BACKUPS

Important data must be secured reliably. Using the backup services of SCC, you can generate a backup copy of your data, such that they can be restored in case of an accidental deletion, hardware defect, or attack (e.g. by malware). Contact your IT appointee of the business unit. For further information, click:
http://www.scc.kit.edu/dienste/datensicherung

PATCH MANAGEMENT (UPDATES)

Providing devices and systems with security updates is an important protection mechanism. As a rule, repairs (so-called patches) of known (security) problems are provided rather promptly. To minimize the risk on your devices, it is important to install updates promptly and, if possible, automatically.
Instructions for the most common operation systems can be found at:
https://www.scc.kit.edu/dienste/patchmanagement

USE OF CLOUD/ONLINE SERVICES

When using online or cloud data services, we have to decide whether your data can be stored there. For the best known services, decision support is provided for you to assess whether they can be used or to apply one of the given alternatives.
This decision support is given at:
https://www.scc.kit.edu/dienste/clouddienste

OBLIGATION TO REPORT IT SECURITY INCIDENTS

IT security incidents must be reported promptly.
You are obliged to report the following IT security incidents:

- Loss of devices (e.g. PCs, laptops, smartphones) that are either property of KIT or private devices, via which you access services or data of KIT.
- Loss of data carriers (e.g. USB sticks, CDs) on which important or personal data are stored (e.g. passwords, exams, applications, grades, salary statements).
- Discovery of devices (e.g. WLAN routers, small boxes, other PCs/laptops) in your rooms, which are suddenly found there, but have never been announced.
- Blackmail or coercion to not behave in agreement with the rules (e.g. if an unknown person wishes to have access to your devices or your rooms).
- Identity theft after you have accidentally shared a password on a phishing website or over the phone.
- Discovery of malware on devices (e.g. PCs, laptops, smartphones) via which you access the service or data of KIT.

Please report IT security incidents promptly to your IT appointee of the business unit or send an e-mail to **cert@kit.edu**. Together with you, we will analyze the risk and discuss potential solutions to minimize it.

More information can be found at
https://s.kit.edu/it-security.reporting-obligation

Contact
Karlsruhe Institute of Technology (KIT)
Steinbuch Centre for Computing (SCC)
Service Desk
76131 Karlsruhe, Germany
Phone: +49 721 608-8000
E-mail: servicedesk@scc.kit.edu
www.scc.kit.edu

100 % Recyclingpapier mit dem Gütesiegel „Der Blaue Engel"

Issued by
Karlsruhe Institute of Technology (KIT)
President Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe, Germany
www.kit.edu

Karlsruhe Institute of Technology

Practical Tips for IT Security at KIT

Protecting the IT Infrastructure of KIT Together

STEINBUCH CENTRE FOR COMPUTING (SCC)

PROTECTING THE IT INFRASTRUCTURE OF KIT TOGETHER.

IT is indispensable for work at KIT. The SCC tries to protect the IT infrastructure of KIT (including e.g. all PCs, laptops, tablets, smartphones, servers, WLAN routers) by technical measures. But effective protection is possible only when everyone helps.
The corresponding provisions are outlined in the IT Security Concept of KIT:
https://s.kit.edu/it-security-concept

This brochure contains important information on security of KIT's IT infrastructure as well as links to more details.

If you have a question concerning the contents of this brochure or concerning protection against cyber attacks on KIT, contact
servicedesk@scc.kit.edu

DETECTING FRAUDULENT MAILS

Criminals use various strategies to harm companies and universities and, hence, also KIT. A very popular strategy is sending fraudulent messages for

- the dissemination of malware to e.g. gain access to your devices and, in the next step, to KIT's IT infrastructure or
- deceiving end users in order to obtain sensitive information (e.g. access data) and money at the expense of you or KIT.

As a rule, the messages pretend to have been sent to you for a legitimate reason. If fraudulent mails are aimed at gaining access to sensitive information, they are called phishing mails. As not all fraudulent mails are identified and removed by the tools of SCC, it is important that you know how to detect fraudulent messages. This is explained in a separate brochure, click:
https://s.kit.edu/it-security.fraudulent-messages

In case you will identify a fraudulent message in future, delete it directly. You may also register for the procedure to report fraudulent mails and shift these mails to the corresponding folder in your mailbox.
Doing this, you help protect KIT's IT infrastructure.

For more information on the procedure to report fraudulent messages, click:
https://s.kit.edu/it-security.reporting-procedure

SECURE PASSWORDS

Unfortunately, many of the security measures used have no effect when passwords are not sufficiently secure. Whoever knows or can guess your password, has access to your data, can send e-mails in your name, or can access your documents.

Here, you can find information on how to select a secure password and on handling passwords:

- Use a long password, a password with 12 characters at least.
- Use different passwords outside and inside of KIT.
- Use different passwords for different user accounts. If you have several user accounts at KIT and cannot remember all the passwords, use a password manager.
- Keep your passwords secret. Do not disclose your passwords to superiors, secretaries, IT appointee of the business unit, service staff, colleagues, friends, relatives, or partners. When entering your password, take care that nobody watches you.
- If you suspect your password to be known, change it directly.

ENCODED AND SIGNED E-MAILS

On their way from the sender to the recipient, electronic mails may be read or even modified by criminals. To prevent this and to be sure about the sender of an e-mail, encode your e-mails and sign them (this also helps detect e.g. fraudulent messages). You can do this as soon as you have a user certificate issued by KIT. E-mails should be encoded in particular, if they contain personal or other data worth protecting. If you do not have a user certificate, contact your IT appointee of the business unit.

ANTIVIRUS SOFTWARE

Use of antivirus software also is an important protection mechanism. SCC makes available a centrally administrated antivirus service for this purpose. If the antivirus service has not yet been configured on your PC, contact your IT appointee of the business unit.

SECURE WORKPLACE

At your workplace, any information worth protecting shall not be disclosed to unauthorized persons. Note the following rules and recommendations:

- Always lock your rooms when you leave them.
- Close the windows when you leave your office, such that nobody can enter.
- Lock your screen or log out whenever you leave your workplace.
- Activate your screensaver with password protection and set it, such that your computer is locked automatically after 15 minutes at the latest.
- Encrypt your notebooks and other mobile devices.
- Shut down your notebooks and other mobile devices after work or lock them up.
- Lock cupboards and desks in which sensitive documents are stored.
- Keep the keys of desks and cupboards safe.

CONSCIOUS USE OF INFORMATION AND DATA

Always take care when you handle internal or other information worth protecting. This information may be used to make targeted attacks against you or KIT. Observe the following rules:

- Transmit such information consciously and economically to external persons.
- Keep the distribution list small.
- Store documents as long as necessary only.
- Destroy no longer needed data carriers (e.g. paper, CDs or DVDs).
- Delete no longer needed data on mobile devices (e.g. notebook, PDA, mobile phone, USB sticks, etc.). Also remember to delete data carriers when you take them out of operation.