Freie Universität Berlin

Recommendations for IT Security

IT Security

Motivation

Information technology (IT) has become an integral part of the workplace. To maintain the security of data and IT systems, users must obey certain "rules of the game". Technical security measures alone are of little benefit, if (for instance) passwords are carelessly managed. The issues to be considered are detailed in the IT Security Principles [1)] published by the Freie Universität Berlin. This current flyer briefly summarizes the most important principles for new users. IT security forms a fundamental basis for data privacy, which thus has been integrated into the IT Security Principles of the Freie Universität Berlin.

The IT Security Workgroup

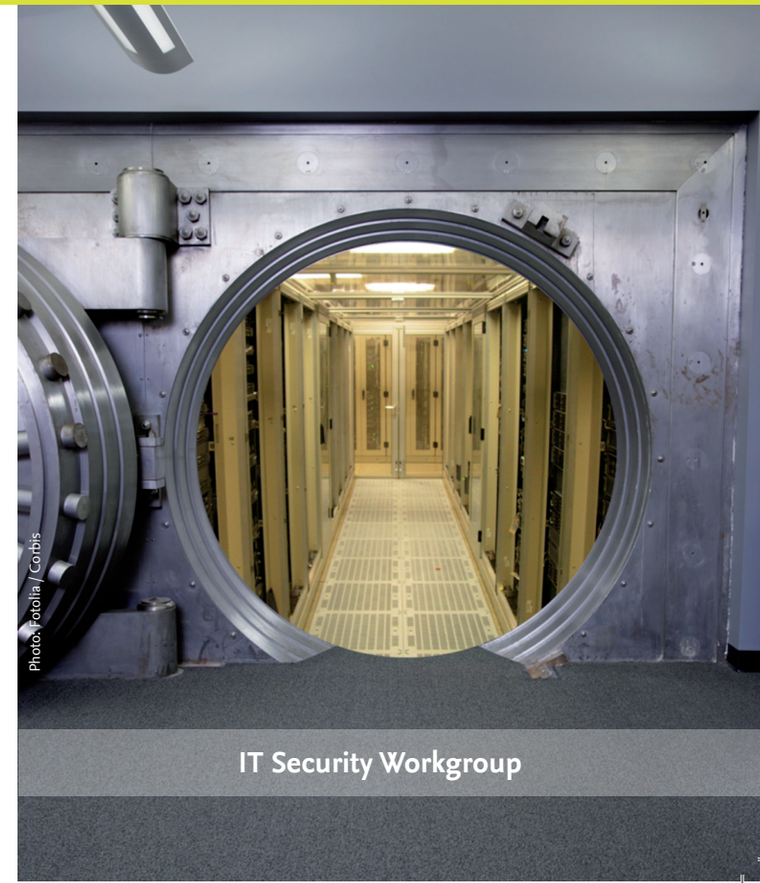
Contacts

- Urgent security problems:
  IT information service
  Tel.: (030) 838-77777 (Hotline)
  E-mail: hilfe@zedat.fu-berlin.de
- For further questions, please consult the designated IT representative for your department [2)]

---

1) *www.fu-berlin.de/it-sicherheit/IT-Sicherheitsrichtlinie (IT Security Principles)*
2) *www.fu-berlin.de/it-sicherheit/IT-Beauftragten-Liste (List of IT Representatives)*
3) *www.fu-berlin.de/it-sicherheit/Cloud-Papier (Use of Data Clouds)*
4) *www.zedat.fu-berlin.de*

Published by:
The IT Security Workgroup of the Freie Universität Berlin
2013



Please pay careful attention to the following:

Passwords
- Personal passwords should not be shared or communicated in any way.

E-mail addresses
- The FU e-mail address should be used for all issues concerning the university.
- University matters include all activities in connection with research, instruction, studies, and administration.

Data storage in the Cloud [3)]
- Cloud data storage is not suitable for all types of information.
- Sensitive data should be stored in clouds only in encrypted form.
- Certain types of data (such as personnel files) are not to be stored in a cloud under any circumstances.

Data storage on mobile devices and transportable media
- Sensitive data should be stored only in encrypted form on notebooks, laptops, smart phones, or USB sticks, etc.

Responsible use of software
- Take care to use reliable software sources. Some programs can cause problems and should not be installed.

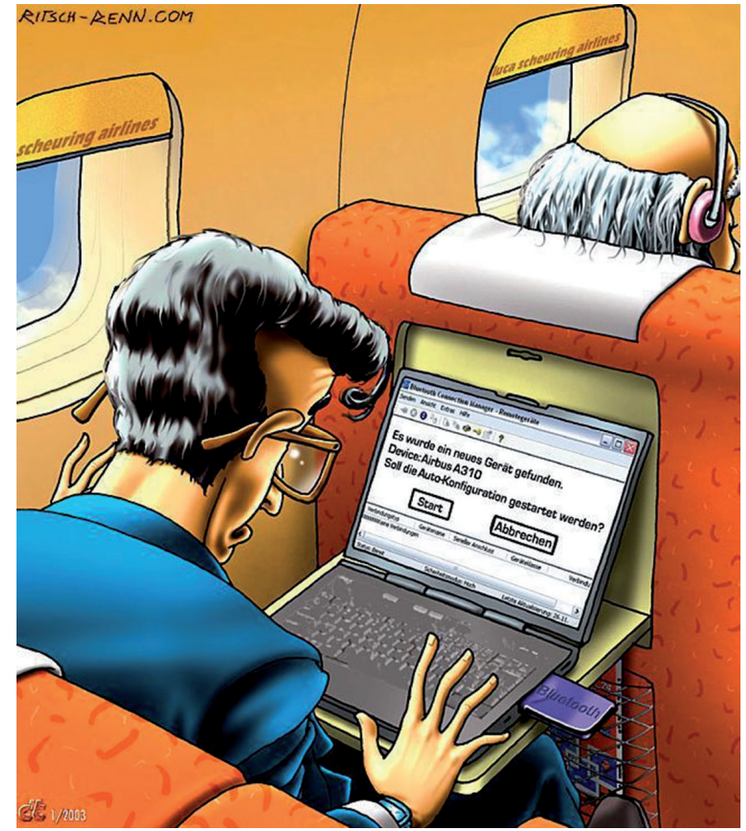
Protection from malicious software
- Every computer should be equipped with a modern virus scanner that is automatically updated on a continual basis.
- Every member of the Freie Universität Berlin may use the virus scanner offered by ZEDAT [4)] free of charge, including for personal use.

Logging out and shutting down
- Unsupervised devices must be protected from unauthorized access or use.

Access protection for mobile devices
- Mobile telephones, notebooks, laptops, etc. must be secured against unauthorized use with passwords, in as much as they access IT resources of the Freie Universität Berlin.

Loss or misplacement of mobile devices
- The loss of any work-related mobile device must be reported immediately to the appropriate authorities.

Data backups
- Important data should be backed up in a reliable manner. One very good option is to use centralized data storage systems.
- If no central data storage system is available, then in addition to local hard disk storage, the data should be backed up to an further storage medium, such as USB stick or DVD.



External computer transfers
- If a computer is transferred to any third party (such as to an external company for the purpose of service or repair), then all important or sensitive data must be backed up and then irretrievably deleted from the hard disk.

Deletion and disposal of data and data carriers
- Data carriers and media to be discarded, such as USB sticks, CDs, DVDs, etc., must be appropriately disposed of, so that no unauthorized individuals can obtain access to the stored data.