AARHUS BSS
INSTITUT FOR FORRETNINGSUDVIKLING
OG TEKNOLOGI
AARHUS UNIVERSITET

Retningslinjer for **IT- og informationssikkerhed** på AU og BTECH

Alle ansatte på AU, såvel forskere, undervisere og teknisk/administrativt personale som studerende, skal have det størst mulige fokus på informationssikkerhed. Det vil i praksis sige alle de informationer, som AU kan gøres ansvarlig for: F.eks. **forsøgs- og forskningsdata, alle data om personale, data om finansielle forhold, alle data ifm. administrationen af Aarhus Universitet samt informationer, som er overladt Aarhus Universitet af andre ifm. forskningsprojekter**.

Bliv på den næste side klogere på, hvad du som ansat skal gøre for at overholde Aarhus Universitets regler for informationssikkerhed.

Find flere oplysninger, kontaktpersoner mv. på **informationssikkerhed.au.dk**

1. Læs AU's informationssikkerhedsfolder, som ligger i dit dueslag, eller find folderen her:

   medarbejdere.au.dk/informationssikkerhed/informationssikkerhedspolitik/

2. Lås altid din computer, når du forlader den. Det gælder også din mobil, tablet mv., hvis der er følsomme og fortrolige informationer på disse.

3. Indholdet på din computer skal være krypteret. Læs om, hvordan du sikrer dig, at det er tilfældet:

   medarbejdere.au.dk/administration/it/vejledninger/sikkerhed/kryptering-data/

4. Bruger du USB-stik, eksterne harddiske mv., skal de være krypteret, hvis de bruges til andet end undervisningsmateriale og præsentationer. Spørg IT-support, hvis du er i tvivl om, hvorvidt det er tilfældet.

5. Sørg for, at dit kontor altid er aflåst, når du ikke opholder dig på kontoret.

6. Papirer med følsomme og fortrolige informationer, adgangskort, nøgler mv. må ikke ligge på skriveborde, i reoler eller andet, som ikke er aflåst – heller ikke selvom døren til dit kontor er låst.

7. Dropbox, Google Drive mv. må ikke bruges til at udveksle følsomme og fortrolige informationer eller forskningsdata. Fra efteråret 2019 kan alle AU-ansatte dog bruge OneDrive, da AU har indgået en databehandleraftale med Microsoft. Ukrypterede e-mails må heller ikke bruges til at udveksle forskningsdata samt følsomme og fortrolige informationer. Læs mere på:

   medarbejdere.au.dk/informationssikkerhed/informationssikkerhedspolitik/mailpolitik

8. Du skal sætte dig ind i, om de data, du arbejder med, er klassificeret som offentlige data, interne data, følsomme data eller fortrolige data – og hvordan data på den baggrund skal beskyttes:

   medarbejdere.au.dk/informationssikkerhed/klassifikation-af-data/

9. AU IT sikrer, at der altid er backup på alle netværksdrev. Du bør derfor altid gemme dine data på AU's netværksdrev. Gemmer du data lokalt på din computer, flytbart medie eller f.eks. en fremmed testserver, har du pligt til at sikre, at dine arbejdsdata altid er behørigt sikkerhedskopieret.

10. Mister du din computer eller andet AU it-udstyr, så kontakt IT-support hurtigst muligt. Det gælder også, hvis du bliver hacket, dine data bliver stjålet eller din e-mailkonto misbruges.

11. Bliver du opmærksom på sikkerhedsbrud (f.eks. materiale på AU's web, som ikke burde være offentligt tilgængeligt, eller at en bruger af et AU it-system har adgang til information, som vedkommende ikke burde have), så kontakt ligeledes IT-support hurtigst muligt.

12. Følg de ni råd, og bidrag til informationssikkerheden på Aarhus Universitet - uanset om du arbejder med forskning, uddannelse, rådgivning eller administration:

    medarbejdere.au.dk/informationssikkerhed/

Som **forsker** skal du være særligt opmærksom på informationssikkerhed ifm. opstart af projekter og ved anskaffelse af it-udstyr og software til forskningsprojekter.

Læs mere om databeskyttelse og databehandleraftaler, medarbejdere.au.dk/informationssikkerhed/databeskyttelse/saerligt-om-forskning/, og find inspiration til datamanagementplaner (DMP) ifm. forskningsprojekter, https://deic.dk/da/data-management.