UNIVERSITETET I BERGEN

	Arkivreferanse	Dokumentdato
	2015/11386	05.03.2026
Styre	Styresak	Møtedato
Universitetsstyret	26/26	12.03.2026

VEDTAKSSAK

Oppdatering av UiBs styringssystem for informasjonssikkerhet og personvern

Henvisning til bakgrunnsdokumenter

- Styresak 11/24, *Oppdatering av UiBs styringssystem for informasjonssikkerhet og personvern*

Saken gjelder

UiBs Styringssystem for informasjonssikkerhet og personvern legger rammer for UiBs løpende arbeid med informasjonssikkerhet og personvern. Universitetsstyret beslutter styringssystemets styrende del, og det legges i denne saken frem forslag til en oppdatert versjon av denne delen av styringssystemet basert på nye krav knyttet til helsedata og kartlegging av informasjonsverdier.

Kravet om å ha et styringssystem for informasjonssikkerhet og personvern er hjemlet i forvaltningsloven med tilhørende forskrifter, i personopplysningslovens bestemmelser, samt i Kunnskapsdepartementets Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. UiB etablerte sitt styringssystem for informasjonssikkerhet i 2015 og det er oppdatert i tråd med nye krav og generelle innstramminger i flere omganger etter dette.

UiB fikk i juni 2025 i samarbeid med Universitetet i Oslo og NTNU, i oppdrag fra Kunnskapsdepartementet å etablere en nasjonal infrastruktur for personsensitive data, NORTRE. Formålet er å legge til rette for sekundærbruk av helsedata i tråd med kravene fra det Europeiske helsedataområdet (EHDS). Disse bestemmelsene omfatter også krav om ISO27001-sertifisering av vårt arbeid med informasjonssikkerhet på dette området. Styringssystemet bygger på ISO27001 og det er nødvendig å gjøre noen mindre, men vesentlige endringer i hoveddokumentet for å knytte styringssystemet til bestemmelsene i ISO-standarden. For å bli sertifisert må UiB etablere et styringssystem i tråd med ISO27001.

I saksforelegget er det gjort rede for endringene som foreslås nå. Endringene omfatter i hovedsak nødvendig endring for ISO-sertifisering og en utfylling av roller og prosesser knyttet til kartlegging av informasjonsverdier som har kommet som et krav i nevnte policy for informasjonssikkerhet og framhevet i tildelingsbrev. I tillegg er det gjort noen redaksjonelle endringer. Det er også foreslått noen mindre justeringer i IKT-reglementet.

Forslag til vedtak

Universitetsstyret vedtar endringene i Del I av Styringssystem for informasjonssikkerhet og Personvern, samt revidert IKT-reglement slik de framgår av saken.

Tore Tungodden

Universitetsdirektør

12.02.2026/Jimmy Thomsen/Monica Nielsen Øen/Tore Burheim (avd. dir.)

Vedlegg:

1. Saksframstilling
2. Forslag til revidert Styringssystem for informasjonssikkerhet og personvern (SIP), Del I –Styrende del
3. Forslag til revidert IKT-reglement

Saksframstilling

Styre	Styresak	Møtedato
Universitetsstyret	26/26	12.03.2026

Oppdatering av UiBs styringssystem for informasjonssikkerhet og personvern

Bakgrunn

Universitet i Bergen har i sin strategi at vi skal utvikle gode forskningsinfrastrukturer og styrke samarbeidet om infrastruktur nasjonalt og internasjonalt. Forskning på personsensitive data, herunder helsedata, er viktig for mange fagområder og det stilles særlige krav til informasjonssikkerhet og personvern i denne konteksten. UiB har over en tiårsperiode utviklet, driftet og forvaltet infrastrukturen SAFE for dette formålet og denne er viktig for å kunne legge til rette for slik forskning og tiltrekke oss forskningsprosjekter.

I etableringen av det europeiske helsedataområdet (EHDS) stilles det krav til deltakerlandene om etablering av sikre analyserom for sekundærbruk av helsedata. Den primære funksjonen i SAFE er å tilby slike sikre analyserom der SAFE p.t. har ca. 2000 brukere og 500 sikre analyserom (prosjekter).

Etter at Helsedirektoratet avlyste etablering av Helseanalyseplattformen i 2022 har det pågått et arbeid med sikte på gjenbruk av infrastrukturene for sikre analyserom på Universitetet i Oslo med TSD (Tjenester for Sensitive Data), Universitetet i Bergen med SAFE og NTNU med HUNT Cloud, for å kunne etablere en nasjonal infrastruktur for sikre analyserom. I juni 2025 fikk de tre universitetene det formelle oppdraget fra Kunnskapsdepartementet i samarbeid med Helse og omsorgsdepartementet å etablere en nasjonal infrastruktur for personsensitive data. Denne nasjonale infrastrukturen der disse tre inngår ble etablert med virkning fra 1.januar 2026 og har fått navnet NORTRE (Norwegian trusted research infrastructure). Det legges opp til en langsiktig og forutsigbar finansiering av NORTRE over statsbudsjettet. Denne etableringen er viktig for UiB med sikte på å holde på og tiltrekke oss forskningsprosjekter framover.

Basert på reguleringene av det europeiske helsedataområdet er det utarbeidet både tekniske, juridiske og funksjonelle krav til sikre analyserom. UiB har deltatt i arbeidet med utforming av disse kravene både på nasjonalt og europeisk nivå. Ett av kravene er etablering av styringssystem for informasjonssikkerhet i tråd med ISO27001, og sertifisering av organisasjonen som tilbyr sikre analyserom som etterlever kravene i ISO27001. Som en følge av dette er det behov for en revisjon av UiBs styringssystem slik at styringssystemet ikke bare er *basert på* ISO27001, som er forvaltningsforskriftens formulering, men *i tråd med* ISO27001 som er en forutsetning for sertifisering. Revisjonen av styringssystemet er hovedsak knyttet til underliggende retningslinjer, rutiner og dokumentasjon, men det er også nødvendig med en formalisert knytning fra styrende del i SIP til de relevantene kravene i ISO27001. Dette er det gjort rede for i forslaget under.

I tillegg har Kunnskapsdepartementet og Riksrevisjonen i flere sammenhenger påpekt nødvendigheten av verdivurderinger av informasjonsverdier som grunnlag for arbeidet med informasjonssikkerhet, ansvarlig

internasjonalt samarbeid og øvrig sikkerhetsarbeid. For å synliggjøre ansvaret i denne konteksten er det formålstjenlig å forankre rollen som informasjonseier i styringssystemet og formulere ansvaret til informasjonseier i denne konteksten.

Om UiBs styringssystem for informasjonssikkerhet og personvern

UiBs styringssystem for informasjonssikkerhet og personvern er hjemlet i forvaltningsloven med forskrift, samt i personopplysningsloven. I henhold til e-forvaltningsforskriften med tilhørende beslutninger hos relevante myndigheter skal styringssystemet være bygd på ISO 27001 som er den standarden UiBs system bygger på. Universitetsstyret vedtok UiBs styringssystem i 2015. Systemet består av en styrende del, en gjennomførende del og en kontrollerende del. Kravene til formalisering av arbeidet med informasjonssikkerhet har økt de siste årene og dette har medført nødvendige revisjoner av styringssystemet.

I 2020 ble styringssystemet oppdatert for å tydeliggjøre UiBs styringsmodell for IKT. Styringsmodellen bygger på at alle IT-systemer har en definert systemeier og at ansvar for sikker implementering, drift og forvaltning påligger vedkommende. De siste årene har krav om verdivurderinger og kartlegging av informasjonsverdier blitt mer sentralt, ikke bare i arbeidet med informasjonssikkerhet, men også i arbeidet med sikkerhet mer generelt. Dette framkommer både i styringsdokumenter fra Kunnskapsdepartementet og tildelingsbrev. Det er derfor formålstjenlig å ta informasjonsverdier og informasjonseier inn i UiBs styringssystem.

I 2024 ble styringssystemet oppdatert basert på tilbakemeldinger fra henholdsvis Riksrevisjonen og internrevisjonen. Områder som ble revidert var oppdatering av rollebeskrivelser i sikkerhetsorganisasjonen, tydeliggjøring rundt IRT-team og beredskap, andrelinje internkontroll, samt årlig rapportering til styret.

Endringer i Styringssystem for informasjonssikkerhet og personvern

Basert på saksforholdene som er beskrevet over fremmes det i denne saken forslag til endringer i styrende del av UiBs styringssystem for informasjonssikkerhet og personvern og i IKT reglementet.

Endring 1: Knytte styringssystemet til ISO-standarden og hjemle en sertifisering og relevanserklæring

Dagens styringssystem hjemler revisjoner og eksterne gjennomganger inkludert sertifiseringer gjennom et av avsnittene i hoveddokumentets omtale av UiBs sikkerhetsstrategi (kapittel 2.4):

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

Imidlertid trenger vi for en sertifisering en erklæring om hvilke deler av ISO27001-standarden som er relevante for UiB, hvordan hvert enkelt punkt i standarden er innarbeidet i UiBs styringssystem og hvilke deler av UiBs organisasjon som skal sertifiseres. Denne relevanserklæringen skal være begrunnet i risiko og vil derfor kunne endre seg over tid. Samtidig må disse to punktene formelt knyttes til styringssystemet. Den mest optimale måten å løse dette på er gjennom retningslinjer fastsatt av rektor og universitetsdirektør. Avsnittet over foreslås derfor endret til følger:

Det skal gjennomføres sikkerhetsrevisjoner som verifiserer at UiBs og eksterne myndigheters krav til informasjonssikkerhet er ivaretatt og fungerer etter sin hensikt. Utfyllende beskrivelse av dette gis i retningslinjer for revisjon og sertifisering, fastsatt av rektor og universitetsdirektør i fellesskap.

Endring 2: Inkludere digital motstandskraft som sikkerhetsmål

Dagens styringssystem har en målformulering i tre punkter der det første omtaler konfidensialitet, integritet og tilgjengelighet av informasjon, det andre omhandler behandling av informasjon basert på risikovurderinger og klassifisering og det tredje omhandler kjennskap til krav hos brukere av UiBs systemer.

Samtidig har robusthet og digital motstandskraft kommet mer fram som en kvalitets- og kontinuitetsdimensjon i sikkerhetsarbeidet. Mye av det vi gjør i dag, er relatert til det, men en målformulering på dette området trekker fram erkjennelsen av at vi må være forberedt på trusler og hendelser og at vi må planlegge for at slike han opptre. Da må vi ha planer og tiltak som bidrar til kontinuitet i UiBs virksomhet. Ut fra dette foreslår vi at følgende formulering legges inn:

- *UiB skal sikre evnen til å motstå, respondere på og gjenopprette virksomheten ved digitale trusler og hendelser.*

Endring 3: Beskrivelsen av informasjonseier som del av sikkerhetsorganisasjon og klassifisering av informasjon

I relasjon til arbeidet med verdikartlegging og verdivurdering ser vi at det har manglet en rollebeskrivelse for rollen som informasjonseier i styringssystemet. Siden verdikartlegging og klassifisering av informasjon har fått en mer framtredende plass i risikovurderinger, styring og rapportering de siste årene er det naturlig å definere denne rollen og dens oppgaver i styringssystemet. Det er i enkelte situasjoner slik at systemeierskapet og informasjonseierskapet ikke sammenfaller, og da er det kritisk at informasjonseier tar ansvar for risikostyring rundt behandlingen av informasjonsverdiene de er eiere av. Både informasjonssikkerhet og personvern må ivaretas rundt behandlingen av disse informasjonsverdiene. Rollebeskrivelsen er strukturelt beskrevet mest mulig likt systemeier.

Informasjonseier er i definert som følger i kapittel 1.5 Definisjoner:

Den øverste leder ved den enhet som har et overordnet ansvar for en spesifikk informasjonsverdi. Alle informasjonsverdier på UiB skal ha en definert eier.

I kapittel 4 er oppgavene til informasjonseier beskrevet som følger:

Ansvarlig for å sette rammer, prioritere sikkerhetstiltak, og sikre at informasjonen brukes og behandles på en sikker og ansvarlig måte (dvs. styre risiko) i tråd med UiBs retningslinjer. Ansvarlig for å dokumentere og revidere oversikt over informasjonsverdier med verdivurdering og klassifisering på sitt ansvarsområde. Ansvarlig for å gjennomføre årlig egenrapportering til bruk i ledelsens gjennomgang.

I kapittel 1,5 er det tatt med definisjonen på klassifisering av informasjon

Klassifisering av informasjonsverdier er en systematisk prosess for å gruppere data basert på sensitivitet og betydning, typisk langs aksene konfidensialitet, integritet og tilgjengelighet. Dette gir grunnlag for riktig sikkerhetsnivå (fysisk, teknisk og organisatorisk)

Endring 4: Mindre redaksjonelle justeringer og definisjoner

Det er lagt inn noen mindre redaksjonelle og språklige endringer i hoveddokumentet. I tillegg er det tillagt definisjon av verdikartlegging, verdivurdering og avvik.

Endring 5: Justering knyttet til IKT på reiser i IKT reglementet

UiBs IKT-reglement er også en del av UiBs styringssystem for informasjonssikkerhet. Håndtering av informasjonssikkerhet på reise er en viktig problemstilling for UiB. I relasjon til den endrede verdenssituasjonen og det økte risikobildet vi ser, er det viktig at vi har gode prosesser for å veilede for bruk av IKT på reise. Det praktiseres ikke en ordning med en samlet oversikt over reiseaktiviteten hos våre ansatte, og av den grunn ønskes det en formulering i IKT reglementet som forplikter brukere om å sette seg godt inn i de retningslinjer og rutiner som gjelder dersom man skal reise til land utenfor Norge. Dette vil bidra til at IT-avdelingen og andre kan bistå med nødvendig rådgivning og eventuelle utstyrsleveranser der det er formålstjenlig ut fra en risikovurdering. Denne dialogen vil i tillegg kunne bidra til at det bygges en enda bedre sikkerhetskultur i organisasjonen.

Rapportering av avvik er viktig for å ivareta informasjonssikkerhet, beredskap, gjennomføre kontinuerlig forbedring, samt våre forpliktelser ved myndighetsrapportering (eksempelvis Datatilsynet). Det er tatt inn en formulering om brukeres ansvar for rapportering av avvik i IKT reglementet for å synliggjøre dette ytterligere ovenfor våre brukere. Foreslåtte formuleringer er skrevet i samråd med HR avdelingen.

Universitetsdirektøren sine kommentarer

Gode forskningsinfrastrukturer er viktige for å kunne tiltrekke oss og holde på forskningsprosjekter og forskningsaktivitet. Utvikling av SAFE over en periode på 10 år har vært et svært vellykket digitalt initiativ som støtter direkte opp om forskningsaktiviteter på UiB, hos våre samarbeidspartnere og ellers.

I løpet av en periode på tre år har det vært arbeidet for gjenbruk av infrastrukturene på UiB, UiO og NTNU for sekundærbruk av helsedata i tråd med kravene fra Det europeiske helsedataområdet (EHDS). Etableringen av NORTRE fra 1.januar 2026 er også viktig milepæl i arbeidet med å sikre nasjonale datainfrastrukturer langsiktig og forutsigbar finansiering i tråd med systemmeldingen. Samtidig skal infrastrukturene brukes på tvers av sektorer og vil for NORTRE sin del legge til rette for et tettere samarbeid med spesialisthelsetjenesten og øvrig forvaltning. NORTRE-samarbeidet sørger for å ivareta forankringen i forskningens behov i denne konteksten.

Samtidig stiller etableringen av det europeiske helsedataområdet krav til slike infrastrukturer, men disse infrastrukturene vil bli gjeldende uavhengig av hvem som utvikler og forvalter disse. Universitetet vil måtte

forholde seg til dette og de nye kravene vil gjelde både tilbydere og brukere av dette. Realisering av NORTRE og SAFE som en likeverdig partner i dette er viktig for UiBs aktiviteter på helsedata framover.

Videre ser vi at informasjonsverdier og kartlegging samt dokumentasjon av disse etterspørres i større krav fra departementet og øvrige som grunnlag for alt sikkerhetsarbeid. Samtidig er det et nyttig redskap i vårt eget arbeid i forhold til prioriteringer og bevisstgjøring. Det er derfor formålstjenlig at denne dimensjonen får en strukturert plass i arbeidet med informasjonssikkerhet.

Vurderinger av digital motstandskraft og totalforsvaret er noe som etterspørres i større grad. Å trekke dette fram som et mål i tillegg til de etablerte målene er formålstjenlig og vil avspeile behovet for robusthet, kontinuitet og beredskap.

02.03.2026/Jimmy Thomsen/Monica Nielsen Øen/Tore Burheim (avd. dir.)

Styringssystem for informasjonssikkerhet og personvern (SIP)

Del 1 – Styrende del

Universitetet i Bergen

Versjon 5

Vedtatt i Universitetsstyret 12.03.2026

Innhold

1 Styringssystem for informasjonssikkerhet og personvern (SIP) 3
1.1 Formål 3
1.2 Struktur 3
1.3 Virkeområde 4
1.4 Aktuelle lover, forskrifter og regler 4
1.5 Definisjoner 5
2 Sikkerhetspolicy og policy for personvern 7
2.1 Identifisering av kritiske verdier ved UiB 7
2.2 Overordnede sikkerhetsmål 7
2.3 Overordnede styringsmål for personvern 7
2.4 Sikkerhetsstrategi 7
2.5 Strategi for personvern 8
2.6 Kompetanse 8
3 Risikostyring 8
4 Sikkerhetsorganisasjon, roller, ansvar og myndighet 8
4.1 Kontinuitetsplanlegging 13
4.2 Fysisk sikkerhet 13
4.3 Beredskap 13
4.4 Rapportering 13

Versjonshistorikk

Dato	Versjon	Endring	Godkjent
26.11.2015	1	Første versjon vedtatt av Universitetsstyret	Styresak 131/15
28.05.2019	2	Oppdatert i hht Ny personvernlov, GDPR og utvidet til Styringssystem for informasjonssikkerhet og personvern	Styresak 53/19
20.02.2020	3	Oppdatert i henhold til UiBs styringsmodell for IKT med tydeliggjøring av systemeiers ansvar	Styresak 16/20
01.02.2024	4	Oppdatert i henhold til revisjoner og styrket organisering i 2023	Styresak 11/24
12.03.2026	5	Oppdatert i henhold til revisjon og forberedelse til ISO sertifisering av SAFE	Styresak xx/26

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, formidling og øvrig virksomhet. 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.

For å ivareta disse behov og krav er det etablert et Styringssystem for informasjonssikkerhet og personvern (heretter kalt SIP), som 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 Struktur

Styringssystem for informasjonssikkerhet og personvern (SIP) ved Universitetet i Bergen (UiB) består av tre deler:

I. Styrende del
II. Gjennomførende del
III. Kontrollerende del

Den styrende delen (del I) består av to dokumenter *Styringsdokument* og *IKT-reglementet ved UiB*. I Styringsdokumentet, det vil si dette dokumentet, beskrives virkeområdet for styringssystemet, sikkerhetsmål, sikkerhetsstrategi og fordeling av ansvar og arbeidsoppgaver i sikkerhetsorganisasjonen. IKT-reglementet regulerer bruken av UiBs IT-systemer, IT-utstyr og IT-anlegg.

Den gjennomførende del (del II) sammen med dets vedlegg gir utfyllende opplysninger om oppgaver og aktiviteter som skal gjennomføres i henhold til styringssystemet.

I tillegg gjelder bestemmelsene i *Retningslinjer - Overordnede rammer for behandling av personopplysninger ved Universitetet i Bergen*.

Den kontrollerende del (del III) sammen med dets vedlegg, beskriver kontrollerende aktiviteter som inngår i SIP.

Universitetsstyret beslutter del I Styrende del. Universitetsdirektør i samråd med rektor beslutter del II Gjennomførende del og del III Kontrollerende del.

IT direktør forvalter styringssystemet, og beslutter underliggende retningslinjer, instrukser, øvrige dokumenter og vedlegg som inngår i styringssystemet med mindre annet er bestemt i

dette dokumentet.

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 for informasjonssikkerhet og personvern 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)
- Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale (epostforskriften) kombinert med arbeidsmiljøloven
- Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
- Lov om dokumentasjon og arkiv [arkivlova] og Forskrift om dokumentasjon og arkiv (arkivforskrifta)
- 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.
Klassifisering	Klassifisering av informasjonsverdier er en systematisk prosess for å gruppere data basert på sensitivitet og betydning, typisk langs aksene konfidensialitet, integritet og tilgjengelighet. Dette gir grunnlag for riktig sikkerhetsnivå (fysisk, teknisk og organisatorisk).
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.
Informasjonsverdier	Alle typer data, opplysninger og dataressurser (IT-utstyr, applikasjoner, systemer, datanettverk m.m.) som har betydning for UiB sin virksomhet
Informasjonseier	Den øverste leder ved den enhet som har et overordnet ansvar for en spesifikk informasjonsverdi. Alle informasjonsverdier på UiB skal ha en definert eier.
Verdikartlegging	Verdikartlegging er en systematisk prosess for å identifisere og beskrive hvilke verdier som skal beskyttes, herunder verdivurdering.
Verdivurdering	Verdivurdering er en faglig vurdering av hvor stor betydning de identifiserte verdiene har, gjerne uttrykt gjennom konsekvensnivåer for tap av konfidensialitet, integritet og tilgjengelighet, samt å vurdere operativ, økonomisk, juridisk og samfunnsmessig påvirkning. Formålet med verdivurdering er å etablere et grunnlag for videre risikovurderinger og prioritering av sikkerhetstiltak.
IRT	Incident Response Team, en egen gruppe av ressurspersoner som er utpekt særskilt til å håndtere sikkerhetshendelser på IKT området
IKT	Informasjons- og kommunikasjonsteknologi
EduCSC	Cybersikkerhetssenteret hos SIKT, forebygger, oppdager og håndterer sikkerhetshendelser i kunnskapssektoren. Dette er et sektorvist responsmiljø som er etablert i henhold til Regjeringens strategi for informasjonssikkerhet
Avvik	Et avvik oppstår når det foreligger en uønsket hendelse/forhold som ikke er i samsvar med myndighetskrav eller interne regler.

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.
- UiB skal sikre evnen til å motstå, respondere på og gjenopprette virksomheten ved digitale trusler og hendelser.
- Alle ansatte, studenter, eksterne brukere, samarbeidspartner og gjester skal være kjent med UiBs krav til informasjonssikkerhet, og er ansvarlig for å 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, med mindre det foreligger lovkrav eller skriftlige vurderinger som tilsier fortsatt oppbevaring.
- 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, og nasjonale anbefalinger 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. Utfyllende beskrivelse av dette gis i retningslinjer for revisjon og sertifisering.

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).

2.6 Kompetanse

UiB skal sørge for nødvendig opplæring og kompetanseheving for ledere og ansatte som har ansvar for informasjonssikkerhet og personvern.

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, og tar utgangspunkt i informasjonsverdier som skal sikres. Risikovurderinger skal gjennomføres for alle system og personopplysningsbehandlinger og dokumenteres skriftlig i det til enhver tid gjeldende system UiB benytter.

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.

4 Sikkerhetsorganisasjon, roller, ansvar og myndighet

Rolle / funksjon	Ansvar	Myndighet
Rektor	Forskningsansvarlig ved UiB og behandlingsansvarlig for UiB sin behandling av personopplysninger som inngår i UiB sin faglige virksomhet.	Beslutter sammen med universitetsdirektør del II og del III av SIP. Kan sammen med universitetsdirektør

		beslutte retningslinjer for behandling av personopplysninger
Universitetsdirektør	Har overordnet ansvar for informasjonssikkerheten ved UiB. Ansvarlig for sentral beredskap ved UiB, inkludert informasjonssikkerhetsberedskap. Overordnet ansvarlig for å sikre UIB sine eiendommer og fysiske gjenstander mot brann, tyveri og skadeverk. Overordnet ansvarlig for sikring mot uautorisert adgang i bygningsmassen. Gjennomfører sammen med rektor ledelsens årlige gjennomgang og godkjenner fremlagt rapport til denne.	Utpeker systemeiere for administrative systemer og gir føringer for behandlingen. Kan sammen med rektor beslutte retningslinjer for behandling av personopplysninger. Godkjenner eventuell restrisiko der det fremdeles foreligger risiko etter tiltaksgjennomføring. Godkjenner årsplan for informasjonssikkerhet. Beslutter sammen med rektor del II og del III av SIP.
IT direktør	Operativt ansvarlig for informasjonssikkerheten ved UIB. Ansvarlig for forvaltning av SIP med alle vedlegg. I samråd med HR-direktør ansvarlig for forvaltning av IKT reglementet. Ansvarlig for utarbeidelse av nødvendige retningslinjer og rutiner for å ivareta sikkerhet i UiBs systemer. Ansvarlig for å utarbeide årsplan for informasjonssikkerhet, samt oppfølging og gjennomføring av denne. Ansvarlig for å vedlikeholde oversikt over hvilke sikringstiltak som er etablert ved UIB. Systemeier for IKT infrastruktur og sentrale IKT tjenester, inkludert kommunikasjon, sikkerhetsløsninger, datalagring og sikkerhetskopiering. Ansvarlig for at det tilbys opplæring for systemeiere i deres roller. Ansvarlig for at det tilbys opplæring i informasjonssikkerhet for ansatte og studenter som brukere av informasjonsteknologi. Ansvarlig for å forvalte en oversikt over godkjente IT systemer der systemeiere er ansvarlige for å registrere sine systemer, og en oversikt over UiBs informasjonsverdier der informasjonseiere kan registrere sine verdier.	Kan iverksette tiltak eller beslutte gjennomføring av tiltak for å hindre skade, forebygge fare for skade, samt å iverksette tiltak med sikte på bevissikring og koordinere tiltak for å utbedre eventuelle skader. Beslutter alle instrukser, retningslinjer og rutiner samt øvrige vedlegg til SIP.

	Ansvarlig for å varsle universitetsledelsen og UiBs beredskapsledelse ved alvorlige hendelser og avvik. Ansvarlig for beredskap innen informasjonssikkerhet inkludert helhetlig kontinuitetsplanlegging. Ansvarlig for at sikkerhetsrevisjoner gjennomføres.	
Informasjonssikkerhetsleder	Informasjonssikkerhetsleder er av IT-direktøren tildelt ansvar og myndighet innen informasjonssikkerhetsområdet og rapporterer til denne. Leder det løpende arbeidet med informasjonssikkerhet ved UiB og ser til at UiB overvåker sikkerhet i nettverk og systemer. Ansvar for at det gjennomføres sikkerhetsrevisjoner og -kontroller på tvers av UiBs virksomhet etter en helhetlig verdi- og risikovurdering og i henhold til UiBs struktur for andrelinje internkontroll. Behandler avvik på informasjonssikkerhet og personvern, og varsler relevante parter slik at det iverksettes tiltak ved behov. Holde IT-direktør orientert om arbeidet, og varsle ved vesentlige hendelser og avvik. Leder IRT Teamet og vedlikeholder beredskapsplaner for informasjonssikkerhet. Bidra til at opplæring og rådgivning innenfor informasjonssikkerhet og personvern gjennomføres.	
Systemeier	Ansvarlig for sikker drift og forvaltning av systemene de eier i henhold til lover, forskrifter, regler og øvrige bestemmelser i hele systemets levetid. Ansvarlig for å sette sikkerhetsnivå i system man eier ut fra dokumentert klassifisering av informasjon og personinformasjon, samt å ha dokumentasjon på at informasjonssikkerhet og personvern ivaretas. Ansvarlig for å ha nødvendige risikovurderinger og at risikohåndtering gjennomføres slik at gjenværende risiko er på et akseptabelt nivå. Ansvarlig for at nødvendig opplæring tilrettelegges og gjennomføres i tilknytning til systemer de er eier av. Ansvarlig for verdivurdering av systemets komponenter, herunder maskin- og hyllevare, egenutviklet programvare og	

	dokumentasjon som grunnlag for etterlevelse av eksportkontrollregelverket og sikkerhetsloven. Ansvarlig for å lage en arkiveringsplan dersom finansieringsgrunnlaget for trygg drift og forvaltning er tidsbegrenset. Ansvarlig for å gjennomføre årlig egenrapportering til bruk i ledelsens gjennomgang.	
Dekan	Er delegert det operative forskningsansvaret inkludert personopplysningsbehandling. Ansvarlig for å ivareta forskningsaktivitetene på en forsvarlig måte i henhold til lover, regler, retningslinjer mv.	Kan delegere det operative forskningsansvaret videre til instituttleder, senterleder eller tilsvarende (eks. prosjektleder for forskningsprosjekter)
Instituttleder, senterleder eller tilsvarende (eks. prosjektleder)	Kan ha fått delegert fra Dekan det operative forskningsansvaret på sitt område, dette inkluderer personopplysningsbehandling	
Klinikkleder	Operativt ansvarlig for behandling av personopplysninger om pasienter. Ansvarlig for at det er innført nødvendige rutiner for å sikre konfidensialitet og kvalitet, samt at personopplysningene ikke lagres lenger enn nødvendig. Ansvarlig for at det tilbys nødvendig opplæring i bruk av IT systemer og gjeldende rutiner	
Avdelingsdirektør ved studieavdelingen	Operativt ansvarlig for behandling av personopplysninger om søkere og studenter. Ansvarlig for at det er innført nødvendige rutiner for å sikre konfidensialitet og kvalitet, samt at personopplysningene ikke lagres lenger enn nødvendig. Ansvarlig for at det tilbys nødvendig opplæring i bruk av IT systemer og gjeldende rutiner	
HR direktør	Operativt ansvarlig for behandling av personopplysninger om ansatte. Ansvarlig for at det er innført nødvendige rutiner for å sikre konfidensialitet og kvalitet, samt at personopplysningene ikke lagres lenger enn nødvendig. Ansvarlig for at det tilbys nødvendig opplæring i bruk av IT systemer og gjeldende rutiner	
Driftspersonell IT	Ansvarlig for å kjenne til alle deler av SIP og i særlig grad driftsinstruksen og de sikringstiltak som er etablert ved UiB. Ansvarlig for å varsle ved brudd på sikkerheten	
Brukere	Ansvarlig for å holde seg oppdatert på gjeldende regler for informasjonssikkerhet	

	og personvern, og følge disse. Ansvarlig for å gjennomføre pålagt opplæring innenfor informasjonssikkerhet og personvern. Ansvarlig for å ivareta informasjonssikkerheten og sikre ivaretakelse av personvern i forbindelse med utførelse av eget arbeid. Ansvarlig for å melde avvik i henhold til gjeldende rutiner ved brudd på informasjonssikkerheten eller personvernet.	
Personvernombud	Skal informere og gi råd til UiB sine brukere om forpliktelsene etter personvernlovgivningen. Skal kontrollere UiB sin etterlevelse av personvernlovgivningen. Skal involveres på rett nivå i spørsmål som vedrører personvern. Skal gi råd ved utarbeidelse av DPIA. Skal involveres ved behov i håndtering av avvik. Skal håndtere henvendelser fra de registrerte. Skal årlig rapportere om status på personvernområdet til universitetsstyret.	Har en uavhengig rolle og kan varsle Datatilsynet om avvik på eget initiativ uten godkjenning fra UiB
Direktør ved eiendomsavdelingen	Operativt ansvarlig for å sikre UiBs eiendommer og fysiske gjenstander mot brann, tyveri og skadeverk. Operativt ansvarlig for å sikre mot uautorisert adgang.	
IRT – Incident Response Team	Være virksomheten sin operative vaktstyrke for å overvåke, oppdage og håndtere IKT sikkerhetshendelser, og ha tett dialog med sektorvist responsmiljø i eduCSC (SIKT).	

Informasjonseier	Ansvarlig for å sette rammer, prioritere sikkerhetstiltak, og sikre at informasjonen brukes og behandles på en sikker og ansvarlig måte (dvs. styre risiko) i tråd med UiBs retningslinjer. Ansvarlig for å dokumentere og revidere oversikt over informasjonsverdier på sitt ansvarsområde. Ansvarlig for å gjennomføre årlig egenrapportering til bruk i ledelsens gjennomgang.	

4.1 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.

4.2 Fysisk sikkerhet

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.

4.3 Beredskap

Beredskap for informasjonssikkerhet og personvern inngår i UiBs beredskapsplaner og beredskapsorganisasjon. IT-avdelingen skal ha en beredskapsplan og en beredskapsorganisasjon med særlig ansvar for informasjonssikkerhet. Beredskapen for informasjonssikkerhet og personvern bygger på ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet. Som en del av beredskapen skal det eksistere et eget Incident Respons Team (IRT) ved IT avdelingen for særskilt håndtering av sikkerhetshendelser. Mandat og instruks for dette er et vedlegg til styringssystem for informasjonssikkerhet og personvern del II, gjennomførende del.

4.4 Rapportering

Ivaretagelse av informasjonssikkerhet og personvern er et lederansvar. Årlig skal det utarbeides en rapport til ledelsens gjennomgang. Rapporten oppsummerer arbeidet med informasjonssikkerhet og personvern. Rapporten fremmes til universitetsstyret i løpet av første kvartal påfølgende år av universitetsdirektør.

Personvernombudet utarbeider egen årsrapport som fremmes universitetsstyret i separat sak, men bør såfremt det er mulig legge denne frem sammen med rapport for informasjonssikkerhet og personvern.

I tillegg til denne faste årlige rapporteringen, skal universitetsledelsen holdes orientert om status for informasjonssikkerhet og personvern ved UiB.

Universitetsstyret kan be om ytterligere rapportering utover årlig statusrapportering ved behov.

Godkjent av:	Universitetsstyret ved UiB	**Godkjent dato:**	dd.mm.2026
Versjon: 3.0		**Arkivsak nr:**	

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 som skal på reise og oppholde seg i land utenfor Norge, plikter å sette seg inn i hvilke retningslinjer og rutiner som gjelder for bruk av IKT-systemer i slike tilfeller, samt forholde seg til disse.

Brukerne plikter straks å rapportere forhold som kan ha betydning for IKT-sikkerheten og personvernet ved UiB. Dette rapporteres til UiBs brukerstøtte for IT-tjenester BRITA.

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.

Versjonshistorikk

Rev.nr	Endring	Revisjonsdato	Godkjent av
3.0	Lagt til regulering av reise. Oppdatert kontaktpunkt for avvik.	12.03.2026	