



EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN



Geschäftsordnung

IT-Sicherheit

des Universitätsklinikums Tübingen und der Medizinischen Fakultät Tübingen

Stand: 13.04.2010

Hinweis: Sämtliche in diesem Dokument verwendeten Funktionsbezeichnungen sind geschlechtsneutral zu verstehen.

Der Bereich IT-Sicherheit soll die sichere Verarbeitung von Informationen am Universitätsklinikum Tübingen (UKT) und der Medizinischen Fakultät Tübingen (MFT) gewährleisten. Diese Geschäftsordnung regelt dazu den Geltungsbereich, die Aufgaben, die Zuständigkeiten und Befugnisse sowie die Organisation und Berichtspflicht für die IT-Sicherheit des Universitätsklinikums und der Medizinischen Fakultät Tübingen..

§ 1 Geltungsbereich

Die Festlegungen dieser Geschäftsordnung gelten für

- alle Organisationseinheiten von UKT und MFT, die nicht vom ZDV betreut werden,
- alle Bereiche, in denen eine Informationstechnik oder Infrastruktur oder ein IT-System von UKT oder MFT eingesetzt wird und die nicht vom ZDV betreut werden, auch wenn diese außerhalb der Dienstgebäude genutzt werden,
- alle Einrichtungen, mit denen ein Kooperationsvertrag bzgl. IT-Sicherheit abgeschlossen wurde.

§ 2 Ziele, Aufgaben

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein.

IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz der elektronisch gespeicherten Informationen und ihrer korrekten Verarbeitung im Sinne der IT-Sicherheit. Die IT-Sicherheit an UKT und MFT soll sich in Zukunft im Sinne der Informationssicherheit weiterentwickeln.

IT-Sicherheit umfasst dabei die Summe aller organisatorischen, personellen und technischen Maßnahmen, die geeignet sind, die nachfolgend genannten Ziele zu erreichen:

- Verfügbarkeit der Daten
- Vertraulichkeit der Daten
- Integrität der Daten
- Authentizität der Daten
- Nichtabstreitbarkeit der Daten

§ 3 Organisation

Die Organe der IT-Sicherheitsorganisation sind:

- Klinikums- und Fakultätsvorstand

- der IT-Sicherheitsbeauftragte
- das Sicherheits-Notfall-Team

Der IT-Sicherheitsbeauftragte ist in dieser Funktion direkt den Vorständen unterstellt.

§ 4 Zuständigkeiten

Klinikums- und Fakultätsvorstand

- Tragen die Hauptverantwortung für die IT-Sicherheit für die im §1 Geltungsbereich aufgeführten Bereiche
- Stellen die für diese Aufgaben notwendigen und wirtschaftlich vertretbaren Ressourcen und Mittel zur Verfügung
- Legen das Sicherheitsniveau für den Geltungsbereich fest und beschließen die IT-Sicherheitsleitlinie, das IT-Sicherheitskonzept, die IT-Sicherheitsorganisation, die Realisierungsplanung und die Informationsmaßnahmen
- Benennen einen IT-Sicherheitsbeauftragten und übertragen ihm die operativen und konzeptionellen Aufgaben der IT-Sicherheit
- Benennen ein Vorstandsmitglied, mit dem der IT-Sicherheitsbeauftragte operative Entscheidungen und Fragestellungen erörtern kann
- können dem Fachausschuss für Informationstechnologie operative Entscheidungen übertragen.

IT-Sicherheitsbeauftragter

Übernimmt die konzeptionellen und operativen Aufgaben der IT-Sicherheit.

Zu diesen Aufgaben zählen insbesondere:

- Erstellen und Pflegen einer IT-Sicherheitsleitlinie
- Sensibilisierung von Mitarbeiterinnen und Mitarbeiter sowie Führungskräften für den verantwortungsvollen Umgang mit Informationstechnik in Zusammenarbeit mit dem Datenschutzbeauftragten
- Einrichten und Weiterentwickeln der IT-Sicherheitsorganisation
- Erstellung und Pflege des IT-Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte sowie weiterer Richtlinien und Regelungen zur IT-Sicherheit
- Erstellung der Realisierungsplanung und Initiierung für IT-Sicherheitsmaßnahmen sowie die Überprüfung der Umsetzung
- Regelmäßige Überprüfung des Ist-/Soll-Zustandes

- sicherheitsrelevante Vorfälle zu untersuchen
- Ansprechpartner für alle IT-Sicherheitsfragen

Geplante Maßnahmen des IT-Sicherheitsbeauftragten sind mit den zuständigen und/oder betroffenen IT-Dienstleistern abzustimmen.

Sicherheits-Notfall-Team

Es besteht aus folgenden Mitgliedern

- IT-Sicherheitsbeauftragter - Koordination und Vorsitz
- Ein Mitglied von Klinikums- und Fakultätsvorstand
- Vertretung der betroffenen Organisationseinheiten.

In Abhängigkeit des Vorfalls können dies sein: EDV-Beauftragter, Bereichsleitung, Stationsleitung, Ltd. Oberarzt, Ärztlicher Direktor oder dessen Vertretung

- Vom IT-Sicherheitsbeauftragten festzulegende Spezialisten

Es wird durch den IT-Sicherheitsbeauftragten einberufen.

Das Sicherheits-Notfall-Team wird dann einberufen, wenn UKT oder MFT durch einen bevorstehenden oder eingetretenen Sicherheitsvorfall eine massive Gefährdung und damit ein massiver Schaden droht.

§ 5 Befugnisse

Der IT-Sicherheitsbeauftragte ist befugt einen IT-Verbund, eine Informationstechnik, eine Infrastruktur, ein IT-System oder eine Anwendung ganz oder teilweise außer Betrieb nehmen zu lassen, wenn die unter §2 Ziele, Aufgaben genannten Punkte so gefährdet sind, dass Patienten, Mitarbeitern oder UKT oder MFT ein Schaden droht. Hierüber informiert er unverzüglich den Leiter der betreibenden Organisationseinheit, die durch den Systemausfall betroffenen Organisationseinheiten sowie die Vorstände von UKT und MFT. Ist ein massiver Schaden zu erwarten oder eingetreten, beruft der IT-Sicherheitsbeauftragte unverzüglich das Sicherheits-Notfall-Team zusammen, mit dem Ziel das weitere Vorgehen bei diesem Sicherheitsvorfall zu entscheiden.

Bei einem solchen Vorfall ist der IT-Sicherheitsbeauftragte als Notfallmanager allen Mitarbeitern der betreibenden und der betroffenen Organisationseinheit hinsichtlich der Belange der IT-Sicherheit weisungsbefugt. Im Einzelnen wird dies im IT-Sicherheitskonzept beschrieben.

§ 6 Berichtspflicht

Der IT-Sicherheitsbeauftragte berichtet Klinikums- und Fakultätsvorstand einmal im Jahr zusammen mit dem Datenschutzbeauftragten. Dabei stellt der IT-Sicherheitsbeauftragte seine Informationen in einem „Managementreport IT-Sicherheit“ dar.

Bei überraschend auftretenden IT-Sicherheitsvorfällen oder aufgrund von Risiken, die aus neuen technischen Entwicklungen resultieren und nicht auf der Arbeitsebene geklärt werden können, erstellt der IT-Sicherheitsbeauftragte einen anlassbezogenen Managementreport und legt diesen Klinikums- und Fakultätsvorstand unverzüglich vor.

Bei akuten IT-Sicherheitsproblemen wird der Klinikums- bzw. Fakultätsvorstand über die Einberufung des Sicherheits-Notfall-Teams informiert.

Klinikums- und Fakultätsvorstand können bei Bedarf den IT-Sicherheitsbeauftragten verpflichten, dem Fachausschuss für Informationstechnologie in dessen Sitzung einen Bericht abzugeben.

§7 Pflicht zur Beteiligung der/des IT-Sicherheitsbeauftragten

Der IT-Sicherheitsbeauftragte ist unaufgefordert zu beteiligen, sofern die unter §2 Ziele, Aufgaben genannten Bereiche betroffen sind.

Näheres regeln die Leitlinien der IT-Sicherheit.

§ 8 Zusammenarbeit mit dem Datenschutzbeauftragten

Der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte arbeiten vertrauensvoll zusammen. Sie informieren sich gegenseitig aktiv.

Beide Arbeitsbereiche haben den Schutz der Daten als Ziel und es treten daher Überlappungen auf. Die Überlappungen sind in dem zu erstellenden Sicherheitskonzept gemeinsam zu erarbeiten und die daraus resultierenden Maßnahmen gemeinsam abzustimmen.

§ 9 Inkrafttreten

Die Geschäftsordnung tritt nach ihrer Verabschiedung durch Klinikums- und Fakultätsvorstand mit sofortiger Wirkung in Kraft.

Tübingen, den 13.04.2010

Prof. Bamberg
Leitender Ärztlicher Direktor

Prof. Autenrieth
Dekan Med. Fakultät

Sonntag
Kaufmännische Direktorin