Inhaltsverzeichnis

1. Informationen zu dieser Dienstanweisung 1

2. Sicherheitsanforderungen.....2

3. Umsetzungshinweise zu den Anforderungen 3

4. Anhang 5

1. Informationen zu dieser Dienstanweisung

1.1 Ziel und Zweck

Diese Dienstanweisung definiert verbindliche Vorgaben für die **Nutzung** von Systemen mit künstlicher Intelligenz (KI-Systeme[1]) unter Berücksichtigung der Zweckbindung sowie dem Schutzbedarf. Weitere Regelungen zur Planung, Beschaffung und Betrieb werden später bei Bedarf erstellt.

1.2 Geltungsbereich

Diese zentrale Dienstanweisung gilt für alle Beschäftigten des UKT und der MFT, die KI-Dienste in den bereitgestellten Netzen nutzen oder Aufgaben im Kontext der Patientenversorgung wahrnehmen. Ausgenommen von der Dienstanweisung ist das Forschungsnetz (Netz der Universität).

1.3 Gültigkeit

Die fachliche Freigabe der Dienstanweisung erfolgt durch das ISecBoard. Die disziplinarische Freigabe erfolgt durch den Vorstand des Klinikums und das Dekanat der Medizinischen Fakultät.
Sie wird unmittelbar nach der Beschlussfassung gültig und bleibt es bis zur Freigabe der nachfolgenden Version.

1.4 Referenzen

Im Folgenden werden die Referenzen für die normativen Anforderungen gelistet. Informelle Referenzen werden in Kapitel 4.3 gelistet.

[1] DIN e.V., „DIN ISO/IEC 27001 - Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen“, 2015

[2] ISO/IEC, „ISO/IEC 27017 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services“, 2015

[3] Bundesamt für Sicherheit in der Informationstechnik, „Konkretisierung der Anforderungen an die gemäß §8a Absatz 1 BSIG umzusetzenden Maßnahmen“, Version 1.0, 2020

[4] Uniklinikum Tübingen, „Prüfgrundlage §8a BSIG, Sektor ‚Gesundheit‘ für das Uniklinikum Tübingen“, 2021

[5] Bundesamt für Sicherheit in der Informationstechnik, „Cloud Computing Compliance Criteria Catalogue – C5:2020“, 2020

[1] Definition siehe: 4.1.1 **künstliche Intelligenz**

2. Sicherheitsanforderungen

Die in diesem Kapitel formulierten Anforderungen sind normative Anforderungen im Sinne eines ISMS nach ISO 27001 (siehe [1]). Abweichungen von diesen Anforderungen sind zu begründen und in das Risikomanagement aufzunehmen.
Bei der Formulierung der Anforderungen wird auf die folgenden Modalverben, deren Interpretation dem BSI IT-Grundschutz-Kompendium (siehe [6]) entnommen ist, zurückgegriffen.

Modalverb	Interpretation
MUSS / DARF NUR	Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss.
DARF NICHT / DARF KEIN	Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf.
SOLLTE	Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss sorgfältig abgewogen und stichhaltig begründet werden.
SOLLTE NICHT / SOLLTE KEIN	Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.
KANN	Hier handelt es sich um eine Empfehlung, deren Umsetzung nicht verpflichtend ist.

Die nachfolgenden Anforderungen werden in den Umsetzungshinweisen in Kapitel 3 detailliert beschrieben und sind von den technischen Fachabteilungen nachvollziehbar zu berücksichtigen.

KI.1 Regelungen für die Nutzung von KI-Diensten		
KI.1.1	Verarbeitbare Informationen in öffentlichen KI-Diensten[2]	*Anforderung* In öffentlichen KI-Diensten **DÜRFEN NUR** Informationen der Informationsklassen „öffentlich“ und „Intern“ verarbeitet werden. Personenbezogene Daten, besondere Kategorien personenbezogener Daten, pseudonymisierte Personendaten oder Geschäftsgeheimnisse **DÜRFEN NICHT** in öffentlichen KI-Diensten verarbeitet werden.
KI.1.2	Verarbeitbare Informationen in KI-Diensten des UK Tübingen[3]	*Anforderung* Bei KI-Diensten des UK Tübingen **MÜSSEN** bei dessen Einführung, die zu verarbeitenden Informationsklassen in Abhängigkeit des Schutzbedarfs festgelegt und den zukünftigen Nutzenden mitgeteilt werden.
KI.1.3	Qualitätssicherung der Ergebnisse	*Anforderung* Die aus einem KI-Dienst produzierten Inhalte **MÜSSEN** qualitätsgesichert werden. Bei Herausgabe der Informationen an Dritte MUSS der Ersteller den Inhalt verantworten.
KI.1.4	Compliance und Datenschutz	*Anforderung* Bei einer Nutzung von KI-Diensten **MÜSSEN** die rechtlichen Risiken hinsichtlich eines Verstoßes gegen Geschäftsgeheimnisse, Geheim-

[2] Definition siehe: 4.1.2 **Öffentliche KI-Systeme**

[3] Definition siehe: 4.1.3 **KI-Dienst des UK Tübingen**

		haltungsverbote, Urheberrechte und das Thema Haftung für inkorrekte Informationen vom Nutzenden vor der Weitergabe an Dritte abgeklärt werden.
KI.1.5	Vorgehen bei Nutzung von Hochrisiko-KI-Systemen	*Anforderung* Bei der Planung eines Hochrisiko-KI-Systems **MUSS** vom Fachbereich mindestens der Datenschutz, die Compliance und die Informationssicherheit eingebunden werden. Es **MUSS** eine Risikobeurteilungen erstellt und bewertet werden.
KI.1.6	KI-Systemen mit „Unannehmbaren Risiken“	*Anforderung* KI-Systeme mit „Unannehmbaren Risiken“ DÜRFEN NICHT am UK Tübingen eingesetzt werden.

3. Umsetzungshinweise zu den Anforderungen

Dieses Kapitel enthält Informationen und Hinweise zur Umsetzung der normativen Anforderungen aus Kapitel 0.

KI.1. Regelungen für die Nutzung von KI-Diensten

KI.1.1 Verarbeitbare Informationen in öffentlichen KI-Diensten

Öffentlich zugängliche KI-Dienste lernen u.a. durch die Eingabe der Nutzenden und speichern diese Daten nach einem nicht öffentlich zu verifizierendem Algorithmus in Ihrem Modell ab. In öffentlichen KI-Diensten dürfen nur Daten der Informationsklassen „öffentlich“ und „Intern“ verarbeitet werden.
Personenbezogene Daten und besondere Kategorien personenbezogener Daten (z.B. Gesundheitsdaten, genetische Daten, biometrische Daten, rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Daten zum Sexualleben oder der sexuellen Orientierung, Patientendaten) dürfen nicht verwendet werden. Hierzu zählen auch pseudonymisierte Daten. Ebenso dürfen keine vertraulichen oder streng vertraulichen Daten und Geschäftsgeheimnisse verwendet werden (z.B. Finanzdaten, Besprechungsprotokolle o.ä.).

KI.1.2 Verarbeitbare Informationen in KI-Diensten des UK Tübingen

KI-Dienste vom UK Tübingen sind durch einen Prozess für das UK Tübingen beschafft und eingeführt worden. Während der Beschaffung wurden Prüfungen vorgenommen. Bei der Implementierung sind die Regelungen zum Umgang mit diesem spezifischen KI-Dienst zu erstellen und anzuwenden.
Bei den KI-Systemen kann es sich um Dienste handeln, welche im Haus oder Extern betrieben werden.

KI.1.3 Qualitätssicherung der Ergebnisse

Nicht alle Ergebnisse eines KI-Dienstes sind korrekt und sofort weiterzuverwenden. Die aus einem KI-Dienst produzierten Inhalte müssen daher inhaltlich und fachlich qualitätsgesichert werden. Werden diese Inhalte an Dritte weitergegeben, so ist der Ersteller für den Inhalt verantwortlich.
KI-Systeme können selbstständig keine Diagnosen, Befunde und Therapievorschläge erstellen. Die Ergebnisse einer KI können nur unterstützend verwendet werden.

KI.1.4 Compliance und Datenschutz

Compliance Risiken sind zu beachten. Bei einer Nutzung von KI-Diensten müssen die rechtlichen Risiken hinsichtlich eines Verstoßes gegen Geschäftsgeheimnisse, Geheimhaltungsverbote, Urheberrechte und das Thema Haftung für inkorrekte Informationen abgeklärt werden. So könnten Inhaltsvorschläge oder Teile von Bildern oder Musik durchaus Urheberrechten unterliegen. Die Rechtsprechung ist hier noch nicht so weit, dass es Präzedenzfälle gibt. Als Unternehmensrisiko ist dies zu beachten. Datenschutzaspekte sind zu beachten und sind in den Regelungen KI.1.1 und KI.1.2 verankert.

KI.1.5 Vorgehen bei Nutzung von Hochrisiko-KI-Systemen[4]

KI-Systeme, die ein hohes Risiko für die Gesundheit und Sicherheit darstellen, gelten als hochriskant. Hierunter fallen KI-Systeme, die in medizinischen Geräten und Systemen verwendet werden und die in der Verwaltung und dem Betrieb von kritischen Infrastrukturen essentiell sind.
Für den Einsatz solcher KI-Systeme, sind neben der fachlichen Prüfung durch den Fachbereich zwingend vom Fachbereich die Bereiche Datenschutz, Compliance und Informationssicherheit einzubeziehen um eine Risikobewertung vorzunehmen.

KI.1.6 KI-Systemen mit „Unannehmbaren Risiken“[5]

KI-Systeme stellen ein unannehmbares Risiko dar, wenn sie als Bedrohung für Menschen gelten. Diese KI-Systeme sind nach EU Auffassung verboten. Im Kontext des UK Tübingen könnten dies Systeme sein, die eine biometrische Identifizierung und Kategorisierung natürlicher Personen ermöglicht, biometrischen Echtzeit-Fernidentifizierungssystemen (u.a. Gesichtserkennung) oder ein soziales Scoring ermöglichen. Diese Systeme sind am UK Tübingen nicht zugelassen.

[4] Quelle des Textes: Europäisches Parlament – KI-Gesetz [7]

[5] Quelle des Textes: Europäisches Parlament – KI-Gesetz [7]

4. Anhang

4.1 Terminologie

4.1.1 künstliche Intelligenz

„Künstliche Intelligenz ist die Eigenschaft eines IT-Systems, »menschenähnliche«, intelligente Verhaltensweisen zu zeigen.“ (Quelle: Bitkom e. V. und Deutsches Forschungszentrum für künstliche Intelligenz)
Dies umfasst das Lernen, Schlussfolgern, Problemlösen und das Verstehen natürlicher Sprache.
Ausgaben sind u.a. Texte, Bild-, Audio- oder Videoinhalte.

4.1.2 Öffentliche KI-Systeme

Ein öffentlicher KI-Dienst ist ein frei zugänglicher Dienst, der durch das UK Tübingen **NICHT** freigegeben ist und dessen NutzerID‘s **NICHT** durch das UK Tübingen verwaltet sind.

4.1.3 KI-Dienst des UK Tübingen

Ein KI-Dienst des UK Tübingen ist ein Dienst, der vom UK Tübingen **geprüft und freigegeben** wurde und dessen **NutzerID’s durch das UK Tübingen verwaltet** sind.

4.2 Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz (Gesetz über das BSI)
DIN	Deutsche Institut für Normung
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DSGVO	EU-Datenschutz-Grundverordnung
EU	Europäische Union
GB IT	Geschäftsbereich IT
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Informationstechnik

4.3 Weiterführende Literatur

Die folgenden informellen Referenzen sind als weiterführende Informationen zum Verständnis der Ausführungen in dieser Dienstanweisung hilfreich.

[6] Wikipedia “künstliche Intelligenz“
https://de.wikipedia.org/wiki/K%C3%BCnstliche_Intelligenz

[7] Europäisches Parlament – künstliche Intelligenz – KI Gesetz
https://www.europarl.europa.eu/topics/de/topic/artificial-intelligence

4.4 Zuordnung der Anforderungen zu den Maßnahmenzielen der ISO 27001

Die folgende Tabelle enthält eine Zuordnung der in Kapitel 0 formulierten Anforderungen zu den Maßnahmenzielen aus dem Anhang A der Norm ISO 27001 (siehe [1]). Maßnahmenziele, die in der vorliegenden Dienstanweisung nicht adressiert werden, werden in der folgenden Tabelle nicht aufgeführt.

Maßnahmenziele gemäß ISO 27001	**Anforderungen aus Kapitel 0**
A.8.1.3 Zulässiger Gebrauch von Werten	KI.1.1 Verarbeitbare Informationen in öffentlichen KI-Diensten KI.1.2 Verarbeitbare Informationen in KI-Diensten des UK Tübingen KI.1.3 Qualitätssicherung der Ergebnisse
A.18.1.2 Geistige Eigentumsrechte	KI.1.4 Compliance und Datenschutz

4.5 Zuordnung der Anforderungen zur Prüfgrundlage §8a BSIG

Die folgende Tabelle enthält eine Zuordnung der in Kapitel 0 formulierten Anforderungen zu den Anforderungen an die Prüfgrundlage §8a BSIG (siehe [4]). Anforderungen aus [4], die in der vorliegenden Dienstanweisung nicht adressiert werden, werden in der folgenden Tabelle nicht aufgeführt.

Anforderungen gemäß [4]	**Anforderungen aus Kapitel 0**
Anf.01.026.RL	KI.1.1 Verarbeitbare Informationen in öffentlichen KI-Diensten KI.1.2 Verarbeitbare Informationen in KI-Diensten des UK Tübingen KI.1.3 Qualitätssicherung der Ergebnisse

4.6 Zuordnung der Anforderungen zu den Anforderungen der Konkretisierung des BSIG §8a des BSI

Die folgende Tabelle enthält eine Zuordnung der in Kapitel 0 formulierten Anforderungen zu den Anforderungen der Konkretisierung des BSIG §8a des BSI (siehe [3]).Die in [3] formulierten Anforderungen basieren auf einer älteren Version des Anforderungskatalogs für das Cloud-Computing des BSI (siehe [5]). In der folgenden Tabelle werden die entsprechenden Kriterien aus der aktuellen Version des Anforderungskatalogs für das Cloud Computing des BSI (siehe [5]) mit aufgeführt. Anforderungen aus [3], die in der vorliegenden Dienstanweisung nicht adressiert werden, werden in der folgenden Tabelle nicht aufgeführt.

Anforderungen gemäß [3]	**Basiskriterien gemäß [5]**	**Anforderungen aus Kapitel 2**
AM-03 AM-06		KI.1.1 Verarbeitbare Informationen in öffentlichen KI-Diensten KI.1.2 Verarbeitbare Informationen in KI-Diensten des UK Tübingen KI.1.3 Qualitätssicherung der Ergebnisse