IT-regler gældende for Danmarks Medie- og Journalisthøjskole

Retningslinjer for studerende og medarbejdere ved Danmarks Medie- og Journalisthøjskole vedrørende brugen af organisationens IT-ressourcer

Indhold

1. Formål med IT-reglerne
Danmarks Medie- og Journalisthøjskole (højskolen) ønsker med IT-reglerne at fastlægge rammerne for opretholdelsen af et stabilt og velfungerende IT-system med et minimum af forstyrrelser af driften, samtidig med at brugernes privatliv, brevhemmelighed og personlige oplysninger søges beskyttet som foreskrevet i lovgivningen. Retningslinjerne er udstedt af rektoratet i samarbejde med IT-funktionen.

For at opretholde en optimal drift af organisationens IT-systemer og undgå diverse forstyrrelser er det nødvendigt med interne retningsliner, der klart præciserer den gældende lovgivning i forbindelse med anvendelsen af organisationens IT-ressourcer.
Persondataloven af 1. juli 2000 kræver, at højskolen, i lighed med andre virksomheder og institutioner, udformer en skriftlig information, der klart beskriver formålet med indsamling og registrering af persondata, hvis en sådan indsamling eller registrering forekommer i forbindelse med opretholdelsen af IT-systemerne. Derfor præciserer IT-reglerne også klart, hvordan og i hvilke tilfælde IT-funktionen overvåger/inspicerer indholdet af studerende eller medarbejderes e-mail eller på anden måde registrerer disses aktiviteter på eksempelvis Internettet.
Alle studerende og medarbejdere ved højskolen skal gøre sig bekendt med disse retningslinjer.

2. Hvem er omfattet af IT-reglerne

Alle medarbejdere og studerende ved højskolen er omfattet af IT-reglerne i de tilfælde, hvor organisationens IT-ressourcer benyttes.

3. Hvad er omfattet af IT-reglerne

IT-reglerne omfatter al benyttelse af højskolens IT-ressourcer, også i de tilfælde, hvor IT-ressourcerne benyttes til rent private formål.

Med IT-ressourcer forstås:

- organisationens computere
- servere
- fællesarkiver
- mailservere
- Intranet (lokalt netværk)
- Internetforbindelse
- andet hard- og software, der er at betragte som højskolens ejendom, herunder IT-udstyr som er stillet til rådighed for medarbejdere i hjemmet.

I situationer, der falder ind under punkt 5.3 i disse retningslinjer, forbeholder højskolen sig ret til at slette, flytte og inspicere data, der befinder sig på organisationens IT-ressourcer. Dette gælder således også dokumenter, arkiver, e-mails etc.
Elektronisk post (e-mails) sendt og modtaget af medarbejdere på højskolen kan, i lighed med et hvert anden type dokument, i visse tilfælde være en sagsakt, hvorfor medarbejdere altid skal foretage en konkret vurdering af, om den enkelte e-mail bør gemmes og evt. videresendes til journalisering i rektoratet, hvor der er oprettet et særskilt automatisk elektronisk arkiv.

4. Generelle regler vedr. brugen af højskolens IT-ressourcer

Både studerende og medarbejdere på højskolen er forpligtet til at overholde retningslinjerne, når de benytter sig af højskolens IT-ressourcer. Du kan læse mere om organisationens IT-ressourcer på Intranettet.

Brugernavn og password er personligt og må aldrig overdrages til andre. Ved mistanke om at brugernavn/password er kendt af andre, skal IT-funktionen kontaktes.

Generelt gælder det, at højskolens IT-ressourcer (i form af CPU-kapacitet, terminaladgang, lagerplads, netværkstrafik mv.) er begrænsede, hvorfor de udelukkende må benyttes til deres rette formål, dvs. til undervisning, forskning og arbejdsopgaver. Det er dog ligeledes tilladt at anvende organisationens IT-ressourcer til private formål, så længe dette foregår på et acceptabelt niveau og i øvrigt ikke hindrer andre brugere i at bruge udstyret til undervisning, forskning eller arbejde.
For at undgå skader på organisationens IT-udstyr og for at sikre rene og ryddelige lokaler er det ikke tilladt at spise, drikke eller ryge i computerrum, der stilles til rådighed for de studerende på højskolen. Overtrædes disse ordensregler vil det medføre midlertidig eller permanent bortvisning fra de nævnte lokaler.

4.1 Forholdsregler i forbindelse med beskyttelse af IT-hardware og følsomme data
For, så vidt muligt, at forhindre tyveri af computere og deraf følgende tab og/eller spredning af følsomt datamateriale,

skal højskolens medarbejdere tage følgende forholdsregler:

- **Elektronisk lås (password) på alle computere som indeholder følsomme oplysninger**
  For at undgå spredning af fortroligt datamateriale som eksempelvis klagesager, detaljer om medarbejderes lønforhold og lign., skal alle computere som benyttes af administrative medarbejdere forsynes med et personligt password. Andre medarbejdere, hvis computere indeholder følsomme oplysninger (evalueringer, breve, højskolens brevpapir mv.), bør også beskytte disse oplysninger ved at forsyne computeren med en elektronisk lås. Herved er det muligt at forhindre uvedkommende i at få adgang til fortroligt datamateriale, hvad enten dette forsøges i det daglige arbejde, eller i den situation hvor computeren er blevet stjålet.
- **Tag systematisk backup af data**
  For at undgå at tabe vigtigt datamateriale ved tyveri eller beskadigelse af hardware, skal alle medarbejdere systematisk foretage backup af deres data. Dette kan foregå på højskolens fælles personaleserver. Ved henvendelse til IT-funktionen udleveres det password, som er nødvendigt for at få adgang til denne server. Meningen med backup er, at datamateriale gemmes to forskellige steder. Så det er altså ikke tilstrækkeligt (eller mere sikkert), udelukkende at gemme data på højskolens fællesserver, da denne i princippet ikke er bedre sikret imod funktionsfejl end medarbejdernes egne computere (se dog næste punkt). Medarbejdere i økonomifunktionen skal benytte afdelingens egen filserver. Alle studerende, som bruger højskolens fællesarkiver, skal også tage sikkerhedskopi af data, for det tilfælde, at systemet skulle gå ned og data derved gå tabt.

4.2 Brug af elektronisk post (e-mail)

4.2.1. Generelle regler for alle

Følgende regler gælder generelt vedrørende brugen af den af højskolen tildelte e-mailkonto:

- **Tjek din postkasse med elektronisk post jævnligt (flere gange om ugen)**
  Tjekkes postkassen jævnligt, er du sikker på at modtage alle vigtige oplysninger udsendt af højskolen og andre via e-mail.
- **Det er ikke tilladt at "spamme", dvs. sende uopfordrede e-mails ud til en stor gruppe modtagere**
  Det ikke er tilladt at anvende højskolens e-mailkonto til at chikanere andre ved brug af spam eller misbruge det elektroniske postsystem til at sende store mængder "junk mails", dvs. e-mails uden relevant indhold, som modtageren(e) ikke selv har indvilliget i at modtage.
- **Tjek modtagne e-mails for virus, inden du åbner eventuelle vedhæftede filer**
  Brugerne har selv ansvaret for skader på egne computere og evt. tabt data i forbindelse med computervirus. Computervira optræder bl.a. i form af inficerede programmer og dokumenter. Er du i tvivl om, hvordan du tjekker vedhæftede filer for kendte vira, er du velkommen til at henvende dig til IT-funktionen.
- **Det er ikke tilladt at påtage sig andre brugeres identitet**
  Ved udsendelse af e-mails skal afsenderen altid identificere sig med korrekt navn. Af samme grund er det ikke tilladt at videregive det personlige password til højskolens e-mailsystem til andre brugere. Ved mistanke om at brugernavn/password er kendt af andre, skal IT-funktionen kontaktes.

4.2.2. Ansatte

Fastansatte får udleveret et brugernavn og tilhørende DMJX -mailadresse.
Alle it-ydelser på højskolens netværk er bundet til brugernavn og password.
Dokumentation og manualer kan findes på www.dmjx.dk/manualer (Bemærk specielt afsnit 4.1, 5.2 og 5.3).
Man skal være ansat på højskolen i 3 måneder for at kunne få en DMJX.dk-mailadresse, hvilken - ud over at have Notes kalenderfunktion - giver adgang til at læse højskolens mailopslag. Alle andre kan få en mail.DMJX.dk-adresse (Mailport) ved henvendelse til Personaleafdelingen.
Mailpostadresseindehavere kan via nærmeste leder få adgang til at læse opslag. Lederen skal kontakte Personaleafdelingen skriftligt.
Når ansættelse ophører, inddrages brugerrettighederne (herunder også e-mailadressen) omgående. Der kan, såfremt det i særlige tilfælde er absolut nødvendigt, oprettes en meddelelse på den pågældende mailadresse om, at medarbejderens ansættelse er ophørt.
Det er personaleafdelingen, der opretter og sletter brugere.

4.2.3. Studerende

Studerende får udleveret et brugernavn og tilhørende mail.DMJX.dk-mailadresse.
Alle it-ydelser på højskolens netværk er bundet til brugernavn og password. (udleveres med e-mail-adressen).
Studerende får udleveret en opdateret beskrivelse af ydelser ved studiestart.
Dokumentation og manualer kan findes på www.dmjx.dk/manualer.
Ved endt studie slettes brugerrettighederne omgående .
Det er Studieadministrationen der opretter og sletter brugere.

4.3 Brug af netværk (herunder også trådløst) og Internetforbindelse
Ved brug af højskolens netværk og Internetforbindelse gælder følgende regler:

- **Kopiering af programmer er ikke tilladt uden forudgående tilladelse fra IT-funktionen**
  Hovedparten af de programmer, som højskolens computere er udstyret med, er underkastet licensbestemmelser, der forbyder, at programmerne kopieres og benyttes på andre maskiner. Dette forbud mod kopiering gælder også, selvom det rent teknisk skulle være muligt at foretage en kopiering uden at bryde sikkerhedssystemet.
- **Det er ikke tilladt at forsøge at bryde sikkerhedssystemer**
  Brud på sikkerhedssystemer eller forsøg på dette er strafbart, hvad enten der er tale om højskolens, andre virksomheders eller institutioners sikkerhedssystemer, hvorfor dette under ingen omstændigheder må foregå fra højskolens computere eller via højskolens Internetforbindelse.
- **Det er ikke tilladt at skaffe sig adgang til data eller programmer i andre brugeres filsystemer**
  Der må ikke gøres forsøg på at tilegne sig programmer eller data i andre brugeres filsystemer uden forudgående aftale med de pågældende brugere om dette. Reglen gælder også selvom det, rent teknisk, skulle være muligt at skaffe sig adgang til andre brugeres private data og programmer uden derved at bryde sikkerhedssystemet.
- **Distribution af ulovlig software eller data er ikke tilladt**
  Det er ikke tilladt at distribuere eller "share" (dele med andre på Internettet) software, herunder programmer, film og mp3-filer, som du ikke selv har rettighederne til.

4.4 Publicering af private www-sider
Ved publicering af private www-sider fra højskolens server gælder følgende regler:

- **Indholdet af web-siderne må ikke krænke dansk lovgivning**
  Indholdet må derfor eksempelvis ikke krænke de ophavsretlige regler eller indeholde personoplysninger, der ikke er tilladt i henhold til lovgivningen.
- **Alle www-sider skal være mærket med forfatterens navn og e-mailadresse**
- **Publicering af www-siderne må ikke medføre unødig belastning af højskolens IT-ressourcer**
  Ekstremt stort diskforbrug eller nettrafik må således ikke forekomme uden forudgående aftale med IT-funktionen.

4.5 Trådløst netværk
• Brugerne af det trådløse netværk har selv det fulde ansvar for medbragt computer og software
Hverken højskolen eller medarbejdere i IT-funktionen kan gøres ansvarlige for eventuelle ødelæggelser af hardware, software eller tab af data i forbindelse med benyttelse af det trådløse netværk på højskolen.

5. IT-funktionens overvågning og registrering af brugernes aktiviteter

Højskolen og IT-funktionen respekterer privatlivets fred, brevhemmeligheden, hemmeligholdelsen af personlige oplysninger og ophavsrettigheder i forbindelse med opretholdelsen af organisationens IT-ressourcer. I øvrigt er det højskolens opfattelse, at studerende såvel som medarbejdere som udgangspunkt respekterer og overholder de opstillede regler vedrørende brugen af organisationens IT-ressourcer. Derfor udføres der heller ikke rutineinspektioner eller andre former for rutineovervågninger af den enkelte bruger. Men, ved rutinegennemgang af IT-systemerne, kan medarbejderne i IT-funktionen uforvarende komme i kontakt med brugernes personlige oplysninger (se også afsnit 5.4).
Som det fremgår af afsnit 5.1, 5.2, 5.3 og 5.4 forbeholder højskolen sig ret til at overvåge og gennemgå den enkelte brugers aktiviteter og data, men kun i de tilfælde, hvor lovgivningen kræver det, eller hvor der er begrundet mistanke om misbrug af IT-ressourcerne.
5.1 Formålet med IT-funktionens overvågning og registrering af brugernes aktiviteter
Af hensyn til opretholdelsen af drift, sikkerhed, og eventuel genetablering og dokumentation foretages der sikkerhedskopiering/backup af stort set alle aktiviteter, der foregår på højskolens IT-system. Hvis denne sikkerhedskopiering/backup ikke blev foretaget, kunne der opstå situationer, hvor det ville være umuligt for højskolen at genetablere betydningsfulde oplysninger, dokumenter og andre former for sagsakter, som højskolen er forpligtet til at kunne genetablere jf. journalpligten. Manglende sikkerhedskopiering/backup, kan endvidere besværliggøre, at højskolen kan sikre effektiv opgradering.
5.2. Hvilken type oplysninger gemmer IT-funktionen
Alle transaktioner foretaget fra computere tilsluttet højskolens netværk logges. Transaktioner vedr. elektronisk post logges og gemmes i maksimalt en måned. Mht. transaktionerne på højskolens netværk, har IT-funktionen mulighed for at identificere oplysninger om:

1) hvilken computer/arbejdsstation der er brugt til en given transaktion,
2) hvilken bruger, der har været logget på netværket og foretaget en given transaktion,
3) adresserne på de søgte hjemmesider
4) dato og klokkeslæt for de foretagne søgninger.

Derudover har IT-funktionen mulighed for at overvåge brugernes e-mailkonti og i yderste konsekvens inspicere indholdet af afsendte og modtagne e-mails.

5.3 I hvilke situationer registrerer og gennemgår IT-funktionen den enkelte brugers aktiviteter
De i afsnit 5.2 nævnte oplysninger om brugernes aktiviteter der gemmes af højskolens IT-system, hører alle ind under betegnelsen "personlige data" og er derfor omfattet af Persondataloven af 1. juli 2000. Kun i ganske særlige tilfælde må højskolen/medarbejdere i IT-funktionen benytte oplysningerne om brugernes aktiviteter. De særlige tilfælde omfatter følgende situationer:

- **Når det kræves af gældende dansk lovgivning**
  Eksempelvis på forlangende af dansk politi i forbindelse med efterforskningen af overtrædelser af straffeloven.
- **Hvis der eksisterer begrundet mistanke om misbrug af højskolens IT-ressourcer**
  Eksempelvis chikane i form af afsendelse af "spam-mails" eller "junk-mails" i meget stor stil, jf. i øvrigt afsnit 4.2.
- **Ved reparation eller service af dataudstyr**
  I en sådan forbindelse skal IT-funktionen behandle oplysninger, som de måtte blive bekendt med, som fortroligt materiale, der under ingen omstændigheder må videregives eller anvendes.
- **Særlige omstændigheder**
  Herunder tekniske omstændigheder, hvor en gennemgang af den enkelte brugers aktiviteter er nødvendig for at lokalisere tekniske fejl og derved opretholde driften af IT-systemet. Indbefattet under særlige omstændigheder er også situationer, hvor en gennemgang af den enkelte brugers aktiviteter er nødvendig for at undgå personskade, tab af højskolens ejendom eller grove overtrædelser af højskolens interne retningslinjer i øvrigt.

5.4 Hvem har adgang til at gennemgå oplysningerne om den enkelte brugers aktiviteter
Som hovedregel er det udelukkende medarbejderne i højskolens IT-funktion, der har adgang til disse oplysninger med henblik på fejlfinding og opretholdelse af organisationens IT-systemer. Medarbejderne i IT-funktionen har strenge pålæg om ikke at forfølge brugernes personlige aktiviteter uden at have et klart og sagligt grundlag for at gøre dette. Hvis IT-medarbejderne under den normale vedligeholdelse af IT-ressourcerne uforvarende kommer i kontakt med personlige oplysninger, som f.eks. en brugers private e-mails, er det ikke tilladt for IT-medarbejderne at læse eller på anden måde gøre sig bekendt med indholdet af en sådan e-mail. I tilfælde med grove eller gentagne brud på de opstillede retningslinjer i denne IT-politik kan højskolens ledelse gives adgang til oplysningerne med henblik på en endelig vurdering af de studiemæssige/tjenstlige konsekvenser heraf (se også afsnit 6. vedrørende procedurerne ved mistanke om overtrædelser af reglerne vedr. højskolens IT-ressourcer).
I alle tilfælde, hvor en gennemgang af en brugers aktiviteter skønnes at være nødvendig, skal brugeren forinden informeres herom. Undtaget fra denne regel er særlige tilfælde, hvor det ikke umiddelbart er muligt at komme i kontakt med den pågældende bruger, og hensynet til opretholdelsen af IT-systemets drift klart overskygger hensynet til den enkelte bruger.

6. Procedurer ved mistanke om misbrug af højskolens IT-ressourcer

Overtrædes de opstillede regler for brugen af højskolens IT-ressourcer vil den enkelte bruger i første omgang modtage en henstilling fra IT-funktionen om for fremtiden at følge det opstillede regelsæt.
I alvorligere tilfælde med grove eller gentagne forsøg på misbrug af højskolens IT-ressourcer, kan IT-funktionen lukke for brugerens adgang til e-mail-systemet/netværket og efterfølgende foretage indberetning om misbruget/mistanken herom til rektoratet.
Særligt grove overtrædelser af de opstillede regler kan i sidste ende resultere i bortvisning af de studerende fra højskolen og få tjenstlige konsekvenser for medarbejderne.