Retningslinje for ledelsens adgang til medarbejdernes mails og elektroniske data

1. Baggrund og formål

Denne retningslinje har bl.a. til formål at orientere KU's medarbejdere om, at KU's ledelse under visse særlige betingelser og under iagttagelse af visse formelle procedurer[1] (se afsnit 2), via særligt betroede IT-medarbejdere kan skabe adgang til at tilgå og/eller læse medarbejderes relevante mails samt relevante elektroniske data. Formålet er desuden at beskrive rammerne om denne ret til adgang.

KU-computere, KU-iPads, KU-internet og relaterede ressourcer er KU's ejendom, og bør som hovedregel kun anvendes til arbejdsrelaterede formål. Som udgangspunkt har KU's ledelse[2] ikke adgang til indholdet i medarbejderes mails eller elektroniske data, som f.eks. browserhistorik. Det kan dog være nødvendigt at skabe adgang til at tilgå og/eller læse medarbejdernes mails/elektroniske data. Det kan ske af driftsmæssige grunde, eller når der er et andet konkret begrundet sagligt formål som fx, hvis medarbejderen er længerevarende syg, og ligger inde med materiale, som det ikke er muligt at tilgå på anden vis, eller hvis der er begrundet mistanke om brud på IT-sikkerheden eller begrundet mistanke om ulovlige aktiviteter på KU's IT-udstyr.

2. Rammer for ledelsens adgang

KU´s ledelse har som udgangspunkt ikke ret til at gøre sig bekendt med indholdet i elektroniske mails/data til og fra medarbejderne. KU´s ledelse kan dog gøre sig bekendt med en medarbejders elektroniske mails /data i tilfælde, hvor det konkret kan begrundes, at tjenstlige eller tekniske hensyn klart overstiger hensynet til fortrolighed. Andre undtagelser kan gøres, f.eks. på anmodning fra en afdød medarbejders efterladte. Adgangen forudsætter godkendelse af rektor, prorektor, dekan eller universitetsdirektør som beskrevet i Sikkerhedsvejledning om adgangsstyring.

Medarbejderen skal på forhånd orienteres om, at der gives adgang til dennes mail og/eller elektroniske data samt om begrundelsen for dette. Er det ikke muligt at orientere medarbejderen i forvejen og kan adgangen ikke udskydes, skal medarbejderen efterfølgende og hurtigst muligt orienteres om, at der er givet adgang.

Medarbejdere kan for at sikre sig mod, at private mails eller anden privat elektronisk data læses, sørge for at disse tydeligt er markeret "Privat" fx i emnefeltet på mails eller i titlen på mapper og lignende.

I tilfælde, hvor der er begrundet mistanke om misligholdelse af ansættelsesforholdet eller strafbare forhold vil medarbejderen ikke blive orienteret på forhånd. Medarbejderen skal dog altid orienteres hurtigst muligt efterfølgende. Hvis en gennemgang af medarbejderens mails eller elektroniske data underbygger mistanken om misligholdelse af ansættelsesforholdet, følges reglerne i KU's retningslinjer om håndtering af misligholdelse af ansættelsesforholdet og uansøgt afsked. Medarbejderen opfordres i alle situationer, hvor der er givet adgang, til at lade sig bistå af sin tillidsrepræsentant eller en anden bisidder.

---

[1] Adgangen forudsætter godkendelse af rektor, prorektor, dekan eller universitetsdirektør. Det er yderligere beskrevet i "KU's informationssikkerhedspolitik" og "Sikkerhedsvejledning om adgangsstyring"

[2] Med ledelse forstås her den afskedigelsesbemyndigede leder.

Gennemgang af en medarbejders mails eller elektroniske data forudsætter, at der er to betroede it-medarbejdere til stede mens det sker.

KU's IT-afdeling udfører løbende maskinel overvågning af KU's IT-systemer. De betroede medarbejdere, der følger op på denne maskinelle overvågning, må kun dele de opnåede informationer med nødvendige kolleger i IT-afdelingen og bl.a. ikke med den berørte medarbejders nærmeste ledelse, medmindre der er tale om mistanke om misligholdelse af ansættelsesforholdet.3

3. Samarbejdsudvalgets rolle

Samarbejdsudvalg på alle niveauer er med til at udbrede kendskabet til retningslinjen blandt medarbejdere og ledere. Samarbejdsudvalg kan desuden drøfte om retningslinjerne giver anledning til særlig indsats lokalt. Hovedsamarbejdsudvalget har til opgave at sikre, at retningslinjen fortsat er aktuel og justeres når det skønnes nødvendigt med henvisning til den tekniske, it-sikkerheds- og systemmæssige udvikling.

4. Gyldighed og opsigelse

Retningslinjerne træder i kraft ved vedtagelse i HSU.

Opsigelse følger samarbejdsudvalgscirkulærets regler, ifølge hvilke hver af parterne kan opsige fastlagte retningslinjer med 3 måneders varsel. Inden opsigelsen skal samarbejdsudvalget forsøge at ændre de hidtidige retningslinjer på en måde, som er tilfredsstillende for samarbejdsudvalgets parter.

Retningslinjerne er behandlet og vedtaget af Hovedsamarbejdsudvalget den 28.november 2022 og erstatter de tidligere retningslinjer vedtaget 22.oktober 2008.

Henrik C. Wegener
Rektor, formand for HSU

Ingrid Kryhlmand
Næstformand for HSU

[3] Dette er nærmere beskrevet i notat om sikkerhedsaktiviteter på IT-systemer. Den kan findes i medarbejderguiden under IT-vejledninger