KlinikumDarmstadt GmbH Akademisches Lehrkrankenhaus	*Richtlinie* **Sicherheitsrichtlinie für Dienstleister und Lieferanten**	**Informationssicherheit**

Inhalt

A. Zweck

Der Zweck dieses Dokuments ist die Festlegung der Vorschriften für Beziehungen zu Lieferanten, Dienstleistern und Partnern (im Folgenden Lieferanten genannt).

In diesem Dokument werden die Festlegungen zum Informationssicherheitsmanagementsystem (ISMS) so zusammengefasst, dass Lieferanten ein Grundverständnis für die Sicherheitsanforderungen und Verfahren der Klinikum Darmstadt GmbH (im Folgenden KDA genannt) entwickeln können. Die KDA orientiert sich an der ISO 27001-Norm, mit dem Ziel, die geltenden Sicherheitsanforderungen entlang der gesamten Liefer- und/ oder Unterstützungskette für die KDA aufrecht zu erhalten. Die Lieferanten der KDA sind angehalten, sich konform zu der Informationssicherheitsleitlinie der KDA und den Anforderungen dieser Richtlinie und allen daraus abgeleiteten Sicherheitsanweisungen zu verhalten.

B. Geltungsbereich

Dieses Dokument gilt für alle Mitarbeitenden, Dienstleister und Lieferanten, welche im und für den Anwendungsbereich des ISMS der Klinikum Darmstadt GmbH tätig sind.

C. Begriffe und Abkürzungen

DSGVO	Datenschutz-Grundverordnung
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
KDA	Klinikum Darmstadt GmbH
MiLoG	Mindestlohngesetz
S/MIME	Secure / Multipurpose Internet Mail Extensions
StGB	Strafgesetzbuch
TLS	Transport Layer Security

D. Verantwortlichkeit Informationssicherheit

Die Geschäftsführung der KDA hat einen Informationssicherheitsbeauftragten (ISB) ernannt. Dieser ist für die Belange der Informationssicherheit innerhalb der KDA zuständig.
Der Lieferant ist für alle Belange der Informationssicherheit verantwortlich, die sich auf seine Geschäftsbeziehung mit der KDA auswirken bzw. direkten Einfluss haben. Der Ansprechpartner innerhalb der KDA wird dem Lieferanten im Rahmen der Vertragsbeziehung genannt und steht als Ansprechpartner für Fragen zum ISMS zur Verfügung.

Lieferanten der KDA sind angehalten, sich konform zu der Informationssicherheitsleitlinie der KDA und den Anforderungen dieser Richtlinie und allen daraus abgeleiteten Sicherheitsanweisungen zu halten.

E. Grundsätzliche Anforderungen an Lieferanten

1. Der Lieferant oder Dienstleister der KDA verpflichtet sich bei Ausführung seines Auftrages zur Einhaltung aller einschlägigen Vorschriften, Normen, Verordnungen und Gesetze sowie der allgemein anerkannten Regeln der Technik. Er sichert zu, auch seine Subunternehmer sowie von diesen eingesetzte weitere Auftragnehmer entsprechend zu verpflichten.
2. Der Lieferant ist insbesondere zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet. Er hat seine Mitarbeiter und von ihm beauftragte Subunternehmer auf die gesetzlichen Vorschriften zum Datenschutz hinzuweisen und zu verpflichten.
   Im Falle einer Verarbeitung mit personenbezogenen Daten ist ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO durch die Abteilungen, die selbständig Bestellungen tätigen, abzuschließen. Im Rahmen dieser Auftragsverarbeitung sind außerdem gesonderte Vereinbarungen zur Einhaltung der technischen und organisatorischen Maßnahmen nach Art.32 DSGVO zu treffen.
   Zur Wahrung der ärztlichen Schweigepflicht sind Unternehmen als Dienstleister im Vertrag zur Auftragsverarbeitung, Einzelpersonen in einer gesonderten Verpflichtungserklärung seitens der Abteilungen, die selbständig Bestellungen vornehmen, nach § 203 StGB zu verpflichten.
3. Der Lieferant oder Dienstleister verpflichtet sich bei Ausführung seines Auftrages, alle ihm aus dem Mindestlohngesetz (MiLoG) obliegenden Pflichten zu erfüllen. Der Auftragnehmer verpflichtet sich

insbesondere, den Mindestlohn an alle von ihm im Inland beschäftigten Arbeitnehmerinnen und Arbeitnehmer rechtzeitig im Sinne des MiLoG zu zahlen und die Arbeitszeiten gemäß den gesetzlichen Bestimmungen zu dokumentieren. Soweit in dem Bundesland, in dem die Leistung erbracht wird, ein länderspezifisches Mindestentgelt nach Tariftreue- oder Vergabegesetz geregelt ist, verpflichtet sich der Lieferant oder Dienstleister zur Zahlung dieses Mindestentgelts an alle von ihm im Inland beschäftigten Arbeitnehmerinnen und Arbeitnehmer. Er sichert zu, auch seine Subunternehmer sowie von diesen eingesetzte weitere Auftragnehmer entsprechend zu verpflichten.

4. Der Lieferant oder Dienstleister ist zur Vertraulichkeit über Betriebsgeheimnisse, Know-how und sonstige vertrauliche Informationen verpflichtet, es sei denn, die vertraulichen Informationen sind allgemein bekannt oder werden ohne Verletzung der Geheimhaltungspflicht durch den Lieferanten oder Dienstleister allgemein bekannt. Der Lieferant oder Dienstleister hat seine Mitarbeiter und von ihm beauftragte Subunternehmer entsprechend zur Vertraulichkeit zu verpflichten. Die Vertraulichkeitsverpflichtung gilt auch für die Zeit nach Beendigung des Vertrages.
5. Es besteht das Recht der KDA, auf die beim Lieferanten/Partner gespeicherten oder verarbeiteten Information zuzugreifen.
6. Der Lieferant stellt sicher, dass seine Mitarbeiter und Subunternehmer Kenntnis von den wichtigsten Sicherheitsrichtlinien und Verfahrensanweisungen der KDA haben und diese Regelungen einhalten.
7. Der Lieferant verpflichtet sich, bei der Ausführung seines Auftrages nur fachlich geeignetes sowie ausreichend geschultes Personal einzusetzen.
8. Der Lieferant erkennt an, dass die Nutzung oder Schaffung von allen Zugangsberechtigungen verboten ist sofern sie nicht ausdrücklich seitens der KDA erlaubt sind.
9. Die Vertragssprache und die Sprache der zukünftigen Kommunikation zwischen der Organisation und Lieferanten ist, wenn möglich, Deutsch.

F. Mitarbeit des Lieferanten im Rahmen des ISMS

1. Einhaltung der Sicherheitsrichtlinie für Lieferanten (dieses Dokument).
2. Unterzeichnung des Dokumentes „Verpflichtung Mitarbeiter durch externe Firmen §203 StGB“.
3. Handeln entsprechend der Informationsrichtlinie der KDA.
4. Melden von Informationssicherheitsvorfällen/ Schwachstellen (siehe Kapitel F.1).
5. IT-Geräte, Dokumente, Informationen usw., die die KDA dem Lieferanten zur Verfügung stellt, bleiben Eigentum der KDA.
6. Die Informationen auf/in den genannten Geräten und Dokumenten unterliegen ausnahmslos der Schweigepflicht. Das gleiche gilt für alle Informationen, von denen der Lieferant im Zuge der Umsetzung eines Vertrags möglicherweise Kenntnis erlangt.
7. Der Austausch von (sensiblen) Daten erfolgt durch die vom KDA zur Verfügung gestellten Plattformen oder via verschlüsselter E-Mail.
8. Datenschutzrelevante Dokumente müssen ordnungsgemäß der Vorgaben des Datenschutzes entsorgt werden.

F.1. Informationssicherheitsmeldungen

Verstöße gegen die Informationssicherheit sind an folgende E-Mail-Adresse zu senden:

isv@mail.klinikum-darmstadt.de

Der Lieferant muss seinen Ansprechpartner bei der KDA über sämtliche Probleme oder Alarme im Hinblick auf einen bestätigten oder vermuteten Verstoß gegen die Sicherheitsregeln informieren.
Der Lieferant muss eine erste Statusinformation innerhalb einer Stunde auf alle Anträge oder Anfragen seitens der KDA reagieren, die im Zusammenhang mit bestätigten oder vermuteten „Sicherheitsvorfällen“ stehen, sowie allgemein auf alle Fragen zur Sicherheit von Verbindungen nach außen und zur Sicherheit der vom Lieferant oder seinen Subunternehmern zur Erbringung der Dienstleistungen verwendeten IT-Einrichtungen oder -Ressourcen.

F.2. Passwörter

Folgende Regeln der KDA sind hierzu einzuhalten:

- Jeder Zugriff auf ein System oder dessen Daten muss mit einem personalisierten Benutzerkonto erfolgen, um eine eindeutige Nachvollziehbarkeit der Zugriffe lückenlos gewährleisten zu können.
- Die Länge des Passwortes muss bei der Erstellung automatisch überprüft werden. Alle Passwörter müssen mindestens
    - 8 Zeichen lang sein (für administrative Zugriffe: 15 Zeichen) und

  - mindestens aus zwei Buchstaben und
  - aus zwei Ziffern bestehen.
- Ein User Account sollte nach drei aufeinander folgenden Fehlversuchen dauerhaft gesperrt werden, so dass nur ein Administrator diesen wieder freischalten kann.
- Falls ein Passwort neu angelegt oder durch den Administrator zurückgesetzt wurde, ist der User dazu aufgefordert, dieses bei der nächsten Anmeldung sofort zu ändern.
- Administrative Passwörter dürfen nur in einem Passwortmanager gespeichert werden.
- Die Weitergabe der Passwörter ist generell untersagt. Muss ein Passwort in Notfällen nach sorgfältiger Prüfung der Sachlage zur Wiederherstellung der Betriebsbereitschaft eines Systems einem Dritten übermittelt werden, so ist das betroffene Passwort unverzüglich nach Beendigung des Notfalls zu ändern. Zusätzlich ist eine Informationssicherheitsmeldung abzusetzen (siehe F.1).

F.3. Verschlüsselung

Daten mit einem erhöhten Schutzbedarf, wie z.B. personenbezogene Daten, Gesundheitsdaten oder vertrauliche Daten, dürfen per E-Mail oder per Datenträger außerhalb des hausinternen Netzwerkes der KDA nur verschlüsselt (via S/MIME oder vergleichbare Verfahren) weitergegeben werden.
Der Austausch von (nicht) vertraulichen Dokumenten zwischen Dienstleistern und dem KDA erfolgt in der Regel über E-Mail oder verschlüsselte Clouddienste (z.B. Sharefile).

Eventuelle Passwörter oder Schlüssel sind über einen anderen Kommunikationsweg als die Daten zu versenden.

Die Übertragung schutzbedürftiger Daten ist durch die Anwendung vorhandener Sicherheitsstandards wie z.B. TLS grundsätzlich abzusichern.

F.4. Umgang mit Daten und Geräten der KDA

Generell sind alle personenbezogenen oder vertraulichen Informationen der KDA, unabhängig vom Informationsträger (Datenträger, Papier, Speicherung auf Servern, etc.), besonders zu schützen.
Folgende Maßnahmen tragen hierzu bei und sind daher bei der Arbeit mit Daten der KDA oder auf Systemen der KDA verpflichtend einzuhalten:

- Beim kurzzeitigen Verlassen des Arbeitsplatzes (z.B. Pause, Besprechung, etc.):
  - Sperren des Bildschirms mit Kennwort
- Beim Beenden der täglichen Arbeit
  - Alle personenbezogenen oder vertraulichen Informationen sind nach einem Arbeitstag vom Schreibtisch zu entfernen, sodass sie nicht „zufällig" gesehen werden können (siehe Clean Desk Policy)
- Bei längerer Abwesenheit vom Arbeitsplatz wie z. B. Urlaub
  - Alle personenbezogenen oder vertraulichen Informationen vom Schreibtisch entfernen und an einem sicheren Ort aufbewahren.

F.5. Verhalten im Gebäude der KDA

Die Registrierung und Einweisung von Dienstleistern und Lieferanten für die informationssicherheitsrelevanten Bereiche mit Zutrittsberechtigungen erfolgt über den Fachverantwortlichen des Bereiches bei der KDA.

Jeder Lieferant ist verpflichtet, die Sicherheitszonen innerhalb der KDA zu wahren. Das Betreten von Bereichen nicht erteilter Zutrittsberechtigung ist untersagt. Unberechtigten Dritten ist der Zutritt zu verwehren. Die Türen zwischen den Sicherheitsbereichen sind immer ordnungsgemäß zu schließen (kein Blockieren). (siehe Richtlinie Zutritt)

G. Auditierung von Lieferantendienstleistungen

Die KDA ist dazu verpflichtet, die Einhaltung der Informationssicherheit bei ihren Lieferanten zu überprüfen und zu bewerten. Die KDA behält sich vor, die Leistungen der Lieferanten nach vorheriger Abstimmung per Audit zu überprüfen.
Ein Sicherheitsaudit kann jeden sicherheitsrelevanten Bereich abdecken, z. B. physische Sicherheit, logische Sicherheit, die Sicherheitsorganisation oder Sicherheitsverfahren. Zur Durchführung dieser Audit kann die KDA auch externe Dienstleister beauftragen.
Sicherheitsaudits müssen im Ergebnis zu Empfehlungen und Maßnahmenplänen führen.

H. Training und Awareness

Der Ansprechpartner entscheidet, welche Mitarbeiter von Lieferanten ein Sicherheitstraining- und Awareness-Programm absolvieren müssen. Bei Bedarf kann er dies mit dem Informationssicherheitsbeauftragten (ISB) abstimmen.

I. Entzug von Zugangsberechtigungen

Wenn der Lieferantenvertrag abgeändert oder storniert wird, müssen den Mitarbeitern des Lieferanten die Zugangsberechtigungen entsprechend angepasst werden.

Wird der Vertrag storniert, muss der hausinterne Ansprechpartner außerdem sicherstellen, dass jegliche Gerätschaft, Software oder Information in elektronischer oder Papierform zurückgegeben werden.

J. Mitgeltende Unterlagen

- ISO/IEC 27001 Standard, Abschnitte A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15
- Informationssicherheitsleitlinie
- Clean Desk Policy
- Richtlinie Zutritt
- Verpflichtung Mitarbeiter durch externe Firmen §203 StGB

Vermerke

Freigegeben von:	Funktion des Verantwortlichen	**Maurer Clemens (GF)** **Name**	**18.05.2020** **Datum**	**Unterschrift**

Version	Datum	Beschreibung der Änderung	Erstellt von:
2	18.05.2020	Aktualisierung	Rojewski Benita Elke (STAB IS)