Sicherheitsrichtlinien für die Nutzung der informationstechnischen Systeme (IT-Systeme) des Asklepios Campus Hamburg

- Persönliche Verpflichtung und Haftungsunterwerfung für Studierende der medizinischen Fakultät der Semmelweis Universität -

Hiermit verpflichte ich, der/die Unterzeichnende

……..
(Name in Druckbuchstaben)

mich dazu, folgende **Sicherheitsrichtlinien** persönlich einzuhalten:

1. Verpflichtung zur Datensicherheit und zur verantwortungsbewussten Nutzung der IT-Systeme

Die Sicherheit und der Fortbestand unseres Unternehmens sind in hohem Maße vom fehlerfreien Funktionieren der technischen Einrichtungen, speziell auch der informationstechnischen Systeme (Abk. IT-Systeme) abhängig. Dazu gehören z.B. Computer (PCs und Notebooks), Netzwerke, Software aber auch viele medizintechnische Systeme und die Telefonanlage. Durch Computerviren, Spionage und Sabotage sind diese Einrichtungen besonders gefährdet. Unsachgemäße Nutzung, bewusster und unbewusster Missbrauch der IT-Systeme erhöhen nicht nur das Gefährdungspotential. Sie verursachen erhebliche Mehrkosten für Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung und für die ausfallsichere Auslegung der informationstechnischen Komponenten. Außerdem müssen laut Datenschutzgesetz Patientendaten, personenbezogene Daten von Mitarbeitern, Kunden und Lieferanten besonders geschützt werden.
Um die Sicherheit und der Schutz der IT-Systeme und der gespeicherten Daten zu gewährleisten und die Kosten der Informationstechnologie in akzeptablen Grenzen zu halten, ist es notwendig, dass alle Mitarbeiter und Studenten unseres Unternehmens mit den IT-Systemen verantwortungsbewusst und kostenbewusst umgehen. Die nachfolgend aufgeführten Regelungen sind von allen Mitarbeitern und Studenten einzuhalten. Mit seiner Unterschrift wird dieses anerkannt:

2. Schutz der informationstechnischen Systeme

- Im IT-Netzwerk des Unternehmens und besonders auf allen Servern, Computern und Laptops dürfen nur Softwareprodukte installiert und genutzt werden, die von der Geschäftsleitung genehmigt wurden und die rechtmäßig lizenziert wurden.

- Die Installation von Software darf ausschließlich durch Personen erfolgen, die durch den Konzernbereich IT (KB IT) damit beauftragt wurden. Insbesondere gelten folgende Regelungen:

- Betriebssysteme, Anwendungsprogramme, Updates und Hotfixes dürfen nur von Mitarbeitern des KB IT installiert werden.

- Mitarbeiter und Studenten dürfen keine fremde Software aus dem Internet herunterladen oder auf anderem Weg auf Computern des Unternehmens installieren. Dazu gehören auch Bildschirm-schoner, Demoprogramme, Computerspiele oder Utilities.

- Es dürfen keine fremden Programme direkt aus dem Internet oder aus E-Mail-Anhängen gestartet werden.

- Datenbestände, die von außerhalb des Firmengeländes (z.B. auf externen Datenträgern wie externen Festplatten, Disketten, CDs, DVDs, Memory-Sticks etc.) kommen, müssen durch den Vorgesetzten überprüft werden, bevor sie verwendet werden.

- Der Nutzer sichert zu, IT-Systeme ausschließlich mit seinen persönlichen Zugangsdaten zu nutzen und sich nach Beenden der Nutzung vom IT-System abzumelden. Passwörter dürfen nicht offen einsehbar hinterlegt werden, weder als Notiz noch als Datei auf Computern oder Datenträgern. Passwörter dürfen unter keinen Umständen an Dritte weitergegeben werden.

- Der Nutzer sichert zu, dass er alle ihm im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente über die Angelegenheiten des Unternehmens, seiner Mitarbeiter, Lieferanten, Kunden und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich behandelt und geheim hält. Er versichert, dass er derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben wird, außer in Erfüllung seiner vertraglichen Pflichten. Der unverschlüsselte Transport von personenbezogenen Daten oder Wirtschaftsdaten auf Datenträgern, per E-Mail oder über Internet-Verbindungen ist verboten.

- Der Nutzer darf nicht versuchen, auf Bereiche des LANs oder WANs vorzudringen, die nicht für den Mitarbeiter/Student und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist der Vorgesetzte oder der User Help Desk ohne Verzug zu informieren.

- Bei Verdacht auf Virengefahr, Datenspionage oder anderer Umstände, die die Sicherheit der Informationstechnologie des Unternehmens betreffen, ist unverzüglich ein Vorgesetzter oder der der User Help Desk zu informieren.

- Störungen und Defekte bei IT-Systeme und auftretende Fehler in der Software sind unverzüglich den dafür verantwortlichen Personen bzw. dem User Help Desk zu berichten.

- Verlässt ein Mitarbeiter / eine Mitarbeiterin das Unternehmen, so ist mit dem Vorgesetzten die Übergabe der dienstlich verwendeten Daten zu vereinbaren, nicht mehr benötigte Datenbestände und E-Mails zu löschen und die Löschung des Benutzerkontos zu veranlassen.

- Die IT-Systeme, besonders E-Mail und der Zugriff auf das Internet, dürfen prinzipiell nicht für private Zwecke gebraucht werden. Auf den Computern dürfen prinzipiell keine privaten Daten gespeichert werden.

3. Schlussbestimmung

Bei Verletzung einer oder mehrerer dieser Verpflichtungen ist der Unterzeichner als Benutzer der IT-Systeme der Medical School gegenüber der Asklepios-Gruppe zum Ersatz des gesamten ihnen daraus entstehenden Schadens verpflichtet.

Hamburg, den ……

……
(Unterschrift)