**Anwendungshinweis (Bitte vor Benutzung entfernen):**

Die vorliegenden Empfehlungen und Arbeitshilfen wurden mit größter Sorgfalt erstellt und geprüft, erheben jedoch keinen Anspruch auf Vollständigkeit. Sie geben ausschließlich den Stand zum Zeitpunkt ihrer Erstellung wieder und ersetzen keine individuelle Prüfung. Insofern übernimmt die Deutsche Krankenhausgesellschaft keine Haftung für die Anwendung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen.

**Bestellung zum**

**Informationssicherheitsbeauftragten (ISB)**

Hiermit wird Frau/Herr xxxxx

**mit Wirkung zum xx.xx.xxxx** zum Informationssicherheitsbeauftragten (ISB) in unserem Unternehmen bestellt.

**Organisation**

Der ISB besitzt eine unabhängige und organisatorisch herausgehobene Stellung. Er ist in dieser Rolle direkt der Klinikleitung unterstellt und berichtet direkt an diese.

Er soll in seiner Funktion maßgeblich dazu beitragen, dass die Vertraulichkeit, Integrität und Verfügbarkeit von schützenswerten Informationen in unserem Unternehmen auf Dauer gewährleistet werden kann und diese mit der Patientensicherheit und Behandlungseffektivität in Einklang zu bringen.

Die Klinikleitung trägt weiterhin die Gesamtverantwortung für alle Belange der Informationssicherheit.

**Verantwortlichkeiten/Aufgaben**

Zu den Aufgabenschwerpunkten zählen:

* Beratung der Klinikleitung in allen Belangen der Informationssicherheit.
* Aufbau eines Berichtswesens zur Informationssicherheit.
* Entwicklung und Fortschreibung des Informationssicherheitsmanagementsystems (ISMS).
* Untersuchung und Meldung informationssicherheitsrelevanter Ereignisse.
* Steuerung und Durchführung von Schulung- und Sensibilisierungsmaßnahmen.
* Identifikation, Analyse und Bewertung von Risiken für die Informationssicherheit.
* Unterstützung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten
* Unterstützung aller Projekte des Klinikums hinsichtlich Fragen der Informationssicherheit.
* Initiierung, Vorbereitung und Begleitung von Audits und Zertifizierungen.
* Unterstützung bei der Umsetzung datenschutzrelevanter IT-Prozesse auf Basis der EU-DSGVO.
* Erstellung und Überarbeitung von Vorgaben zur Steigerung des Sicherheitsniveaus der Informationstechnik.
* Leitung des Informationssicherheitsmanagementteams.
* Fortschrittskontrolle der Realisierung von Informationssicherheitsmaßnahmen.
* Koordination der Informationssicherheitsziele mit den Unternehmenszielen.

Die konkreten Ziele des Informationssicherheitsmanagements werden jährlich nach Vorlage des Jahresberichtes zur Informationssicherheit separat vereinbart.

**Befugnisse/Kompetenzen**

Der Informationssicherheitsbeauftragte

* ist in allen für die Informationssicherheit relevanten Themen zu informieren (sowohl auf Nachfrage als auch unaufgefordert, soweit eine Relevanz für die Informationssicherheit besteht).
* ist in Vorhaben und Änderungen, die die Informationssicherheit berühren können (z.B. neue IT-Projekte, Änderungen der IT-Infrastruktur, Änderungen von Rahmenbedingungen mit Auswirkungen auf die Informationssicherheit) frühzeitig mit einzubinden.
* hat ein Mitsprache- und Vetorecht bei allen Entscheidungen die seinen Verantwortungsbereich betreffen (z.B. bei der Initiierung von IT-Projekten, Beschaffung von Informationsverarbeitenden Systemen, Änderungen von Geschäftsprozessen, Ausbildung von Mitarbeitern).
* hat ein direktes Vortragsrecht bei der Geschäftsführung.
* hat ein Vorschlagsrecht bei der Geschäftsführung zu Maßnahmen zur Verbesserung der Informationssicherheit
* hat Zutrittsrecht zu allen Bereichen, in denen Informationstechnik eingesetzt wird und damit zusammenhängende Daten verarbeitet werden, und zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden.
* hat im Rahmen seiner Tätigkeit ein zeitlich, auf die Dauer der wahrzunehmenden Aufgabe, begrenztes Zugriffsrecht auf alle betroffenen IT-Systeme und damit verarbeitete Daten. Je nach Art der Daten müssen Sie sich hierzu vorab mit dem Datenschutz- oder Geheimschutzbeauftragten abstimmen.
* führt regelmäßig Revisionen im Themenbereich der Informationssicherheit durch bzw. veranlassen Revisionen durch unabhängige Dritte und überprüfen so das aktuelle Informationssicherheitsniveau in Ihrem Aufgabenbereich.
* führt regelmäßig Risikoanalysen für den Bereich Informationssicherheit durch.
* vertritt das Unternehmen im Bereich des Informationssicherheitsmanagements.

**Geltungsbereich**

Die in dieser Bestellung festgelegten Befugnisse gelten unternehmensweit und umfassen alle Bereiche, in denen Daten und Informationen verarbeitet, übertragen und gespeichert werden.

|  |  |  |
| --- | --- | --- |
| **XXXXX,** |  |  |
| **Ort, Datum** |  | **Verantwortlicher****(Vorname Name)** |
|  |  |  |
| **XXXXX,** |  |  |
| **Ort, Datum** |  | **Informationssicherheitsbeauftragter****(Vorname Name)** |