Policy

Security-Related Incidents:

Reporting Requirements & Immediate Actions

(Non-binding translation)

I Scope

This policy is binding on all members and affiliates of the university, as well as external IT service providers and other third parties who use or process the university's information or IT systems.

II Reporting Obligation and Reporting Channels

All members and affiliates of the university, as well as the aforementioned IT service providers and other third parties, are required to report any potential security-related incidents to the IT Service Desk immediately – even if they are only suspected – in order to minimize damage and prevent further risks:

- By phone via extension **1818**
  or
- By email to **security@tu-freiberg.de**.

If possible, please have the following information ready:

- Who is reporting (name, email address, phone number)?
- Which IT system is affected (type and identifier of the system, building, room)?
- How were you using the IT system? What did you observe?
- When did the incident occur (date, time)?

In addition, if there are persons responsible for decentralized administration, they should be notified.

III Immediate Actions and Guidelines

If you suspect a (successful) attack on your work computer or another IT system, take the following immediate actions:

1. Stay calm.
2. Leave the device turned on and immediately disconnect it from the network by unplugging the network cable and disabling wireless connections (e.g., Wi-Fi, mobile communications).
3. Stop working on the affected device or IT system.
4. Immediately notify the IT Service Desk (see above) of the incident.

In general, the following guidelines apply when responding to security-related incidents:

a) Document your observations, e.g., by taking photos or screenshots.
b) Passwords must be changed if they have become known to third parties or if there is suspicion that this has occurred (https://password.tu-freiberg.de).
c) Take further action only as instructed by the URZ, the Information Security Officer, or the persons responsible for decentralized administration.

IV Identifying Security-Related Incidents

A security-related incident is defined as an observation or deviation that indicates a potential compromise of information security and that may jeopardize the confidentiality, integrity, or availability of information or IT systems. Typical consequences of these incidents include information being compromised, tampered with, or destroyed.

The following examples are intended to help you recognize a potential information security incident as such:

- Open windows and doors in security-sensitive areas,
- PCs left unlocked when unattended,
- Unknown individuals in areas not accessible to the public,
- Suspicious emails containing attachments or links,
- unusual phone calls,
- unexpected error or warning messages on an IT system,
- IT systems responding very slowly or being completely inaccessible,
- loss or theft of devices or data storage media,
- data leaks (accidental or intentional disclosure of confidential data to third parties),
- malware infections (viruses, Trojans, other malicious software).

Further information on security-related incidents and information security at our university can be found on the Information Security Office’s website (https://tu-freiberg.de/en/infosec).