# Beispiel Sicherheitsleitlinie des Kreiskrankenhauses Aussap

## Stellenwert der Informationssicherheit und Bedeutung dieser Leitlinie

Der Erfolg des Kreiskrankenhauses Aussap hängt in besonderem Maße davon ab, dass die Geschäftsinformationen aktuell und unverfälscht sind und bei Bedarf mit der gebotenen Vertraulichkeit behandelt werden. Speziell die Krankendaten der Patienten stellen eine äußerst sensible Form von personenbezogenen Daten dar und bedürfen eines besonderen Schutzes.

Informationstechnik ist in allen Geschäftsbereichen eine wichtige Ressource. Sie wird auch immer wichtiger in den Beziehungen zu Patienten, Krankenkassen, Zulieferern, Partnerunternehmen, der öffentlichen Verwaltung und anderen Institutionen. Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind daher ein wesentlicher Eckpfeiler des Unternehmenserfolges.

Mit der Leitlinie erkennt die Geschäftsführung ausdrücklich an, dass die Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit der geschäftskritischen Informationen eine kontinuierlich zu verfolgende Aufgabe ist und geeignete organisatorische Grundlagen erfordert.

Die Leitlinie wird durch ein Sicherheitskonzept für die Abrechnungsabteilung ergänzt, welches zu einem späteren Zeitpunkt alle Unternehmensbereiche umfassen wird. Bei der Entwicklung dieses Konzepts stützt sich das Kreiskrankenhauses Aussap auf die IT-Grundschutz-Methodik und die Vorgaben im IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik. Regelmäßige Überprüfungen sollen dafür sorgen, dass Leitlinie und das Sicherheitskonzept angemessen und aktuell bleiben.

## Sicherheitsniveau und Ziele

Insbesondere der Schutz der hochsensiblen, personenbezogenen Patientendaten ist für das Ansehen des Krankenhauses neben den rechtlichen Folgen unabdingbar. Ausfälle der Informationstechnik, die zum Verlust der Vertraulichkeit oder Beeinträchtigungen bei der Behandlung von Patienten führen, sind nicht vertretbar.

Die Geschäftsführung des Kreiskrankenhauses Aussap hat entschieden, dass zuerst ein angemessenes Sicherheitsniveau für einen hohen Schutzbedarf im Rahmen der Kernabsicherung innerhalb der Abrechnungsabteilung angestrebt werden soll. Grundlage für diese Entscheidung war eine Gefährdungsabschätzung über die Werte der wichtigsten zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit. Dies bedeutet im Einzelnen:

1. Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Beschäftigten die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur Informationssicherheit können hierbei unterstützen.

2. Vertraulichkeit und Integrität der für das Unternehmen wichtigen Informationen insbesondere der Patientendaten sind zu schützen, unabhängig davon in welcher Form sie vorliegen. Auch im Umgang mit elektronischen Dokumenten und Informationen ist daher Geheimhaltungsanweisungen strikt Folge zu leisten.

3. Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für das Unternehmen relevanten Gesetze, Vorschriften und vertragliche Verpflichtungen eingehalten werden.

4. Die Informationstechnik muss so betrieben werden, dass Geschäftsinformationen bei Bedarf hinreichend schnell verfügbar sind. Ausfälle, die zu Terminüberschreitungen von mehr als einem halben Tag bei der Behandlung von Patienten oder anderen wichtigen Geschäftsvorhaben führen, sind nicht tolerierbar.

5. Durch fahrlässigen Umgang mit Informationen verursachte rechtliche Probleme, finanzielle Schäden und ein negatives Image für das Unternehmen müssen verhindert werden. Der Zugriff auf und der Zugang zu allen wichtigen Informationen im Unternehmen werden daher beginnend bei der Abrechnungsabteilung strikt geregelt und kontrolliert.

## Verantwortlichkeiten

Die **Geschäftsführung** hat die Gesamtverantwortung für die Informationssicherheit im Unternehmen, den Sicherheitsprozess und die zugehörigen Maßnahmen.

Für die Koordination und Überwachung aller auf Informationssicherheit bezogenen Aktivitäten wird von der Geschäftsführung die Stabsstelle eines **Informationssicherheitsbeauftragten** geschaffen. Der zuständige Mitarbeiter ist gleichzeitig zentraler Ansprechpartner für alle Fragen rund um das Thema Informationssicherheit und der Geschäftsführung berichtspflichtig.

Der Informationssicherheitsbeauftragte bildet gemeinsam mit weiteren von der Geschäftsführung benannten Mitarbeitern ein **IS-Management-Team**, das für die Aufrechterhaltung und Weiterentwicklung der organisatorischen und technischen Sicherheitsmaßnahmen im Unternehmen zuständig ist.

Für alle Informationen, Geschäftsprozesse sowie die unterstützenden informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (**Informations-, Prozess- und Systemeigentümer**) benannt. Diese sind dafür zuständig, die geschäftliche Bedeutung von Informationen und Technik einzuschätzen und darauf zu achten, dass die Mitarbeiter dieser Bedeutung entsprechend handeln. Sie verwalten Zugriffsrechte und Autorisierungen in ihrem Zuständigkeitsbereich und sind gegenüber der Leitung rechenschaftspflichtig. Sie sind auch dafür verantwortlich, externen Dienstleistern und Kooperationspartnern die Vorgaben des Kreiskrankenhauses Aussap zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

Jeder **Mitarbeiter** soll dazu beitragen, Sicherheitsvorfälle und Verletzungen der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen zu vermeiden. Erkannte Fehler sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

## Geltung und Folgen von Zuwiderhandlungen

Diese Leitlinie zur Informationssicherheit gilt **zunächst für die Abrechnungsabteilung** und wird zu einem s**päteren Zeitpunkt** auf das **gesamte Kreiskrankenhaus** Aussap erweitert. Jede Mitarbeiterin und jeder Mitarbeiter ist daher angehalten, sicherheitsbewusst mit betrieblich wichtigen Informationen und der Informationstechnik umzugehen und verbindliche Sicherheitsregeln zu befolgen.

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Patienten schädigen oder den Ruf des Krankenhauses gefährden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.