1 Präambel

Dieses Dokument ist eine **„Vorgabe“** des Universitätsklinikums Heidelberg (im Folgenden „UK“).
Vorgaben der Informationssicherheit beschreiben allgemeine Anforderungen (MUSS, SOLL, KANN), die von allgemeinen Verfahren unabhängige Sicherheitsthemen des UK betreffen.
Anforderungen sind in den unterschiedlichen Einheiten des UK durch deren Fachpersonal bei deren spezifischen Abläufen, Verfahren und Verfahrensanweisungen zu berücksichtigen und umzusetzen.

Dieses Dokument bezieht sich ausschließlich auf die **Ziele und Belange der Informationssicherheit** am UK, andere Bereiche bzw. Aspekte werden nicht betrachtet.

2 Gegenstand

Dieses Dokument zur Personalsicherheit legt Vorgaben fest, die sich vor, während und nach einer Anstellung / Beschäftigung von Personen am UK aus Sicht der Informationssicherheit ergeben.
Die Vorgaben gelten für alle UK Beschäftigten und für das UK tätigen Personen (Dienstleister) sowie Geräte, sofern diese Personen / Geräte Informationen bzw. Daten des UK verarbeiten.
Die Vorgaben sind nur in Bereichen der medizinischen Versorgung im UK, deren direkt unterstützenden Systeme, Komponenten oder Prozesse sowie des „medizinischen IT-Netzwerks“ (gemäß DIN EN 80001-1) am UK zwingend anzuwenden.

3 Begriffe, Definitionen und Abkürzungen:

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der verschiedenen Geschlechter in der Sprachform verzichtet. Sämtliche Personenbezeichnungen gelten gleichwertig für alle Geschlechter.

Bei den Vorgabentypen wird (in Anlehnung an RFC 2119) unterschieden zwischen:

MUSS-Vorgaben	Diese Vorgaben sind zwingend einzuhalten.
SOLL-Vorgaben	Sind ebenso verbindlich wie Muss-Vorgaben, solange nicht besondere Umstände ausnahmsweise ein Abweichen von der Vorgabe erzwingen / erfordern (= intendiertes Ermessen). Diese Abweichung ist nachweislich und schriftlich zu begründen. Damit weist der Betreiber nach, dass er sich über die Konsequenzen seines abweichenden Verfahrens im Klaren ist.
KANN-Vorgaben	Diese Vorgaben sind Empfehlungen (= freies Ermessen).

Beschreibungen der wichtigsten im Dokument verwendeten Begriffe:

Begriffe	Beschreibungen
Lieferant	Lieferant im Sinne der Informationssicherheit ist eine juristische oder natürliche Person (ausgenommen Subunternehmen und Subdienstleister), die einem Empfänger (Kunden) Waren und/oder Dienstleistungen auf vertraglicher Basis bereitstellt oder überlässt.
Maßnahme	Negative Abweichung eines Objekts oder dessen Eigenschaften von der Vorgabe bzw. von der erwarteten Qualität.
Stand der Technik	Gängiger allgemein formulierter juristischer Begriff. Stark gekürzte Fassung: Fortschrittliche erfolgversprechende Verfahren, Systeme und Betriebsweisen, die sich in der Praxis bewährt haben oder im Betrieb erfolgreich erprobt wurden (d.h. "die besten verfügbaren Techniken").

4 Ziele

Ziel dieser Vorgabe ist die Aufrechterhaltung der Informationssicherheit im Bereich / Themengebiet der Personalsicherheit durch die Ergreifung angemessener Schutzmaßnahmen, die dem Stand der Technik und Best Practice für Krankenhäuser entsprechen.
Diese Vorgabe soll sicherstellen, dass Beschäftigte des UK und am UK eingesetzte Beschäftigte von Auftragnehmern bzw. Externe ihre Verantwortlichkeiten im Bereich / Themengebiet der Personalsicherheit kennen und sensibilisiert für die Informationssicherheit im UK sind.

5 Vorgaben zur Personalsicherheit

5.1 Überprüfungen (i.d.R. vor Beschäftigungsbeginn)

(1) Alle Mitarbeiter MÜSSEN im Einvernehmen mit einschlägigen Gesetzen, Verordnungen und ethischen Grundsätzen im erforderlichen Umfang (mindestens Authentizität) überprüft werden.
(2) Die Überprüfung SOLL direkt vor der Einstellung sowie regelmäßig während der Beschäftigungszeit erfolgen.
(3) Die Personalabteilung SOLL festlegen, welche Überprüfung für Personen bzgl. der zu besetzenden Stelle / Tätigkeit / Funktion erforderlich ist und welche Verpflichtungen notwendig sind. Die Überprüfung SOLL den Abgleich mit „Terror- und Sanktionslisten“ umfassen. Bei Bedarf KÖNNEN aus Sicht der Informationssicherheit weitere besondere Prüfungen bzw. Verpflichtungen gefordert werden.
(4) Die Personalabteilung SOLL festlegen in welchem Turnus / Zyklus die Überprüfung (auch teilweise) wiederholt wird.
(5) Prüfungen von Personen SOLLEN in einem angemessenen Verhältnis zu den Geschäftsanforderungen des UK, der Bedeutung der Tätigkeiten für das UK und zum möglichen Risiko für das UK durch die Informationsverarbeitung stehen.
(6) Die Personalabteilung KANN unterschiedliche Sicherheitsklassen für zu besetzende Stellen / Tätigkeiten / Funktionen festlegen und beschreiben welche Prüfungen bzw. Verpflichtungen bei welchen Sicherheitsklassen notwendig sind. Diese KÖNNEN bei Bedarf um weitere besondere Prüfungen bzw. Verpflichtungen aus Sicht der Informationssicherheit ergänzt werden.
(7) Für eingesetzte Externe oder Beschäftigte von beauftragten Dienstleistern MÜSSEN die **„Vorgaben Lieferantensicherheit“** angewendet werden und Personen entsprechend überprüft werden.

5.2 Verpflichtung von Beschäftigten und Dienstleistern

(1) Sämtliche Personen, die im oder für das UK tätig sind, MÜSSEN schriftlich über ihre Rechte, Pflichten, Verantwortlichkeiten, Zuständigkeiten, zu erfüllenden Tätigkeiten und der organisatorischen Anforderungen im Bereich / Themengebiet der Informationssicherheit am UK auf geeignete Weise und im erforderlichen Umfang informiert werden und die Einhaltung, Erfüllung der Informationssicherheit durch Unterschrift bestätigen.

(2) Mit sämtlichen Personen, die im oder für das UK tätig sind, MÜSSEN schriftliche Geheimhaltungs- oder Vertraulichkeitserklärungen auf Basis der Anforderungen der Informationssicherheit und im Hinblick auf den Schutz sensibler Daten und betrieblicher Details geschlossen sein. Die Anforderungen der Informationssicherheit SOLLEN jährlich überprüft werden und bei Änderungen SOLLEN mit internen und externen Personen neue angepasste Vereinbarungen / Erklärungen getroffen werden.

(3) Geheimhaltungs- oder Vertraulichkeitserklärungen mit sämtlichen Personen, die im oder für das UK tätig sind, MÜSSEN so formuliert sein, dass diese auch über das Dienst- bzw.- Beschäftigungsverhältnis hinaus zeitlich wirksam sind.

(4) Sämtliche Personen, die im oder für das UK tätig sind, MÜSSEN vor Aufgabenwahrnehmung / Tätigkeitsbeginn oder bei einem Arbeitsplatzwechsel noch vor Aufnahme ihrer neuen Tätigkeiten und in Abhängigkeit zu ihrer Stellenbeschreibung / Tätigkeitserbringung auf folgende Punkte im Bereich / Themengebiet der Informationssicherheit nachweisbar verpflichtet werden:
   - Kenntnis und Einhaltung der Informationssicherheit (beinhaltet die „Grundsätze zur Informationssicherheit“, die „Regelwerk der Informationssicherheit“)
   - die Wahrung von Betriebs- und Geschäftsgeheimnissen (auch „Verschwiegenheitserklärung“)
   - bei Ärzten der Wahrung von gesetzlichen / ärztlichen Schweigepflichten

(5) Sämtliche Personen, die im oder für das UK tätig sind, MÜSSEN darauf hingewiesen werden, dass im Bereich / Themengebiet der Informationssicherheit zur Überprüfung der Einhaltung von Schutzmaßnahmen, Regelungen, Verpflichtungen, etc. Kontrollen und Stichproben im Einklang mit den gesetzlichen Bestimmungen und den Regelungen am UK durchgeführt werden.

5.3 Verantwortung des Managements

(1) Die Führungs- / Leitungspositionen und disziplinarisch Verantwortliche SOLLEN verantwortlich in ihrem Bereich die Schutzmaßnahmen im Bereich / Themengebiet der Informationssicherheit entsprechend den festgelegten Leitlinien und Verfahren der UK-Organisation motiviert anwenden und in ihrem Bereich tätige Personen dazu anweisen.

(2) Damit Personen im Unternehmen anonym über Verletzungen von Regelungen zur Informationssicherheit Bericht erstatten können, SOLL von der Leitung des UK eine Möglichkeit eingerichtet, und eine Vertrauensperson (z.B. Ombudsperson) zur anonymen Meldung benannt werden.

5.4 Verantwortung der Mitarbeitenden und Dritte

(1) Mitarbeitende sowie Dritte, welche zu schützenden Informationen des UK im Hoheitsbereich des UK verarbeiten, SOLLEN verantwortlich die Schutzmaßnahmen im Bereich / Themengebiet der Informationssicherheit entsprechend den festgelegten Leitlinien und Verfahren der UK-Organisation motiviert anwenden.

(2) Mitarbeitende sowie Dritte, welche für das UK tätig sind, SOLLEN bei relevanten Verstößen bzw. relevanten Informationssicherheitsvorfällen tätig werden, indem sie die Auswirkungen von Verstößen oder Vorfällen mitigieren, andere Personen zur Mitigation der Auswirkungen auffordern oder Verstöße / Vorfälle melden.

5.5 Aus- / Weiterbildung und Sensibilisierung

(1) Sämtliche Personen, die im oder für das UK tätig sind, SOLLEN regelmäßig Informationen zur Informationssicherheit über Maßnahmen, Verfahrensanweisungen, Richtlinien und Anforderungen zur Informationssicherheit erhalten, die für ihre dienstliche Funktion / Tätigkeiten maßgeblich sind und aufgefordert werden sich regelmäßig selbst dazu zu informieren.

(2) Es SOLL hierzu ein regelmäßig aktualisiertes Sensibilisierungs- / Awarenessprogramm zur Informationssicherheit erstellt werden. Dieses ist sämtlichen Personen, die im oder für das UK tätig sind, barrierefrei zugänglich. Es SOLL die aktuelle Informationssicherheitslage und den Schutzbedarf der Informationen des UK berücksichtigen.
(3) Sämtliche Personen, die im oder für das UK tätig sind, MÜSSEN die für ihre dienstliche Funktion / Tätigkeiten erforderlichen informationssicherheitsrelevanten Fähigkeiten und Kompetenzen besitzen. Aus- und Weiterbildungsbedarfe MÜSSEN durch die Vorgesetzten erkannt bzw. durch die Mitarbeiter an die Vorgesetzten kommuniziert werden. Diese MÜSSEN geeignete Maßnahmen einleiten, um die erforderlichen Fähigkeiten und Kompetenzen aufzubauen und zu erhalten.
(4) Am UK neu tätige Personen SOLLEN innerhalb der ersten drei Monate zu Themen der Informationssicherheit geschult werden.
(5) Die Leitung des UK und die Führungskräfte SOLLEN die am UK tätigen Personen unterstützen bedarfsgerechte Informationen und eine bedarfsgerechte Fort- und Weiterbildung zu erhalten. Die Leitung des UK und die Führungskräfte sind dafür mitverantwortlich.
(6) Die geplanten und wahrgenommenen Teilnahmen an Aus- und Weiterbildungsmaßnahmen zur Informationssicherheit SOLLEN durch geeignete Nachweise dokumentiert, nachgehalten und überprüft werden.

5.6 Beendigung oder Änderung des Beschäftigungsverhältnisses

(1) Beim Ausscheiden oder bei Tätigkeitswechsel MÜSSEN sämtliche am oder für das UK beschäftigten Personen alle nicht mehr von ihnen benötigte Dokumente (in elektronischer und nicht-elektronischer Form), Informationen, Zutrittsmittel, zur Informationsverarbeitung geeignete Leihgaben, IT- und Kommunikationsgeräte (im Allgemeinen – Gebrauchsgüter) an das UK übergeben. Verbrauchsgüter KANN das UK zurückfordern.
(2) Für Personen, die in andere Bereiche des UK wechseln, das Beschäftigungsverhältnis beenden oder im Rahmen einer anderen vertraglichen Beziehung weiterhin im UK tätig sind, SOLLEN mindestens die jeweils aktuellen informationssicherheitsrelevanten Pflichten eingehalten werden.
(3) Bei Personen, die ihre Tätigkeit am oder innerhalb des UK wechseln, MÜSSEN vor dem Wechsel in den neuen Tätigkeitbereich die hierzu erforderlichen Prüfungen vorgenommen werden.
(4) Wechselnde oder ausscheidende Personen SOLLEN – falls erforderlich – in dokumentierter Weise von ihren bisherigen Verantwortlichkeiten und Pflichten, die nicht weiter gelten sollen, entbunden werden.

5.7 Sanktionierung bei Verstößen

(1) Ein offizielles, festgelegtes Verfahren, um disziplinarische oder rechtliche Maßnahmen gegen im oder für das UK tätige Personen einzuleiten, die gegen die Informationssicherheit schuldhaft verstoßen haben, MUSS vorhanden sein. Art und Umfang des Verfahrens und der disziplinarischen oder rechtlichen Maßnahmen erfolgt durch das Personalmanagement bzw. der Personalabteilung.

6 Weiterführende Unterlagen / Dokumente

- Vorgaben für Lieferantensicherheit
- ISO 27001:2013
  - Kapitel 7 "Unterstützung": 7.2 "Kompetenzen" und 7.3 "Bewusstsein"
  - Anhang A. 7 "Personalsicherheit"
  - Anhang A. 13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
  - Anhang A. 18.1.2 Rechte an geistigem Eigentum