Goethe University recommendations and best practices for using email services

The following recommendations apply to all members of Goethe University Frankfurt. They regulate the official use of email services. Goethe University regulations and statutes, in particular IT security regulations, IT security guidelines and the IuK use regulation[1], are not affected by these recommendations.

Email services are an extensively used means of communication both professionally and privately. Emails consist not only of text, but also often include links to websites and downloads, and attachments such as pictures or documents. This leads to risks in email communication. Hackers and criminals exploit people's curiosity to spread malware by email and to gain access to confidential data such as passwords, access codes and credit card numbers.

When using email services, the following rules of the Security Management Team (SMT) should be heeded:

1) For all **official matters**, the official Goethe University email address must be used for both recipient and sender for all electronic communication.

2) It is **not permissible** to use the **automatic forward** function to forward official emails to email addresses belonging to external mail systems that are not operated by Goethe University. Using **external email addresses** for official purposes has to be approved by Goethe University's official **data protection officer** (dsb@uni-frankfurt.de).

3) **Official email addresses** may **not** be used to access personal third-party services (e.g., social networks, online shopping, etc.).

4) For security reasons, **students** are advised to use their **university email accounts** for all electronic communication with university members.

5) If possible, all Goethe University employees should only contact students via university email addresses (**@xxx.uni-frankfurt.de addresses**), except when answering an external email directly.

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt – General use regulations for information processing and communication infrastructure at Goethe University Frankfurt

6) Contaminated **email attachments and links** are among the most frequent vehicles for infiltrating computers with malware. For this reason, it is important to be cautious before clicking on a link or opening an attachment. Sender, subject and email text should be consistent and plausible.

7) **Applications** and **application documents** may only be submitted in **PDF format**. If you are sent zip files or word documents, you can direct the applicant to resubmit the application in PDF format.

8) **Digital certificates** attest to the trustworthiness of communication partners. Make sure that the certificate is valid and trustworthy when you receive a signed email.

9) Please contact your IT support or your IT security officer if you have any questions.

Further information:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) - (Federal Office for Information Security)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) - Goethe-University IT Security Management Team
  https://www.uni-frankfurt.de/smt

- Goethe University Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) – Goethe University Computing Centre
  https://www.uni-frankfurt.de/hrz/it-sicherheit