**Beauftragung zur Übernahme von**

**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.

**Tätigkeiten eines externen**

**Informationssicherheitsbeauftragten**

**(ISB / CISO)**

Hiermit wird Frau/Herr/Firmenname

XXXX

mit Wirkung zum xx.xx.xxxx mit der Übernahme der Tätigkeiten des

Informationssicherheitsbeauftragten (ISB / CISO) in der

Musterklinik

Musterstrasse

 12345 Musterhausen

beauftragt. Dabei gilt folgendes:

**Allgemein**

Mit dieser Beauftragung übernimmt die xxxx für die Musterklinik Tätigkeiten, die im Zusammenhang mit der Stellung eines Informationssicherheitsbeauftragten (ISB / CISO) innerhalb einer Klinik und im Zusammenhang mit dem §8a BSI-Gesetz in Verbindung stehen. Dazu wird die xxxx aus ihrer Organisation, Unterauftragnehmer eingeschlossen, Personen für die Rolle des Informationssicherheitsbeauftragten (ISB / CISO) für die Musterklinik bereitstellen.

Sie achtet bei den Personen auf ausreichendes Wissen und Erfahrung auf dem Gebiet der Informationssicherheit und Informationstechnologie und stellt selbst angemessene Ressourcen zur Erfüllung der Aufgaben zur Verfügung und ermöglicht zudem die Fortbildung in dem gebotenen und angemessenen Umfang.

Die beauftragten Personen sind namentlich gegenüber der Musterklinik zu benennen („benannte Personen‘). Aus wichtigem Grund kann die Musterklinik die Beauftragung einzelner Personen ablehnen. Als wichtiger Grund gilt fehlende Fachkenntnis oder ein zerrüttetes Vertrauensverhältnis zwischen der Person und der Geschäftsführung der Musterklinik.

**Verantwortlichkeiten/Aufgaben**

Die XXXX übernimmt für die MUSTERKLINIK folgende Tätigkeiten auf dem Bereich der Informationssicherheit. Die von der XXXX benannten Personen

* stimmen die Informationssicherheitsziele für die MUSTERKLINIK mit den

Unternehmenszielen der MUSTERKLINIK ab.

* erstellen die Leitlinie zur Informationssicherheit und stimmen diese mit der

Geschäftsführung der MUSTERKLINIK ab.

* erstellen Richtlinien und Regelungen die Informationssicherheit betreffend für die MUSTERKLINIK und legen diesen zur Implementierung vor.
* erstellen Vorschlage, wie die abgestimmten Dokumente zur
* Informationssicherheit allen Mitarbeitern des Unternehmens bekannt gegeben werden können.
* setzen den Aufbau, den Betrieb, die Pflege und die Weiterentwicklung eines Informationssicherheitsmanagementsystems innerhalb der MUSTERKLINIK um.
* unterbreiten Vorschlage zum Aufbau, Betrieb und Weiterentwicklung der Informationssicherheitsorganisation und zur Informationssicherheits-Governance in den Managementsystemen innerhalb der MUSTERKLINIK.
* überprüfen die Erstellung und die Pflege des Informationssicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien des Unternehmens nach den Vorgaben des BSI-Gesetzes.
* beraten die Leitungsebene in allen Fragen der Informationssicherheit.
* berichten relevante die Informationssicherheit betreffende Vorkommnisse an die Geschäftsführung der MUSTERKLINIK und an die im Rahmen des Informationssicherheitsmanagements definierten Stellen.
* übernehmen die Aufgaben der KRITIS Meldestelle gegenüber dem BSI für die MUSTERKLINIK.
* berichten der Geschäftsführung der MUSTERKLINIK regelmäßig über den aktuellen Stand der Informationssicherheit.
* stellen den notwendigen Informationsfluss für das Informationssicherheitsmanagement sicher (z. B. durch Berichtswesen, elektronische Dokumentation).
* initiieren und kontrollieren die Realisierung von Sicherheitsmaßnahmen innerhalb der MUSTERKLINIK.
* koordinieren zielgruppenorientierte und regelmäßige Sensibilisierungs- und Schulungsmaßnahmen zum Thema Informationssicherheit.
* planen das Geschäftsfortführungsmanagement und erstellen ein Notfallhandbuch zur Bewältigung von Notfallen nach den Anforderungen des §8a BSI-Gesetz.
* binden alle Mitarbeiter des Unternehmens in den Informationssicherheitsprozess und die Notfallvorsorge ein.
* übernehmen die Leitung der Analyse und Nachbearbeitung von Informationssicherheitsvorfallen.
* arbeiten mit anderen Beauftragten aus dem Gebiet der (Informations-) Sicherheit zusammen (z. B. Datenschutzbeauftragter, Notfallbeauftragter).
* nehmen regelmäßig an Fortbildungen zur Informationssicherheit teil. Die regelmäßige Teilnahme an entsprechenden Fortbildungen ist verpflichtend.

**Mandat der benannten Personen**

* Die benannten Personen haben ein Mitspracherecht bei allen Entscheidungen die Ihren Verantwortungsbereich betreffen (z. B. bei der Initiierung von IT-Projekten, Beschaffung von Informationsverarbeitenden Systemen, Änderungen von Geschäftsprozessen, Ausbildung von Mitarbeitern).
* Die benannten Personen haben direktes Vortragsrecht gegenüber der Geschäftsführung der MUSTERKLINIK.
* Die benannten Personen haben Zutrittsrecht zu allen Bereichen, in denen Informationstechnik eingesetzt wird und damit zusammenhangende Daten verarbeitet werden, und zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden.
* Die benannten Personen haben im Rahmen ihrer 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 Datenschutzbeauftragten abstimmen.
* Die benannten Personen fuhren regelmäßig Revisionen im Themenbereich der Informationssicherheit durch bzw. veranlassen Revisionen durch unabhängige Dritte und überprüfen so das aktuelle Informationssicherheitsniveau in Ihrem Aufgabenbereich.
* Die benannten Personen fuhren regelmäßig Risikoanalysen für den Bereich Informationssicherheit durch.

**Pflichten der Musterklinik**

Die MUSTERKLINIK erfüllt im Rahmen dieser Beauftragung folgen Mitwirkungspflichten:

* Die von der XXXX benannten Personen sind in allen für die Informationssicherheit relevanten Themen von der Geschäftsführung der MUSTERKLINIK und weiteren relevanten Stellen zu informieren. Dies schließt Informationen über die Geschäftsziele der MUSTERKLINIK ein, soweit diese für die Erstellung einer Informationssicherheits-Strategie relevant sind.
* Die Geschäftsführung der MUSTERKLINIK wirkt an der Erstellung Richtlinien und Verfahrensanweisungen der Informationssicherheit mit, indem sie diese prüft und freigibt.
* Die Geschäftsführung der MUSTERKLINIK stellt einen Mechanismus bereits, um Richtlinien und Verfahrensanweisungen der Informationssicherheit in der Organisation der MUSTERKLINIK zu verteilen und diese durchzusetzen.
* 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) werden frühzeitig mit den benannten Personen der XXXX abgestimmt.
* Die von der XXXX benannten Personen sind bei allen größeren internen und externen Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung und Anforderungen haben, durch die Geschäftsführung der MUSTERKLINIK zu beteiligen, um die Beachtung von Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten.
* Die MUSTERKLINIK stellt den benannten Personen notwendige Ressourcen zur Erledigung der hier genannten Aufgabe bereit. Die betrifft insbesondere Mitwirkung in Risikoanalysen, Erstellung und Implementierung von Verbesserungsmaßnahmen, Teilnahme von fachkundigem und verantwortlichem Personal seitens der MUSTERKLINIK bei von den benannten einberufenen Meetings.

**Geltungsbereich**

Die in dieser Beauftragung festgelegten Befugnisse gelten innerhalb der MUSTERKLINIK und der mit ihr verbundenen Unternehmen und umfassen alle Bereiche, in denen Daten und Informationen verarbeitet, übertragen und gespeichert werden, soweit dies den Geltungsbereich des §8a BSI-Gesetz betrifft.

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