MNC-Richtlinie zur Informationssicherheit

Medical Netcare GmbH

Stand: 28.08.2024

Inhalt

1. Stellenwert der Information

Information ist die Basis jeder geschäftlichen Tätigkeit. Der Umgang mit Information muss geregelt sein, um den Anforderungen interner und externer interessierter Parteien gerecht zu werden.

Diese Anforderungen ergeben sich wesentlich aus dem gesetzlichen Kontext des SGB V, spezifischen Richtlinien und Verträgen mit Kunden, ggf. Partnern und Mitarbeitern.

Informationsverarbeitung spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf unser Geschäft nicht zusammenbrechen.

Da unsere Kernkompetenz am Standort Mendelstraße 11 in Münster in dem Handling großer Datenmengen und der Auswertung und Evaluation pseudonymisierter und/oder anonymisierter Sozialdaten sowie Strukturdaten liegt, ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von existenzieller Bedeutung.

2. Übergreifende Ziele

Unsere Information und unsere IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer *Verfügbarkeit* so gesichert, dass die zu erwartenden Stillstandzeiten toleriert werden können (normales Schutzniveau). Fehlfunktionen und Unregelmäßigkeiten in IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel, die *Integrität* uns anvertrauter Daten ist absolut zu wahren (Maximumprinzip: hohes Schutzniveau). Die Anforderungen an *Vertraulichkeit* haben ein normales, im Fall von personenbezogenen Daten bzw. personenbezogenen Sozialdaten ein hohes, an Gesetzeskonformität orientiertes Niveau. Es gelten maximale Anforderungen an die Vertraulichkeit.

Für die das auch prospektive Projektmanagement und die wissenschaftliche bzw. medizinische Dokumentation betreffenden Daten und Dokumente wird ein ebenfalls hoher Schutzbedarf im Hinblick auf die Vertraulichkeit angenommen. Die Sicherung vor Verlust bewegt sich auf einem normalen Niveau, um Fristen und Termine von geschäftskritischer Bedeutung einzuhalten.

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

Aus diesen Überlegungen ergibt sich eine Priorisierung der Sicherheitsmaßnahmen zu den Themen *Zugangssteuerung* sowie *Physische und umgebungsbezogene Sicherheit*, die in der Normversion 27001:2013 als Controls A9 und A11 enthalten sind. Der hohe Stellenwert dieser Maßnahmen und das verbundene Potenzial für die Risikominderung bedingt eine höhere Überprüfungsrate der Umsetzung und der Wirksamkeit der betreffenden Maßnahmen.

Alle Mitarbeitenden des Unternehmens halten die einschlägigen Gesetze (z.B. Gesetze und Regelungen zum Datenschutz) und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeitenden und die Unternehmensführung sind sich ihrer Verantwortung beim Umgang mit Information bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

3. Informationssicherheitsmanagement

Zur Erreichung der Informationssicherheitsziele wurde Frau Alexandra Berendes zur Informationssicherheitsbeauftragten benannt. Die Informationssicherheitsbeauftragte berichtet in ihrer Funktion direkt an die Geschäftsführung.

Der Informationssicherheitsbeauftragten, dem Datenschutzbeauftragten und den Administratoren werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vom Management festgelegten Informationssicherheitsziele zu erreichen. Der Datenschutzbeauftragte ist angehalten, sich regelmäßig weiterzubilden.

Die Informationssicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen und Risiken zu analysieren. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten. Die Mitarbeitenden haben sich in informationssicherheitsrelevanten Fragestellungen an die Anweisungen der Informationssicherheitsbeauftragten zu halten.

4. Geltungsbereich der Sicherheitskonzeption

Der Geltungsbereich umfasst die strukturellen Voraussetzungen sowie die vorhandene Information in den Räumlichkeiten der MNC GmbH im Technologiehof Münster.

Die Sicherheitskonzeption hat darüber hinaus auch im Fall von notwendigem oder vereinbartem Home-Office bei Arbeiten im Dienstverhältnis für MNC Geltung. Ausgeschlossen ist dabei notwendig der Zugriff auf das abgeschlossene interne Netz.

Outgesourcte Bereiche werden ggf. perspektivisch entsprechend dem erforderlichen Maß an Informationssicherheit und Qualität beschafft und regelmäßig überprüft. Aktuell gibt es keine outgesourcten Bereiche.

Die mit der Information verbundenen Tätigkeiten des Instituts erstrecken sich auf Datenverarbeitung im Bereich Gesundheitswesen, Weiterentwicklung von Leit- und Richtlinien, statistische Auswertungen, Evaluation und Reporting.

5. Sicherheitsmaßnahmen

Für alle Prozesse, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertretende ihre Aufgaben erfüllen können. Die entsprechenden Unterlagen finden sich im Prozesshandbuch.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Alle Schutzprogramme auf IT-Systemen werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzenden durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Datenverluste können nie *vollkommen* ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann,

wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Darüber hinaus werden Datenträger, die Voraussetzung für die Lauffähigkeit eines für die betrieblichen Abläufe wichtigen Systems sind, in gespiegelten RAID-1-Verbünden betrieben (alle Domaincontroller und DB-Server).

Informationen werden so aufbewahrt, dass sie schnell auffindbar sind. Dazu ist ein Dokumentenmanagementsystem (DMS) im Firmennetzwerk vorgegeben und implementiert.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, werden Risikoanalysen vorgenommen. Im Fall eines trotzdem auftretenden Sicherheitsvorfalls muss zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten *Notfallvorsorgekonzept* zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

6. Verbesserung der Sicherheit

Die Maßnahmen werden regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitenden bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Leitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeitende sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten. Das Vorgehen sowie die Definition der Kategorien von Vorfällen sind in der Prozedur Vorgehen bei IT-Vorfällen geregelt.

7. Skizzierung von Zuständigkeiten im Sicherheitsprozess

Der IT-Verantwortliche ist erster Ansprechpartner bei Verdacht auf Datenpannen/IT-Sicherheitsvorfälle.

Zweite Ansprechpartnerin ist die Informationssicherheitsbeauftragte Frau Alexandra Berendes.

Die Informationssicherheitsbeauftragte Frau Berendes wird in die Entscheidungen zu neuen Maßnahmen und Sensibilisierungsprozessen eingebunden und prüft die Einhaltung geplanter Maßnahmen und Prozesse. Dieses Monitoring ist definiert im Kennzahlensystem, das jährlich durch die Geschäftsführung im Management Review mit ausgewertet wird.

Münster, den 16.09.2024

_____

Frank Potthoff, Geschäftsführer