UNIVERSITETET I BERGEN

Styre: Universitetsstyret **Dato:** 16.05.2019
Styresak: 53/19 **Arkivsaksnr:** 2015/11386
Møtedato: 29.05.2019

Styringssystem for informasjonssikkerhet og personvern

Henvisning til bakgrunnsdokumenter

- Styresak 131/2015 – Styringssystem for informasjonssikkerhet
- Styresak 4/2019 – Tildelingsbrev for 2019 fra Kunnskapsdepartementet til UiB
- Styresak 120/2017 – Internrevisjon, UiBs arbeid med personvernforordningen

Saken gjelder:

Norge fikk ny personopplysningslov med virkning fra 20. juli 2018. Universitetet i Bergen har et Styringssystem for informasjonssikkerhet (SIS) som blant annet bygger på personvernlovgivningen. Det er derfor behov for å oppdatere styringssystemet i tråd med det nye lovverket. Forslag til nytt styringssystem fremmes for universitetsstyret i denne saken.

Den nye personvernlovgivningen stiller strengere krav til internkontroll med hensyn på personvern. Oppfølging av informasjonssikkerhet og av personvern er tett integrert og delvis overlappende. Det foreslås derfor å omgjøre det eksisterende *Styringssystem for informasjonssikkerhet* (SIS) til et *Styringssystem for informasjonssikkerhet og personvern* (SIP).

Styringssystemet vil med de nye lovkravene og de foreslåtte endringene i større grad enn tidligere berøre behandling av personopplysninger i forskningssystemer. Gjennom innføring av styringssystem tydeliggjør man ansvaret og innfører krav om dokumentasjon og rapportering for å sikre forsvarlig behandling og oppfyllelse av de nye lovkravene.

Det er krav om at styringssystem for informasjonssikkerhet skal bygge på anerkjente standarder. Styringssystemet bygger på ISO27001 og består av I) Styrende del, II) Gjennomførende del og III) Kontrollerende del. Styrende del består av to deler, et policydokument og IKT-reglement for UiB. Universitetsstyret beslutter styrende del. Gjennomførende del som inneholder retningslinjer, prosedyrer og rutiner besluttes av universitetsdirektøren i samråd med rektor eller den de bemyndiger til dette.

Den nye personvernlovgivningen innebærer en innføring av EUs personvernforordning (GDPR) i Norge. I tildelingsbrevet til UiB for 2019 vises det til at det er et ansvar for den enkelte virksomhet å etterleve den nye personvernlovgivningen. Vi gir derfor styret en orientering om UiBs arbeid med å sikre etterlevelse av GDPR.

Forslag til vedtak:

1. Universitetsstyret vedtar forslag til «Styringssystem for informasjonssikkerhet og personvern – styrende del». Dette erstatter «Styringssystem for informasjonssikkerhet», fastsatt av Universitetsstyret 26.11.2015.
2. Universitetsstyret vedtar forslag til «Styringssystem for informasjonssikkerhet og personvern – IKT-reglement for Universitetet i Bergen». Dette erstatter «IKT-reglement for Universitetet i bergen» fastsatt av Universitetsstyret 26.11.2015.
3. Universitetsstyret tar gjennomgangen av UiBs arbeid med oppfyllelse av EUs personvernforordning til orientering.

Kjell Bernstrøm
universitetsdirektør

16.05.2019/Sidsel Storebø/Tore Burheim (avd.dir.)

Vedlegg
1) Saksframstilling
2) Forslag til Styringssystem for informasjonssikkerhet og personvern - styrende del
3) Forslag til Styringssystem for informasjonssikkerhet og personvern – IKT-reglement

Saksframstilling

Styre:	Styresak:	Møtedato:	Arkivsaksnr:
Universitetsstyret	53/19	29.05.2019	2015/11386

Styringssystem for informasjonssikkerhet og personvern (SIP)

Introduksjon

For å sikre et systematisk og strukturert arbeid med informasjonssikkerhet har UiB etablert et styringssystem for informasjonssikkerhet (SIS)[1]. Styringssystemet skal sørge for forsvarlig internkontroll på saksområdet, og gjennom dette sørge for at UiB følger de relevante lover, forskrifter og retningslinjer. Blant relevante lovverk i denne sammenhengen er personvernlovgivningen. Norge fikk ny personopplysningslov[2] 15.juni 2018 etter innføring av EUs personvernforordning (GDPR). Endringene i det nye loverket er såpass vesentlige at det er behov for å oppdatere styringssystemet.

Den nye personvernloven stiller strengere krav til internkontroll enn den forrige. Oppfølging av informasjonssikkerhet og personvern er tett integrert og delvis overlappende. Man kan velge å ha separate internkontrollregimer (styringssystemer) for hver av disse, eller man kan velge å ha et felles system. Godt personvern fordrer god informasjonssikkerhet og vise versa. Mange rutiner, prosedyrer og policyer vil være felles og evt. doble dersom man velger to separate systemer. Vi finner det derfor formålstjenlig å samle disse i *ett* styringssystem. Det foreslås derfor å omgjøre det tidligere *Styringssystem for informasjonssikkerhet* (SIS) til et *Styringssystem for informasjonssikkerhet og personvern* (SIP).

Den nye personvernloven innebærer en innføring av EUs personvernforordning (GDPR) i Norge. I tildelingsbrevet til UiB for 2019 vises det til at det er et ansvar for den enkelte virksomhet å etterleve den nye personvernlovgivningen. Vi gir derfor styret en orientering om UiBs arbeid med å sikre etterlevelse av GDPR.

Styringssystem for informasjonssikkerhet

Det er et krav i eForvaltningsforskriften[3] at forvaltningsorgan skal ha et styringssystem for informasjonssikkerhet bygd på anerkjente standarder. Både eksisterende og det nye styringssystemet for UiB er basert på ISO 27001 som er den mest brukte standarden.

---

[1] Styresak 131/2015 – Styringssystem for informasjonssikkerhet
[2] Lov om behandling av personopplysninger (personopplysningsloven) av 15. juni 2018 nr 38. https://lovdata.no/dokument/NL/lov/2018-06-15-38
[3] Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), §15 https://lovdata.no/dokument/SF/forskrift/2004-06-25-988

Styringssystemet er bygget opp slik:

Del	Innhold	Besluttes av
I) Styrende del Består av: • Policydokument • IKT-reglement for UiB	o sikkerhetsmål for informasjonssikkerhet og styringsmål for personvern, o sikkerhetsstrategi, og strategi for personvern, o organisering og myndighetskart for informasjonssikkerhet og personvern, o rammer for risikostyring o IKT-reglementet for UIB.	Universitetsstyret
II) Gjennomførende del	Prosedyrer, retningslinjer og rutiner for å kunne oppfylle den styrende delen, herunder kartlegging av informasjonssystemer, prosedyrer og rutiner for informasjonssikkerhet og rutiner for å sikre konfidensialitet og kvalitet og at personopplysningene ikke lagres lengre enn nødvendig.	Rektor og universitetsdirektør
III) Kontrollerende del	Årlig sikkerhetsrevisjon av informasjonssystemer, risikovurderinger, hendelse- og avviksrapportering, årlig rapportering fra Personvernombudet og sikkerhetsrapportering til ledelsen/ledelsens gjennomgang av informasjonssikkerheten ved UiB.	

Styringssystem for informasjonssikkerhet og personvern ved UiB skal bidra til å støtte opp under institusjonens mål, verdier og hovedoppgaver og bidra til at UiBs informasjonsverdier inkludert personopplysninger sikres på en systematisk, planmessig og tilfredsstillende måte.

Endringene i styringssystemet for informasjonssikkerhet

Hovedendringene i styrende del er at personvern tas eksplisitt inn i styringssystemet. Det er gitt styringsmål og strategi for personvern i policydokumentet på linje med tilsvarende for informasjonssikkerhet. Det er videre tatt med definisjoner og roller knyttet til forvalting av personopplysninger blant annet i forskning og personkonsekvensvurdering.

Videre er henvisninger til og endringer i forskrifter og prosedyrer innarbeidet, spesielt i IKT-reglementet. Vi har også valgt å ta med en eksplisitt referanse til åndverksloven som relevant lovverk. I IKT-reglementet er den viktigste endringen at muligheter for innsyn strammes noe inn og at prosedyrer og lovreferanser oppdateres i tråd med det nye lovverket og personvernforordningen.

UiB har i sin praksis vært restriktiv med innsyn og benyttet dette kun i forbindelse med berettiget innsyn fra dødsbo, uthenting av forskningsdata etter plutselige dødsfall og i

forbindelse med etterforskning av straffbare forhold. I beredskapssammenhenger kan det være behov for å se på trafikkdata. (Typisk i forbindelse med savnede studenter eller andre for å finne siste tid og sted for pålogging.) UiBs praksis er godt innenfor det nye lovverket.

Det er utarbeidet et avsnitt om operativt ansvar for behandling av personopplysninger. Her er det tydeliggjort at faglig linje har ansvar for behandling av informasjon i forskningssystemer. Det operative ansvaret er delegert til dekanene ved det enkelte fakultet.

I det nye lovverket er det strenge krav til oversikt over behandling av personopplysninger. Dette omfatter også behandling av personopplysninger i forskning. For å sikre en slik oversikt og å sikre at personopplysningene behandles forsvarlig legges det opp til at dette skal dokumenteres med en årlig rapportering. For å gjøre dette effektivt ved UiB legges det opp til at dette gjøres i et eget system RETTE med planlagte integrasjoner mot CHRIstin og NSD.Derigjennom kan man få til en samlet oversikt.

Status for ny personverlovgivning og EUs personvernforordning (GDPR)

Universitetet i Bergen gjennomførte våren 2017 en internrevisjon av UiBs arbeid med å imøtekomme kravene i EUs Personvernforordning (GDPR), som ble rapportert til styret[4]. Denne gjennomgangen ble gjennomført før utkast til lov forelå, men var basert på selve forordningen. Basert på denne gjennomgangen ble det igangsatt et arbeid med sikte på oppfylle forordningen. Følgende ble gjennomført:

- UiB opprettet og ansatte personvernombud
- Det er utarbeidet en Personvernerklæring som ligger på UiB sin nettside.[5]
- Internkontrollsystemet for forskning er oppdatert.
- Det er etablert en oversikt over behandlingsaktiviteter (art. 30 protokoll), og etablert en løsning for å ha oversikt i administrative og i felles IT-tjenestene.
- Det er under utvikling et system for registrering, dokumentasjon og rapportering av alle forsknings, -student og kvalitetssikringsprosjekter som behandler personopplysninger og andre sensitive data (RETTE – Risiko og etterlevelse). Systemet skal i tillegg til å gi oversikt iht. art. 30, sikre internkontroll av prosjekter og tilhørende informasjonssikkerhet.
- Det et etablert et personvernnettverk ved UiB med ansatte fra alle avdelinger.
- Informasjon om personvern er oppdatert på UiB sine nettsider i tråd med det nye lovverket.
- Det er gjennomført opplæring ved alle fakulteter og administrative avdelinger.
- Det er etablert et samarbeid rundt GDPR i sektoren, og Unit sine veiledere benyttes. I tillegg er det etablert et personvernombudnettverk i sektoren.
- Det er påbegynt arbeid med å sikre rutine for håndtering av innsynsforespørsler.

For å få en grundig gjennomgang på UiBs arbeid med oppfyllelse av GDPR ble det ved årsskiftet 2018/2019 igangsatt en evaluering av implementering av GDPR ved UiB og resultatet av arbeidet. Oppsummert var funnene som følger:

- Det er behov for mer informasjon og kompetanse på området i UiBs organisasjon

[4] Styresak 120/2017 – Internrevisjon, UiBs arbeid med personvernforordningen
[5] https://www.uib.no/personvern/118933/personvernerkl%C3%A6ring-universitetet-i-bergen

- Det er behov for å gjøre rutiner og praksis mer synlige og mer tilgjengelige, blant annet for å sikre at avvik fanges opp og meldes på riktig måte.
- UiB bør realisere en personvernportal på sine nettsider
- Man bør innføre et felles verktøy og gjennomføring av risikovurderinger for å sikre en bedre oversikt.
- Man bør sørge for ens dokumentasjon og oppfølging av tiltak fra risikovurderinger for å sikre at alle tiltak blir fulgt opp
- Det er behov for å utarbeide felles maler og veiledninger og på enkelte områder retningslinjer og rutiner
- Det bør utarbeides veileder for lokalt driftet utstyr.
- Det bør utarbeides en veileder for klassifisering og lagring av informasjon,
- RETTE bør implementeres og rulles ut i organisasjonen.
- UiBs styringssystem bør oppdateres slik at det fanger opp endringene i lovverket.

For å følge opp disse punktene er det igangsatt et eget prosjekt som har som mål å gjennomføre alle tiltakene innen utgangen av 2019. Dette sees også i sammenheng med det løpende arbeidet med bedring av IT-sikkerhet på UiB.

Gjennom innføring av Styringssystem for informasjonssikkerhet og personvern vil oppfølging av personvern i tillegg komme med i en formalisert struktur for kontinuerlig forbedring, inkludert ledelsens årlige gjennomgang, årsplan mv.

16.05.2019/Sidsel Storebø/Tore Burheim (avd.dir.)

Styringssystem for informasjonssikkerhet og personvern (SIP)

Del 1 – Styrende del

Universitetet i Bergen

Versjon 2

Vedtatt i Universitetsstyret dd.mmm 2019

Innhold

Versjonshistorikk

Dato	Versjon	Endring	Utført av
26.11.2015	1	Første versjon vedtatt av Universitetsstyret	
28.05.2019	2	Oppdatert i hht Ny personvernlov, GDPR og utvidet til Styringssystem for informasjonssikkerhet og personvern	

1 Styringssystem for informasjonssikkerhet og personvern (SIP)

1.1 Formål

Universitetet i Bergen (UiB) forvalter betydelige mengder informasjon inkludert personopplysninger. Denne informasjonen er av avgjørende betydning for UiBs forskning, utdanning og formidling. For å ivareta UiB sitt samfunnsoppdrag er det nødvendig at all informasjon som forvaltes er tilfredsstillende sikret mot brudd på konfidensialitet, integritet og tilgjengelighet i tråd med gjeldende lover, forskrifter og retningslinjer.

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 personopplysninger. UiB er videre underlagt eierstyring fra Kunnskapsdepartementet.

For å ivareta disse behov og krav er det etablert et Styringssystem for informasjonssikkerhet og personvern (SIP).

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

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

1.2 Beslutningsmyndighet

Den styrende delen av SIP besluttes av universitetsstyret.

Den styrende delen angir øvrig sikkerhetsorganisering med blant annet ansvar og mandat fordelt på øvrige roller, samt retningslinjer for behandling av personopplysninger.

Gjennomførende del av SIP besluttes av universitetsdirektøren i samråd med rektor eller den de bemyndiger til dette. Forvaltningen av SIP ved UiB er underlagt IT direktøren.

1.3 Virkeområde

Styringssystem for informasjonssikkerhet og personvern 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 behandling av personopplysninger (personopplysningsloven) inkludert personvernforordningen, GDPR.
- Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) og Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
- Lov om arkiv [arkivlova] og Forskrift om offentlige arkiv
- Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen)
- Lov om opphavsrett til åndsverk mv. (åndsverkloven)
- 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 informasjon og systemer kun er tilgjengelig for de som skal ha tilgang.
Integritet	Sikre at informasjon er korrekt, oppdatert og fullstendig, og hindre uønsket endring, sletting eller manipulering.
Tilgjengelighet	Sikre at brukere har tilgang til informasjon ved behov innenfor de tilgjengelighetskrav som er satt.
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 et system eller en IT-tjeneste. Alle systemer ved UiB skal ha en definert systemeier.
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.
Personvern	Omhandler retten til et privatliv og retten til å bestemme over egne personopplysninger.
Personopplysning	Alle former for data, informasjon, opplysninger og vurderinger som kan knyttes til en enkeltperson.
Behandlingsansvarlig	Den som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.
Særlige kategorier av personopplysninger	Opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, genetiske og biometriske opplysninger, helseopplysninger eller opplysninger om seksuelle forhold.
Personvern-konsekvensvurdering (DPIA)	Lovpålagt vurdering når det er sannsynlig at behandlingen av personopplysninger medfører høy risiko.

2 Sikkerhetspolicy og policy for personvern

2.1 Identifisering av kritiske verdier ved UiB

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

2.2 Overordnede 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 Overordnede styringsmål for personvern

Følgende styringsmål skal gjelde for arbeidet med personvern:

- UiB skal kun samle inn personopplysninger for berettigete formål, og behandle opplysningene på en lovlig, rettferdig og åpen måte.
- UiB skal ikke behandle personopplysninger i større utstrekning enn det som er nødvendig for å oppfylle universitetets formål. Når personopplysningene ikke lenger er nødvendige for formålet skal de slettes eller anonymiseres.
- Personopplysningene som behandles skal være korrekte og oppdaterte, og hvis ikke slettes eller rettes.
- Alle som behandler personopplysninger ved UiB skal være kjent med kravene i personopplysningsloven og etterleve disse kravene.

2.4 Sikkerhetsstrategi

Alt arbeid med informasjonssikkerhet ved UiB skal basere seg på risikovurderinger.

I tillegg skal arbeidet med informasjonssikkerhet basere seg på anbefalte og anerkjente standarder for styringssystemer for informasjonssikkerhet i offentlig sektor.

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

UiB skal utvikle en sikkerhetskultur hvor alle brukere har god kunnskap om, holdning og adferd med tanke på 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.

2.5 Strategi for personvern

Arbeidet med personvern ved UiB skal basere seg på krav i personopplysningsloven i tillegg til bransjestandard.

Det skal utarbeides retningslinjer for behandling av personopplysninger ved UiB for både forskningsdata, administrative data og andre data.

For alle aktiviteter der det behandles personopplysninger skal det utføres risikovurderinger, og det skal vurderes om det må gjennomføres en personvernkonsekvensvurdering (DPIA).

Det skal gjennomføres årlig rapportering fra fakultet med underliggende institutt og forskningsgrupper med hensyn på etterlevelse i behandling av persondata og andre forskningsdata. Universitetsdirektør eller den han eller hun utpeker kan gjennomføre stikkprøvekontroller for å sikre etterlevelse av personopplysningsloven.

2.6 Kompetanse

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

Alle som skal bruke UiB sine informasjonssystemer og som skal behandle personopplysninger skal ha nødvendig kunnskap om og få opplæring i informasjonssikkerhet og personvern.

Brukerne skal være informert om rutiner for rapportering av avvik og sikkerhetsbrudd samt hensikt med dem.

3 Risikostyring

Alt arbeid med informasjonssikkerhet og personvern skal basere seg på risikovurderinger. Risikovurderingen baseres på konkret vurdering av trusler og sårbarheter ved UiB. For systemer som er virksomhetskritiske eller der det behandles personopplysninger, skal det være utarbeidet risiko- og sårbarhetsanalyser.

Systemeier og de operativt ansvarlige for personvern er ansvarlige for at det gjennomføres risikovurderinger etter veiledning i SIP sin 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 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 for personopplysninger

UiB ved rektor er behandlingsansvarlig for universitetets behandling av personopplysninger, herunder i både de administrative- og forskningssystemene.

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

4.2 Operativt ansvar for behandling av personopplysninger

Rektor ved UiB har det overordnede faglige ansvar for forskningen som utføres ved universitetet, herunder i forskningssystemene, og er forskningsansvarlig.

Det operative forskningsansvaret er delegert til dekan på det enkelte fakultet. Det som i dette styringssystemet gjelder dekan gjelder også øverste faglige leder ved tilsvarende enheter på universitetet. Som forskningsansvarlig skal dekan sørge for at fakultetet til enhver tid er organisert for og har kapasitet til å ivareta forskningsaktiviteten ved fakultetet på en forsvarlig måte i hht lover, regler, retningslinjer mv, herunder behandling av personopplysninger. Dekan kan delegere oppgaver til instituttleder, senterleder eller tilsvarende. Forskningsansvaret gjelder all informasjon innsamlet til forskningsformål som behandles, uavhengig av lagringsform.

Avdelingsdirektør for Studieadministrativ avdeling er delegert det operative ansvaret for behandling av personopplysninger om søkere og studenter.

HR-direktøren er delegert det operative ansvaret for behandling av personopplysninger om ansatte.

Klinikkledere ved universitetsklinikkene er delegert det operative ansvaret for behandling av personopplysninger om pasienter.

Rektor kan sammen med universitetsdirektør beslutte retningslinjer for behandling av personopplysninger. De operativt ansvarlige skal sørge for at det er innført nødvendige rutiner for å sikre konfidensialitet og kvalitet, og at personopplysningene ikke lagres lengre enn nødvendig.

De operativt ansvarlige er også ansvarlig for at det tilbys nødvendig opplæring i bruk av IT-systemer og gjeldende rutiner.

4.3 Overordnet ansvar for informasjonssikkerhet

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

4.4 Operativt ansvar for informasjonssikkerhet

IT-direktør har operativt ansvar for informasjonssikkerheten ved UiB, 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 i systemet 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 systemeier ansvar for fastsetting av sikkerhetsnivået i systemene og kontroll av at informasjonssikkerheten og personvernet 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 og personvern 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 for 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, samt de som behandler personopplysninger, har et ansvar for å ivareta informasjonssikkerheten og sikre ivaretagelse av personvernet i forbindelse med utførelsen av eget arbeid.

Alle er pliktig å melde avvik ved brudd på informasjonssikkerheten eller personopplysningsloven så snart de gjøres kjent med avviket. Avvik meldes i henhold til gjeldende retningslinjer for avviksrapportering ved UiB.

IKT- reglement for Universitetet i Bergen

Del av Styringssystem for informasjonssikkerhet og personvern

Fastsatt av Universitetsstyret 3.12.09, sist endret xx.05.2019

1 Formål

Formålet med IKT-reglementet er å regulere bruken av IKT-systemer ved Universitetet i Bergen (UiB).

2 Virkeområde

Med *IKT-systemer* menes her all programvare, datasystemer, infrastruktur og utstyr som benyttes til digital informasjons- og databehandling, samt informasjon og data som lagres i disse. Digital kommunikasjon knyttet til disse inngår også samt IKT-systemer som inngår i annen infrastruktur og utstyr.

Med IKT-systemer *ved UiB* menes IKT-systemer som finnes på UiB, eies eller disponeres av UiB, eller som stilles til rådighet for UiBs brukere fra eksterne parter, leverandører eller andre på oppdrag, avtale eller i forståelse med UiB, og som benyttes av UiBs brukere eller samarbeidspartnere til formål knyttet til UiBs virksomhet.

Reglementet gjelder for:

- For ansatte, studenter, gjester og andre som er gitt tilgang til IKT-systemer ved UiB heretter kalt brukere.
- All bruk av UiBs IKT-systemer.

I tillegg gjelder reglementet for

- Brukernes og annen tredjeparts IKT-systemer, i den utstrekning de benyttes til å utføre oppgaver knyttet til UiBs virksomhet, uavhengig av om anlegget er plassert på UiBs område eller ikke.
- Privat og annet tredjeparts IKT-utstyr som er koblet til UiBs IKT-infrastruktur (f.eks. nettverk) uavhengig av hvilket formål det brukes til.

3 Tilgang til UiBs IKT-tjenester og -systemer

Studenter og ansatte skal ha en brukerkonto hos UiB som gir tilgang til IKT-systemer.

Andre kan gis tilgang til IKT-systemer 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. Ansattes e-postkasse avsluttes ved arbeidsforholdets opphør, med mindre det foreligger særskilt behov for å holde e-postkontoen åpen i en kort periode etter opphøret. Pensjonister ved UiB kan søke om å få beholde sin brukerkonto med endrede tilganger. Dette godkjennes av leder ved den enheten pensjonisten var sist ansatt.

Andre brukere sin brukerkonto ved UiB sperres når tilknytningen til UiB opphører, eller godkjent tidsperiode utløper.

Data knyttet til brukerkonto slettes automatisk seks måneder etter at brukerkontoen ble sperret. Data kan bli lagret i backup-systemer ut over denne perioden, men ikke lenger enn ett år.

Ved brukers dødsfall blir brukerkontoen sperret umiddelbart. Brukerkontoen slettes etter seks måneder med mindre det er krevd innsyn eller gjort gjeldende rett til materiale som beskrevet i dette reglementet.

4 Bruk av UiBs IKT-tjenester og -systemer

UiBs IKT-systemer skal brukes til å utføre oppgaver knyttet til UiBs virksomhet. Bruken må ikke stride mot lov, forskrift eller UiBs regler.

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

Brukerne skal hindre at uønskede personer får tilgang til UiBs IKT-systemer.

Brukerne skal ikke uten tillatelse endre eller modifisere UiBs IKT-systemer, eller på annen måte forårsake at de virker på en annen måte enn forutsatt.

Brukerne plikter å respektere opphavsrett og lignende rettigheter til programvare, data og annen digital informasjon som publikasjoner, bilder, musikk, film etc.

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

Brukerne plikter straks å rapportere forhold som kan ha betydning for IKT-sikkerheten og personvern ved UiB til IT-avdelingen.

5 Aktivitetslogg og kontroll

UiBs IKT-systemer er tilrettelagt med løsninger for registrering av aktiviteter (logging) og sikkerhetskopiering. Disse skal blant annet kunne brukes til å dokumentere lovbrudd eller avvik fra interne regler og rutiner, og avdekke/oppdage brudd på sikkerheten i IKT-systemene.

IT-avdelingen ved IT-direktør har hovedansvar for kontroll med tilgang til UiBs nettverk og generelle IKT-systemer, samt for bærbart utstyr og utstyr som benyttes utenfor UiB, og har myndighet til å utøve denne kontrollen i henhold til UiBs styringssystem for informasjonssikkerhet.

6 Arbeidsgivers innsyn

6.1 Virkeområde for forskrift om arbeidsgivers innsyn

UiB har på visse vilkår rett til innsyn i arbeidstakers e-postkasse m.v., jfr. arbeidsmiljøloven § 9-5 og forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale. Forskriften gjelder både nåværende og tidligere arbeidstakere.

Med e-postkasse menes e-postkasse arbeidsgiver har stilt til arbeidstakerens disposisjon til bruk i arbeidet. Reglene gjelder tilsvarende for arbeidsgivers adgang til gjennomsøkning av og innsyn i arbeidstakerens personlige område i virksomhetens datanettverk, IKT-systemer eller annet elektronisk utstyr som arbeidsgiver har stilt til arbeidstakerens disposisjon til bruk i arbeidet. Bestemmelsene gjelder tilsvarende for innsyn i opplysninger som er slettet fra de nevnte områdene, men som finnes på sikkerhetskopier eller tilsvarende.

6.2 Vilkår for innsyn

UiB har bare rett til innsyn i opplysninger som er lagret på områder nevnt under punkt 6.1

a) når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller

b) ved begrunnet mistanke om at arbeidstakerens bruk av e-postkasse eller annet elektronisk utstyr medfører grovt brudd på de plikter som følger av arbeidsforholdet eller kan gi grunnlag for oppsigelse eller avskjed.

UiB har ikke rett til å overvåke arbeidstakerens bruk av elektronisk utstyr, herunder bruk av Internett, med mindre formålet med overvåkingen er

a) å administrere virksomhetens datanettverk eller
b) å avdekke eller oppklare sikkerhetsbrudd i nettverket.

6.3 Prosedyrer ved innsyn

Arbeidstakeren skal så langt som mulig varsles og få anledning til å uttale seg før UiB gjennomfører innsyn. I varselet skal UiB begrunne hvorfor vilkårene for innsyn anses å være oppfylt og orientere om arbeidstakers rettigheter ved innsyn.

Arbeidstakeren har innsigelsesrett etter personvernforordningens artikkel 21.

Arbeidstakeren skal så langt som mulig gis anledning til å være til stede under gjennomføringen av innsynet og har rett til å la seg bistå av tillitsvalgt eller annen representant.

Er innsyn foretatt uten forutgående varsel eller uten at arbeidstakeren var til stede, skal arbeidstakeren gis skriftlig underretning om dette 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.

Unntakene fra rett til informasjon i personopplysningsloven § 16 gjelder tilsvarende.

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

Åpnede e-poster, dokumenter eller tilsvarende som det viser seg at ikke er nødvendige eller relevante for formålet med innsynet, skal straks lukkes. Eventuelle kopier skal slettes.

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

Beslutning om innsyn fattes av universitetsdirektør.

Ved dødsfall kan universitetsdirektør beslutte at det skal foretas innsyn

- når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller
- når dødsboet har gjort gjeldende rett til materiale

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

Universitetsdirektøren 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 brukeren nektes tilgang til hele eller deler av institusjonens IKT-systemer. I tillegg kan det medføre sanksjoner etter andre regler, så som disiplinærreaksjoner etter statsansatteloven, advarsel eller utestenging fra studier og eksamen etter universitets- og høyskoleloven, erstatningsansvar, straffeansvar o.a.

Midlertidig utestenging i inntil 14 virkedager kan besluttes av øverste leder ved enheten (institutt, fakultet eller avdeling i sentraladministrasjonen) 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 statsansatteloven, universitets- og høyskoleloven og forvaltningsloven følger disse lovenes regler om klage.