

Vorgaben zur Erstellung eines Konzeptes für die Übernahme der Funktion des Informationssicherheitsbeauftragten (ISB/CISO)

Max-Planck-Institut für Psychiatrie (MPIP)

1. Einleitung

- Kurzvorstellung des Bewerbers (Einzelperson oder Firma)
- Relevante Erfahrungen in vergleichbaren Einrichtungen, idealerweise im Krankenhausumfeld
- Motivation für die Übernahme der Aufgabe

2. Fachliche Qualifikation

- Darstellung der Qualifikationen im Bereich Informationssicherheit (z. B. Zertifizierungen wie ISO/IEC 27001 Lead Implementer/Auditor, CISSP, etc.)
- Nachweis der Kenntnisse im Bereich Krankenhaus-IT und gesetzlicher Anforderungen (z. B. B3S, NIS2, BSI-Gesetz)
- Erfahrung mit Aufbau, Betrieb und Weiterentwicklung von ISMS-Systemen

3. Methodik und Vorgehensweise

- Vorgehen zur Abstimmung und Umsetzung der Informationssicherheitsziele mit den Unternehmenszielen
- Methodik zur Entwicklung und Pflege von Leitlinien, Richtlinien und Sicherheitskonzepten
- Vorgehen bei der Integration der Informationssicherheit in das GRC-Managementsystem
- Beschreibung der geplanten Sensibilisierungs- und Schulungsmaßnahmen
- Verfahren zur Analyse und Nachbearbeitung von Sicherheitsvorfällen

4. Organisation und Kommunikation

- Vorschläge zur Sicherstellung des Informationsflusses innerhalb des Instituts
- Darstellung der Einbindung relevanter Stakeholder (z. B. Datenschutz, Compliance, Risikomanagement)
- Berichtswesen: Turnus, Inhalte, Adressaten (inkl. direktem Bericht an Geschäftsführung)

5. Umsetzung und Zeitplanung

- Grober Projektplan für die ersten 6 bis 12 Monate
- Einschätzung des wöchentlichen Zeitbedarfs (in Abgleich mit dem geschätzten Bedarf von 6–11 Wochenstunden)
- Flexibilitätsoptionen bei erhöhtem Bedarf (z. B. bei Sicherheitsvorfällen)

6. Qualitätssicherung und Weiterentwicklung

- Maßnahmen zur Qualitätssicherung und laufenden Verbesserung des Informationssicherheitsniveaus
- Regelmäßige Revisionen und Risikoanalysen: Vorgehensweise, Tools, Häufigkeit
- Einbindung externer Audits

7. Vertraulichkeit und Compliance

- Umgang mit vertraulichen Daten
- Zusammenarbeit mit Datenschutzbeauftragten
- Einhaltung gesetzlicher und interner Vorgaben

8. Referenzen und Nachweise

- Referenzprojekte (optional mit Ansprechpartnern)
- Zertifikate und Qualifikationsnachweise
- Nachweis über berufliche Zuverlässigkeit (z. B. Führungszeugnis bei Einzelpersonen)

9. Anlagen

- Lebenslauf / Unternehmensprofil
- Ggf. ergänzende Dokumente