IT-reglement for HØGSKULEN I VOLDA
VOLDA UNIVERSITY COLLEGE

Høgskulen i Volda (HVO) er av lovpålagt 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 konfidensialiteten, 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. La sikkerhet starte med deg – La sikkerhetsholdning være en del av dine daglige rutiner uansett om du befinner deg på kontoret, på reise eller arbeider hjemme.

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 sikkerhetsansvarlig. 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 på nettverket i henhold til gjeldende regler:
   - HVO sine fellesområder lagres på nettverksdisker og med relevante tilganger, og som det tas backup av
   - Data av privat art og som ikke er ment å deles med andre, skal lagres lokalt på egen PC hvor det ikke tas backup

6. **Lagringsmedier** (eksempelvis USB minnepinne, CD-plater o.l., samt papirdokumenter) som inneholder opplysninger som eies og/eller forvaltes av HVO, skal jeg håndtere slik at dette ikke kommer på avveie.

7. **Privat bruk** av datautstyr (PCer/servere/øvrig infrastruktur), kan bare tillates i begrenset omfang. Bruk i egen næringsvirksomhet er under ingen omstendigheter tillatt.

8. **Innsyn.** HVO har ikke adgang til min e-post og «private dataområder» uten min godkjennelse. Dersom noe uforutsett (ulykke e.l.) gjør det nødvendig å gå inn på ansattes e-post, gjør nærmeste leder dette sammen med lokalt verneombud. Du oppfordres derfor til å samle personlig e-post i en egen mappe i ditt e-postarkiv. Det gjør et slikt arbeid enklere og det hindrer innsyn i dine private e-post. E-post og filer som HVO forstår eller burde forstå er av privat karakter, forblir beskyttet etter reglene om personvern.

9. **Internett** oppkobling ved bruk av HVOs datamaskiner kan kun skje via HVOs nettløsning. Tilgang til internett skal primært brukes som en informasjonskilde relatert til min jobbsituasjon.

10. **HVO sin epost.** Å sende e-post fra min HVO-konto er å betrakte som å
sende et brev med HVO sitt brevhode. Junk-mail, kjedebrev o.l. tillates
ikke distribuert/videreformidlet. Registreringer o.l. på internett, skal
ikke skje med HVO sin epost i den grad det er mulig.

11. **Nedlasting** for oppdatering og test av eksisterende programvare tillates. Nedlastning av ny programvare fra ukjente leverandører og/eller nettsteder, tillates ikke uten godkjenning fra IT-leder. For ordens skyld påpekes det at søk og nedlasting ikke må være i strid med norsk lov, eksempelvis åndsverksloven. All aktivitet på internett kan logges av sikkerhetsgrunner.

12. **Personopplysninger** skal krypteres ved distribusjon.

13. **Kartlegging av systemsvakheter.** Medarbeidere skal ikke på eget initiativ foreta kartlegging eller testing av mulige svakheter i HVO sine systemer og/eller nettverket, eller på annen måte drive «hacking» mot interne eller eksterne systemer.

14. **Privat PC** skal ikke tilknyttes det kabelbaserte interne nettet. Den ansatte har ansvar for selv å sikre at enheten til enhver tid er sikkerhetsmessig oppdatert (antivirus, OS oppdateringer o.l.)

15. **Bruk av nettbrett/mobiltelefon** koplet til HVOs nettverk (slik som for eksempel synkronisering mot Exchange), skal være godkjent av IT-kontoret. Den ansatte har ansvar for selv å sikre at enheten til enhver tid er sikkerhetsmessig oppdatert (antivirus, OS oppdateringer o.l.)

16. **Kontroll mot fiendtlig kode.** Det skal vises aktsomhet ved åpning av e-post fra ukjente og aktivisering av linker og vedlegg i ukjente e-postmeldinger, chat-samteler og websider ol. Alt som mottas gjennom USB-minnebrikker, CD-er o.l., skal virussjekkes uavhengig av avsender. Ved mistanke om virus, kontaktes IT-kontoret.

17. **Rapportering.** Sikkerhetshendelser og mistanke om sikkerhetshendelser skal rapporteres til nærmeste leder, og/eller sikkerhetsansvarlig.

18. **Som vert for besøkende** som skal arbeide på/med HVOs 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, ref. sikkerhetspolicy.

Jeg har lest og 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 arbeidsforhold. Denne signering gjelder den til enhver tid gjeldende Datadisiplinerklæring. Avvik skal uten opphold meldes sikkerhetsansvarlig.	*Navn:* *Sted:* *Dato:*	*Signatur:*