

IT-reglement for Universitetet i Stavanger

Dette reglement gjelder for bruk av universitetets IT-tjenester. Med *IT-tjenester* siktes det til felles maskiner og IT-systemer, nettverk, programmer, data m.v. som stilles til disposisjon av universitetet inklusive lokale, nasjonale og internasjonale nettverk eller andres maskiner og systemer som man får tilgang til gjennom slike ressurser. Reglementet gjelder for ansatte, studenter og andre som får tilgang til IT-tjenestene, såkalt *brukere*.

Reglementet skal være oppslått på egnede steder som f.eks. pc-stuer samt finnes tilgjengelig på elektronisk form. Det kan fås ved henvendelse til den lokale IT-avdelingen. Reglementet skal også deles ut ved første gangs brukerregistrering, eller på annen måte gjøres kjent for brukerne.

En bruker plikter å holde seg informert om det til enhver tid gjeldende reglement og eventuelle supplerende bestemmelser. Slike bestemmelser skal godkjennes av IT-faglig råd.

Brudd på regler om personvern, taushetsplikt m.m. kan føre til erstatningsplikt og/eller straff. De vanlige regler om oppsigelse eller avskjed av arbeidstakere eller disiplinærforføyning mot studenter vil kunne ramme misbrukere av IT-tjenestene.

Innhold

1. **Ivaretagelse av rettigheter**
2. **Brukers plikter**
3. **Bruk av privat IT-utstyr ved UiS**
4. **Datasikkerhet**
5. **Personvern**
6. **UiS-ITs rett til innsyn**
7. **Sanksjoner ved brudd på reglementet**
8. **Informasjonstjenere ved UiS**
9. **Nettikette**

1. **Ivaretagelse av rettigheter**

- Brukerne forplikter seg til å respektere andres rettigheter, og er derfor avhengig av avtale med rettighetshaver. Dette gjelder både programvare og annen rettighetsbelagt informasjon som tekst, bilde og lyd.
- Brukerne har selv ansvaret for bruk av opplysninger, programmer m.v. som gjøres tilgjengelig gjennom IT-tjenestene.
- Brukerne har ikke adgang til å kopiere programmer og data ved hjelp av universitetets utstyr utover det som følger av de lisensavtaler som universitetet har inngått.

- Brukerne har selv ansvaret for bruk av opplysninger, programmer m.v. som gjøres tilgjengelig gjennom IT-tjenestene.
- Universitetet fraskriver seg ansvar for økonomisk tap som følge av feil eller mangler i programmer, data, bruk av opplysninger fra tilgjengelige databaser eller andre opplysninger innhentet gjennom nettet m.v.

2. Brukers plikter

IT-ressursene ved Universitetet i Stavanger er et redskap til støtte i daglig arbeid, undervisning, forskning og studier. Dette omfatter datamaskiner, skrivere, nettverk, internett og programvare. Ressursene er begrensede og alle har et ansvar for at utstyret blir brukt effektivt til de oppgaver det er beregnet for. Mange av ressursene er knyttet sammen via nettverket, lokalt og nasjonalt, og kan benyttes til kommunikasjon og informasjonsinnhenting. I denne sammenheng må man oppføre seg i henhold til enkle etiske standarder, likt med de regler man har for alminnelig god oppførsel i andre sammenhenger i samfunnet.

Ved Universitetet i Stavanger forventes det at brukere av IT-tjenestene følger visse regler:

- UiS har regler for bruk av IT-tjenestene som både ansatte og studenter skal følge.
- I visse sammenhenger er det mulig for master- og doktorgradsstudenter ved universitetet å knytte eget datautstyr til universitetets nettverk. Alt annet utstyr som ikke er kjøpt inn gjennom IT-avdelingen tillates ikke knyttet opp mot skolens nett.
- Studenter skal til enhver tid kunne legitimere seg med studiekort når datautstyr brukes.
- Når en bruker skal identifisere seg ved bruk av IT-tjenestene er vedkommende forpliktet til alltid å identifisere seg med sitt eget brukernavn, passord eller på annen regulær måte.
- Brukerne har plikt til å følge driftspersonalets anvisninger om bruk av IT-tjenester. De har også plikt til å sette seg inn i bruksanvisning, dokumentasjon m.v. på forsvarlig måte, slik at muligheten for av uvitenhet å skape risiko for driftsforstyrrelser eller tap av data, programmer eller utstyr reduseres.
- Ved opphør av ansettelses-, studie- eller brukerforhold er brukeren ansvarlig for at kopier av data, programmer m.v. som eies/disponeres av universitetet sikres av IT-avdelingen. Andre filer m.v. som er lagret under brukerens navn eller lignende skal brukeren selv slette. Skjer dette ikke innen rimelig tid, og **senest innen 3 måneder**, kan IT-avdelingen (UiS-IT) slette slike filer.

3. Bruk av privat IT-utstyr ved UiS

Master- og doktorgradsstudenter har anledning til å knytte egen datamaskin til Universitetets nett forutsatt at reglene for dette følges:

- IT-avdelingen har intet ansvar for utstyret. Eventuelle skader og tap som oppstår ved bruk eller misbruk av utstyret bæres av utstyrets eier(e). IT-avdelingen kan ikke forventes å stille utstyr til disposisjon for å gjøre det mulig å knytte utstyr til lokalnettet. Før utstyr plasseres i universitetets lokaler, må følgende avklares med IT-avdelingen:
 - hvem som er eier(e) av enheten
 - hvem som har driftsansvar for enheten (en person)
 - hvem som har adgang til å bruke enheten evt. nettverksadresse fysisk lokalisering av IT-utstyret.
- Utstyret og evt. programvare skal konfigureres slik driftspersonale i IT-avdelingen anviser.
- Utstyret skal ikke brukes av andre personer enn de som allerede er registrert som brukere av universitets datautstyr. Dette innebærer at det ikke skal registreres brukere på Unix-maskiner eller andre flerbrukermaskiner som ikke er ansatt eller studerer ved universitetet eller som har annen tilknytning til universitetet.
- Tjenerfunksjoner, informasjonsbaser o.l. for eksempel ftp- eller www-tjenere som vil være tilgjengelige fra utstyr utenfor skolens lokalnett via eksterne kommunikasjonskanaler skal ikke igangsettes uten spesiell og eksplisitt tillatelse fra driftspersonalet i IT-avdelingen.
- Utstyret skal ikke benyttes til ikke-autorisert lagring eller distribusjon av programvare. Dette gjelder også lovlig programvare som freeware og shareware.

4. Datasikkerhet

- Brukere ved universitetet registreres som brukere av datasystemet og tildeles et brukernavn med tilhørende passord. Det er brukerens plikt å beskytte brukernavn og passord for å unngå uautorisert bruk. Det er ikke tillatt å skaffe seg uautorisert adgang til dataressursene ved å benytte andre brukernavn enn ens eget.
- Det er ikke tillatt å skaffe seg adgang til andre brukeres data, programvare og lagringsområder uten eksplisitt tillatelse fra den andre brukeren.
- En bruker må ikke bidra til at det oppstår avbrudd i noen del av systemet eller på annen måte forårsake ulempe for andre.
- Det er ikke tillatt å opptre anonymt, bruke pseudonym eller oppgi falsk identitet på nettverket. Dette gjelder også alle tjenester på internett.
- Det blir daglig tatt sikkerhetskopiering av alle data som ligger på de sentrale serverne. For data som ligger på andre lagringsenheter er brukeren selv ansvarlig for sikkerhetskopiering.

- Datamaskiner skal ikke modifiseres uten eksplisitt tillatelse fra ved IT-drift. Det er ikke tillatt å skru fra hverandre utstyr, fjerne deler, sette inn deler, forandre maskin- og/eller programkonfigurasjoner, eller fjerne utstyr fra det stedet hvor det befinner seg. Alle må være observante, og være med på å sikre universitetet mot tyverier ved at regler for adgang til bygninger og utstyr følges.
- Brukere har ikke lov å sette opp eller bruke selveie IT-utstyr på universitetet uten at dette er klarert med IT-avdelingen (se søknadsskjema).
- Det er ikke lov å sette opp egne informasjonstjenere (www, ftp, irc o.l.) eller flerbrukersystemer (Linux, Unix, NT-server o.l.) uten avtale med IT-avdelingen (se søknadsskjema).
- Universitetet reserverer seg retten til uten varsel å kontrollere, inspisere, endre eller fjerne enhver datafil eller systemressurs som undergraver autorisert bruk av datautstyret.
- Forsøk på å hindre systemansvarlige adgang til systemressurser anses som uautorisert bruk.
- Universitetet fraskriver seg ansvar for ethvert tap som oppstår som følge av arbeidet med å bevare systemintegriteten i datanettverket.

5. Personvern

- En bruker må ikke søke å oppnå uautorisert tilgang til andres data, programmer m.m, eller søke å gjøre seg kjent med andres passord eller andre sikkerhetslementer.
- En bruker plikter å gjøre seg kjent med de regler som særlig gjelder for personlige opplysninger. Datamaskinbaserte filer som inneholder opplysninger om enkeltpersoner eller om selskaper eller organisasjoner (fysiske og juridiske personer) vil normalt bare kunne opprettes etter samtykke fra Datatilsynet.
- Hvis en bruker ønsker å registrere personlige opplysninger, plikter vedkommende å forsikre seg om at det er adgang til dette etter personregisterloven eller forskrifter gitt med hjemmel i loven, eller i medhold av konsesjon gitt til universitetet. Dersom registeret ikke vil være tillatt etter de nevnte regler, plikter brukeren selv å søke om nødvendig tillatelse. Den som har ansvar for driften vil kunne gi veiledning om hvordan brukere skal forholde seg.

6. UiS-ITs rett til innsyn

- IT-avdelingen har rett til å søke tilgang til den enkelte brukers reserverte områder i anlegget med sikte på:

1. sikre anleggets funksjonalitet

2. kontrollere at brukeren ikke krenker eller har krenket dette reglements bestemmelser. Det forutsettes at slik tilgang bare søkes når det er av stor betydning for driften eller universitetets ansvar, og kun ved særlig grunn til mistanke. Tillatelse til innsyn i elektronisk post skal søkes særskilt. IT-avdelingen har ikke adgang til en brukers reserverte områder uten etter spesiell tillatelse fra IT-sjefen, Ressursdirektøren eller Universitetsdirektøren.
- Hvis IT-avdelingen søker slik tilgang, skal det på forhånd innhentes tillatelse fra Universitetsdirektøren, med mindre det foreligger særlig tungtveiende grunner til øyeblikkelig inngrep. Slike tungtveiende grunner skal dokumenteres overfor Universitetsdirektøren i etterkant av inngrepet.
 - Hvis bruken av arbeidsstasjon, terminal eller annet sluttbrukerutstyr på grunn av driftssikkerhet eller av andre hensyn overvåkes av IT-avdelingen, skal dette opplyses med merke på enheten eller på annen hensiktsmessig måte.
 - IT-avdelingen har taushetsplikt med hensyn til opplysninger om brukeren eller brukerens virksomhet som fås på denne måten, med det unntak at forhold som kan representere brudd på reglementet kan meddeles til overordnede instanser.

7. Sanksjoner ved brudd på reglementet

- Ved brudd på dette reglementet kan brukers tilgang til Universitetets dataanlegg stenges helt eller delvis. For å avklare om et brudd har skjedd og omstendighetene rundt det kan driftsansvarlig stenge ute en bruker i inntil 5 arbeidsdager.
- Ved brudd på reglementet foretatt fra definerte deler av dataanlegget kan koblingen mellom denne delen og Universitetets øvrige nettverk stenges helt eller delvis. For å avklare om et brudd har skjedd og for å sikre mot nye brudd, kan driftsansvarlig stenge tilkoblingen helt i inntil 5 arbeidsdager. Ressursdirektøren eller Universitetsdirektøren bemyndiger avgjør om tilknytningen til Universitetets øvrige nettverk deretter skal stenges helt eller delvis.
- Brudd på reglementet skal rapporteres vedkommendes fakultet eller enhet som avgjør om brukerens tilgang til Universitetets dataanlegg skal stenges helt eller delvis. Vedkommendes fakultet eller enhet skal også vurdere om overtredelsen skal føre til disiplinære forføyninger.

8. Informasjonstjenere ved UiS

- I undervisningsøyemed kan det være praktisk at ansatte, studenter eller grupper ved UiS får tillatelse til å drive en egen informasjonstjenere knyttet til nettverket. Etter avtale med IT-avdelingen kan dette gjøres under forutsetning av at følgende regler blir fulgt.

- IT-avdelingen og universitetet har intet ansvar for programvaren og informasjonen som formidles. Eventuelle skader og tap som oppstår ved bruk eller misbruk bæres av den som har ansvaret for driften av tjeneren.
- IT-avdelingen kan ikke forventes å stille utstyr og programvare til disposisjon for å gjøre det mulig å knytte tjeneren til lokalnettet. Før en informasjonstjener etableres i universitetets lokaler, må følgende avklares med driftspersonalet i IT-avdelingen:
 - Hvem som har driftsansvaret for tjeneren (en person).
 - Hva slags informasjon som skal lagres.
 - Fysisk lokalisering av tjeneren.
 - Tjeneren skal konfigureres slik driftspersonalet i IT-avdelingen anviser.
 - Tjeneren skal ikke under noen omstendighet brukes til lagring og distribusjon av programvare og informasjon som ikke er lovlig og offentlig tilgjengelig.
- Personen som har driftsansvaret for tjeneren er også ansvarlig for at disse regler følges:
 - Tjeneren skal til enhver tid være tilgjengelig for driftspersonalet i IT-avdelingen.
 - IT-avdelingen kan ved behov koble tjeneren fra nettverket når som helst og uten forvarsel.
 - Tillatelsen er tidsbegrenset og gis bare for inneværende semester, dvs. frem til 31. juni eller 31. desember.

9. Nettikette (God oppførsel på nettet)

- Brukeren har et medansvar for at IT-ressursene utnyttes best mulig. Det siktes her til tid og kapasitet både for maskiner, nettverk og personale knyttet til virksomheten rundt IT-tjenestene.
- En bruker skal være meget tilbakeholden med bruk av IT-tjenestene til virksomhet som ikke har direkte tilknytning til faglig virksomhet, administrasjon, egen forskning, studier eller organisasjonsarbeid i tilknytning til universitetet.
- IT-tjenestene skal ikke brukes i kommersiell sammenheng eller til aktiviteter uten tilknytning til virksomheten som foregår ved universitetet.
- Brukere skal ikke benytte IT-tjenestene til å fremsette ærekrenkelser eller diskriminerende uttalelser, ulovlig nedlasting av musikk/film/pornografi eller formidle taushetsbelagte opplysninger, krenke privatlivets fred eller oppfordre eller medvirke til ulovlige eller reglementsstridige handlinger.
- Bruk av datautstyr og programvare som innebærer ressursbruk utenfor universitetet, skal begrenses og ikke utnyttes til eget tidsfordriv. Adgangen til internasjonale åpne dataressurser er et privilegium, og brukeren ved universitetet plikter å vise seg tilliten verdig.

All bruk av IT-tjenestene må skje i henhold til norsk lov.