

Muster für eine Bestellung eines IT-Sicherheitsbeauftragten (Mindestumfang)

[Überarbeitung eines Vorschlags des BSI unter www.bsi.de]

Hiermit wird
Herr/Frau <Name>
zum/zur IT-Sicherheitsbeauftragten
der <Name-Unternehmen>
bestellt.

Organisatorisches

Die Leitungsebene trägt nach außen die Gesamtverantwortung für alle Belange der Informationssicherheit. Intern wird die Verantwortung an die Rolle des IT-Sicherheitsbeauftragten delegiert.

Der IT-Sicherheitsbeauftragte besitzt eine organisatorisch herausgehobene Stellung und ist der Leitungsebene direkt unterstellt bzw. berichtet direkt an diese. Die notwendige Unabhängigkeit von anderen Stellen innerhalb der Organisation ist gegeben.

Es ist sichergestellt, dass die Wahrnehmung der Rolle des IT-Beauftragten zu keinen Konflikten mit weiteren von dieser Person wahrgenommenen Rollen führt.

Der IT-Sicherheitsbeauftragte verfügt über ausreichendes Wissen und Erfahrung auf dem Gebiet der IT-Sicherheit bzw. wird noch fehlende Qualifikationen zeitnah erwerben.

Die Leitungsebene unterstützt den IT-Sicherheitsbeauftragten bei der Wahrnehmung seiner Aufgaben und stellt hierfür ausreichende Ressourcen bereit. Die Leitungsebene gewährleistet eine der Funktion angemessene Aus- und Fortbildung.

Als Abwesenheitsvertretung ist Herr/Frau <Name> vorgesehen. Die Vertretung ist / wird eingearbeitet und hat ausreichend Ressourcen zur Wahrnehmung der Aufgaben.

Verantwortlichkeiten/Aufgaben

Der IT-Sicherheitsbeauftragte ist zuständig und gegenüber der Leitung verantwortlich für alle Belange der Informationssicherheit:

- Abstimmen der Sicherheitsziele mit der Leitungsebene
- Erstellen, Abstimmen, Bekanntmachung und zukünftige Anpassung einer Sicherheitsleitlinie, eines Sicherheitskonzeptes (mit Risikoanalysen und Maßnahmenfestlegungen) und notwendiger Sicherheitsrichtlinien
- Mitwirkung bei Sensibilisierungs- und Schulungsmaßnahmen für das Personal
- Überwachen / Überprüfen der Sicherheit: Kontrolle der korrekten Umsetzung von Maßnahmen, Beurteilung der Wirksamkeit, Analyse und Nachbearbeitung von Sicherheitsvorfällen

- Berichte über erhebliche Sicherheitsvorkommnisse an die Leitungsebene, sowie jährlich über den Stand der Informationssicherheit im Unternehmen
- Informationsmanagement und Informationsfluss: Berichtswesen, Dokumentation, Aufzeichnungen
- Zusammenarbeit mit anderen Rollen (Datenschutzbeauftragter, Notfallbeauftragter, Compliance Management, Asset Management, Betriebsrat)

Befugnisse

Der IT-Sicherheitsbeauftragte verfügt über folgende Befugnisse:

- Steuerung des Sicherheitsprozesses, insbesondere Anberaumen von Meetings und Herbeiführen von Abstimmungen
- Zugang zu allen relevanten Informationen
- Begehungs- und Überprüfungsrecht (Liegenschaften, Gebäude, Räume, Arbeitsplätze)
- Zugriffsrechte auf alle betroffenen IT-Systeme und damit verarbeitete Daten (ggf. in Abstimmung mit dem Datenschutzbeauftragten und dem Betriebsrat)
- Veranlassung interner und externer Audits
- Vermittlung von Sicherheitsinformationen
- Vorschlagsrecht zur Verbesserung der Sicherheit
- Eskalieren von Entscheidungen über Sicherheitsfragen
- Anhörung bei geplanten Beschaffungen, die die IT-Sicherheit tangieren
- Einbindung bei neuen Projekten des Unternehmens
- Einbindung in operative Sicherheitsaktivitäten (Auswerten von Aufzeichnungen, Abnahme sicherheitstechnischer Einrichtungen, Erteilen von Weisungen bei gravierenden Sicherheitsvorkommnissen)

Diese Befugnisse gelten unternehmensweit für alle Bereiche, in denen Informationen verarbeitet, übertragen und gespeichert werden.

Diese Bestellung tritt mit Wirkung vom <Datum> in Kraft und gilt zunächst für die Dauer von <Zeitraum>.

<Unterschrift der Leitung>