§ 1 Geltungsbereich
Die hier festgelegten Informations- und Datenschutzrechtlich relevanten Bestimmungen gelten ergänzend zu den allgemeinen Einkaufbedingungen des Ökumenischen Hainich Klinikums gGmbH (ÖHK) und sind somit Bestandteil des zugehörigen Hauptvertrages.
Die zugehörigen Begrifflichkeiten werden analog zur ISO/IEC 27000 Normreihe verwendet.

§ 2 Schwachstellen-Management
2.1 Der Auftragnehmer (nachfolgend kurz AN) unterzieht die Produkte einer kontinuierlichen Prüfung auf Schwachstellen in Form eines sogenannten Vulnerability-Managements, um auf neue Schwachstellen so schnell als möglich zu reagieren. Es basiert auf der Funktionalität, der technischen Architektur inkl. der zugehörigen Unterkomponenten einschließlich der Betriebssysteme, Datenbanken, Server, Middleware und Bibliotheken. Diese werden verwendet, um neue Schwachstellen in Bezug auf die Kritikalität der geschäftlichen Auswirkungen zu beurteilen.
Sind vom AN entwickelte Software-, Firmware- oder Hardware-Komponenten tangiert, ist der AN verpflichtet, zeitnah die Schwachstellen an den Auftraggeber (nachfolgend kurz AG) zu melden.
2.2 Der AN ist verpflichtet, kontinuierlich relevante Quellen für Sicherheitsempfehlungen zu sichten und diese in Bezug auf die an den AG gelieferten Assets zu bewerten.
2.3 Die vom AN an den AG gemeldeten Schwachstellen müssen vom AN in Hinsicht auf mögliche funktionale und sicherheitsrelevante Auswirkungen bewertet werden.
2.4 Vom AN wird erwartet, dass eine Problemlösung (Patch, Workaround o.ä.) nach einem Best-Effort-Ansatz und somit nach bestem Wissen erarbeitet wird.

§ 3 Patch-Management
3.1 Der durch den AN zur Verfügung gestellte Patch-Umfang muss das gesamte System umfassen. Dazu gehören das Betriebssystem, alle Softwarepakete und Services des Betriebssystems, alle Tools und Applikationen des Herstellers (inkl. derer zu Wartungszwecken sowie alle genutzten Middleware-Applikationen, Datenbanken, Access-, Monitoring- oder Applikationsserver bzw. Systeme).
3.2 Der AN hat sicherzustellen, dass alle Systeme vor der Abnahme durch den AG gepatcht und aktualisiert sind. Der Patchstand sollte nicht älter als sechs Monate sein. Der AN muss alle verfügbaren und freigegebenen Patches als Teil der Lieferung/Leistungserbringung installieren.
3.3 Der AN verpflichtet sich, mindestens zweimal pro Jahr (bei entsprechender Dringlichkeit siehe §2 auch öfters) Updates und Patches bereitzustellen und bei einem entsprechenden Support-Vertrag diese in Absprache mit dem AG zeitnah zu installieren. Der AN erstellt hierzu für jede im Patchzyklus adressierte Schwachstelle einen detaillierten Bericht und stellt diesen dem AG zu.
3.4 Kündigt ein (Dritt-)Anbieter einer Komponente (Software, Datenbanken, Anwendungen, o.ä.) das Supportende (Lifecycle) an, so informiert der AN den AG zeitnah, spätestens jedoch 6 Monate vor dem „End of Life“.

§ 4 Härtung der Systeme
4.1 Der AN ist verpflichtet, die von ihm gelieferten Systeme zu härten, um potenzieller Sicherheitsrisiken zu minimieren.
Nach den Grundsätzen „security and privacy by design“ werden vom AN nach dem Minimalprinzip nur die Systemkomponenten, Services und Anwendungen installiert, welcher für die vertraglich definierte Funktion erforderlich sind. Dies schließt ein, dass jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) deaktiviert ist. Die Nutzung jedes Zugangs muss in der Dokumentation des AN erläutert werden.
4.2 Der AN gewährleistet, dass die vom AG vorgegebenen Konfigurationsstandards und Sicherheitsvorschriften eingehalten und umgesetzt werden. Dies schließt ein, dass Standardpasswörter vom AG jederzeit geändert werden können und die Komponenten frei von Lösungen sind, welche Sicherheitsmechanismen umgehen, bzw. der AN informiert den AG vollumfänglich und ohne schuldhaftes Zögern über Existenz, Funktion und Verwendung von dem AN bekannten „Backdoors“.

§ 5 Fernzugänge
5.1 Der AN stellt sicher, dass Fernzugänge die Vertraulichkeit, Verfügbarkeit und Integrität der Assets und Services des AG nicht beeinträchtigen. Dies beinhaltet auch die Verwendung von Informationen, von denen der AN während eines Fernzugriffes Kenntnis erlangt.
5.2 Der AG erwartet vom AN, dass prinzipiell jeder Nutzer des AN über ein eigenes Nutzerkonto verfügt. Der AG zeigt Verständnis für etwaige Ausnahmen z.B. Unternehmen mit mehreren Supportcentern und einer großen Anzahl an Personal, die dies erschweren. Solche Ausnahmen müssen vom AN dokumentiert werden. In diesem Fall wird der AN die Rückverfolgbarkeit der Nutzung der Accounts (wer, wann) gewährleisten und dem AG bei Bedarf aushändigen.

§ 6 Anforderung an die (Software-/Hardware) Entwicklung Es wird vom AN erwartet, dass die Entwicklungsprozesse so ausgelegt sind, dass sie sich an anerkannten Industriestandards orientieren. Die Entwickler das AN (inkl. etwaiger Sub-Unternehmer) halten sich an vorhandene Standards zur sicheren Programmierung, um Schwachstellen zu verhindern. Diese Standards des AN müssen dokumentiert vorliegen und den Entwicklern z. B. in Schulungen vermittelt werden. Z.B. müssen die eigenentwickelten Webapplikationen, die für den Betrieb in nicht geschützten Netzen vorgesehen sind, ein Code-Review nach einem Industriestandard wie dem Open Web Application Security Project (OWASP) durchlaufen. Die Testverfahren beim AN müssen Sicherheitsmechanismen (wie Verschlüsselung, Zugriffskontrollen, Authentisierung) beinhalten. Der AN führt regelmäßig Sicherheitsüberprüfungen z. B. unabhängige Penetrationstests für die Systeme, die aus den externen bzw. nicht abgesicherten Netzen erreichbar sind durch. Die Ergebnisse der Secure-Code-Reviews bzw. Penetrationstests werden dem AG bei Bedarf (mindestens für die finale Version der eingesetzten Produkte) zur Verfügung gestellt werden.

§ 7 Kryptografie
Es wird vom AN erwartet, dass er zulässige Kryptographiealgorithmen (nach dem Stand der Technik) definiert und dokumentiert sowie verwendet und regelmäßig überprüft.
Wenn eine Kryptographielösung in der Industrie als nicht mehr sicher bekannt wird, muss der AN zeitnah und angemessen darauf reagieren. Wenn eine solche unsichere Kryptographielösung in dem bereits beim AG eingesetzten Produkt verwendet wird, muss der AN sie im Rahmen des Schwachstellen-Managements bewerten und dem AG melden.
Der AN muss sicherstellen, dass der Einsatz der kryptographischen Absicherung überall erfolgt, wo es notwendig ist, um die Grundsätze einer sicheren Softwarearchitektur (security by design) zu unterstützen. Der Einsatz der kryptographischen Absicherung ist insbesondere

dort notwendig, wo Daten mit hohem Schutzbedarf (z. B. Steuerungsdaten der Kritischen Infrastruktur oder vertrauliche bzw. personenbezogene Daten) über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden müssen.

§ 8 Dokumentation

Es wird vom AN erwartet, dass er eine hinreichende Dokumentation zur Verfügung stellt, welche eine benutzerfreundliche Nutzung der Lösung gewährleistet.
Der Umfang dieser Dokumentation beinhaltet mindestens folgende Punkte: Liste der Hardware, Liste der Software (inklusive Betriebssystem und Patch-Level), Überblick über die Systemarchitektur (kann Teil einer Designdokumentation sein), Kommunikationsmatrix, existierende Benutzerkonten und Rollen sowie deren Berechtigungen.

§ 9 Benachrichtigung bei relevanten Vorfällen

Der AN ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potenziell Auswirkung auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte des AG haben könnten, umgehend dem AG zu melden. Dies könnten auch Spionage, Angriffe oder Sicherheitslücken im Source-Code sein.

§ 10 Organisatorische Sicherheit

10.1 Der AN soll, wenn vorhanden, ein ISO27001-Zertifikat oder Äquivalente bereitstellen, sowie weitere Dokumente wie Berichte und Vorschriften in diesem Kontext.
10.2 Es wird erwartet, dass der AN alle Assets in seinem Informationssystem identifiziert und dokumentiert, welche einen Bezug zum Informationssystem des AG zwecks Wartung oder Betriebszugang haben können. Die Verantwortlichkeiten und Zuständigkeiten beim AN sollten klar geregelt und dokumentiert sein. Die beim AN gespeicherten Daten müssen in dessen Besitz verbleiben (besonders Kundeninformationen), da er für die Daten z.B. im Falle eines Datenverlustes haftet.
10.3 Jeder der im Auftrag des AN agiert und Zugriff auf das Informationssystem des AG haben könnte, muss Informationen zu seiner Identität bereitstellen. Der AN stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die Verantwortung und Haftung übernimmt, sollte dies nicht der Fall sein.
Sollte der AN mit Sub-Unternehmern arbeiten muss der AN diesen identifizieren und sicherstellen, dass dieser die gleichen Anforderungen erfüllt. Der Auftragnehmer beauftragt nur Personen, die über entsprechend ausreichende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung verfüge

§ 11 Anforderungen an den IT-Betrieb

11.1 Es wird vom AN erwartet, dass er ein Informationssicherheitsmanagementsystem (ISMS) nach einem anerkannten Sicherheitsstandard implementiert, betreibt und weiterentwickelt.
11.2 Die zugehörigen Prozesse und Kontrollen zum Zugriffsschutz und zur Berechtigungsvergabe werden implementiert, inkl. dokumentierter Freigabeprozesse für Berechtigungen auf Systemen und Informationen, Prozesse zur zeitnahen Löschung von Zugriffsrechten bei Austritt oder Abteilungswechsel, definierte und angemessene Passwortkomplexität und -gültigkeit, Bildschirmsperren nach Inaktivität.
11.3 Standards zur sicheren Löschung von Daten und Datenträgern werden definiert, um zu vermeiden, dass Daten von Dritten unautorisiert wiederhergestellt oder verwendet werden.
11.4 Security-Awareness-Trainings für die Mitarbeiter werden periodisch durchgeführt. Die Inhalte der Schulungen werden entsprechend den aktuellen Erkenntnissen regelmäßig aktualisiert.
11.5 Der AN trifft ausreichende Vorkehrungen zur physischen Sicherheit und zum Zutrittsschutz. Besonders Maßnahmen zum Schutz gegen Feuer und Wasser, Schutz vor bzw. zur Vermeidung von extremen Temperaturen (Klimaanlage) sowie zur (unterbrechungsfreien) Notstromversorgung. Weiterhin ist der Zutritt zu Bereichen mit Informationen oder Systemen mit Schutzbedarf auf den autorisierten Personenkreis beschränkt, dazu gehören auch die Zutrittsschutzmaßnahmen für Rechenzentren inklusive Überwachung der kritischen Bereiche, Zutrittsprotokoll und Sicherung gegen Einbruch, Sabotage o.ä.
11.6 Netzwerksegmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen sind (z.B. durch Firewalls) voneinander getrennt bzw. segmentiert.
11.7 Authentisierungsinformationen (wie z.B. Passwörter, PINs) sind nur verschlüsselt im Netzwerk zu übertragen.
Aus dem Internet erreichbare administrative Zugänge oder Netzwerkports für den technischen Zugriff müssen angemessen abgesichert (z.B. durch eine 2-Faktor-Authentisierung) oder deaktiviert werden.
11.8 Netzwerkverbindungen, Systemzugriffe und administrative Tätigkeiten sollten zur Nachvollziehbarkeit von Angriffen oder Fehlbedienungen protokolliert werden. Die Aufbewahrungsdauer der Protokolle richtet sich nach geltenden gesetzlichen Anforderungen und den Anforderungen des AG. 11.9 Ein hinreichender Virenschutz (für Server, Workstations sowie andere IT-Komponenten mit Zugriff auf Informationen und Systeme mit Schutzbedarf) muss implementiert und aktuell sein.
11.10 Ein etablierter Datensicherungs- und Wiederherstellungsprozess inkl. regelmäßiger Datenwiederherstellungstests ist gegeben.
11.11 Ein sicherer physischer Transport von Speichermedien (Verschlüsselung, physische Absicherung) ist gewährleistet.
11.12 Ein Change-Prozess ist etabliert, d.h. auch, dass ein Prozess zu regelmäßigen Schwachstellenscans und Behebung von Schwachstellen gegeben ist.
11.13 Wenn drahtlose Netzwerke benutzt werden, sollten diese kryptographisch abgesichert sein.
11.14 Wenn der AN Teile der Leistungserbringung für den AG oder anderer Dienstleistungen, welche für den AG Auswirkungen haben auslagert, müssen die genannten Sicherheitsanforderungen in den Vereinbarungen mit dem jeweiligen Dienstleister berücksichtigt werden. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich Sub-Unternehmer ist gegenüber dem AG bei Bedarf nachzuweisen. Der AN muss den AG im Vorfeld von Entscheidungen über eine Auslagerung von Betriebs- oder Dienstleistungen informieren und bei negativen Auswirkungen für den AG diese mit ihm einvernehmlich regeln.

§ 12 Audit

12.1 Der AN stellt nachweislich sicher, dass seine Produkte und Leistungen allen hier genannten Anforderungen entsprechen.
12.2 Der AN stimmt zu, dass der AG oder ein anderer vom AG beauftragter Dritter die Organisation des AN in Bezug auf Informationssicherheit bzw. Datenschutz auditieren darf. Dies kann mehrmals geschehen. Die Prüfungen werden auf der Grundlage der von dem AN zur Verfügung gestellten Dokumentation bzw. vor Ort beim AN durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden im Vorfeld jeweils einvernehmlich vereinbart. Zusätzlich muss der AN Abweichungen von den vereinbarten Sicherheitsanforderungen dem AG melden.