## Motivation

Aus der Arbeitswelt ist IT nicht mehr wegzudenken. Damit Daten und IT-Systeme sicher sind, müssen auch die Nutzer einige „Spielregeln" einhalten. Technische Sicherheitsmaßnahmen allein nützen wenig, wenn beispielsweise mit Passworten sorglos umgegangen wird. Worauf geachtet werden muss, steht in der IT-Sicherheitsrichtlinie[1)] der Freien Universität Berlin. Im vorliegenden Flyer finden Sie die wichtigsten Regeln für IT-Anwender in Kurzform. Datenschutz erfordert IT-Sicherheit als Grundlage und ist insoweit in die IT-Sicherheitsrichtlinie der Freien Universität Berlin integriert.

Ihre AG IT-Sicherheit

## Ansprechpartner

- Akute Sicherheitsprobleme:
  Infoservice IT
  Tel.: 838-77777 (Hotline)
  E-Mail: hilfe@zedat.fu-berlin.de
- Weitergehende Fragen:
  Die/Der IT-Beauftragte Ihres (Fach-)Bereichs[2)]

---

1) *www.fu-berlin.de/it-sicherheit/IT-Sicherheitsrichtlinie*
2) *www.fu-berlin.de/it-sicherheit/IT-Beauftragten-Liste*
3) *www.fu-berlin.de/it-sicherheit/Cloud-Papier*
4) *www.zedat.fu-berlin.de*

Verfasser: AG IT-Sicherheit Stand: 2013

Freie Universität Berlin

# Praxistipps zur IT-Sicherheit

IT-Sicherheit

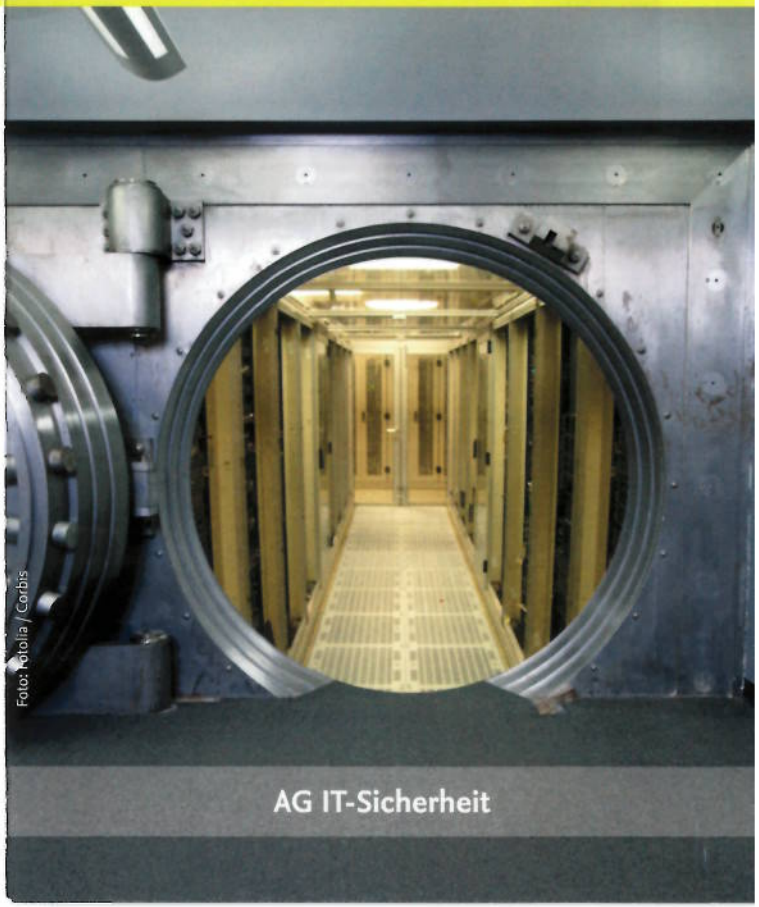


Foto: Fotolia / Corbis

AG IT-Sicherheit

## Worauf Sie achten sollten

### Passworte
- Persönliche Passworte dürfen nicht weitergegeben werden.

### E-Mail-Adressen
- Bei universitären Angelegenheiten muss die FU Mail-Adresse verwendet werden.
- Universitäre Angelegenheiten umfassen alle Tätigkeiten im Zusammenhang mit Forschung, Lehre, Studium und Verwaltung.

### Datenablage in der Cloud[3)]
- Nicht alle Daten eigenen sich zur Ablage in der Cloud.
- Sensible Daten dürfen nur verschlüsselt abgelegt werden.
- Bestimmte Daten (z. B. Personalakten) dürfen auf keinen Fall in der Cloud abgelegt werden.

### Datenablage auf mobilen Geräten und Medien
- Sensible Daten dürfen nur verschlüsselt auf Notebooks, Smartphones, USB-Sticks usw. abgelegt werden.

### Verantwortungsvoller Softwareeinsatz
- Achten Sie auf eine vertrauenswürdige Softwarequelle. Nicht jedes beliebige Programm darf installiert werden.

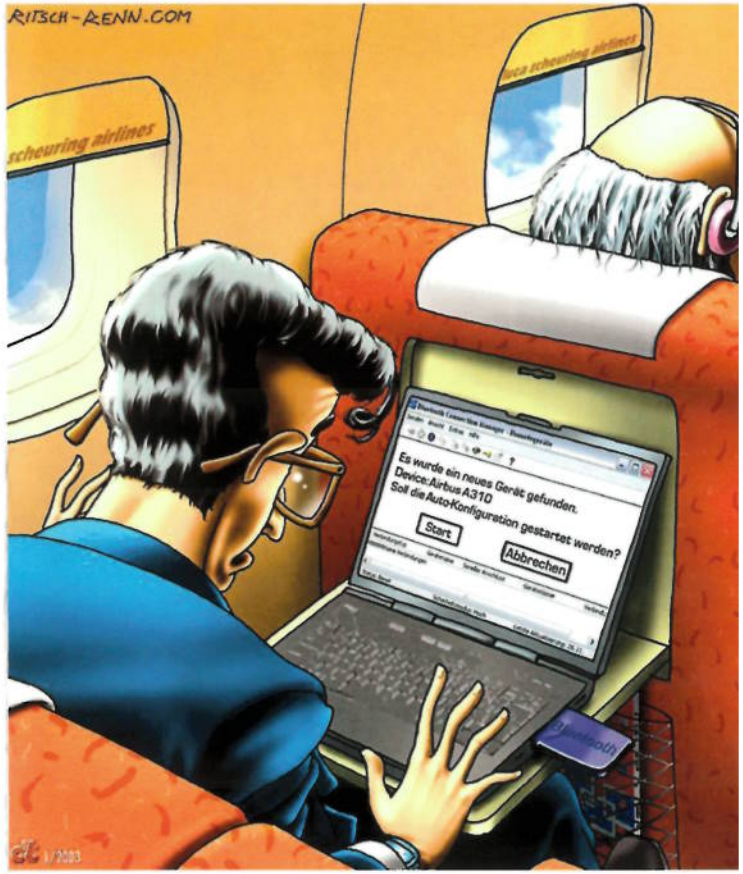
### Schutz vor Schadprogrammen
- Der Rechner muss durch einen modernen Virenscanner geschützt sein, der sich automatisch aktualisiert.
- Alle Mitglieder der Freien Universität Berlin können den von der ZEDAT[4)] angebotenen Virenscanner kostenlos nutzen – auch für private Zwecke.

### Abmelden und Ausschalten
- Unbeaufsichtigte laufende Geräte müssen gesperrt werden oder anderweitig vor unbefugtem Zugriff geschützt werden.

### Zugriffsschutz mobiler Geräte
- Handys, Laptops usw. müssen durch Passworte vor unbefugtem Zugriff geschützt werden, soweit sie IT-Ressourcen der Freien Universität Berlin nutzen.

### Verlust eines mobilen Geräts
- Der Verlust dienstlicher mobiler Geräte ist unverzüglich der zuständigen Stelle zu melden.

### Datensicherung
- Wichtige Daten sollten zuverlässig gesichert werden. Eine sehr gute Möglichkeit dazu bieten zentral angebotene Speichersysteme.
- Wenn keine zentralen Speichersysteme zur Verfügung stehen, müssen die Daten zusätzlich zur Speicherung auf der Festplatte auf ein weiteres Speichersystem gesichert werden (z. B. USB-Stick, DVD).


### Abgabe eines Rechners
- Bei Abgabe eines Rechners, zum Beispiel zu Reparaturzwecken an externe Dienstleister, ist dafür zu sorgen, dass sensible oder wichtige Daten gesichert und anschließend von der Festplatte gelöscht werden.

### Löschen und Entsorgen von Datenträgern
- Es muss sichergestellt werden, dass Datenträger, wie USB-Sticks, CDs, DVDs und dergleichen, fachgerecht entsorgt werden, damit Unbefugte keinen Zugriff auf die gespeicherten Daten erhalten.