December 2018

VUC Vests IT-politk

1.1 Forord

I dag er det en naturlig ting, at medarbejderen i en virksomhed eller skole har en PC til sin rådighed for at kunne udføre sit arbejde. PC'en har typisk adgang til internettet, og medarbejderen benytter såvel internet som e-mail i sit daglige arbejde. VUC Vest er ansvarlig for korrekt og lovlig anvendelse af IT-systemerne og skal til enhver tid kunne redegøre for den software, som er installeret såvel på serverne som på PC'erne. VUC Vest pådrager sig et strafansvar, hvis der forefindes software, hvortil der ikke findes gyldig licens, eller hvis PC'en på anden vis anvendes i strid med gældende lovgivning. Udgangspunktet er, at IT-værktøjer stilles til rådighed for medarbejderen med henblik på, at vedkommende kan udføre de arbejdsopgaver, som påhviler vedkommende.

VUC Vests IT-udstyr, både det på arbejdspladsen og evt. udstyr til hjemmearbejdspladser, skal benyttes i henhold til denne IT-politik. Det forudsættes, at udstyret behandles forsvarligt og efter forskrifterne.

1.2 Brugen af VUC Vests udstyr

VUC Vests IT-udstyr skal benyttes på en fornuftig og ansvarlig måde, idet beskadigelse af dette kan være til gene for både en selv og alle andre brugere af IT-udstyret.

Eksterne operatører må under ingen omstændigheder installere programmer og/eller tilrette indstillingen af skolens IT-udstyr uden tilladelse fra IT-afdelingen.

1.3 Brugen af PC

VUC Vests personale må anvende den PC, de har fået stillet til rådighed af VUC Vest, til private formål, ligesom kursister, der har lånt en PC af VUC Vest, kan benytte PC'en til private formål (i et rimeligt omfang). Anvendelsen må dog ikke begrænse PC'ens eller skolens IT-systemers funktionsdygtighed på grund af omfanget af datamængder, overførsel af virus eller lignende forhold.

Det forudsættes, at VUC Vests medarbejdere og kursister ved både privat og almindelig brug af IT-udstyr udviser ansvarlighed og en høj moral/etik i brugen af IT-udstyret - herunder også deres anvendelse af internet og mail. Privat anvendelse af PC'ere m.v. begrænser ikke VUC Vests råderet over eller adgang til det udstyr, der er stillet til rådighed og den data, der er lagret herpå herunder private mails (læs mere i afsnit 1.8.), dokumenter m.v.

VUC Vest accepterer installering af programmer, filer m.v. til privat brug, (når brugen af disse filer/programmer er lovlige og ikke begrænser IT-systemets funktionsdygtighed eller påfører skolen udgifter. Ved enhver tvivl om, hvorvidt et program må installeres, skal spørgsmålet afklares med VUC Vests IT-afdelingen, inden det forsøges installeret).

Bærbare og stationære PC'er må ikke efterlades i åben stand, hvorved uvedkommende måtte have adgang til dem. **Der må ikke gemmes arbejdsrelaterede materiale (notater, mails, regneark osv.) på PC'ens C-drev, da al information om kursister, medarbejdere og institutionen skal kunne findes på fælles drev, såfremt der spørges om aktindsigt.** Ved aflevering af såvel lærer-PC, som kursist-PC, vil alt indhold på computerne og andet udstyr blive slettet af IT-afdelingen.

1.4 Backup

Med jævne mellemrum tages der sikkerhedskopi af alle data lagret på serverne. Der tages ikke sikkerhedskopi af data på PC'ens SSD/harddisk. Brugeren skal selv tage løbende backup til SD-kort. Det er brugerens pligt at sørge for at rydde op på sit eget personlige drev. Dvs. at man skal slette alle dokumenter, databaser, indscannede billeder mv., som ikke skal bruges længere.

1.5 Password

Password er strengt personligt og skal identificere brugeren (over for systemets servere).

- Udlever derfor **ALDRIG** dit password til nogen.
- Log altid af eller lås skærmen, når du forlader maskinen.
- Undgå at nedskrive dit/dine password*.

**Det administrative personale noterer deres passwords ned, og listen opbevares i en lukket kuvert i pengeskabet.*

Følgende regler gælder for dit password:

- Antal dage før password **SKAL** skiftes: 120 dage
- Minimum antal karakterer: 8
- Passwordet skal indeholde en kombination af store og små bogstaver, tal og specielle tegn.
- Antal af mislykkede login-forsøg før konto låses: 3

Arbejder du 'uden for' systemet og dermed ikke via den tynde klient, skal du benytte en tofaktorkode, som du modtager via sms, for at tilgå Citrix og dermed VUC Vests systemer.

1.6 Virus

Virus kan ødelægge/slette egne og andres data, forhindre maskinen i at logge på nettet m.m. Hvis antivirusprogrammet fortæller, at der er virus, eller man i øvrigt har mistanke om, at en PC er inficeret med virus, så meld det straks til VUC Vests IT-afdeling.

1.7 Defekt udstyr og fejl

Man skal fejlmelde defekt IT-udstyr og øvrige IT-problemer til VUC Vests IT-afdeling.

1.8 E-mailpolitik

For at forebygge eventuelle problemstillinger angående de ansattes e-mailkorrespondance, der foregår i VUC Vests e-mailsystem, skal følgende regler og retningslinjer vedrørende korrespondancen opretholdes. Det er vigtigt, at alle ansatte har forståelse for og er bevidste om deres anvendelse af e-mails. Der kan opstå situationer, hvor det af driftsmæssige hensyn er nødvendigt at foretage kontrol med brugen af såvel internettet som e-mail. Specifikke kontrolforanstaltninger vil kun finde sted, hvis det kan begrundes i væsentlige hensyn til VUC Vests drift og omdømme.

VUC Vest har tre mailkonti:

1. vucvest.dk: Ligger på lokal Exchange-server.

    - Denne mailkonto benyttes af det administrative personale.
    - E-mails lukkes som udgangspunkt dagen efter fratrædelse, hvis ikke andet anses som nødvendigt (ledelsesbeslutning).
    - E-mails slettes som hovedregel efter 30 dage fra fratrædelsesdato i LUDUS.

2. vucvestnet.dk: Exchange-server i 365.

    - Denne mailkonto benyttes både af det administrative personale og undervisere.
    - E-mails deaktiveres dagen efter fratrædelse og vil være deaktiveret i 90 dage, hvor der er mulighed for at genskabe alle data med hjælp fra IT-afdelingen.
    - Efter 90 dage slettes alle data.

3. vucvestuv.dk: Exchange-server i 365.

    - Denne mailkonto benyttes af kursister.
    - E-mails deaktiveres dagen efter udmeldelse og vil være deaktiveret i 90 dage, hvor der er mulighed for at genskabe alle data med hjælp fra IT-afdelingen.
    - Efter 90 dage slettes alle data.

Alle arbejdsrelaterede e-mails, der er modtaget efter fratrædelsen, vil blive åbnet af VUC Vest. Private e-mails, som modtages i denne periode, vil blive slettet.

Private mails
Der må godt sendes private e-mails fra i VUC Vests mailsystem. Der kan i mindre omfang sendes og modtages private mails på din VUC Vest e-mailadresse i arbejdstiden, idet det forudsættes, at dette ikke er i vejen for optimal udførelse af medarbejderens arbejdsopgaver. VUC Vest opfordrer dog til, at man benytter egen privat e-mail til private mails. Desuden understreges det, at benytter man VUC Vests mailsystem til private mails, må disse IKKE indeholde personfølsomme data.

Der vil ikke finde gennemsyn sted af medarbejderes private e-mails, som er mærket "privat", uden der er indhentet samtykke til dette. Den eneste undtagelse er, hvis der opstår en specifik sag, og det er dokumenterbart, sagligt og driftsmæssigt begrundet. Kun VUC Vests øverste ledelse kan anmode om et specielt gennemsyn.

E-mailkonto på mobil eller tablet
Installere man en VUC Vest e-mailkonto på en mobil eller tablet (det gælder også privatejede enheder), så vil det være opsat således, at man skal have en kode på telefonen, for at kunne installere e-mailkontoen. Desuden accepterer man, at IT-afdelingen på VUC Vest kan slette alt, der ligger på enheden, hvis man får enheden stjålet/mister den. (Alt hvad man har liggende i 'skyen' eller lignende bliver ikke slettet, kun det, der er gemt lokalt på ens telefon).

Indskærpet tavshedspligt
De medarbejdere, som står for serverdriften af e-mailsystemet, har en indskærpet tavshedspligt i overensstemmelse med reglerne om persondataloven.

Fravær fra arbejdspladsen og autosvar
Hvis en medarbejder har planlagt fravær fra arbejdspladsen, skal man sørge for, at der er taget stilling til, hvad der skal ske med den indkomne post (evt. videresendes til en stedfortræder). Der skal altid opsættes autosvar, hvoraf det fremgår, hvornår man er retur på sin arbejdsplads, og hvem der modtager post indtil da.

Ordentlig mailskik
Når man anvender e-mails eller andre elektroniske kommunikationsformer i forhold til kursister, kolleger, eksterne samarbejdspartnere eller myndigheder, er det forbudt:

- at afsende e-mails med et strafbart indhold
- at afsende e-mails med et krænkende eller chikanøst indhold - fx filer med truende, anstødeligt, pornografisk, racistisk eller obskønt indhold - er du i tvivl, så undlad at sende
- at bruge VUC Vests e-mail på en sådan måde, at det skaber konflikt med VUC Vests interesser
- at bruge VUC Vests e-mail på en sådan måde, at der er risiko for systemnedbrud.

Aktiviteter af ovenstående og lignende karakter betragtes som væsentlig misligholdelse af ansættelses- eller kursistforholdet - med de deraf følgende konsekvenser.

Det er derudover ikke tilladt at rundsende jokes eller lignende til et større antal af postmodtagere fx via vores fælles distributionslister.

Deling af billeder
Vær opmærksom på, at hvis man deler billeder af kursister og kolleger via e-mail (eller anden elektronisk kommunikationsform), og hensigten er, at billederne skal bruges offentligt, så skal der som

minimum indhentes mundtlig samtykke fra de personer, der er på billederne – skal de benyttes til markedsføring, skal der foreligge skriftligt samtykke. Læs mere om dette i *Procedurer for brug af billeder*, der ligger her: VUCintra/1. Administration/procedurer – hvor man også kan finde de forskellige samtykkeerklæringer.

Malware (skadelig software)

Vær særlig opmærksom på e-mails, som kan indeholde malware, og derfor kan udgøre en trussel for såvel egne som andres data. Åbn aldrig vedhæftede filer eller klik på links i e-mails fra afsendere, som ikke kendes. Henvendelse til VUC Vests IT-afdeling i tvivlstilfælde.

1.9 Internet og netværk

Vi opfatter internettet som en uvurderlig kilde til information, men vi tillader under ingen omstændigheder surfing efter/på eller download af pornografisk eller på anden måde anstødeligt materiale, fx hjemmesider tilhørende ekstremistiske eller voldsbaserede grupperinger (Undtaget i undervisningsøjemed). Vi tager månedlige stikprøver, hvor vores IT-systemer logger internetaktiviteten for et par dage, hvorefter loggen bliver gennemgået og sidenhen slettet, hvis der ikke er noget at følge op på. Ud over stikprøver, kan der af sikkerhedsmæssige årsager forekomme analyser af vores netværkstrafik.

Overtrædelse af disse regler anses som en væsentlig misligholdelse af regler og retningslinjer på VUC Vest, og det kan i yderste tilfælde medføre ophævelse af ansættelsesforholdet og/eller bortvisning af både kursister og ansatte - uden varsel.

Navne standarder til netværket

For at kunne håndtere kursister og medarbejderes PC'ere på netværket, så det kører så optimalt som muligt, navngives PC'er udlånt til kursister med deres serienummer, og alle medarbejdernes PC'ere navngives med et fortløbende nummer.

Tilslutning af andet udstyr

Der må ikke tilsluttes udstyr til VUC Vests netværk ud over klienter i administrationen samt bærbare PC'er og mobiltelefoner.

Der må ikke være installeret fildelingsprogrammer på den bærbare PC, og der skal være installeret antivirus og nyeste Microsoft Software-opdateringer.

Udstyr og netværk

IP-adresser tildeles via DHCP server.

Anbefalinger for brug af offentligt tilgængelige netværk (Wifi)

Det er vigtigt, at du er opmærksom på, hvad du foretager dig, når du bruger ukendte offentlige tilgængelige netværk (Wifi) på fx hoteller, lufthavne og i tog – også hvis der er tilknyttet en adgangskode. En adgangskode til netværket er ikke en garanti for at selve netværket er sikkert. Det kan ikke garanteres, at andre der også har mulighed for at logge på det samme offentligt tilgængelige netværk ikke vil og kan finde svagheder i netværket og udnytte det til at overvåge, hvad andre på netværket foretager sig.

Derfor anbefaler vi, hvis det er muligt, at du bruger din mobil til at gå på nettet via internetdeling med sikker kode.

1.10 Mobiltelefoner og tablets

Smartphones til arbejdsbrug skal låses i form af adgangskode for at forhindre uautoriseret brug i tilfælde af, at man mister eller efterlader sin telefon. En låst enhed forhindrer uvedkommende direkte adgang til VUC Vests IT-systemer og fortrolige informationer. Man skal også opsætte telefonen til at låse automatisk efter fem minutter, hvis den ikke har været i brug. Opbevar pinkode og pukkode et sikkert sted. Se også retningslinjer for e-mailkonto installeret på mobil eller tablet i afsnit 1.8.

Kobles telefon eller tablet på et trådløst netværk, som man ikke kender, så undlad at udveksle fortrolig information. Vær kritisk, når der surfes på internettet. Download ikke filer fra hjemmesider, som man ikke er sikker på.

Opbevar ikke kodeord, brugernavne, netbankoplysninger eller cpr-numre på Smartphonen, uden at de er krypteret eller beskyttet af sikkerhedskoder.

1.11 Brug af USB-stik

Alle ansatte skal bruge krypterede USB-stik (USB-stik med kode), såfremt det materiale der gemmes indeholder personfølsomme oplysninger som navn, adresse, telefonnummer, cpr-nummer m.v.

1.12 Benyttelse af digital virksomhedssignatur, *IndFAK2, Statens Lønsystem (SLS), Danske Bank m.v.*.

Medarbejdere med digital virksomhedssignatur til VUC Vest, adgang til IndFAK2, Statens Lønsystem (SLS), Danske Bank m.v. må udelukkende anvende disse systemer i arbejdsøjemed.

Ethvert erstatningskrav og de deraf evt. kommende sagsomkostninger, der måtte blive rettet mod VUC Vest som følge af misbrug af ovennævnte, vil blive videreført og gjort gældende mod medarbejderen.

1.13 Skrotning af gammelt hardware

Ved udfasning af hardware, tages harddisk ud og ødelægges, inden udstyret sendes til skrot.

1.14 Sletning af data på printserver og printere

Data slettes inden for 48 timer.

1.15 Sikkerhedsbrud på data

Ved sikkerhedsbrud på data kontaktes IT-afdelingen **STRAKS** på tlf.: 29 22 13 45. Der henvises i øvrigt til QUICKGUDE om ***Persondata og IT-sikkerhed***, som hænger på opslagstavlen i alle klasseværelser samt procedure for brud på persondatasikkerheden. Begge dokumenter kan findes på VUCintra, på VUC Vests hjemmeside i "footeren" nederst på alle sider på hjemmesiden og via nedenstående direkte links.

Direkte link:

Sikkerhedsbrud:
https://www.vucvest.dk/media/13048/procedure-ved-brud-paa-persondatasikkerheden.pdf

QUICKGUIDE:
https://www.vucvest.dk/media/13107/quickguide-persondata-og-it-sikkerhed.pdf