

Belehrung : Hinweise und Regeln für die Arbeit mit den DV-Ressourcen des Institutes für Technische Chemie der Universität Leipzig

Die Rechentechnik des Institutes für Technische Chemie der Universität Leipzig (ITCL) steht allen Mitarbeitern, berechtigten Studenten und berechtigten Gästen des Institutes zur Verfügung. Gäste und Studenten müssen beim Verantwortlichen für die Rechentechnik des Institutes (Herrn Moros: TA Zi 526, Tel.: 0341 97 36 329) ein LOGIN und eine zeitlich befristete Nutzungsberechtigung beantragen.

Die DV-Ressourcen des Institutes werden Studenten, Mitarbeitern und Gästen nur für die Erfüllung von Aufgaben innerhalb der studentischen Ausbildung bzw. den Mitarbeitern und Gästen nur für Erfüllung dienstlicher Aufgaben bereitgestellt.

1. Der Zugang zum Hochschulnetz und die Nutzung der Arbeitsplatzrechner ist nur über das personengebundene LOGIN gestattet. Das mit dem LOGIN-Kennzeichen verbundene Paßwort ist geheim zu halten. **Die Arbeit mit einem fremden LOGIN-Kennzeichen bzw. die Weitergabe des LOGIN-Kennzeichen führt zum Entzug der Nutzungsberechtigung. Eine mißbräuchliche Nutzung der DV-Ressourcen (siehe Anhang I) kann ebenfalls zum Entzug der Nutzungsberechtigung führen oder auch gerichtliche Konsequenzen nach sich ziehen.**

2. Für die Benutzung der zur Verfügung gestellten Rechentechnik sollten die Empfehlungen zur Nutzung (Anhang II) beachtet werden.
3. Die gesamte zur Verfügung gestellte Software unterliegt den Copyright-Bestimmungen. Die Nutzung fremder Software muß schriftlich mit einem Nachweis der Lizenzierung beim Rechnerverantwortlichen (s.o.) beantragt werden. Eigene Datenträger (Disketten/CD/DVD/..) müssen vor Benutzung auf einem bereitgestellten PC auf Virenbefall überprüft werden.
4. Das Nichtbeachten der Nutzungshinweise kann zum Ausschluß von der weiteren Arbeit mit den DV-Ressourcen des ITCL und zur Sperrung des LOGINs führen.

Anhang I:

Die nachstehend aufgeführten Tatbestände stellen eine mißbräuchliche Nutzung der DV-Ressourcen des ITCL dar. Dabei wird mit nachfolgender Aufzählung keine Vollständigkeit beansprucht. In jedem Einzelfall kann ein Mißbrauch auch die Verletzung strafrechtlicher oder zivilrechtlicher Bestimmungen beinhalten.

- eigenmächtige Installation von Software, die Benutzung privater Hardware.
- das Ausspähen von Daten, das Mithören von Datenübermittlungen; die Weitergabe unberechtigt verschaffter oder erhaltener Daten
- das Auskundschaften von Schwachstellen in Systemen sowie die Aktivierung hierfür geeigneter Software
- die Verletzung der Integrität von Daten durch Verändern oder Löschen; die Störung des laufenden DV-Betriebs (Computersabotage); die Manipulation von Programmen oder Daten in betrügerischer Absicht (Computerbetrug); die unbefugte Nutzung von DV-Systemen und der unautorisierte Zugang zu Netzdiensten
- die Bereitstellung und der Abruf von urheberrechtlich geschützten Daten (Programmen, Texten, Bildern etc.) ohne Freigabe einer entsprechenden Verwendung durch den Urheber
- die Herstellung oder Verbreitung von Raubkopien
- die unbefugte Speicherung, Veränderung, Übermittlung und Verarbeitung geschützter personenbezogener Daten; die Vernachlässigung der gebotenen Sorgfaltspflicht bei der berechtigten Verarbeitung personenbezogener Daten

- die Verbreitung von Informationen pornographischen, jugendgefährdenden, gewalt-verherrlichenden, rassistischen, den demokratischen Rechtsstaat oder die öffentliche Ordnung gefährdenden Inhalts; die Verarbeitung oder Abspeicherung solcher Informationen mit Hilfe der DV-Ressourcen des ITCL
- die Verletzung der Persönlichkeitsrechte eines einzelnen durch Verbreitung ehrkränkender Werturteile oder Tatsachenbehauptungen
- Belastung von Netzen durch übermäßige Verbreitung (gezielte oder ungezielte) von Informationen (Informationsverschmutzung). Die Nutzung des Internet darf nur unter Anerkennung der "Netikette" (nachzulesen unter <http://www.uni-leipzig.de/netikett.htm>) erfolgen
- Verbreitung und Speicherung von für Forschung, Lehre und Studium irrelevanten Informationen; Verteilen nicht ausdrücklich angeforderter Werbung
- Nutzung der Ressourcen für kommerzielle Zwecke
- Änderungen an der Systemsoftware, unangekündigtes Experimentieren mit den DV-Ressourcen; Nutzung von Spielsoftware
- Mißachtung bereitgestellter Schutz- und Prüfmechanismen gegen Computerviren

Anhang II : Empfehlungen / besondere Verbote

VIREN: Der Betrieb eines Rechners sollte nur mit installierter und aktivierter Anti-Virensoftware erfolgen.

DATEN: Jeder ist selbst für seine Daten verantwortlich. Es wird jedoch empfohlen regelmäßig Sicherheitskopien der eigenen Datenbestände durchzuführen.

Betriebssystem: Regelmäßige Updates (Sicherheitspatches, Sicherheitspakete,..)

Passwortregeln:

- 1) **Jeder User muß ein eigenes User-ID/Passwort besitzen**
- 2) nicht Nachnamen und Vornamen verwenden als Passwort
- 3) nicht **gast user admin**
- 4) kein leeres Passwort
- 5) mindestens 6 Zeichen lang
- 6) möglichst Buchstaben in Kombination mit Zahlen
- 7) Passworte nicht öffentlich zugänglich aufbewahren
- 8) Passworte sind Privatsache
- 9) Passworte auch für Bildschirmschoner aktivieren

besondere VERBOTE:

- 1) Installation jeder Art von Serversoftware
- 2) Installation von Viren
- 3) Installation von Trojaner
- 4) Installation von Passwort-Schnüffelprogrammen
- 5) Keine Videos, Bilder, Musik, die nicht zum Arbeitsgebiet gehören
- 6) Kein IRC + ICQ
- 7) keine Portscanner