KUNSTHØGSKOLEN I OSLO

Data disiplinerklæring vedtatt på styremøtet 28.04.2009

KHiO er av lovmessige grunner forpliktet til å kontrollere risiko og sikkert håndtere informasjon og tekniske ressurser. Når du gis tilgang til disse ressurser (informasjon, applikasjoner og utstyr), tillegges du samtidig et ansvar i forbindelse med informasjonssikkerhet. Vi deler alle et ansvar for å beskytte konfidensialitet, integritet og tilgjengelighet i den informasjon vi behandler og sikkerheten i det tekniske utstyret som benyttes.
Alle brukere av våre ressurser må være bevisst sine roller og sitt ansvar

1. **Sikkerhetstiltak** som blir satt i verk, skal følges. Jeg har lest, og er innforstått med de krav som stilles i Sikkerhetspolicy og denne erklæringen.
2. **Bruker-ID**. Jeg er selv ansvarlig for all bruk som gjøres med min bruker-ID. Avlogging skal skje ved arbeidets slutt og skjermbeskytter må benyttes med avlogging ved fravær (minimum 5 minutter og med passordaktivering) fra arbeidsplassen.
3. **Passord** legitimerer meg som rettmessig bruker av min bruker-ID. Passordet skal være personlig, og jeg skal holde det hemmelig for andre. Når jeg får beskjed om å bytte det, skal jeg velge et passord som ikke lett kan knekkes av andre (dvs. ikke navn, fødselsdato osv). Dersom andre har fått kjennskap til passordet, skal det umiddelbart byttes.Ved mistanke om misbruk av mitt passord, skal jeg gi beskjed til IT-avdelingen. Jeg er kjent med passordreglene.
4. **Kopiering** av lisensiert programvare er forbudt, med mindre virksomhetens avtale med leverandør uttrykkelig gir adgang til dette.
5. **Data** skal lagres i henhold til følgende regler:
   a. KHiO sine fellesområder lagres på nettverksdisker, med relevante tilganger, og som det tas backup av
   b. data av privat art og data som ikke er ment å deles med andre, kan lagres lokalt på egen PC på eget ansvar.
6. **Lagringsmedier** (eksempelvis USB memorystick, CD-plater, tape ol., samt papirdokumenter) som inneholder opplysninger som eies og/eller forvaltes av KHiO, skal jeg håndtere slik at dette ikke kommer på avveie.
7. **Skolens eiendom.** Utstyr som ansatte får i jobben er skolens eiendom og skal leveres tilbake når behov for bruk ikke lenger er tilstedet. IT-avdelingen har en lokal administrator konto på skolens maskiner. Denne kontoen skal ikke brukes av ansatte. Privat bruk av KHiOs datautstyr kan bare tillates i begrenset omfang etter avtale med nærmeste overordnet. Bruk i egen næring eller interesseområde er ikke tillatt.
8. **Innsyn.** KHiO har kun adgang til min e-post og "private dataområder" etter vilkårene i personopplysningsforskriftens § 9-2 og med prosedyrer for innsyn beskrevet i §9-3. Innsyn kan etter dette foretas når det er nødvendig for den daglige driften, og ved mistanke om grove brudd på arbeidsplikter eller norsk lovgivning. Prosedyrene for innsyn innebærer at jeg skal varsles så langt dette er mulig og med saklig begrunnelse. Personlig e-post skal samles i en egen mappe i mitt e-postarkiv. Det gjør et slikt arbeid enklere og det hindrer innsyn i mine private e-post.
9. **Internett** oppkobling i KHiO kan kun skje via KHiOs nettløsning. Tilgang til Internett skal primært brukes som en informasjonskilde relatert til min jobb/studiesituasjon.
10. **KHiO sin epost.** Å sende e-post fra din KHiO konto er å betrakte som å sende et brev med KHiO sitt brevhode. Junk-mail, kjedebrev o.l. tillates ikke distribuert/ videreformidlet. Registreringer ol på Internett, skal ikke skje med KHiO sin epost i den grad det er mulig.
11. **Nedlasting av programvare** tillates ikke uten at det er eksplisitt tillatt av IT avdelingen. For ordens skyld påpekes det at søk og nedlasting av annet materiale ikke må være i strid med norsk lov, eksempelvis åndsverksloven. All aktivitet på virksomhetens nettverk kan logges av sikkerhetsgrunner.
12. **Personopplysninger** skal krypteres ved distribusjon.
13. **Kartlegging av systemsvakheter.** Medarbeidere/studenter skal ikke, på eget initiativ, foreta kartlegging eller testing av mulige svakheter i KHiO sine systemer og/ eller nettverket, eller på annen måte drive "Hacking" mot interne eller eksterne systemer.
14. **Private bærbare maskiner** skal ikke tilknyttes det kabelbaserte interne nettet uten forhåndsgokjenning fra IT-avdelingen. Den ansatte/studenten har ansvar for selv å sikre at enheten til enhver tid er sikkerhetsmessig oppdatert (antivirus, OS oppdateringer, ol.).
15. **Bruk av PDA** koplet til KHiOs nettverk (slik som for eksempel synkronisering mot Exchange), skal være godkjent av IT avdelingen. Den ansatte/studenten har ansvar for selv å sikre at enheten til enhver tid er sikkerhetsmessig oppdatert (antivirus, OS oppdateringer, kryptering etc).
16. **Kontroll mot fiendtlig kode.** Det skal vises aktsomhet ved åpning av epost fra ukjente, bruk av "Lynmeldingstjeneste" (IM), og aktivisering av linker og vedlegg i ukjente epost, lynmeldinger og websider ol. Alt som mottas gjennom USB-minnebrikker, CD-er ol., skal virussjekkes uavhengig av avsender. Ved mistanke om virus, kontaktes IT avdelingen.
17. **Rapportering.** Sikkerhetshendelser og mistanke om sikkerhetshendelser skal rapporteres til nærmeste leder/studieleder, og/eller sikkerhetsansvarlig (CSO).
18. **Som vert for besøkende** som skal arbeide på KHiO eller på KHiOs utstyr, forplikter jeg meg i samarbeid med den besøkende, å påse at taushetserklæring er forstått og akseptert (underskrevet), samt at Sikkerhetspolicy blir overholdt.
19. **Sanksjoner.** Brudd på ovennevnte vil medføre sanksjoner

Jeg har lest, forstått og aksepterer innholdet i denne erklæring. Jeg er kjent med at jeg kan bli holdt ansvarlig for brudd på regler gitt i denne datadisiplinerklæringen, og at slike brudd kan få erstatningsmessige konsekvenser i tillegg til konsekvenser for mitt arbeids/studieforhold. Denne signering gjelder den til enhver tid gjeldende Datadisiplinerklæring. Siste versjon er tilgjengelig på intranett. Avvik skal uten opphold meldes sikkerhetsansvarlig (CSO).

Navn: .....

Sted: .....

Dato: .....

Signatur: