen und regelmäßige Schwachstellenscans. Drahtlose Netze sichert er kryptografisch; Verbindungen zu unautorisierten Zugangspunkten und das Einrichten unautorisierter Netze verhindert er.

10.4 Er betreibt ein Verfahren für Sicherheitsvorfälle und IT Notfälle nach einem Allgefahrenansatz, berücksichtigt auch nicht technische Auslöser, definiert Rollen und Eskalationen und führt Schulungen und Übungen durch. Die Verfahren stimmt er mit dem eigenen Kontinuitätsmanagement ab.

11 Personal und Vertraulichkeit

Der Auftragnehmer setzt nur fachlich geeignete und regelmäßig zu Informationssicherheit geschulte Personen ein. Personen mit lokalem oder entferntem Zugang sind identifizierbar; der Auftragnehmer dokumentiert ihre Berechtigungen und verpflichtet sie auf Vertraulichkeit. Soweit für besonders sensible Systeme eine vereinbarte, rechtlich zulässige Sicherheitsüberprüfung erforderlich ist, setzt er dort ausschließlich entsprechend überprüfte Personen ein. Informationen aus Fernzugriffen verwendet er nur zur Vertragserfüllung.

12 Dokumentation und Nachweise

12.1 Der Auftragnehmer hält die Sicherheits und Betriebsdokumentation aktuell und stellt sie in einem für die Prüfung der Leistung erforderlichen Umfang zur Verfügung. Dazu gehören, soweit einschlägig: Hardware und Softwareverzeichnis mit

Versionen und Patchständen, Systemarchitektur, Kommunikationsmatrix, Datenflüsse, Konten, Rollen und Berechtigungen, Sicherheitsmechanismen, Betriebsprozesse und Unterauftragnehmerkette. Änderungen pflegt er zeitnah ein.

12.2 Auf Anforderung legt er geeignete Nachweise über die Einhaltung dieser Anlage vor, insbesondere Richtlinien, Prüfberichte, Zertifikate mit Geltungsbereich und Laufzeit, Schwachstellen und Patchberichte sowie Maßnahmenpläne. Vertrauliche Inhalte dürfen in abgestimmter geeigneter Form nachgewiesen werden, sofern die Prüfbarkeit erhalten bleibt.

13 Meldungen und Behandlung von Vorfällen

13.1 Der Auftragnehmer meldet Sicherheitsvorfälle mit möglicher Auswirkung auf die Leistung oder auf Informationen und Systeme des Auftraggebers sowie wesentliche Abweichungen von dieser Anlage unverzüglich über den vereinbarten Sicherheitsmeldeweg, bei erheblichen Sicherheitsvorfällen spätestens innerhalb von 24 Stunden nach Kenntniserlangung. Die erste Meldung enthält die verfügbaren Angaben zu Zeitpunkt, Art, betroffenen Leistungen, möglichen Auswirkungen, bereits ergriffenen Maßnahmen und Ansprechperson. Fehlende Angaben reicht er ohne schuldhaftes Zögern nach.

13.2 Er begrenzt Schäden, sichert erforderliche Beweise, informiert fortlaufend über wesentliche Erkenntnisse und Maßnahmen und übermittelt nach Abschluss einen Bericht zu Ursache, Verlauf, Auswirkungen, Behebung und Vorbeugung. Er unterstützt die Aufklärung und die Erfüllung regulatorischer Meldepflichten des Auftraggebers durch rechtzeitige Bereitstellung der dafür erforderlichen Informationen.

14 Überprüfung und Abweichungen

Der Auftragnehmer ermöglicht nach angemessener Ankündigung sowie anlassbezogen bei erheblichen Sicherheitsbedenken die Prüfung der vertragsbezogenen Sicherheitsmaßnahmen durch den Auftraggeber oder von ihm beauftragte, zur Vertraulichkeit verpflichtete Dritte. Er gewährt Einsicht in geeignete Unterlagen und unterstützt die Prüfung. Die Prüfung erfolgt unter angemessener Berücksichtigung berechtigter Interessen des Auftragnehmers, insbesondere von Geschäfts- und Betriebsgeheimnissen sowie datenschutzrechtlichen Anforderungen. Bei standardisierten Clouddiensten können unabhängige Prüfberichte und Zertifizierungen mit passendem Geltungsbereich als Prüfungsnachweis dienen, soweit sie die betroffenen Maßnahmen hinreichend belegen. Festgestellte Mängel dokumentiert und behebt der Auftragnehmer risikogerecht innerhalb vereinbarter Fristen und berichtet über den Abschluss.

15 Vertragsende und Rückgabe

Bei Beendigung der Leistung unterstützt der Auftragnehmer die sichere Übergabe oder Migration der vertragsbezogenen Daten und Dokumentation nach den Vereinbarungen des Hauptvertrags. Er entzieht Zugänge und löscht oder gibt Informationen und Datenträger nach den vertraglichen und gesetzlichen Vorgaben zurück; die Durchführung weist er auf Verlangen nach. Sicherheits und Meldepflichten für zuvor eingetretene Vorfälle bleiben bis zu deren Bearbeitung bestehen.

Die in dieser Anlage geregelten Sicherheitsanforderungen gelten ergänzend zum Hauptvertrag. Weitergehende gesetzliche, behördliche oder im Hauptvertrag ausdrücklich vereinbarte Sicherheitsanforderungen bleiben unberührt.

16 Anerkennung und Unterzeichnung

Der Auftragnehmer bestätigt mit seiner rechtsverbindlichen Unterzeichnung, diese Anlage erhalten, zur Kenntnis genommen und als Bestandteil des Hauptvertrags anerkannt zu haben. Soweit die Anlage Bestandteil der Vergabeunterlagen ist, ist die darin vorgesehene Anerkennung bzw. Unterzeichnung mit dem Angebot in der jeweils geforderten Form abzugeben.

Auftraggeber	Auftragnehmer
Ort, Datum	Ort, Datum
Name / Funktion	Name / Funktion
Unterschrift	Unterschrift