TISIPs IKT-reglement

1. Formål

Formålet med IKT-reglementet er å regulere bruken av TISIPs informasjons- og kommunikasjonsinfrastruktur (IKT-infrastruktur).

Privateid utstyr som kobles til datanettet er også omfattet av reglementet. Når programvare eller informasjon som eies av TISIP installeres på privat utstyr, er også dette omfattet av reglementet.

2. Hvem TISIPs IKT-reglement gjelder for

Reglementet gjelder for:

- Alle ansatte i TISIP
- Alle studenter ved TISIP fagskole
- Alle som har tilgang til, og /eller bearbeider og forvalter informasjon gjennom TISIPs infrastruktur.

3. Definisjoner

Med TISIPs IKT-infrastruktur menes alt utstyr, digital informasjon, informasjonssystemer og tjenester som benyttes til informasjonsbehandling og kommunikasjon.

4. Overordnede prinsipper

4.1. Tilgang til TISIPs IKT-infrastruktur

Studenter og ansatte skal ha brukerkonto hos TISIP. Med brukerkonto menes unikt brukernavn, passord og e-postadresse. Andre kan gis tilgang til IKT-infrastruktur etter tjenstlig behov. Tilgang til ulike systemer og tjenester autoriseres av systemeier.

4.2. Bruk av IKT-infrastruktur

Den som gis tilgang til TISIPs IKT-infrastruktur (heretter kalt bruker) plikter å sette seg inn i IKT-reglementet og følge det.

TISIPs IKT-infrastruktur skal brukes til å utføre oppgaver knyttet til TISIPs virksomhet. TISIPs IKT-infrastruktur skal anvendes på en måte som ikke strider mot lov, forskrift eller TISIPs interne regler.

Bruker skal hindre at andre får tilgang til egen brukerkonto. Bruker skal heller ikke søke å skaffe seg tilgang til andres brukerkonto.

Bruker skal hindre at uønskede personer får tilgang til TISIPs IKT-infrastruktur, herunder tilgang til rom hvor IKT-utstyr er tilgjengelig. Bruker skal ikke uten tillatelse endre, modifisere eller på annen måte forårsake at IKT-infrastrukturen virker på en annen måte enn forutsatt.

Bruker skal ikke benytte TISIPs IKT-infrastruktur på en måte som kan utsette TISIP for tap av omdømme.

TISIPs IKT-infrastruktur skal kun benyttes for å understøtte aktiviteter som bidrar til å oppnå fagskolens formål og oppgaver knyttet forskning, utdanning, formidling og administrasjon.

Bruker skal påse at den enkeltes personvern overholdes og ikke krenkes.

Bruker plikter å respektere opphavsrett eller lignende rettigheter til programvare, tjenester og annen digital informasjon som bilder, musikk, film etc.

Lisensiert programvare, tjenester, åndsverk eller andre rettighetsbelagte data skal bare benyttes i henhold til bruksavtale, og bruker plikter å sette seg inn i de reglene som gjelder for bruken. Bruker kan holdes ansvarlig for brudd på vilkårene.

Publisering av andres verk, informasjon eller data må bare gjøres etter avtale med rettighets-haveren.

Ved lengre fravær skal bruker sende fraværsmelding til nærmeste overordnede slik at virksomhetsrelatert epost ikke blir liggende uhåndtert i postkassen.

Bruker plikter straks å rapportere forhold som kan ha betydning for IKT-infrastrukturens sikkerhet eller integritet (avvik) til IT-ansvarlig.

4.3. Avslutning av ansettelsesforhold eller studier, mv.

I god tid innen opphør av ansettelsesforhold eller avslutning av studier hos TISIP skal brukeren rydde sin konto. Filer som tilhører saker som en ansatt har hatt til behandling, skal forelegges den ansattes overordnede til vurdering. Filene skal ikke slettes før brukerens overordnede har godkjent dette. Det samme gjelder filer som er etablert som en del av ansettelsesforholdet eller studiene. Den overordnede avgjør om filene skal slettes eller arkiveres. For studenter er det IT-ansvarlig som avgjør om filene skal slettes eller arkiveres.

4.3.1. Avslutning av bruker og e-postkasse mv.

Når arbeidsforholdet, studierett eller annen form for tilknytning til TISIP opphører, stenges brukertilgangen til TISIPs IKT-infrastruktur. Varsel om dette gis per e-post en måned i forveien.

Innhold i e-postkasse og personlige lagringsområder slettes permanent senest seks måneder etter at tilgangen stenges. For studenter slettes de personlige lagringsområdene to måneder etter at studieretten opphørte. **Studenter er selv ansvarlig for å hente ut data de ønsker å ta vare på f.eks. fra LMS systemet (itslearning, o.a.)**

Ved dødsfall blir brukerkonto sperret. E-postkassen og det private hjemmeområdet og dets innhold slettes etter seks måneder med mindre offentlige myndigheter har krevd innsyn og kan fremlegge skriftlig begjæring, eller dødsboet ved skifteattest har gjort gjeldende rett til materialet.

4.3.2. Tilbakelevering av materiell til TISIP

Materiell tilhørende TISIP skal leveres tilbake. Alle kopier av programvare, dokumentasjon og data eid av, eller utlånt fra TISIP, skal slettes på privat utstyr.

Retten til å knytte opp private maskiner til TISIPs nettverk opphører ved avslutning av ansettelsesforhold eller studier.

4.4. Identifikasjon og tilgangsstyring

Tilgang til TISIPs IKT-infrastruktur skal være knyttet til en rolle og med påfølgende rettigheter.

Den som skal ha tilgang til TISIPs IKT-infrastruktur skal identifisere seg ved hjelp godkjent digital identitet(er) som er knyttet til rollen, eller ved signatur.

4.5. Endring av rollen eller avslutning av forholdet til TISIP

Ved endring av rolle i tilknytningen til TISIP skal endringer i rettigheter i IKT-infrastrukturen endres tilsvarende. Når forholdet til TISIP avsluttes (studenter uteksamineres, ansatte slutter skal tilganger og rettigheter trekkes tilbake. Etter en karantenetid skal persondata slettes.

Den som benytter den digitale identiteten har selv ansvar i for å ta vare på personlige data, samt overlevere TISIPs data i henhold til dette IKT-reglementet og gjeldende avtale som gir tilgang til TISIPs IKT-infrastruktur.

4.6. Kontroll med bruken av TISIPs IKT-infrastruktur

All bruk av TISIPs IKT-infrastruktur etterlater elektroniske spor. TISIP samler inn, analyserer og oppbevarer elektroniske spor for å administrere IKT-infrastrukturen, sikre effektiv og kostnadsbærende drift, og for å beskytte TISIPs IKT-infrastruktur mot trusler og misbruk. Innsamling, lagring og bruk av elektroniske spor skal gjøres i henhold til gjeldende lovverk.

TISIPs IKT-infrastruktur er tilrettelagt med løsninger for registrering av aktiviteter (logging) og sikkerhetskopiering blant annet for å kunne dokumentere lovbrudd eller avvik fra interne regler og rutiner, men også for å kunne avdekke / oppdage brudd på sikkerheten i IKT-infrastrukturen.

4.7. Innsyn

TISIP har som arbeidsgiver innen rammen av regelverket, rett til innsyn i arbeidstakernes e-postkasse og brukerkonto mv. Arbeidstaker skal så langt som mulig varsles og få anledning til å uttale seg før innsyn gjennomføres, og arbeidstaker skal som hovedregel ha rett til å være tilstede under innsynet. Arbeidstaker har rett til å la seg bistå av tillitsvalgt eller annen representant.

Dersom innsyn er foretatt uten forutgående varsel, skal arbeidstaker etterpå få skriftlig underretning om innsynet. Beslutningen om gjennomføring av innsyn skal dokumenteres i TISIPs sak- og arkivsystem.

Innsynet må gjennomføres på en slik måte at dataene så langt som mulig ikke endres og at frembrakte opplysninger kan etterprøves.

TISIP har rett til å gjennomsøke, åpne eller lese e-post i arbeidstakernes e-postkasse eller hjemmeområde, mv. i følgende tilfeller:

- Når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten.
- Når det er begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed.

Dersom innsyn i e-postkassen viser at det ikke foreligger dokumentasjon som arbeidsgiver har rett til innsyn i, skal e-postkassen og dokumenter straks lukkes. Eventuelle kopier skal slettes.

Begjæring om innsyn i ansattes e-postkasse fremmes av øverste leder i TISIP i samråd med systemeier. Beslutning om innsyn fattes av styret.

Ved dødsfall kan daglig leder for TISIP beslutte at det skal foretas innsyn for å finne fram til virksomhetsrelatert e-post og annet knyttet til brukerkonto.

TISIP kan gi innsyn i informasjon, logger og sikkerhetskopier til offentlige myndigheter når dette har hjemmel i lov eller forskrift, samt ved fremleggelse av rettslig beslutning.

4.8. Sanksjoner ved brudd på IKT-reglementet

Brudd på IKT-reglementet kan føre til disiplinærtiltak mot brukeren. Brukeren er ansvarlig for å sette seg inn i IKT-reglementet og reglement for bruk av lisensierte system.

Utstyr eller programvare som forårsaker skad på TISIPs IKT-infrastruktur, på TISIPs informasjon/data, andre brukeres informasjon/data, som på annen måte skaper forstyrrelser i IKT-infrastrukturen eller er til hinder for TISIPs oppnåelse av formålet med IKT-infrastrukturen kan uten opphold fjernes fra IKT-infrastrukturen.

Den som bryter reglementets bestemmelser, herunder at bruker forårsaker skade på TISIPs IKT-infrastruktur, på TISIPs informasjon/data, andre brukeres informasjon/data, som på annen måte skaper forstyrrelser i IKT-infrastrukturen eller er til hinder for oppnåelse av TISIPs formål med IKT-infrastrukturen, kan føre til at bruker nektes adgang til hele eller deler av institusjonens IKT-infrastruktur, jf. eForvaltningsforskriften § 14. I tillegg kan det medføre sanksjoner etter andre regler, advarsel eller utestengning fra studier og eksamen etter fagskoleloven, erstatningsansvar, straffeansvar, o.a.

Midlertidig utestengning i inntil 14 dager besluttes av daglig leder, eller rektor dersom bruker er student, i samråd med systemeier. Utestengning ut over 14 virkedager vil anses som et enkeltvedtak for student eller ansatt, og må følge relevante saksbehandlingsregler.

Midlertidig utestengning kan skje ved berettiget mistanke om at:

- Brukeren har gjort seg skyldig i alvorlige overtredelser, eller
- Brukeren eller brukerens IKT-utstyr utgjør en vesentlig trussel for informasjonssikkerheten.

I vurderingen skal det legges vekt på overtredelsens grovhet, om brukeren har overtrådt reglementet, hvilke følger en utestengning vil få for brukeren og forholdene ellers. Klage på vedtak truffet med hjemmel i fagskoleloven og forvaltningsloven (eForvaltningsforskriften) følger disse lovenes regler om klage.

5. Roller og ansvar

5.1. Rektor

- Rektor kan foreta nødvendige endringer i IKT-reglementet etter fullmakt fra styret.
- Rektor er ansvarlig for at studenter er gjort kjent med IKT-reglementet, og at dette aksepteres skriftlig (elektronisk) før de får tilgang til TISIPs IKT-infrastruktur.

5.2. Daglig leder

- Daglig leder reviderer IKT-reglementet hvert annet år.
- Daglig leder skal framlegge IKT-reglementet for styret og rektor for fastsettelse ved revisjoner eller endringer som vil kunne påvirke rettigheter og plikter.
- Daglig leder fatter formell beslutning om innsyn i brukerens e-postkasse.
- Daglig leder fatter beslutning om sanksjoner mot ansatte i henhold til norsk lov.
- Daglig leder er ansvarlig for at ansatte er gjort kjent med IKT-reglementet, og at dette aksepteres skriftlig (elektronisk) før de får tilgang til TISIPs IKT-infrastruktur.

5.3. Bruker

- Bruker er ansvarlig for å sette seg inn i IKT-reglementet og regler for bruken av lisensiert programvare / tjenester og følger dette.

- Bruker skal sørge for at brudd på personopplysningssikkerheten meldes uten ugrunnet opphold til nærmeste leder / IT-ansvarlig.

Reglementet er utformet med referanse til eForvaltningsforskriften §14 og § 20 og personvern-forordningen artikkel 24, 32.

IKT-reglementet er vedtatt av TISIPs styre, Sak 30/20, den 25.09.2020.

Endret den 30.09.20 – studenter har selv ansvar for å hente ut data fra LMS før brukeren slettes!