Anlage 3

zu [VERTRAGSNUMMER/GZ]

Datensicherheitsmaßnahmen

In den Tirol Kliniken ist ein Informations-Sicherheits-Management-System, angelehnt an die ISO 27001/27002/27005, implementiert.

Richtlinie	Anforderungen
Zugriffskontrollen	Die Zugriffsrechte einer Person auf IT-Systeme und Daten bestimmen sich einerseits nach den betrieblichen Aufgaben welche von dieser zu erfüllen sind und andererseits nach den notwendigen Sicherheitsanforderungen. Die Steuerung der Zugriffsrechte erfolgt über Zugriffsregelwerke. Es wird sichergestellt, dass Zugriffe auf IT-Systeme und die darin gespeicherten Daten nur für dafür autorisierte Personen möglich sind.
Management von Informationssicherheits-Vorfällen und –Schwachstellen	Formale Meldewege für Informationssicherheits-Vorfälle und -Schwachstellen sind festgelegt, so dass rechtzeitig korrigierende Maßnahmen getroffen werden können.
Betriebliches Kontinuitätsmanagement	Es sind geeignete Maßnahmen gesetzt, damit Störungen oder Ausfälle von IT-Systemen kritische bzw. wichtige Arbeitsabläufe möglichst wenig beeinträchtigen. Vorkehrungen für große IT-Ausfälle (IT-Krisen) sind getroffen.
Physische und umgebungsbezogene Sicherheit	Die Applikationen werden in zwei technisch autarke Rechenzentren betrieben. Die Rechenzentren sind am Stand der Technik und mit Zutrittskontrollsystemen versehen.
Management von IT-Vermögenswerten	IT-Vermögenswerte sind dokumentiert und Verantwortliche dafür festgelegt.
IT-Risikomanagement	Der IT-RM-Prozess ist definiert und beinhaltet die Risiko-Identifizierung/ Analyse/ Bewertung, die Risiko-Behandlung / Maßnahmenumsetzung, die Risiko-Information (Risiko-Kommunikation) sowie das Monitoring. Die IT-RM-Organisation inklusive der Verantwortlichkeiten ist definiert und etabliert.
Organisation der Informationssicherheit	Für die systematische Weiterentwicklung der Informationssicherheit ist ein Management-Rahmenwerk festgelegt in dem Ziele, Grundsätze, Organisation, Verantwortlichkeiten und Maßnahmenbereiche definiert sind.
Personelle Sicherheit	Es wird sichergestellt, dass Mitarbeiter und Auftragnehmer für die vorgesehenen Aufgaben im Unternehmen geeignet sind. Sie müssen in der Lage sein, die betrieblichen Sicherheitsvorgaben zu befolgen und das Risiko von Fehlern zu verringern. Es wird sichergestellt, dass bei Mitarbeitern und Auftragnehmern, die das Unternehmen verlassen bzw. der Vertrag beendet wird, die erforderlichen Schritte in Bezug auf IT-Sicherheit durchgeführt werden.
Management des IT-Betriebes	Die Verantwortlichkeiten für den IT-Betrieb sind festgelegt. Ein Changemanagement ist implementiert, welches die

	Vorgehensweise bei Systemänderungen festlegt.
Beschaffung, Entwicklung und Wartung von Informationssystemen	Es ist berücksichtigt, dass die Informationssicherheit ein integrierter Bestandteil von Informationssystemen ist, die entsprechenden Standards eingehalten sind und diese auch über den gesamten Lebenszyklus aufrecht erhalten bleiben.
Kommunikation und Kryptographie	Beim Austausch von Informationen und Software ist die Sicherheit bei internem als auch bei externem Austausch gewährleistet. Der angemessene und wirksame Gebrauch von Verschlüsselungsverfahren ist sichergestellt.
Lieferantenbeziehungen	IT-Vermögenswerte, die IT-Lieferanten und IT-Dienstleistern zugänglich sind, werden entsprechend geschützt. Die Leistungen der Lieferanten und Dienstleister werden regelmäßig geprüft.

Vernichtung von Daten bei Beendigung des Auftragsverhältnisses:

Nach Beendigung des Auftragsverhältnisses werden keine Daten mehr zu Zwecken der Register aktiv verarbeitet.

Die in den Registern bereits verarbeiteten, berücksichtigen Daten werden entsprechend der Aufgabe eines Registers (ua. zu Zwecken der Qualitätskontrolle, der Beobachtung von Entwicklungen verschiedener gesundheitsbezogener Merkmale im Zeitverlauf und der Rekonstruierbarkeit von Auswertungsergebnissen) nicht vernichtet.