Melden Sie Vorfälle sofort

- Betrachten Sie Verstösse gegen die Vertraulichkeit oder unerwartete Veränderungen von Daten als einen Vorfall.
- Melden Sie sicherheitsrelevante Vorfälle oder einen Verdacht darauf sofort der für Sie zuständigen IT-Supportstelle.

Report incidents immediately

- *Consider breaches of confidentiality or unexpected changes to data as an incident.*
- *Report any security-related incidents or suspicions immediately to your IT support.*

Informieren Sie sich über Cloud-Computing und Soziale Medien

- Prüfen Sie die rechtlichen Bedingungen des Providers und klären Sie, ob diese in Einklang mit Vorschriften der ETH Zürich sind.
- Die Auslagerung von sensitiven Daten der ETH Zürich ist nicht zulässig (Compliance Guide →). Verwenden sie für solche Daten die ETH-eigene polybox oder andere interne ETH-Services.
- Beachten Sie die Social-Media-Richtlinien ETH Zürich.

Inform yourself about Cloud Computing and Social Media

- *Check the legal conditions of the provider and clarify whether they comply with ETH Zurich regulations.*
- *The outsourcing of sensitive data of ETH Zurich is not permitted (Compliance Guide →). For such data, use ETH's own polybox or other internal ETH services.*
- *Please observe the Social-Media Guidelines ETH Zurich.*

PROTECT YOUR BRAINWORK.

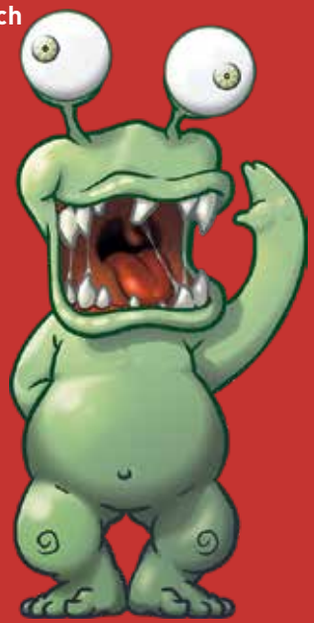
itsecurity.ethz.ch →

Rechtliches / Legal Documents (BOT)

Weisung Informationssicherheit / Compliance Guide

www.id.ethz.ch/guidelines/it-security →
www.its.ethz.ch/guidelines/it-security →

Kontakt / Contact
ETH Zürich
Informatikdienste, ID Service Desk
IT Services, ITS Service Desk
Phone +41 44 632 77 77
Intern 2 77 77
E-Mail servicedesk@id.ethz.ch
Web www.id.ethz.ch →



Circulation 8000 (1.0/2019)
Editors: A. Harder, S. Sheridan, S. Hoffmann, IT Services
Order brochures at kundenkommunikation@id.ethz.ch

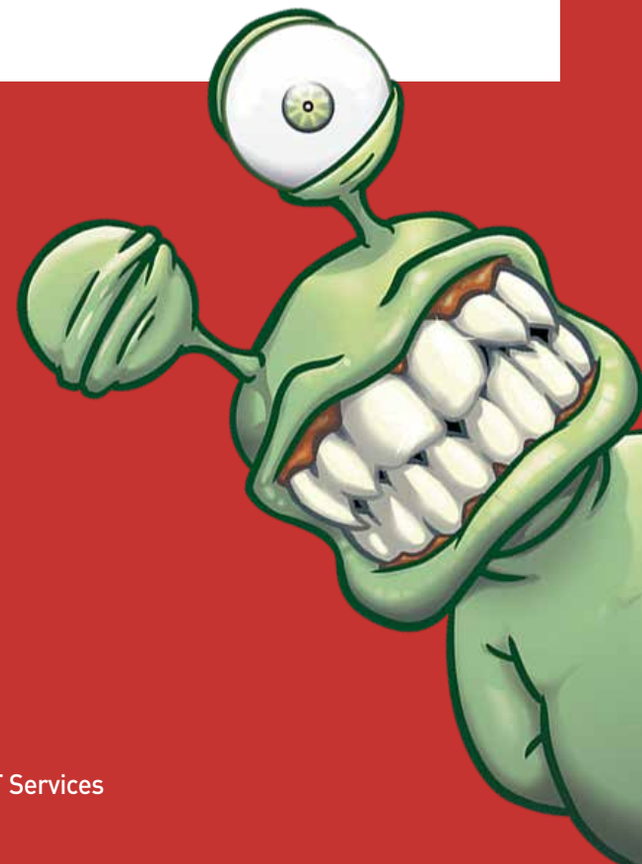
ETH zürich

PROTECT YOUR BRAINWORK.

Hausregeln
Informationssicherheit

House Rules
Information Security

ethz.ch/itsecurity →



IT Services

1

Halten Sie sich an die geltenden Regeln

- Informieren Sie sich über die geltenden Regeln, im Speziellen über die (BOT →).
- Seien Sie sich bewusst, dass Sie für Ihr Handeln persönlich verantwortlich sind.
- Respektieren Sie die Privatsphäre der anderen.

Adhere to applicable rules

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

2

Verhindern Sie den Missbrauch von Geräten und Passwörtern

- Wählen Sie nur schwer zu erratende Passwörter, halten Sie sie geheim und beachten Sie die Passwortregeln →.
- Benutzen Sie einen passwortgeschützten Bildschirmschoner immer, wenn Sie Ihren Arbeitsplatz verlassen.
- Melden Sie sich vom System ab oder schalten Sie den Computer aus, wenn Sie abwesend sind oder das Gerät nicht benötigen.

Avoid the misuse of systems and passwords

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

3

Halten Sie alle Ihre Systeme immer auf aktuellem Sicherheitsstand

- Stellen Sie sicher, dass die Virenscanner regelmässig aktualisiert werden und schalten Sie diesen wichtigen Schutz auf keinen Fall aus.
- Sorgen Sie dafür, dass die Betriebssysteme und Applikationen Ihrer Geräte immer aktuell sind.
- Schalten Sie alle Programme und Dienste ab, die Sie für Ihre Arbeit nicht benötigen.

Always keep your systems up to date

- *Make sure the virus scanner software is being updated regularly. Never disable such security features.*
- *Ensure that systems and applications are updated to current versions.*
- *Turn off all programmes and services that you do not need for your work.*

4

Schützen Sie Ihre Informationen vor Missbrauch

- Gewähren Sie nur Berechtigten Zugriff.
- Lassen Sie mobile Geräte wie Laptops, Smartphones oder USB-Sticks niemals unbeaufsichtigt.
- Nutzen Sie Bildschirmfilter.
- Verschlüsseln Sie sensitive Informationen.
- Erstellen Sie regelmässig Sicherheitskopien.
- Beachten Sie Vertraulichkeitsvermerke in Dokumenten und klassifizieren Sie Ihre Dokumente beim Erstellen.

Protect your information from misuse

- *Grant access only to authorised persons.*
- *Never leave mobile devices such as laptops, smartphones or USB sticks unattended.*
- *Use screen filters.*
- *Encrypt sensitive information.*
- *Make backups regularly.*
- *Observe confidentiality notices in documents and classify your documents as they are created.*

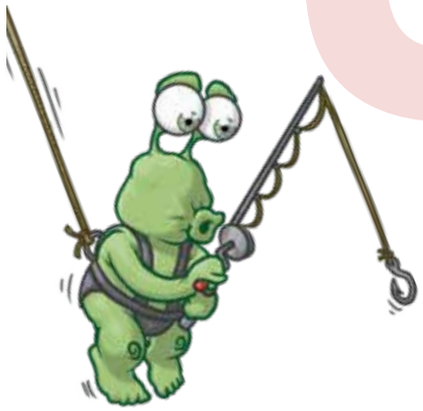
5

Benutzen Sie nur legal bezogene Produkte

- Respektieren Sie Urheberrechte und Lizenzen.
- Benutzen Sie nur Programme und Daten zu deren Gebrauch Sie berechtigt sind.

Use only legally obtained (and licensed) products

- *Respect copyright and license restrictions.*
- *Use only programmes and data for which you are authorised and for their intended use.*



6

Benutzen Sie E-Mail, Internet und Speichermedien mit Vorsicht

- Denken Sie daran, dass E-Mail-Attachments Schadprogramme enthalten können.
- Absender von E-Mails können gefälscht sein. Überprüfen Sie diese, z.B. indem Sie mit der Maus darüberfahren.
- Kontrollieren Sie, wohin Links führen, bevor Sie darauf klicken.
- Laden Sie Programme und Daten vom Internet oder von USB-Sticks nur aus vertrauenswürdigen Quellen.
- Scannen Sie Downloads und externe Speichermedien mit Ihrem Virenschutzprogramm.

Use email, Web and storage media with caution

- *Remember that email attachments may contain malware.*
- *Senders of emails can be fake. Check them, e.g. by moving the mouse over them.*
- *Check where links lead before you click on them.*
- *Download programs and data from the Internet or USB sticks only from trusted sources.*
- *Scan downloads and external storage media with your antivirus software.*