UNIVERSITETET I BERGEN

Styre: Universitetsstyret **Dato:** 12.11.2015
Styresak: 131/15 **Arkivsaksnr:** 2015/11386
Møtedato: 26.11.2015

Styringssystem for informasjonssikkerhet

Henvisning til bakgrunnsdokumenter

- Styresak 7/2015 - Tildelingsbrev for 2015 fra Kunnskapsdepartementet
- Styresak 111/2009 - Revisjon av IKT- reglement og IKT- sikkerhetspolitikk
- Regelsamlingen del 4.3 Informasjons- og kommunikasjonsteknologi

Saken gjelder:

Universitetet i Bergen (UiB) er underlagt en rekke lover og forskrifter hvor det stilles krav til informasjonssikkerhet og personvern.

I tildelingsbrevet for 2015 vises det til at institusjonen skal påse at informasjonssikkerhets-arbeidet er i samsvar med e-Forvaltningsforskriften og den nasjonale strategien for informasjonssikkerhet med tilhørende handlingsplan. I årsrapporten for 2015 skal UiB rapportere på om styringssystem for informasjonssikkerhet er innført.

For å ivareta disse behov og krav etableres et styringssystem for informasjonssikkerhet (SSIS) ved UiB. Dette skal bidra til at UiBs informasjonsverdier sikres på en systematisk, planmessig og tilfredsstillende måte.

Styringssystemet er basert på ISO 27001 standarden og veiledere fra Uninett, Difi og Nasjonal sikkerhetsmyndighet. Styringssystem for informasjonssikkerhet ved UiB består av **styrende del**, **gjennomførende del** og **kontrollerende del**.

Styret skal beslutte den styrende delen av SSIS**.** Denne består av sikkerhetspolicy (sikkerhetsmål og sikkerhetsstrategi), risikostyring, sikkerhetsorganisasjon (roller, ansvar og myndighet), og IKT-reglement ved UIB.

Universitetsdirektørens kommentarer

På bakgrunn av krav i Tildelingsbrevet for 2015 ba universitetsdirektøren IT-direktøren om å etablere en arbeidsgruppe for å utarbeide et styringssystem for informasjonssikkerhet. Den styrende del som skal vedtas av universitetsstyret har vært sendt på høring. Det matematisk-naturvitenskapelige fakultet ved Institutt for informatikk kommenterte sikkerhetspolicy, og dette er innarbeidet i det endelige forslaget. HR-avdelingens forslag om innsyn i IKT-anlegg som ikke er stilt til disposisjon av UiB, men som for øvrig omfattes av IKT-reglementet, er innarbeidet. Øvrige endringer etter høringen er av redaksjonell art. Høringsdokumentene har videre vært til ekstern kvalitetssikring hos Infosec Norge AS, blant annet relatert til kravene i Norm for informasjonssikkerhet i helsesektoren.

Reglene om oppretting, anvendelse og sletting av brukerkonti på UiBs IKT anlegg, vedtatt 11.10.2004 erstattes av nye prosedyrer i den gjennomførende del av styringssystem for informasjonssikkerhet.

Med dette fremmes følgende forslag til

vedtak:

1. Universitetsstyret godkjenner forslag til «Styringssystem for informasjonssikkerhet – styrende del». Dette erstatter «Overordnet IKT- sikkerhetspolitikk ved UiB», fastsatt av Universitetsstyret 3.12.2009.
2. Universitetsstyret godkjenner forslag til revidert «IKT-reglement for Universitetet i Bergen». Dette erstatter «IKT- reglement for Universitetet i Bergen», fastsatt av Universitetsstyret 3.12.09, sist endret 11.9.2015.

Kjell Bernstrøm
universitetsdirektør

Chandini Wijenayake Merkesvik/Ernst Pedersen/Jan Frode Knarvik/Arne R. Ramslien
12.11.2015

Vedlegg:
1. Saksframstilling
2. Styringssystem for informasjonssikkerhet – styrende del
3. Forsalg til nytt IKT-reglement

Saksframstilling

Styre:	Styresak:	Møtedato:	Arkivsaksnr:
Universitetsstyret	131/15	26.11.2015	2015/11386

Styringssystem for informasjonssikkerhetOm Styringssystem for informasjonssikkerhet (SSIS)

SSIS ved UiB er basert på ISO -27001 standard og veileder fra Uninett, DIFI og Nasjonalsikkerhetsmyndighet.

Styringssystem for informasjonssikkerhet ved UiB skal bidra til at UiBs informasjonsverdier sikres på en systematisk, planmessig og tilfredsstillende måte.

Styringssystem for informasjonssikkerhet ved UiB skal bidra til å støtte opp under institusjonens mål, verdier og hovedoppgaver.

Styringssystem for informasjonssikkerhet ved UiB består av styrende del, gjennomførende del og kontrollerende del.

- **Den styrende** del består av sikkerhetsmål og sikkerhetsstrategi, organisering av informasjonssikkerhet, risikostyring, og IKT reglementet ved UIB.
- **Den gjennomførende** del inneholder prosedyrer, veiledninger og rutiner for å kunne oppfylle den styrende delen, herunder kartlegging av informasjonssystemer, prosedyrer og rutiner for informasjonssikkerhet, referanser for sikringsmål og sikringstiltak og IT sikkerhetsårsplan.
- **Den kontrollerende** del består av årlig sikkerhetsrevisjon av informasjonssystemer, risikovurderinger, hendelse- og avviksrapportering, årlig sikkerhetsrapportering til ledelsen og ledelsens gjennomgang av informasjonssikkerheten ved UiB.

SSIS- Styrende del

Den styrende delen av styringssystemet vil erstatte Overordnet IKT- sikkerhetspolitikk ved UiB som ble av Universitetsstyret 3.12.2009.

IKT reglement er oppdatert og skal være en del av Styringssystem for informasjonssikkerhet.

SSIS- gjennomførende del

Det utarbeides UiB interne prosedyrer, rutiner, veiledninger og maler for å oppfylle krav i lover, forskrifter, pålegg eller avtaler med tredjepart, god IT-skikk og etiske normer. Disse er delt i relevante kategorier for eksempel felles for alle brukere, systemeier og forskning.

Regler om oppretting, anvendelse og sletting av brukerkonti for studenter og ansatte som i dag finnes i regelsamlingen er fastsatt av rektor og universitetsdirektør i beslutningsnotat av 11.10.04. Disse revideres og vil inngåinngå i styringsystemets gjennomførende del.

Liste over prosedyrer, rutiner, veiledninger og maler

Disse vil bli vedlikeholdt på intranett. Nedenfor er en skisse for hva som vil komme.

Felles

1. Veileder for sikker bruk av IKT systemer
2. Prosedyrer for avvikshåndtering/rapportering av sikkerhetsbrudd

Systemeier

1. Prosedyrer og rollebeskrivelse for systemeier

2. Prosedyrer for behandling og oppbevaring av personopplysninger for administrative systemer
3. Veileder for klassifisering av informasjon
4. Veileder for sikker drift av IKT systemer
5. Veileder for risikovurdering
6. Veileder for sikkerhetsrevisjon
7. Veileder for sikkerhetskrav til informasjonssystemer
8. Mal for Databehandler-avtale(norsk/engelsk)

Forskning
Internkontrollsystem for forskning skal revideres.

Annet
Gjennomførende del inneholder også en del dokumenter som skal vedlikeholdes jevnlig.

- Referanser for sikringsmål og sikringstiltak (Statement of applicability iht. ISO 27001)
- Oversikt over informasjonssystemer
- Årlig sikkerhetsplan
- Opplæringsmateriell
- UIB Sikkerhetsorganisasjon

SSIS- kontrollerende del

Den kontrollerende delen av styringssystem for informasjonssikkerhet består av:

- Rapporter over årlige sikkerhetsrevisjoner av informasjonssystemer.
- Årlig rapport over sikkerhetsavvik, sikkerhetstilstand /risikovurderinger og tiltak.
- Ledelsens gjennomgang av rapportene og informasjonssikkerhet.

Chandini Wijenayake Merkesvik/Ernst Pedersen/Jan Frode Knarvik/Arne R. Ramslien
12.11.2015

Styringssystem for informasjonssikkerhet

Del 1 – Styrende del

Universitetet i Bergen

Versjon 1.0

Vedtatt i Universitetsstyret 26.11.2015

Innhold

Versjonshistorikk

Dato	Versjon	Endring	Utført av
26.11.2015	1	Første versjon vedtatt av Universitetsstyret	

1 Styringssystem for informasjonssikkerhet (SSIS)

1.1 Formål

Universitetet i Bergen (UiB) forvalter betydelige mengder informasjon. Denne informasjonen er av avgjørende betydning for UiBs forskning, utdanning og formidling. En tilfredsstillende sikring av denne informasjonen med hensyn på konfidensialitet, integritet og tilgjengelighet er nødvendig for at UiB skal ivareta sitt samfunnsoppdrag.

Universitetet i Bergen er underlagt en rekke lover og forskrifter hvor det stilles krav til informasjonssikkerhet og personvern relatert til UiBs håndtering av informasjon og sensitive opplysninger. UiB er videre underlagt eierstyring fra Kunnskapsdepartementet.

For å ivareta disse behov og krav etableres et Styringssystem for informasjonssikkerhet.

Styringssystem for informasjonssikkerhet ved UiB skal bidra til at UiBs informasjonsverdier sikres på en systematisk, planmessig og tilfredsstillende måte.

Styringssystem for informasjonssikkerhet ved UiB skal bidra til å støtte opp under institusjonens mål, verdier og hovedoppgaver.

1.2 Beslutningsmyndighet

Den styrende delen av Styringssystem for informasjonssikkerhet besluttes av universitetsstyret.

Den styrende delen angir øvrig sikkerhetsorganisering med blant annet ansvar og mandat fordelt på øvrige roller.

Prosedyrer som hører til gjennomførende del av SSIS besluttes av Universitetsdirektøren. Forvaltningen av SSIS ved UiB er underlagt IT direktøren.

1.3 Virkeområde

Styringssystem for informasjonssikkerhet ved UiB gjelder for:

- UiBs organisasjon med de roller, oppgaver og myndighet den enkelte har, samt de strukturer og prosesser som er etablert for virksomheten.
- Alle ansatte, studenter, eksterne brukere, innleid personell og gjester (heretter kalt brukere) ved UiB som behandler eller har tilgang til UiBs informasjon, eller informasjon lagret på UiBs utstyr, eller på utstyr tilkoblet UiBs infrastruktur.
- All data- og informasjonsbehandling, lagring og prosesser for dette, uavhengig av lagrings- og prosesseringsform.
- Infrastruktur, utstyr samt privat og annet eksternt utstyr som tilkobles UiBs infrastruktur.

1.4 Aktuelle lover, forskrifter og regler

Styringssystemet bygger på det til enhver tid gjeldende lovverk med forskrifter. Blant disse er:

- Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) og Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Lov om behandling av personopplysninger (personopplysningsloven).
- Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
- Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen)

- Lov om arkiv [arkivlova] og Forskrift om offentlige arkiv
- Lov om universiteter og høyskoler (universitets- og høyskoleloven)
- Lov om medisinsk og helsefaglig forskning (helseforskningsloven)
- Forskrift om organisering av medisinsk og helsefaglig forskning (helseforskningsforskriften)
- Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
- Lov om helsepersonell m.v. (helsepersonelloven).
- UiB regelsamlingen

1.5 Definisjoner

I dette dokumentet benyttes følgende definisjoner:

Begrep	Definisjon
Informasjonssikkerhet	Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet.
Konfidensialitet	Sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang.
Integritet	Sikre at informasjonen og behandlingen er nøyaktig og fullstendig, og vernes mot uautoriserte endringer.
Tilgjengelighet	Sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov.
Risikovurdering	Vurdering av trusler mot, konsekvenser for og sårbarheten til informasjonen og informasjonssystemene, og sannsynligheten for at sikkerhetshendelser kan inntreffe.
Risikostyring	Prosessen med å identifisere, kontrollere og redusere eller eliminere sikkerhetsrisikoer som kan påvirke informasjonssystemer, innenfor en akseptabel kostnadsramme.
Systemeier	Den øverste lederen ved den enheten som er ansvarlig for de enkelte systemene og løsningene. Alle systemer ved UiB skal ha en definert systemeier.
Behandlingsansvarlig	Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
Personopplysning	Opplysninger og vurderinger som kan knyttes til en enkeltperson.
Forskningsansvarlig	Institusjon eller annen juridisk eller fysisk person som har det overordnede ansvaret for forskningsprosjekt, og som har de nødvendige forutsetningene for å kunne oppfylle den forskningsansvarliges plikter.
Sensitive personopplysninger	Opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger.

2 Sikkerhetspolicy

2.1 Identifisering av kritiske verdier ved UiB

Mennesker, informasjon, omdømme, fysiske gjenstander og miljø anses som kritiske verdier ved UIB.

2.2 Overordnet sikkerhetsmål

Følgende sikkerhetsmål skal gjelde for arbeidet med informasjonssikkerhet:

- UiB skal sikre konfidensialitet, integritet og tilgjengelighet av informasjon på en tilfredsstillende måte i henhold til gjeldende lover, forskrifter og regler.
- Informasjon som behandles ved UiB skal ha riktig sikkerhetsnivå basert på klassifisering og risikovurderinger, og behandles i henhold til dette.
- Alle ansatte, studenter, eksterne brukere, samarbeidspartner og gjester skal være kjent med UiBs krav til informasjonssikkerhet og etterleve disse kravene.

2.3 Sikkerhetsstrategi

Arbeidet med informasjonssikkerhet ved UiB skal basere seg på anbefalte og anerkjente standarder for styringssystemer for informasjonssikkerhet i offentlig sektor.

IKT-reglementet regulerer bruken av IKT anlegget ved UiB, og gjelder for alle brukere.

UiB skal utvikle en sikkerhetskultur hvor alle brukerne har god kunnskap, holdninger og adferd i forhold til sikkerhetstrusler og sårbarheter.

Det skal gjennomføres sikkerhetsrevisjoner som verifiserer at UiBs og eksterne myndigheters krav til informasjonssikkerhet er ivaretatt og fungerer etter sin hensikt.

Arbeidet med informasjonssikkerhet skal bygge på prosesser for kontinuerlig forbedring.

2.4 Kompetanse

UiB skal sørge for nødvendig opplæring og kompetanseheving for ledere og ansatte som har ansvar for informasjonssikkerhet. Ledere ved UiB som har ansvar for informasjonssikkerhet skal sørge for ressurser til planlegging, gjennomføring og oppfølging av informasjonssikkerhet innenfor sine ansvarsområder. Dette inkluderer iverksetting av sikringstiltak som er nødvendige for å oppnå tilfredsstillende informasjonssikkerhet.

Alle brukere av informasjonssystemer skal gis nødvendig kunnskap og opplæring om informasjonssikkerhet. Brukerne skal være informert om rutiner for rapportering av avvik og sikkerhetsbrudd samt hensikt med dem.

3 Risikostyring

Alt arbeid med informasjonssikkerhet skal basere seg på risikovurderinger. Risikovurderingen baseres på en konkret vurdering av trusler og utfordringer for UiB. For systemer som er virksomhetskritiske, skal det være utarbeidet sårbarhets- og risikoanalyser.

Systemeier er ansvarlig for å gjennomføre risikovurderinger etter veiledning i SSIS gjennomførende del.

For hvert risikoelement vurderes sannsynligheten for at den skal inntreffe og konsekvensen av at den inntreffer. Konfidensialiteten og integriteten til informasjon skal vektlegges foran hensynet til tilgjengeligheten ved en risikovurdering.

Høye risikoer skal ikke aksepteres før det er gjort et grundig arbeid for å finne realistiske risikoreduserende tiltak. Kun universitetsdirektøren kan akseptere risikoer (restrisikoer) som fremdeles er svært høye etter godkjente tiltak.

4 Sikkerhetsorganisasjon, roller, ansvar og myndighet

4.1 Behandlingsansvarlig

Rektor er behandlingsansvarlig etter lov om behandling av personopplysninger for både administrative systemer og forskningssystemer.

Universitetsdirektøren utpeker systemeiere for administrative system som behandler personopplysninger og gir føringer for behandlingen.

4.2 Forskningsansvarlig

Rektor er forskningsansvarlig etter lov om medisinsk og helsefaglig forskning.

4.3 Overordnet ansvar for informasjonssikkerhet

Universitetsdirektøren har etter delegasjon fra Universitetsstyret overordnet og i samråd med rektor, ansvar for informasjonssikkerheten ved UiB.

4.4 Operativt ansvar for informasjonssikkerhet

IT-direktør har operativt ansvar for informasjonssikkerhet med fullmakt til å treffe tiltak for å hindre skade og forebygge fare for skade, samt å iverksette tiltak med sikte på bevissikring og koordinere tiltak for å utbedre eventuelle skader.

IT-direktør har ansvaret for utarbeidelse og vedlikehold av IKT-Reglement i samråd med HR-direktør. Universitetsstyret beslutter alle endringer.

IT-direktør skal støtte systemeiere ved UiB med utarbeidelse av nødvendige sikkerhetsprosedyrer og rutiner for å ivareta sikkerhet i deres systemer.

IT-direktør er systemeier for IKT-infrastruktur og sentrale IKT–tjenester, inkludert kommunikasjon, sikkerhetsløsninger, datalagring og sikkerhetskopiering.

4.5 Systemeieransvar

Systemeier er den øverste lederen ved enheten og er ansvarlig for de enkelte systemene innenfor enheten.

Systemeier har ansvar for å fastlegge formålet med behandlingen av personopplysninger og alle sider ved forvaltningen av IT-systemene enheten har ansvar for når det gjelder utvikling, oppgradering, drift, tilgangskontroll, brukerstøtte og opplæring. Der det ikke er utpekt en systemeier, regnes den som har utviklet eller anskaffet systemet for bruk ved UiB, som systemeier.

Sammen med IT-direktør har systemeiere ansvar for fastsetting av sikkerhetsnivået i systemene og kontroll av at informasjonssikkerheten ivaretas. Systemeier har også ansvaret for forebyggende informasjonssikkerhet for sine egne systemer, og skal utarbeide nødvendige sikkerhetsdokumentasjon, veiledninger og rutiner for systemene med støtte fra IT-direktør.

Ved anskaffelse av nye systemer har systemeier ansvar for å sørge for at kravene til informasjonssikkerhet blir innfridd.

4.6 Kontinuitetsplanlegging

Basert på en vurdering av relevante risikoer for driftsavbrudd, skal systemeier utarbeide planer og iverksette tiltak som kan redusere avbrudd ved sikkerhetssvikt til et akseptabelt nivå. For de sentrale og kritiske IKT-systemer, skal det utføres realistiske kontroller for å verifisere effektiviteten av de tiltakene som er iverksatt.

4.7 Fysisk sikkerhet

Universitetsdirektøren har overordnet ansvar for å sikre UIBs eiendommer og fysiske gjenstander mot brann, tyveri og skadeverk, samt at lokalene skal være sikret mot uautorisert adgang.

Direktør ved eiendomsavdelingen har operativt ansvar, og har fullmakt til å treffe tiltak for å hindre skade og forebygge fare for skade, samt å iverksette tiltak med sikte på bevissikring og koordinere tiltak for å utbedre eventuelle skader.

Fysiske sikringstiltak skal gjennomføres basert på risikovurdering gjennomført av systemeier.

IKT-utstyr som benyttes som basis for fellesfunksjoner (servere, datalager, nettverkstjenere m.m.) og kritiske systemer skal være plassert i lokaler som er fysisk sikret mot tilkomst for uvedkommende.

4.8 Beredskap

Universitetsdirektøren har overordnet ansvar for den sentrale beredskapen ved UiB. Beredskap for informasjonssikkerhet inngår i den sentrale beredskapen.

4.9 Ansatte og studenter

Alle brukere av systemene ved UiB har et ansvar for å ivareta informasjonssikkerheten i forbindelse med utførelsen av eget arbeid; dette gjelder både den informasjon som behandles i systemene så vel som systemene i seg selv.

IKT- reglement

for

Universitetet i Bergen

Versjon 2.0

Vedtatt i Universitetsstyret 26.11.2015

Innhold

Dato	Versjon	Endring	Utført av
03.12.2009	1.0	Første versjon vedtatt av Universitetsstyret	
26.11.2015	2.0	Ny versjon vedtatt av Universitetsstyret	

1 Formål

Formålet med IKT-reglementet er å regulere bruken av Universitetet i Bergen (UiB) sitt informasjons- og kommunikasjonsteknologianlegg (IKT-anlegg).

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

2 Virkeområde

Reglementet gjelder:

- For alle studenter, ansatte og andre (som eksterne brukere, innleid personell, gjester), heretter kalt brukere, som er gitt tilgang til UiB sitt IKT-anlegg.
- All bruk av IKT-anlegget ved Universitet i Bergen og alt utstyr som kobles til.
- Brukernes private IKT-anlegg og andres IKT-anlegg, i den utstrekning dette benyttes til å utføre oppgaver for institusjonen, uavhengig av om anlegget er plassert i institusjonens lokaler eller ikke.
- Privat IKT-utstyr som kobles til UiB sitt IKT-anlegg.

3 Tilgang til IKT-anlegget

Studenter og ansatte skal ha en brukerkonto hos UiB. Med brukerkonto menes brukernavn, passord, hjemmekatalog og en epostkasse. Andre kan gis tilgang til IKT-anlegg etter tjenstlig behov. Tilgang til de ulike systemer og tjenester autoriseres av systemeier.

Studentenes brukerkonto sperres to måneder etter at studieretten opphørte. Varsel om sperring gis en måned i forveien.

Ansattes brukerkonto sperres ved avslutning av ansettelsesforholdet. Varsel om sperring sendes en måned før sluttdato. Pensjonister ved UiB kan søke om å få beholde sin brukerkonto med endrede tilganger.

Andre sin tilgang til IKT anlegget sperres når tilknytningen til UiB opphører, eller godkjent tidsperiode utløper.

Brukerkonto slettes automatisk seks måneder etter at tilgangen til IKT-anlegget ble sperret, og innholdet blir lagret i backup systemet i ett år.

Ved dødsfall blir brukerkonto sperret. Kontoen slettes etter seks måneder med mindre offentlige myndigheter har krevd innsyn, eller dødsboet ved skifteattest har gjort gjeldene rett til materialet.

4 Bruk av IKT-anlegget

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

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

Brukerne skal hindre at uønskede personer får tilgang til UiB sitt IKT-anlegg, herunder tilgang til rom hvor IKT-utstyr er tilgjengelig. Brukerne skal ikke uten tillatelse endre, modifisere eller på annen måte forårsake at IKT-anlegget virker på en annen måte enn forutsatt.

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

Brukerne skal unngå bruk av IKT-anlegget som kan utsette UiB for vesentlig tap av omdømme.

Brukerne plikter straks å rapportere forhold som kan ha betydning for IKT-anleggets sikkerhet eller integritet IT-avdelingen.

5 Aktivitetslogg og kontroll

IKT-anlegget 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-anlegget.

IT-avdelingen har hovedansvar for kontroll med tilgang til UiBs nettverk og generelle IKT-tjenester, samt for bærbart utstyr og utstyr som benyttes utenfor UiB.

6 Innsyn

UiB har på visse vilkår rett til innsyn i arbeidstakers epostkasse mv, jf. personopplysningsforskriften kap. 9. Forskriften omtaler arbeidsgivers innsynsrett i arbeidstakernes epostkasse, men reglene gjelder så langt de passer også for universiteters innsyn i studenters epostkasse, jf. forskriftens § 9-1, 5. ledd. For andre som får tilgang til UiB sitt IKT-anlegg, er UiB sin rett til innsyn den samme som overfor arbeidstakere.

I avsnittene nedenfor benyttes begrepet" arbeidstaker" fra forskriften, men begrepet omfatter også andre brukere.

Med epostkasse menes epostkasse arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet ved virksomheten. Reglene gjelder tilsvarende for arbeidsgivers adgang til gjennomsøkning av og innsyn i arbeidstakers personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet ved virksomheten. Bestemmelsene gjelder også for arbeidsgivers innsyn i opplysninger som arbeidstaker har slettet fra de nevnte områdene, men som finnes lagret på sikkerhetskopier eller lignende som arbeidsgiver har tilgang til.

Det kan også foretas innsyn i IKT-anlegg som ikke er stilt til disposisjon av UiB men som for øvrig omfattes av IKT-reglementet. Vilkårene for – og prosedyrene ved innsyn vil da bli lagt til grunn så langt de passer.

6.1 Vilkår for innsyn

UiB har bare rett til å gjennomsøke, åpne eller lese e-post i arbeidstakers epostkasse

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

6.2 Prosedyrer ved innsyn

Arbeidstaker skal så langt som mulig varsles og få anledning til å uttale seg før UiB gjennomfører innsyn. I varselet skal UiB begrunne hvorfor vilkårene anses oppfylt og orientere om at arbeidstaker så langt som mulig skal gis anledning til å være tilstede under

gjennomføringen av innsynet, og at vedkommende har rett til å la seg bistå av tillitsvalgt eller annen representant.

Er innsynet foretatt uten forutgående varsel, skal arbeidstaker gis skriftlig underretning så snart innsynet er gjennomført. Underretningen skal, i tillegg til opplysninger om hvorfor UiB anså vilkårene for innsyn som oppfylt, inneholde opplysninger om hvilken metode for innsyn som ble benyttet, hvilke e-poster eller andre dokumenter som ble åpnet samt resultatet av innsynet, jf. personopplysningsforskriften § 2-16.

Unntakene fra rett til informasjon i personopplysningslovens § 23 gjelder tilsvarende. Unntaket gjelder også etterfølgende varsel.

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

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

Begjæring om innsyn i ansattes e-postkassen fremmes av øverste leder ved enheten (ved institutt, fakultet eller avdeling i sentraladministrasjonen) i samråd med HR-avdelingen og systemeier.

Begjæring om innsyn i studenters e-postkasse fremmes av leder av fakultet i samråd med Utdanningsavdelingen og aktuell systemeier.

Beslutning om innsyn fattes av universitetsdirektør.

Ved dødsfall kan universitetsdirektør beslutte at det skal foretas innsyn for å finne fram til virksomhetsrelatert e-post. Slikt innsyn vil bli gjennomført i samarbeid mellom enhetens leder og HR-avdelingen.

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

7 Sanksjoner

Overtredelse av reglementets bestemmelser kan føre til at bruker nektes tilgang til hele eller deler av institusjonens IKT-anlegg. I tillegg kan det medføre sanksjoner etter andre regler, så som disiplinærreaksjoner etter tjenestemannslovgivningen, advarsel eller utestenging fra studier og eksamen etter universitets- og høyskoleloven, erstatningsansvar, straffeansvar o.a.

Midlertidig utestenging i inntil 14 virkedager, vil kunne besluttes av øverste leder ved enheten etter samråd med systemeier. HR-avdelingen skal straks varsles dersom utestengingen gjelder en arbeidstaker. Utestenging ut over 14 virkedager besluttes av universitetsdirektøren.

Midlertidig utestenging 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 tidligere har overtrådt reglementet, hvilke følger en utestenging vil få for brukeren og forholdene ellers.

Klage på vedtak truffet med hjemmel i tjenestemannsloven, universitets- og høyskoleloven og forvaltningsloven følger disse lovenes regler om klage.