Goethe-Universität | 60629 Frankfurt am Main
Der Vizepräsident

An
die Mitarbeitenden und Studierenden der Goethe Universität

Betreff: IT-Sicherheitsbestimmungen der Goethe-Universität

15. Juni 2017

Der Vizepräsident
Prof. Dr. Enrico Schleiff

Aktenzeichen: 8.30.55

Besucheradresse
Campus Westend | PA-Gebäude
Theodor-W.-Adorno-Platz 1
60323 Frankfurt am Main

Postadresse
60629 Frankfurt am Main
Germany

Telefon +49 (0)69 798 11104
Telefax +49 (0)69 798 11109
Schleiff@bio.uni-frankfurt.de
www.uni-frankfurt.de

Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen,
liebe Studierende,

mit stetig steigendem IT-Einsatz an der Goethe-Universität steigen auch die Abhängigkeit vom Funktionieren der IT und die Dringlichkeit der Abwendung von Schadensereignissen.

Zum 01.07.2017 tritt die IT-Sicherheitsrichtlinie der Goethe-Universität in Kraft. Sie wurde vom Sicherheits-Management-Team der Goethe-Universität basierend auf den Empfehlungen und Vorschlägen des Bundesamtes für Sicherheit und Informationstechnik erarbeitet und ist in der IT-Sicherheitsordnung unserer Hochschule verankert. Die dazugehörige Dienstvereinbarung wurde am 24.02.2017 verabschiedet.

Die IT-Sicherheitsrichtlinie ist für alle Mitglieder, Angehörige und Einrichtungen der Goethe-Universität Frankfurt gemäß Hochschulgesetz verbindlich. Die IT-Sicherheitsrichtlinie gilt darüber hinaus auch für alle externen Nutzer der IT-Infrastruktur der Goethe-Universität Frankfurt sowie für alle im Universitätsnetz betriebenen IT-Systeme.

Für die Einrichtungen ergeben sich aus dieser IT-Sicherheitsrichtlinie Verpflichtungen:

a) Bis zum 30.06.2017 (schon vor dem Inkrafttreten der IT-Sicherheitsrichtlinie) sollen alle Einrichtungen der Goethe-Universität IT-Sicherheitsbeauftragte benennen, die für die Koordination und Umsetzung der IT-Sicherheitsrichtlinie zuständig sind. Diese IT-Sicherheitsbeauftragten erhalten kontinuierlich Unterstützung und Beratung. Im Rahmen der Einführung wird auch ein umfangreiches Schulungs- und Informationsprogramm ausgerollt. Teil davon wird eine Online-Schulung sein, in der sich InteressentInnen selbständig mit den Erfordernissen vertraut machen können.

b) Bis zum 30.09.2017 (nach Inkrafttreten der IT-Sicherheitsrichtlinie) ist jedes bestehende IT-Verfahren der Goethe-Universität dem Sicherheitsmanagement-Team (SMT) über eine zentrale Online-Registrierungsplattform anzuzeigen. In einem anschließenden Zeitfenster von 2 Jahren sollen die Verfahren an die Sicherheitsstandards angepasst werden.

Für alle Nutzerinnen und Nutzer gelten die folgenden wichtigen Hinweise zum Umgang mit IT-Verfahren:

- Bitte halten Sie Ihr Virenschutzprogramm aktuell
- Bitte kontrollieren Sie regelmäßig, ob Ihre Software auf dem aktuellen Sicherheits-Stand ist und installieren Sie verfügbare Sicherheitsupdates so zeitnah wie möglich
- Beziehen Sie Software und Programme ausschließlich aus vertrauenswürdigen Quellen
- Denken Sie an das Speichern: Wichtige Daten sollten Sie ausschließlich auf dem Home-Laufwerk bzw. auf den Gruppenlaufwerken (Netzwerklaufwerken) speichern (Falls vorhanden). Ansonsten empfiehlt sich die regelmäßige Datensicherung auf mindestens einem externen Speichermedium (empfohlen sind zwei Speichermedien), das nicht dauerhaft am PC angeschlossen ist
- Bitte verwenden Sie niemals dasselbe Passwort für Accounts auf unterschiedlichen Systemen
- Gehen Sie mit Ihren Passwörtern sorgsam um – sie sollen nicht zu erraten sein und grundsätzlich niemals an andere weitergegeben werden
- Wenn Sie versehentlich auf eine Phishing Mail geantwortet haben und/oder wenn ein Befall mit Schadsoftware vorliegt, melden Sie dies bitte unverzüglich an den zuständigen IT-Support/IT-Sicherheitsbeauftragten

Für alle Verantwortliche für IT-Systeme gilt weiterhin:

- Melden Sie alle erfolgreichen Angriffe auf die IT-Systeme unverzüglich an das Sicherheits-Management-Team und das Rechenzentrum: smt@uni-frankfurt.de, it-sicherheit@rz.uni-frankfurt.de
- Sobald Sie von Sicherheitslücken in Kenntnis gesetzt werden, schließen Sie diese bitte umgehend
- Versehen Sie alle Programme mit den aktuellen Patches (inklusive Neustart der Systeme). Die jeweiligen Institutionen müssen die evtl. damit verbundenen Downtimes in Kauf nehmen – die Sicherheit der Gesamtsysteme geht vor.

Die IT-Sicherheitsrichtlinie und die Dienstvereinbarung können unter folgendem Link abgerufen werden: http://www.uni-frankfurt.de/65585653/DV-IT-Sicherheitsrichtlinie-mit-Anlage.pdf

Weitere Informationen erhalten Sie auf den Webseiten des IT-Sicherheitsmanagement-Teams der Goethe-Universität http://www.smt.uni-frankfurt.de

Mit freundlichen Grüßen

(Prof. Dr. Enrico Schleiff)