Anlage 6 - Fragebogen zur IEC 80001-1 (Risikomanagement für medizinische IT-Netzwerke) / Erklärungen zur IT-Sicherheit Dentale Behandlungseinheiten

Zu jedem der untenstehenden Punkte / Fragestellungen / Themen sind auf einem separaten Dokument umfassende Aussagen / Erläuterungen vorzunehmen! Das entsprechende Dokument ist dem Auftraggeber durch den bezuschlagten Bieter / den Auftragnehmer innerhalb von zwei Wochen nach der Erteilung des Zuschlags unaufgefordert zu übersenden (im PDF-Format; Ansprechpartner: medizintechnik.ukd@ukdd.de).

Erklärung des Bieters:

Der Bieter erklärt bzw. verpflichtet sich hiermit, dem Auftraggeber im Rahmen der Umsetzung des Risikomanagements für medizinisch genutzte Netzwerke gemäß IEC 80001-1 in der aktuell gültigen Fassung, nachfolgende Informationen zu seinem Produkt /Gerät /System / Zubehör zur Verfügung zu stellen. Zusätzliche Unterlagen in Bezug auf die unten aufgeführten Fragen/Themen sind bitte ebenso beizulegen.

Der Bieter erklärt außerdem, dass das angebotene Produkt /Gerät / System / Zubehör den jeweils dafür aktuell gültigen gesetzlichen Anforderungen und Normen entspricht.

Des Weiteren erklärt der Bieter, dass das angebotene Produkt / Gerät / System so konstruiert / hergestellt ist, dass hinsichtlich der Informationssicherheit bestehende Risiken so weit wie möglich reduziert sind (Security by Design) und der Bieter / Hersteller ein diesbezügliches Risikomanagement durchführt. Der Bieter erklärt zudem, dass er bei der Entwicklung und bei der Produktion den Stand der Technik im Hinblick auf die Informationssicherheit seiner Produkte berücksichtigt / umgesetzt hat.

Er wird den Auftraggeber unverzüglich darauf hinweisen, wenn Risiken entstehen / bekannt werden, welche die IT-Sicherheit / Informationssicherheit nicht unerheblich gefährden / beeinträchtigen.

Ort, Datum	.....
vollständige Bezeichnung des Bieters	.....
Rechtsform des Bieters	.....
Anschrift des Bieters	.....
Name der erklärenden Mitarbeiter*in; der Vertreter*in des Unternehmens	.....

Fragen / Themen:

1. Welche Anforderungen bestehen hinsichtlich der Einbindung des Medizinproduktes / des Systems in ein Netzwerk?

   (Insbesondere: Was wird für die Einbindung benötigt? Welche Netzwerk-Schnittstellen und Standard-Protokolle werden verwendet?)

2. Welchen Zweck erfüllt die Netzwerkanbindung des Medizinproduktes / des Systems?

3. Welche Anforderungen bestehen hinsichtlich der Leistungsmerkmale des Netzwerkes sowie der Konfiguration des Netzwerkes und der weiteren Netzwerkumgebung?

4. Erläuterung / Darstellung zum Update- und Patch-Management

   (Insbesondere zu beantwortende Fragen: Welche Berechtigungen / Zuständigkeiten bestehen bzw. wer darf / macht was zu welchem Zeitpunkt?; Erfolgt die Implementierung / Installation von Updates und Patchs im Wege des Fernzugriffs / Remote?; Wie erfolgt die diesbezügliche Dokumentation?; Wenn notwendig ist hier die Betriebssoftware des Bedien-PCs (Windows-Rechner) und die Anwendungssoftware separat zu betrachten.)

5. Dürfen neben den für die Anwendung / Nutzung des Medizinproduktes / Systems benötigten Programmen noch weitere Programme auf dem Bedien-PC (Windows-Rechner) laufen (z. Bsp. Antivirus-Programm, Softwareverteilungsprogramm Baramundi)?

6. Welche Sicherheitsvorkehrungen werden im Hinblick auf IT-Gefährdungen des Medizinproduktes / Systems durch den Bieter / Auftragnehmer getroffen?

   (z.B. Virenscanner, Whitelist; Die in diesem Zusammenhang bestehenden Verantwortlichkeiten sind darzustellen.)

7. Bitte beschreiben Sie in geeigneter Weise (z.B. mit Hilfe einer grafischen Darstellung) den Daten- und Informationsfluss des Medizinproduktes / des Systems mit dem Netzwerk und anderen angebundenen Systemen (z.B. PACS, KIS ORBIS).

8. Bitte führen Sie konkret aus / stellen Sie umfassend dar, welche Gefährdungssituationen daraus resultieren (können), wenn ein IT-Netzwerk nicht die Eigenschaften / Leistungsmerkmale besitzt, die erforderlich sind, um den Zweck der Einbindung des Medizinproduktes in das IT-Netzwerk zu erfüllen.

   (bspw. Hackerangriffe, Netzwerkausfälle, keine oder nur teilweise Übertragung von Daten aus (Planungs-)Software auf das angewendete Medizinprodukt; Die Auswirkungen von Gefährdungssituationen auf die Patient*innensicherheit ist darzustellen.)