Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Universität Würzburg, Sanderring 2, 97070 Würzburg

**President**

Per E-Mail

Würzburg, 22.01.2015

To all

Users of e-mail services at
the University of Würzburg

**Propagation of JMU Accounts**

Dear Madam / Sir,

Security tools newly introduced by JMU's Computer Center recently indicated an overly high access of the university's servers from Google Mail. Further research - which was coordinated with our Data Protection Officer - showed that Google Mail (and presumably other big service providers such as Yahoo, T-Online etc.) have been used to a high degree as a mail-client to access the university's mail systems.

To grant these freemail-providers access to their official mails, **users have to provide both their university user-ID as well as their password to the provider**. Unfortunately, this has happened in many cases.

If users provide their university credentials to external service-providers (Google, Microsoft etc.) for authentication on university servers and to retrieve mail from internal mailboxes, this means that not only the security of the user's data is no longer ensured, because service providers such as Google verifiably access and analyze the content of these mails. Furthermore, this is a prohibited data transmission, which probably allows for data espionage and thus represents a big danger to IT security for all users of the university's IT infrastructure. As e-mails on the JMU IT infrastructure are generally of an official nature, and as such have to be treated with due caution and confidentiality and must not be given to third parties, **forwarding of official data to third party servers, especially transmission of JMU-account information of any kind is prohibited.**

The transmission of a JMU account username and password, which can be used to access the university's systems (e-mail, but also VPN, internal websites etc.), is already prohibited by §5 of the "Benutzungsordnung für IT-Systeme", which all users signed as a precondition for use. Furthermore, this violation of data secrecy will be treated either as a minor breach of the law, and as such one can be fined, or possibly as a criminal act, and as such those sentenced could face imprisonment for up to two years or receive punitive damages. Furthermore, it will be dealt with as a breach of duty or rather as a contractual violation of obligations.

For the reasons stated above, current and future users have been and will be informed by the Computer Center, in close cooperation with the University's Data Protection Officer, about the illegal data transmission and about existing alternatives. Further access for Google and other external e-mail providers to the mail servers of the Computer Center will be blocked. Moreover, users have been and will be requested to immediately change their JMU password and to keep it confidential in the future.

We kindly ask you to follow these instructions when dealing with official data and help to ensure data security at our university by observing data protection appropriate behavior. Ultimately it is your wish, that sensitive data e.g. from research projects, vocation or hiring procedures, exam papers and results remain safe on the university's computers and servers.

For technical questions, please contact the help desk of the Computer Center (http://go.uni-wuerzburg.de/rzberatung).
Questions concerning the legal content of this document can be answered by the official data protection officer (http://www.uni-wuerzburg.de/ueber/universitaet/verwaltung/beauftragte/datenschutzbeauftragter/).

With kind regards,

Prof. Dr. A. Forchel