IT DEPARTMENT

MS OFFICE 365

GUIDELINES

MS OFFICE 365

Guidelines regarding the use of MS Office 365: A cloud-based mail and calendar solution

© IT Department at the IT University of Copenhagen
Rued Langgaards Vej 7
2300 Copenhagen S

IT DEPARTMENT

A New Mail and Calendar Solution

The university has implemented the cloud-based solution called Microsoft Office 365. This means that your ITU mails and calendar entries are no longer stored locally at the university but at Microsoft's operating centers, which are located in Europe and USA.

Implementation of a cloud-based solution does not mean that you need to change the way you treat and/or access your e- mails. But as a precaution, we have collected all the safety guidelines (which also are described in the university's IT security policies), you should be aware of.

E-Mails Containing Confidential and/or Sensitive Personal Information

E-mails containing confidential and/or sensitive personal content must be protected in accordance with the Act on Processing of Personal Data (persondataloven) and the Executive Order No. 528 of 27 June 2000 (sikkerhedsbekendtgørelsen).

Therefore e-mails containing confidential and/or sensitive personal information must not be forwarded or sent outside of the ITU network (e.g. by sending Social Security numbers to a Gmail or Hotmail account).

If confidential and/or sensitive personal information have to be sent to an e-mail address outside of the ITU network, the e-mail must be encrypted with a recognized and strong encryption algorithm. For example by using Digital Signature or NemID.

All ITU e-mail accounts are considered to be within the university's network. All other e-mail accounts are considered to be outside the university's network.

Deletion of E-Mails

According to the Danish Executive Order No. 528 of 27 June 2000 (sikkerhedsbekendtgørelsen) and the DPA's (datatilsynet) security instructions the data controller must set up rules regarding the deletion of mails containing confidential and/or sensitive personal information if the audit requirements in §19 in the Executive Order cannot be implemented. Read more at: https://www.retsinformation.dk/Forms/R0710.aspx?id=842 (in Danish only).

Detailed information about this regulation can be read at the following link, section 3.4.2.4.:
http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/behandling-af-personoplysninger-i-cloud-loesningen-office- 365/ (in Danish only).

Access To E-Mails

In case of operational problems and security events, system administrators and network managers at ITU and Microsoft may need to access log files, etc., which could contain the subject field of your e-mails. No e-mails will be read by Microsoft.

If ITU employees in exceptional cases need to access e-mails this will only take place with a written permission from the Vice Chancellor or by acceptance from the user. To prevent private e-mails from being read, they must be clearly marked 'private' in the subject field.

System administrators and network managers have access to exchange registers, servers and back-up copies. System administrators and network managers are subject to a duty of confidentiality as long as no misuse is found.

Ownership

ITU considers all e-mails to be university property.

Employees' Private Use of E-Mail

ITU permits the use of e-mail systems for private use if the IT security policy is followed. However, it is recommended that staff refrain from using their ITU e-mail for private use and instead use a private e-mail account.

Attached Files

Staff is advised to exercise caution in relation to attached files and not open these uncritically.

Read More About MS Office 365

You can find some useful information about the new mail- and calendar solution in the link below. Please notice that only the mail and calendar function will be available at this time in the MS Office 365 solution.

More information about MS Office 365: http://www.microsoft.com/da-dk/office365/online-software.aspx

IMPORTANT GUIDELINES

!

Do not send or forward confidential and/or sensitive information to an e-mail outside of the ITU network (e.g. by sending to a Gmail or Hotmail account). If confidential and/or sensitive personal information have to be sent to an e-mail address outside ITU network, the e-mail must be encrypted with a recognized and strong encryption algorithm. For example, by using Digital Signature or NemID.

!

When you handle confidential and/or sensitive personal information, do not import e-mails to mobile devices such as your mobile phone, iPad, and/or tablet or to your personal computer via an e- mail client. Instead, use the webmail, where data is encrypted.

!

Please be aware that all mobile devices and personal computers used for work purposes, for example ITU mail access, must be secured with a password that complies with current password policy at the university. If a mobile device is lost or stolen others could potentially access your mail account, so avoid storing your login credentials in web forms and never leave your mobile devices unprotected.

IT DEPARTMENT

IT University of Copenhagen
Rued Langgaards Vej 7
2300 Copenhagen S

Opening hours:
Monday - Friday
10 AM to 13 PM
Wing 2C

it@itu.dk