IT DEPARTMENT

Guidelines for handling of confidential and sensitive personal information

DA

Retningslinjer for håndtering af fortrolige og personfølsomme oplysninger

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

All rights reserved.

IT DEPARTMENT

IT-Universitetet er underlagt persondataloven og sikkerhedsbekendtgørelsen. Det betyder, at der stilles strenge krav til håndteringen af bl.a. fortrolige og/eller personfølsomme oplysninger. Personfølsomme oplysninger er eks. oplysninger om religiøse, fagforeningsmæssige, seksuelle eller etniske tilhørsforhold, strafbare eller helbredsmæssige forhold, m.v. Cpr-numre anses som værende en fortrolige. Disse typer af oplysninger må bl.a. ikke transmitteres udenfor ITUs netværk medmindre de er beskyttet af en anerkendt og stærk krypteringsalgoritme, som f.eks. Digital Signatur eller NemID.

På grund af de lovgivningsmæssige krav, der er stillet til os, skal du, som studerende eller ansat på ITU, være særligt opmærksom på dit ansvar ved håndtering af denne slags oplysninger. Nedenfor er angivet de retningslinjer, som du bør overholde såfremt du håndterer ovenstående typer af oplysninger.

- Send ikke fortrolige og/eller personfølsomme oplysninger til en e-mail udenfor ITUs netværk. F.eks ved at videresende mails til en Gmail eller Hotmail mailkonto. Såfremt fortrolige og/eller personfølsomme oplysninger skal sendes til en e-mailadresse udenfor ITUs netværk skal e-mailen være krypteret med en anerkendt og stærk krypteringsalgoritme. Eksempelvis ved brug af Digital Signatur eller NemID.

- Når du håndterer fortrolige og/eller personfølsomme oplysninger må du ikke importere e-mails til mobile enheder, såsom din mobiltelefon, pad, tablet eller til din privatcomputer via en e-mail klient. Anvend i stedet webmailen, hvor data er krypteret.

- Undgå at lagre fortrolige og/eller personfølsomme oplysninger på et eksternt eller mobilt medie såsom USB stick, ekstern harddisk, mobiltelefon mv.

- Offentliggør ikke fortrolige og/eller personfølsomme oplysninger over internettet (f.eks. gennem udgivelse af journaler, excelark, rapporter, databaser eller ved at offentliggøre oplysninger i diskussionsfora, chatrooms, jobansøgninger, CV'er, opgaver og lignende).

- Fortrolige og/eller personfølsomme oplysninger om andre må under ingen omstændigheder blive videregivet til 3. part, medmindre der foreligger en skriftlig tilladelse herfor.

- Opbevar altid dokumenter med fortrolige og/eller personfølsomme oplysninger sikkert, så uvedkommende ikke kan få adgang til dem.

- Brug den særlige skraldespand i printrummene på universitetet, hvis du skal smide papirer ud der indeholder fortrolige og/eller personfølsomme oplysninger.

- Tænk dig altid om en ekstra gang inden du videregiver fortrolige og/eller personfølsomme oplysninger til andre.

Vær i øvrigt opmærksom på, at alle mobile enheder og private computere, der anvendes til arbejdsmæssige formål, skal være sikret med et password der overholder ITUs gældende passwordpolitik. Hvis du mister eller får stjålet en mobil enhed kan uvedkommende potentielt få adgang til din mail-konto osv., så undgå at gemme dine loginoplysninger i webformularer mv. og efterlad aldrig dine mobile enheder ubeskyttet.

Læs mere om transmission over internettet her:
http://www.datatilsynet.dk/offentlig/sikkerhed/transmission-over-internettet/

EN

Guidelines for handling of confidential and sensitive personal information

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

All rights reserved.

IT DEPARTMENT

The IT-University is subjected to the Act on Processing of Personal Data's (in Danish called persondataloven) and the Executive Order on Security (in Danish called sikkerhedsbekendtgørelsen). This means that there are strict requirements for the handling of confidential and/or sensitive personal information. Sensitive personal information could be information on religious, trade union, sexual or ethnic affiliation, crime or health conditions, etc. Social security numbers is considered as being confidential information. These types of information may not be transmitted outside the ITU network unless they are protected by a recognized and strong encryption algorithm, such as Digital Signature or NemID.

Because of the regulatory requirements that are provided to us, you, as a student or employee at the ITU, must be especially aware of your responsibility in handling this kind of information. Below are the guidelines that you should observe if you handle the above types of information.

- Do not send or forward confidential and/or sensitive information to an e-mail outside of the ITU network (e.g. by using 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, using digital signature or NemID.

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

- Avoid storing confidential and/or sensitive information on external media such as USB sticks, external hard drives, mobile phones, etc.

- Do not release or disclose confidential and/or sensitive information over the Internet (E.g. through the release of records, reports, databases, assignments or by disclosing or posting information in discussion boards, chat rooms, blogs, job applications, CVs, etc.).

- Confidential and/or sensitive information about others must under no circumstances be disclosed unless there is a written consent from the person(s) in question.

- Always keep the documents with confidential and/or sensitive personal information (e.g. print out) secure, so unauthorized persons cannot access them.

- Use the special bin provided in the printing rooms at the university when throwing out papers containing confidential and/or sensitive information.

- Always think twice before providing any confidential and/or sensitive information to others.

Please be aware that all mobile devices and personal computers used for work purposes must be password protected 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, etc, so avoid storing your login credentials in web forms and never leave your mobile devices unprotected.

Read more about transmission over the internet at (DK only):
http://www.datatilsynet.dk/offentlig/sikkerhed/transmission-over-internettet/

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