

safelT – Awareness program

IT House Rules / Use of IT resources at ETH Zurich

IT-Hausregeln / Umgang mit IT-Mitteln an der ETH Zürich

www.safeit.ethz.ch →

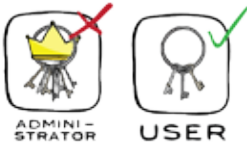


Halte dich an die geltenden Regeln

- Informiere dich über die geltenden Regeln — im Speziellen über die Benutzungsordnung für Telematik (BOT).
- Sei dir bewusst, dass du für dein Handeln persönlich verantwortlich bist.
- Respektiere die Privatsphäre der Anderen.

Adhere to applicable rules

- *Inform yourself regarding the applicable rules, especially the ETH Acceptable Use Policy (BOT).*
- *Be aware that you are responsible for your actions.*
- *Respect the privacy of others.*



Vermeide Missbrauch von Geräten und Passwörtern

- Wähle nur schwer zu erratende Passwörter, halte sie geheim und beachte die Passwort-Regeln.
- Benutze einen passwortgeschützten Bildschirm-schoner, falls du deinen Arbeitsplatz verlässt.
- Melde dich vom System ab oder schalte den Computer aus, wenn du abwesend bist oder das Gerät nicht benötigst.

Avoid the misuse of systems and passwords

- *Select passwords which are difficult to guess. Keep them secret and observe password rules.*
- *Use a password protected screen saver when you leave your workplace.*
- *Logout or turn off computers when you are absent or do not need to use the system.*

Handle vorausschauend

- Stelle sicher, dass der Virens scanner regelmässig aktualisiert wird und schalte diesen wichtigen Schutz auf keinen Fall aus.
- Sorge dafür, dass dein Gerät auf dem aktuellsten Stand des Betriebssystems und der Applikationen gehalten wird (Patches, Updates usw.).
- Schalte alle Programme und Dienste ab, die du nicht für deine Arbeit benötigst.

Think and act with foresight

- *Make sure virus scanner software is being updated regularly. Never disable such security features.*
- *Ensure that systems and applications are updated to current level (Patches, Updates, etc.).*
- *Turn off unnecessary applications and services which are not needed for your work.*



Behandle Informationen und Geräte mit Sorgfalt

- Lass mobile Geräte (Laptop, iPad, Handy usw.) niemals unbeaufsichtigt.
- Schütze wichtige Informationen, wie persönliche Daten vor Missbrauch. Das gemeinsame Benutzen von Accounts ist nicht erlaubt.
- Erstelle regelmässig Sicherheitskopien von deinen Daten (Backup).

Handle information and systems with care

- *Do not leave mobile devices (Laptop, iPad, Cell Phone, etc.) unattended.*
- *Protect important information (such as personal data) from misuse. Account sharing is not allowed.*
- *Backup important data in a safe place regularly.*

Gebrauche nur legal bezogene Produkte

- Respektiere Urheberrechte und Lizenzen von Software-Produkten und Daten.
- Benutze nur Programme und Daten zu deren Gebrauch du berechtigt bist.

Use only legally obtained (licensed) products

- *Respect copyright and license restrictions of applications and data.*
- *Use programs and data for their intended use and for which you are authorized.*



Crack
Downloader



Benutze E-Mail und Internet mit Vorsicht

- Denk daran, dass E-Mail-Anhänge Viren, schädliche Programme (Malware) oder gefährliche Links enthalten können.
- Behandle Programme und Daten, die aus dem Internet geladen werden, mit Vorsicht und beachte die geltenden Bestimmungen.
- Ignoriere jegliche Aufforderung, Zugangsdaten (Username / Passwort) bekannt zu geben.

Use email and Internet cautiously

- *Never forget that email can include links to unsafe web sites or that email attachments can include potentially harmful programs (Malware).*
- *Programs and data downloaded from the Internet should be handled with care and adhere to contractual terms of the product.*
- *Ignore any request to reveal your credentials (username / password).*

Melde Vorfälle sofort

- Betrachte Verstöße gegen die Integrität oder Vertraulichkeit als einen Vorfall.
- Melde sicherheitsrelevante Vorfälle sofort der für dich zuständigen Stelle oder deiner/deinem Vorgesetzten.
- Melde (mögliche) Viren-Infektionen und/oder entdeckte Malware der für deinen Bereich verantwortlichen IT-Supportstelle.

Report incidents immediately

- Consider offenses against integrity and confidentiality as an incident.
- Report security relevant incidents to your local support group or your supervisor.
- Report (possible) virus infections and/or detected malware to your responsible IT support group.

Informiere dich über Cloud Computing und Social Media

- Prüfe die rechtlichen Bedingungen des Providers und kläre, ob diese in Einklang mit ETH-Vorschriften sind. Es gilt das Recht des Speicherortes.
- Personal- und Finanzdaten, sowie Daten Dritter mit vertraglicher Geheimhaltungsvereinbarung dürfen die ETH nicht verlassen (auch nicht verschlüsselt).
- Forschungsdaten müssen zur Nachvollziehbarkeit jederzeit im Zugriff der ETH Zürich bleiben.

Inform yourself about Cloud Computing and Social Media

- Inform yourself regarding legal requirements of providers and make sure these are conform with ETH regulations. Laws are imposed in the country of storage origin!
- Personnel and financial data, as well as data from third parties with nondisclosure agreements, are not allowed to leave ETH (not even encrypted).
- Access to research data must always be available to ETH Zurich due to traceability.



safelT Awareness Cartoons safelT Poetry Slam

Die Regeln gibt es auch in animierter Form.

You can find the rules in animated versions.

www.video.ethz.ch/campus/safelT →

safelT ist eine Aktion zur Förderung der
Informationssicherheit an der ETH Zürich.

safelT is a campaign for promoting
information security at ETH Zurich.

See also «Protect your brainwork. IT Security Initiative»

<https://itsecurity.ethz.ch> →

Kontakt / Contact

ETH Zürich

Informatikdienste, ID Service Desk

IT Services, ITS Service Desk

Phone +41 44 632 77 77 / 2 77 77 (internal)

E-Mail servicedesk@id.ethz.ch

Web www.id.ethz.ch →

ID Netzwerksicherheitsgruppe / ITS Network Security Group

E-Mail security@id.ethz.ch

Web www.safelT.ethz.ch →

