

REGLER FOR SIKKER BRUG AF SKOLENS IT-SYSTEMER

Som medarbejder ved VUC Vest har vi alle et ansvar for at passe på kursisternes og VUC Vests data.

Det er derfor en vigtig del af jobbet at overholde IT-sikkerhedsreglerne.

Så tænk dig ekstra godt om - for en sikkerheds skyld.

I denne pjece finder du de vigtigste råd og regler om IT-sikkerhed og god adfærd.

1. SOM MEDARBEJDER VED VUC VEST HAR DU TAVSHEDSPLIGT

De personfølsomme oplysninger (fx CPR-numre, helbredsoplysninger og lignende) og fortrolige oplysninger, du får kendskab til gennem dit arbejde, må du under ingen omstændigheder dele med uvedkommende. Det gælder både under og efter din ansættelse.

2. DINE PERSONLIGE ADGANGSKODER ER ALTID FORTROLIGE

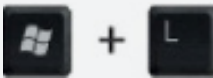
Alle dine personlige adgangskoder til skolens IT-systemer er strengt fortrolige, og det er vigtigt, at du behandler dem varsomt.

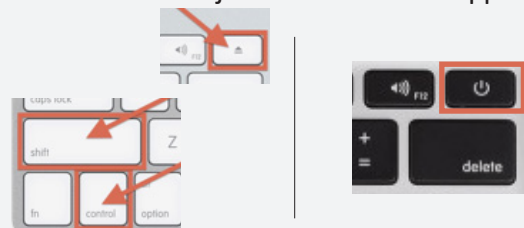
Hvis du har mistanke om, at en adgangskode er blevet kendt af andre, skal du straks skifte den.

Har du mistanke om, at en adgangskode er blevet misbrugt af andre, skal du straks kontakte IT-servicedesk på tlf. 2922 1345.

3. LÅS DIN PC, NÅR DU FORLADER DEN

Dette gør du ved at trykke på:

- Windows-tasten + L 
- Mac: Flere muligheder - bl.a.: 'Control - shift - eject' el. Hold slukknappen inde



4. BRUG SIKRE MAILTJENESTER

Såfremt du undtagelsesvis har behov for at sende fortrolige eller følsomme oplysninger til kursister eller eksterne samarbejdspartnere, skal du benytte:

- Digital post (fx Doc2mail)
- Sikker e-post.

5. GEM DATA OG DOKUMENTER FORSVARLIGT

Gem aldrig følsom og fortrolig data på computerens C:drev, på fildelingstjenester som google docs, på bærbar medier som fx USB-nøgler eller lignende.

6. OPSLAG I FAGSYSTEMER MÅ KUN SKE I FORBINDELSE MED EGNE ARBEJDSOPGAVER

Du må kun slå op i fagsystemer, hvis det er i forbindelse med dine egne arbejdsopgaver. Du må fx ikke slå op på dine venners og familiers oplysninger. Alt, hvad der sker på VUC Vests fagsystemer, herunder internet og e-mail, bliver registreret og kan senere hentes frem, hvis der er mistanke om misbrug.

Er det nødvendigt at hente, dele eller gemme kursistoplysninger i relation til dit arbejde, er det vigtigt at minimere brugen af de følsomme oplysninger. Brug derfor kursistnumre i stedet for cpr-numre og undlad adresse, hvor det ikke er nødvendigt. Noter aldrig personfølsomme data af helbredsmæssig, religiøs eller seksuel karakter.

7. SIKKERHED PÅ MOBILE ENHEDER

Data på mobile enheder, som bærbare computere, iPads og smart-phones, skal beskyttes, så uvedkommende ikke kan få adgang:

- Følsomme og fortrolige oplysninger må aldrig hentes ned på mobile enheder.
- Din mobile enhed er personlig og må ikke deles med andre.
- Lås din mobile enhed når du forlader den.
- Du skal sikre din mobile enhed med en personlig skærm/låskode og/eller fingeraftryk, så den ikke kan misbruges, hvis den kommer i forkerte hænder.

- Når du er i det offentlige rum, skal du have din mobile enhed under opsyn og være sikker på, at fremmede ikke kan kigge med.
- Ryd op på din mobile enhed. Du skal løbende sikre dig, at der ikke ligger dokumenter med fortrolige oplysninger eller lignende data gemt lokalt på din mobile enhed.

Skulle din mobile enhed blive væk eller stjålet, så skal du straks kontakte it-servicedesk på tlf. 2922 1345

8. AFVIS ALTID PHISHING OG MISTÆNKELIGE HJEMMESIDER

Phishing er fup-mails, designet af svindlere, med det formål at lokke personlige oplysninger ud af dig, som fx CPR-nummer, adgangskoder, kontonummer m.v.

VUC Vest er beskyttet mod virus, phishing, spam m.v. Modtager du alligevel en mistænkelig mail, så slet den, svar aldrig på den, og åben aldrig vedhæftede filer eller links fra sådanne mails. Besøg heller ikke mistænkelige hjemmesider og brug altid din sunde fornuft og omtanke.

Hvis du er i tvivl, om en mail er phishing, så kontakt it-servicedesk på tlf. 2922 1345

IT-SERVICEDESK
2922 1345



Maj 2018 QUICKGUIDE

PERSONDATA PÅ VUC VEST

FAKTA OM PERSONDATAFORORDNINGEN

- Persondata er ikke blot cpr. numre eller navn. Persondata er alle oplysninger, der siger noget om en person og kan identificere en person. Eksempel: "Anne" er ikke en personoplysning, vi skal være varsom med, fordi vi har mange kursister og lærere, der hedder Anne. Men "Anne fra hold xxx på VUC Vest" eller "Anne fra VUC i Esbjerg" er en personoplysning, fordi man relativt let kan identificere Anne, når man har både navn og hold id eller afdeling.
- Alle persondata skal håndteres med forsigtighed. Vi skal altid have en grund til at behandle og opbevare persondata.
- Vær ekstra forsigtig med oplysninger om helbred (diagnoser, ikke antal af fraværs- dage), etnisk oprindelse og religion. Det er følsomme oplysninger! Eksempel: Hvis en kursist er fraværende, skal det naturligvis noteres i Ludus. Men hvis kursisten fortæller, at han er fraværende pga. depression, må du ikke skrive dette i Ludus i et felt, der er tilgængeligt for alle brugere, heller ikke selvom kursisten selv fortæller det. Han fortæller det kun til dig, og derfor er det kun dig, der må have adgang til den oplysning. Der kommer nærmere procedurer for, hvordan du kan dele sådanne oplysninger med leder, studievejleder eller andre, når det er nødvendigt for kursistens skyld.

En **god tommelfingerregel er at behandle persondata**, som noget du låner af en kursist, kollega eller medarbejder i en periode, og som du skal aflevere tilbage i ordentligt stand:

PAS GODT PÅ DET

Sørg for at data er beskyttet og opbevaret sikkert, så det ikke er tilgængeligt for andre end dig, der har modtaget persondata.

Det betyder, at du skal have password på din computer, telefon, i-pad og andre elektroniske dimser, som du bruger ifm. dit arbejde på VUC Vest. Når du går fra din computer, skal du låse den, så ingen andre kan tilgå dine dokumenter, mail osv. Der må ikke ligge papirer med persondata på dit skrivebord, når du går fra det. Du må ikke opbevare dokumenter med persondata i ringbind, skuffer, skabe osv., der ikke er aflåste for andre, og du må som udgangspunkt heller ikke tage persondata med ud af VUC Vests bygninger.

LÅN DET IKKE UD TIL ANDRE

Sørg for, at ingen andre har adgang til dine dokumenter med folks persondata, og videregiv dem som udgangspunkt ikke.

AFLEVER DET EFTER BRUG

Slet dit dokument/mail med persondata, så snart du er færdig med at bruge det, eller når det er tastet/arkiveret i Ludus, IMSOFT, Statens lønsystem osv.

Eksempel: Resultatet af en FVU-test kommer på et stykke papir, der indeholder persondata (navn, cpr. nummer og resultater). Resultaterne skal registreres på kursisten i Ludus. Så snart resultatet er tastet, skal printet af testen makuleres og slettes fra alle computere, mails osv. Det må ikke opbevares andre steder end i Ludus og IMSOFT. Du må ikke gemme en kopi andre steder, ikke selvom det er lettest, når du skal finde resultatet efterfølgende eller som en ekstra backup i tilfælde af, at Ludus ikke virker o.lignende.

På VUC Vest har vi tradition for at gemme rigtig meget persondata, og det er jo vigtigt, fordi vi eksisterer for vores kursister. Men for at overholde reglerne i persondataforordningen skal vi ændre en del af vores vaner og procedurer.

Derfor er en række medarbejdere i gang med at lære mere om reglerne og udarbejde de procedurer og politikker, der sikrer, at VUC Vest overholder reglerne. Vi vil løbende orientere om de nye procedurer.

Foreløbigt har vi udarbejdet nogle tommelfingerregler, som vi altid skal følge:

TOMMELFINGERREGLER

1. **Sæt altid tastaturlås på mobiler** med adgang til arbejdsmail eller O365-apps (eller andre arbejdsrelaterede programmer)
2. **Lås din computer**, hver gang du forlader den
3. **Ingen papir/post-its med persondata** på skrivebordet, i mapper, i din taske eller på hjemmearbejdspladsen
4. **Brug så vidt muligt kursistnummer frem for cpr-nummer**
5. **Tænk over, hvor meget info du behøver at få oplyst** (need-to-know!), fx er de sidste 4 cifre i CPR altid nødvendige?
6. **Gem IKKE på desktop** (der er ingen IT-backup, og det er nemt at tilgå)
7. **Slet mails med persondata**, så snart de er behandlet eller arkiveret i det rette system (slet også i slettet post-mappen, så det er helt slettet)
8. **Videregiv ikke kursist- eller medarbejderoplysninger over telefonen** til tredjepart (fx sagsbehandler eller pårørende)

Listen er ikke udtømmende og kan løbende opdateres.

Der vil altid ligge den senest opdaterede version på VUCintra under 1. Administrations/personaleinfo.

HVIS DU HAR SPØRGSMÅL TIL PERSONDATA, KAN DU SKRIVE ELLER RINGE TIL:

Susanne Jensen Bredahl: Mail: sjb@vucvest.dk eller tlf: 29 21 97 63