Karlsruhe Institute of Technology

The obligation to report IT security incidents

Protecting the IT infrastructure of KIT together

Loss of devices (e.g. PCs, laptops, smartphones) via which you access services or data of KIT.

Loss of data carriers (e.g. USB sticks, CDs) on which confidential or personal data are stored (e.g. passwords, exams, job applications, salary statement, research results, inventions).

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, especially 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.

Detection of malicious software on devices (e.g. PCs, laptops, smartphones) via you access IT infrastructure or IT services of KIT.

If you have experienced any of the above IT security incidents, please contact your IT appointee of the business unit directly and/or send an e-mail to KIT-CERT (cert@kit.edu). Together with you, the situation is analyzed and discussed what can be done to minimize the probability of a damage and the severity of a damage to KIT and you.

If you detect **an attempted attack**, please also report this to your IT appointee of the business unit.

If you are unsure whether an incident you have observed is an IT security incident or simply seems a little bit unusual, please contact your IT appointee of the business unit as a precaution or send an e-mail to beratung-itsec@scc.kit.edu.

For additional information on the obligation to report IT security incidents please have a look at our explanations under https://s.kit.edu/it-security.reporting-obligation

Steinbuch Centre for Computing

Informations-sicherheits-beauftragter

aifb

KASTEL

SECUSO
SECURITY · USABILITY · SOCIETY