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.
- Leiten Sie Phishing-E-Mails als Anhang an phishing@ethz.ch weiter.

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.*
- *Forward phishing emails as attachment to phishing@ethz.ch.*

Informieren Sie sich über Cloud-Computing

- Prüfen Sie die rechtlichen Bedingungen des Providers und klären Sie, ob diese in Einklang mit Vorschriften der ETH Zürich sind. Es gelten hier die IT-Richtlinien und IT-Grundschutzvorgaben.
- Lagern Sie interne oder vertrauliche ETH-Daten (z.B. Forschungsdaten, die einer Geheimhaltung unterliegen, Finanz-, personenbezogene Mitarbeitenden- oder Studierendendaten, Benotungen etc.) nur in entsprechend geprüfte und dafür freigegebene Cloud-Dienste oder nutzen Sie die ETH polybox. Informieren Sie sich entsprechend bei Ihrer IT-Supportstelle.
- Streng vertrauliche Daten dürfen nicht in die Cloud.

Inform yourself about Cloud Computing

- *Check the legal conditions of the provider and clarify whether they comply with ETH Zurich regulations. Here, please check the IT guidelines and IT baseline protection rules.*
- *Only store internal or confidential data of ETH Zurich (e.g. research data subject to secrecy, financial, personal employee or student data, evaluations) in appropriately tested and approved cloud services or use ETH polybox. Please inform yourself accordingly by contacting your IT support.*
- *Strictly confidential data are not to be stored in the cloud.*

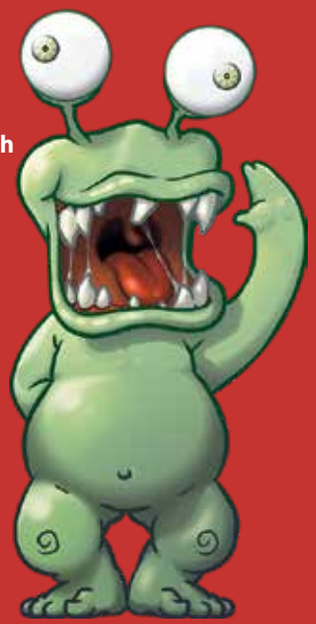
PROTECT YOUR BRAINWORK.

www.ethz.ch/training-it-security

Informationssicherheit an der ETH Zürich

www.ethz.ch/staffnet/de/service/informationssicherheit.html

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



© ETH Zürich, 1.0 / Juni 2024
Circulation 8000 (1.0/2024)
Editors: A. Harder, K. Noack, S. Sheridan, S. Hoffmann, IT Services
Order brochures at kundenkommunikation@id.ethz.ch

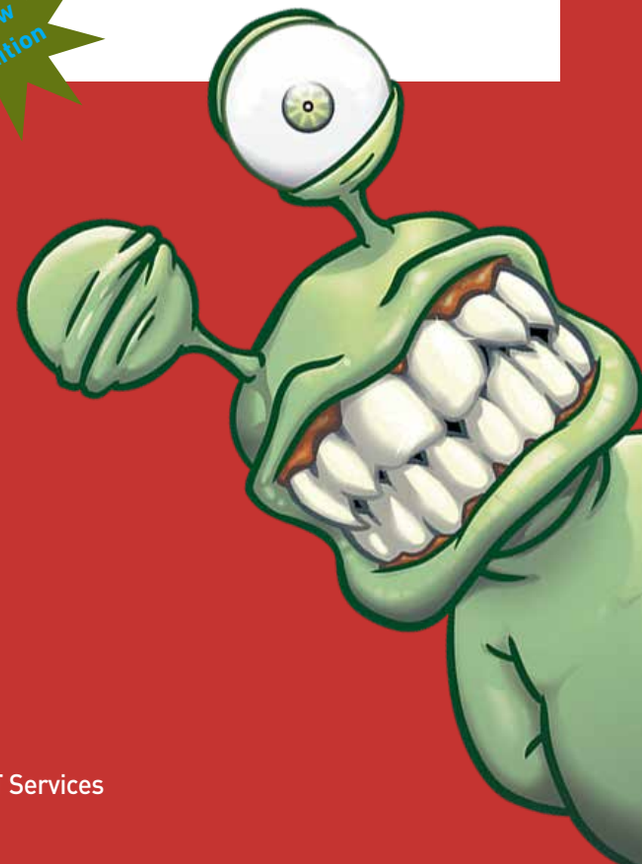
ETH zürich

PROTECT YOUR BRAINWORK.

Hausregeln
Informationssicherheit

House Rules
Information Security
www.ethz.ch/training-it-security

New Edition



IT Services

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.
- Beachten Sie die Social-Media-Richtlinien ETH Zürich.

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.*
- Please observe the Social-Media guidelines ETH Zurich.

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.
- Nutzen Sie Bildschirmfilter.
- 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.*
- *Use screen filters.*
- *Logout or turn off computers when you are absent or do not need to use the system.*

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.*

Schützen Sie Ihre Informationen vor Missbrauch

- Gewähren Sie nur Berechtigten Zugriff.
- Lassen Sie mobile Geräte wie Laptops, Smartphones oder USB-Sticks niemals unbeaufsichtigt.
- Verschlüsseln Sie vertrauliche und streng vertrauliche Informationen.
- Erstellen Sie regelmässig Sicherheitskopien.
- Beachten Sie Vertraulichkeitsvermerke in Dokumenten und klassifizieren Sie Ihre Dokumente beim Erstellen.
- Beachten Sie hierzu die Weisung Informationssicherheit und deren Anhänge.

Protect your information from misuse

- *Grant access only to authorised persons.*
- *Never leave mobile devices such as laptops, smartphones or USB sticks unattended.*
- *Encrypt confidential and strictly confidential information.*
- *Make backups regularly.*
- *Observe confidentiality notices in documents and classify your documents as they are created.*
- *Please check the directive on Information Security and its annexes.*

Benutzen Sie nur legal bezogene (und lizensierte) Produkte

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

Only use 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.*

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, selbst wenn der Name Ihrer/s Vorgesetzten darauf steht. Überprüfen Sie diese, z.B. indem Sie mit der Maus darüberfahren.
- Kontrollieren Sie, wohin Links führen, bevor Sie darauf klicken.
- Geben Sie niemals Passwörter heraus.
- Dringende Bitten nach Geld oder Geschenkkarten-Codes sind Betrugsversuche.
- 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, even if it contain the name of your supervisor. Check them, e.g. by moving the mouse over them.*
- *Check where links lead before you click on them.*
- *Never give out passwords!*
- *Urgent requests for money or gift card codes are scams.*
- *Download programs and data from the Internet or USB sticks only from trusted sources.*
- *Scan downloads and external storage media with your antivirus software.*