INFORMATIONSSICHERHEITSANFORDERUNGEN FÜR LIEFERANTEN

zwischen

A.ö. Bezirkskrankenhaus Lienz
Emanuel von Hibler-Straße 5
A-9900 Lienz

nachfolgend **BKH Lienz** bezeichnet

und

nachfolgend **LIEFERANT** bezeichnet.

EINLEITUNG

Dieses Dokument ist eine Anlage zur Richtlinie „Lieferantensicherheit“ und definiert zusätzliche Anforderungen an Informationssicherheit und Datenschutz für alle Lieferanten des BKH Lienz.

Das BKH Lienz wählt seine Lieferanten sorgfältig aus und stellt insbesondere bei Produkten oder Dienstleistungen zur Unterstützung der medizinischen Versorgung erhöhte Anforderungen.
Ziel dieser Anlage ist es, informationssicherheitsrelevante Risiken in der Lieferkette frühzeitig zu erkennen, zu bewerten und wirksam zu minimieren.

RISIKOMANAGEMENT

Der Lieferant betreibt ein laufend aktualisiertes Risikomanagement für Informationssicherheit, um Risiken, Sicherheitsvorfälle und Änderungen bestehender Bedrohungen, die das BKH Lienz betreffen, nach Stand der Technik und geltenden Vorschriften zu identifizieren, zu bewerten, zu minimieren, zu dokumentieren und unverzüglich zu melden.
Meldungen erfolgen an informationssicherheit@kh-lienz.at und enthalten Angaben zur Anwendung, Schwere, Dauer, Betroffenheit personenbezogener Daten, Auswirkungen sowie ergriffenen oder geplanten Maßnahmen. Sicherheitsrelevante Informationen, insbesondere Schwachstellen oder Änderungen des Sicherheitsniveaus sind dem BKH Lienz frühzeitig mitzuteilen. Änderungen an Verarbeitungsprozessen oder Sicherheitsfunktionen bedürfen vorheriger Genehmigung durch das BKH Lienz.

MITARBEITERQUALIFIKATION

Der Lieferant hat sicherzustellen, dass für Tätigkeiten im Zusammenhang mit Leistungen für das BKH Lienz ausschließlich Mitarbeiter eingesetzt werden, die über die erforderlichen fachlichen Qualifikationen und Kenntnisse verfügen. Alle Mitarbeiter werden nachweislich in Informationssicherheit, Datenschutz und Verschwiegenheit geschult und sensibilisiert. Auf Verlangen sind Nachweise über Prüfungen, Schulungen und Sensibilisierung vorzulegen.

DATENSCHUTZ

Der Lieferant stellt die Einhaltung sämtlicher jeweils geltender datenschutzrechtlicher Vorschriften sicher (Datenschutz-Grundverordnung (DSGVO), der in Österreich unmittelbar anwendbaren europäischen Regelungen sowie der einschlägigen nationalen Datenschutz- und Persönlichkeitsrechtsvorschriften). Zudem wird gewährleistet, dass alle in Österreich geltenden rechtlichen und aufsichtsrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten eingehalten werden und verpflichtet eingesetzte Subauftragnehmer vor Aufnahme ihrer Tätigkeit nachweislich zur Einhaltung der DSGVO. Sofern erforderlich, wird der vom BKH Lienz vorgegebene Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO abgeschlossen.
Für Sicherheitsvorfälle, Datenverlust oder Manipulationen ist ein dokumentierter Prozess zur gerichtsverwertbaren Beweissicherung nach österreichischem Recht vorzuhalten.
Personenbezogene Daten sind nach Wegfall des Verarbeitungszwecks oder bei Vertragsbeendigung unverzüglich und unwiderruflich zu löschen. Die ordnungsgemäße Löschung ist durch dokumentierte Verfahren und geeignete Löschprotokolle nachzuweisen.

SUBAUFTRAGNEHMER

Der Lieferant wählt alle im Zusammenhang mit Leistungen für das BKH Lienz eingesetzten Subauftragnehmer sorgfältig und risikobasiert aus, regelt deren Einbindung in schriftlichen Vereinbarungen und stellt deren regelmäßige, nachweisliche Überwachung sicher. Dabei ist ein dem Risiko angemessenes Niveau an Informationssicherheits- und Datenschutzmaßnahmen sicherzustellen.
Der Lieferant haftet für das Handeln der Subauftragnehmer wie für eigenes Handeln und gewährleistet dem BKH Lienz das Recht auf Überprüfung und Auditierung (auch durch beauftragte Dritte) sowie angemessene Unterstützung und Kooperation bei Sicherheitsprüfungen und Sicherheitsvorfällen.
Alle Subauftragnehmer sind dem BKH Lienz vorab vollständig und schriftlich offenzulegen. Änderungen, insbesondere der Wechsel oder die Beauftragung weiterer Subauftragnehmer, sind unverzüglich mitzuteilen.

PHYSISCHE UND UMGEBUNGSBEZOGENE SICHERHEIT

Der Lieferant stellt sicher, dass nur berechtigte Personen Zugang zu Räumlichkeiten haben, in denen Informationen des BKH Lienz verarbeitet werden. Unbefugten Personen, einschließlich Besuchern, darf weder Zutritt noch Einsicht in diese Informationen gewährt werden. Dies gilt auch für Support- und Wartungstätigkeiten einschließlich Fernwartung.
Hierzu setzt der Lieferant ein risikobasiertes physisches Sicherheitskonzept mit geregelten Zutrittsprozessen, Zutrittsberechtigungen sowie Protokollierung und regelmäßiger Überprüfung von Zutritten um.
Die sichere Handhabung, der Transport und die ordnungsgemäße Entsorgung von Dokumenten, Geräten und Datenträgern mit Informationen des BKH Lienz sind nachweislich sicherzustellen.

BETRIEBSSICHERHEIT

Sofern der Lieferant im Auftrag des BKH Lienz Systeme oder Geräte betreibt, stellt er deren erforderliche Verfügbarkeit durch angemessene finanzielle, personelle und technische Maßnahmen sicher. Übernimmt der Lieferant Aufgaben im Identitäts- und Zugriffsmanagement, gewährleistet er, dass Zugriffsberechtigungen regelmäßig überprüft und nicht mehr benötigte Konten zeitnah deaktiviert werden.

PRODUKTLEBENSZYKLUS

Der Lieferant verpflichtet sich, die Informationssicherheit der gelieferten und hergestellten Produkte und Komponenten während der gesamten Einsatzdauer im BKH Lienz nachhaltig sicherzustellen. Sofern ein IT-Betriebssystem Bestandteil der gelieferten Produkte ist, erstreckt sich diese Verpflichtung auch auf das jeweilige Betriebssystem. Dies gilt unabhängig davon, ob das Betriebssystem vom Lieferanten oder vom BKH Lienz bereitgestellt wird.

PATCHMANAGEMENT

Der Lieferant prüft seine Produkte kontinuierlich auf bekannte Sicherheitslücken und setzt erforderliche, geprüfte Patches aus vertrauenswürdiger Quelle um. Nicht sofort behebbare Schwachstellen werden durch geeignete Maßnahmen minimiert, und das BKH Lienz wird unverzüglich über Status und geplante Schritte informiert.

PROTOKOLLIERUNG (LOGGING)

Der Lieferant stellt auf allen für die Dienstleistung genutzten Systemen Maßnahmen sicher, die System- und Sicherheitsereignisse (z. B. Zugriffe, Warnungen, Änderungen) nachvollziehbar protokollieren.
Log-Dateien sind gegen unbefugte Änderungen zu schützen. Bei Untersuchungen oder forensischen Analysen kooperiert der Lieferant uneingeschränkt und ermöglicht dem BKH Lienz die Einsicht und Auswertung relevanter Protokolle.

SYSTEM-/SOFTWAREENTWICKLUNG UND CHANGE-MANAGEMENT

Der Lieferant stellt sicher, dass die Informationssicherheit nachweislich in allen Phasen der Software- und Systementwicklung sowie im Change-Management berücksichtigt wird, inklusive Analyse, Risikoabschätzung, Freigabe, Tests und Dokumentation. Vor jeder Übergabe an das BKH Lienz ist die Software/das System nach dem Stand der Technik nachweislich zu testen. Wiederherstellungen, Kopien oder Rücksetzungen bedürfen der vorherigen Genehmigung durch das BKH Lienz.

NETZWERKSICHERHEIT

Der Lieferant schützt seine IT-Infrastruktur durch geeignete Sicherheitsmaßnahmen und beschränkt den Netzwerkverkehr auf das jeweils erforderliche Mindestmaß. Test-, Entwicklungs-, Qualitäts- und Produktionsumgebungen sind konsequent voneinander zu trennen und, insbesondere bei gemeinsam genutzten Umgebungen, angemessen zu segmentieren.
Der Netzwerkverkehr wird laufend überwacht, um sicherheitsrelevante Ereignisse frühzeitig zu erkennen und bei Bedarf geeignete Gegenmaßnahmen zu ergreifen (z.B. Einschränkung des Datenverkehrs oder Abschottung von Netzwerksegmenten).

FERN- UND FREMDZUGRIFF

Der Lieferant stellt sicher, dass alle Fern- und Fremdzugriffe auf Geräte, Systeme oder Cloud-Umgebungen BKH Lienz durch geeignete Maßnahmen (z.B. Authentifizierung, Zugriffsprotokolle) abgesichert sind. Zugriffe müssen eindeutig identifizierbar sein und Fernwartungs- sowie Administrationstätigkeiten nachvollziehbar dokumentiert werden. Unbefugte Zugriffe sind wirksam zu verhindern.
Erforderliche Fremdzugriffe müssen gesteuert und abgesichert werden, sodass Daten des BKH Lienz weder unbefugt offengelegt noch manipuliert werden können. Für administrative Tätigkeiten dürfen ausschließlich dafür vorgesehene, sicher konfigurierte Hard- und Softwarekomponenten verwendet werden, die einschließlich Updates, Patchmanagement und Inventarisierung dem Stand der Technik entsprechen.

VERSCHLÜSSELUNG / KRYPTOGRAPHIE

Der Lieferant gewährleistet den Schutz der Integrität, Authentizität und Vertraulichkeit aller Daten. Sensible Daten sind sowohl im Ruhezustand als auch während der Übertragung durch Verschlüsselungstechnologien angemessen zu schützen. Dies gilt insbesondere für Cloud-Zugriffe, die Verarbeitung auf mobilen Geräten und Datenträgern sowie für Updates, um unbefugten Zugriff oder Manipulationen wirksam zu verhindern.

SCHUTZ VOR SCHADSOFTWARE

Der Lieferant stellt sicher, dass alle eingesetzten Geräte und Systeme, einschließlich Wartungs- und Supportsysteme, durch aktuelle Sicherheitsmaßnahmen vor Schadsoftware, Angriffen und unbefugtem Zugriff geschützt sind. Dazu gehören insbesondere Malware-Schutz, Zugriffskontrollen und Multi-Faktor-Authentifizierung nach dem jeweils aktuellen Stand der Technik.

AUDIT

Das BKH Lienz ist berechtigt, nach angemessener Vorankündigung, die Einhaltung der in diesem Zusatzdokument festgelegten Informationssicherheits- und Datenschutzanforderungen beim Lieferanten selbst oder durch beauftragte Dritte während der Geschäftszeiten zu überprüfen. Der Lieferant unterstützt die Prüfung durch Bereitstellung der erforderlichen Informationen und Nachweise. Festgestellte Abweichungen sind ehestmöglich zu beheben.

SYSTEMHÄRTUNG

Der Lieferant stellt sicher, dass die von ihm gelieferten Produkte nach anerkannten Standards (z.B. CIS-Standard) sicher konfiguriert sind. Die Härtungskonfigurationen sind regelmäßig zu überprüfen, an den Stand der Technik anzupassen und nachvollziehbar zu dokumentieren.

MANAGEMENT UND MELDUNG VON SICHERHEITSVORFÄLLEN

Der Lieferant betreibt ein dokumentiertes und wirksam umgesetztes Verfahren zum Umgang mit Informationssicherheitsereignissen und -vorfällen. Dieses umfasst insbesondere klare Zuständigkeiten sowie die Erkennung, Analyse, Bewertung, Behandlung, Dokumentation und Meldung von Sicherheitsvorfällen. Dieses Verfahren wird mindestens einmal jährlich nachweislich getestet und laufend aktualisiert.
Der Lieferant verpflichtet sich, alle tatsächlichen oder vermuteten Sicherheitsereignisse und Schwachstellen, die im Zusammenhang mit den gelieferten Produkten und Dienstleistungen oder eingesetzten Subauftragnehmern stehen und Auswirkungen auf die Informationssicherheit des BKH Lienz haben könnten, unverzüglich nach Bekanntwerden an informationssicherheit@kh-lienz.at zu melden.

Die Meldungen haben, abhängig vom jeweiligen Kenntnisstand, zumindest folgende Informationen zu enthalten:

- Beschreibung des Vorfalls (was und wie?)
- Ursache bzw. vermutete Ursache des Vorfalls
- Datum und Uhrzeit des Auftretens
- Datum und Uhrzeit der Entdeckung
- mögliche Auswirkungen auf das BKH Lienz (betroffene Systeme, Dienste oder Daten)
- bereits ergriffene Maßnahmen zur Behebung des Vorfalls
- weitere geplante Maßnahmen zur Behebung des Vorfalls
- erforderliche Maßnahmen seitens des BKH Lienz
- bereits erfolgte interne oder externe Meldungen

Der Lieferant hat vollständige und laufend aktualisierte Informationen zum Vorfall bereitzustellen und unterstützt das BKH Lienz aktiv und zeitnah bei Analyse, Minimierung und Behebung der Auswirkungen. Gegebenfalls auch bei der Wiederherstellung sowie bei erforderlichen Untersuchungen oder Meldepflichten. Vom BKH Lienz gemeldete Sicherheitsereignisse oder -vorfälle sind vom Lieferanten unverzüglich, priorisiert und gemäß den oben genannten Vorgaben zu bearbeiten und zu beheben.

SALVATORISCHE KLAUSEL

Sollten einzelne Bestimmungen dieser Zusatzvereinbarung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt. Eine unwirksame Bestimmung ist durch eine gültige zu ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Bestimmung möglichst nahekommt.

VERTRAGSÄNDERUNG

Mündliche Nebenabreden zu diesem Dokument sind nicht getroffen. Änderungen oder Ergänzungen dieser Zusatzvereinbarung bedürfen zu Ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Änderung dieser Schriftformklausel.

_____

Ort, Datum

_____

Unterschrift Lieferant

Hinweis: Aus Gründen der besseren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet.