Goldene Regeln – IT-Sicherheitsgrundregeln

Nicht mit Administratorrechten arbeiten!

- Arbeiten Sie, insbesondere an Systemen mit Internetzugang, grundsätzlich mit den eingeschränkten Rechten eines normalen Benutzers

Sichere Passwörter verwenden und diese sicher speichern!

- Mindestens 8 Zeichen besser 12; bestehend aus Zahlen, Buchstaben und Sonderzeichen
- im dienstlichen Umfeld niemals Passwörter aus dem privaten Bereich verwenden
- Nutzen Sie zur Speicherung von Kennworten einen Passwortmanager wie bspw. Keepass

Seien Sie bei E-Mails kritisch bis misstrauisch!

- Prüfen Sie den Absender sorgfältig auf Echtheit; Klicken Sie in E-Mails niemals auf Links oder Anhänge, es sei denn Sie haben den Absender zuverlässig überprüft
- Keine zweifelhaften E-Mails bearbeiten oder beantworten
- Aktuell im Umlauf befindliche gefährliche E-Mais: **www.h2.de/schadmails**

Gehen Sie bewusst mit sensiblen Daten um!

- Speichern Sie dienstliche Daten immer sicher vor dem Zugriff von Unbefugten
- Nutzen Sie zur Speicherung und Austausch von Daten/Dokumenten die von unserer Hochschule bereitgestellten Netzlaufwerke oder die Nextcloud der HS
- Speichern Sie schützenswerte (z.B. personenbezogene) Daten NIEMALS bei Cloud-Anbietern wie Dropbox, Google Drive, Microsoft OneDrive oder auf privaten Geräten

Halten Sie Ihr System aktuell und beachten Sie Systemhinweise!

- Installieren Sie auf Ihren Systemen regelmäßig Sicherheitsupdates
- Beachten Sie Systemmeldungen zur Installation von Updates bzw. zum Neustart

Softwaredownloads nur von vertrauenswürdigen Quellen!

- Installieren Sie Software nur aus vertrauenswürdigen Quellen – etwa den im Smartphone oder PC voreingestellten App-Stores der Hersteller
- Prüfen Sie welche Funktionen und Rechte die jeweilige App beansprucht

Virenscanner einsetzen und aktuell halten!

- Schützen Sie Ihren Rechner vor Infizierung mit Schadsoftware wie Viren, Würmern und Trojanischen Pferden durch die Nutzung eines Scanners wie bspw. Microsoft Defender
- Wichtig! Automatische Updates aktivieren und deren Ausführung regelmäßig überprüfen

Daten regelmäßig sichern!

- alle zentral bereitgestellten Speicherbereiche (Netzlaufwerke, Nextcloud) werden täglich automatisch durch das ITM gesichert

Bei einem Sicherheitsvorfall oder bei Unsicherheit/Fragen: Wenden Sie sich an Fachleute!

- Ihre Ansprechpartner sind: DV-Organisatoren, IT-Sicherheitskoordinatoren der Bereiche
- Alle Mitarbeiter des ITM und speziell der IT-Sicherheitsverantwortliche der HS
- Kontakt: it-sicherheit@h2.de oder Tel. +49 391 886 4977)

Ausführliche IT-Sicherheitsregeln nachlesen unter: **www.h2.de/it-sicherheit**