UNIVERSITETET I BERGEN

Arkivsaksnr.:	Dokumentdato:
2015/11386	24.01.2024

Styre:	Styresak:	Møtedato:
Universitetsstyret	11/24	01.02.2024

Oppdatering av UiBs styringssystem for informasjonssikkerhet og personvern

Henvisning til bakgrunnsdokumenter

- Styresak 16/20 Styringsmodell for IKT
- Styresak 14/23 Internrevisjonsrapport – Informasjonssikkerhet og GDPR
- Styresak 28/23 Oppfølging av internrevisjon informasjonssikkerhet og GDPR

Saken gjelder:

UiB har de siste årene gjennomført en betydelig styrking av sitt arbeid med informasjonssikkerhet. Denne styrkingen har også medført en styrket organisering og forbedret strukturering av arbeidet. Det er derfor behov for å oppdatere UiBs styringssystem for informasjonssikkerhet og personvern i tråd med dette. I tillegg bør styringssystemet korrigeres i tråd med påpekninger fra Riksrevisjonen og fra UiBs internrevisjon. Universitetsstyret beslutter styringssystemets styrende del, og det legges i denne saken fram forslag til en oppdatert versjon av denne delen av styringssystemet.

Kravet om å ha et styringssystem for informasjonssikkerhet følger av forvaltningsloven med tilhørende forskrifter. Styringssystemet legger strukturen for UiBs løpende arbeid med informasjonssikkerhet og personvern, og inngår i Kunnskapsdepartementets og øvrige myndigheters styring og oppfølging av området. UiB etablerte sitt styringssystem for informasjonssikkerhet i 2015. Det ble oppdatert i 2019 med innarbeidelse av personvern i henhold til GDPR-bestemmelsene, og i 2020 med en oppdatering av UiBs styringsmodell for IKT.

I saksforelegget er det gjort rede for endringene som foreslås nå. Endringene omfatter i hovedsak utfyllende beskrivelser av roller og organisering, tydeliggjøring av plassering av andrelinje internkontroll, koble styring av informasjonssikkerhet til UiB sin beredskapsorganisering, samt knytte universitetsstyret tettere på arbeidet gjennom en årlig rapportering til styret. I tillegg er det gjort noen redaksjonelle endringer.

Forslag til vedtak:

Universitetsstyret vedtar endringene i Del I i Styringssystem for informasjonssikkerhet og personvern slik de framgår av saken.

Tore Tungodden
Universitetsdirektør

24.01.2024/Jimmy Thomsen/Monica Nielsen Øen/Tore Burheim (avd. dir.)

Vedlegg:
1. Saksframstilling
2. Forslag til revidert Styringssystem for informasjonssikkerhet og personvern (SIP), Del 1 – Styrende del

Saksframstilling

Styre:	Styresak:	Møtedato:	Arkivsaksnr:
Universitetsstyret	11/24	01.02.2024	2015/11386

Oppdatering av UiBs styringssystem for informasjonssikkerhet og personvern

Bakgrunn

Universitet i Bergen har styrket sitt arbeid med informasjonssikkerhet vesentlig de siste årene. Først gjennom tiltak og omdisponeringer internt på IT-avdelingen, deretter gjennom *Prosjekt sikre forskningssystemer*[1] og senest *Sikkerhetssatsingen*[2] vedtatt i 2023. Denne styrkingen er primært en konsekvens av en mer alvorlig trusselsituasjon, men skyldes i tillegg økte krav til dokumentasjon og etterlevelse fra departementet mv.

Prioriteringen av informasjonssikkerhet ved UiB har resultert i en forsterket organisering, blant annet med oppbygging av en egen sikkerhetsgruppe på IT-avdelingen. I tillegg til sikkerhetsgruppen kommer de ansatte som helt eller delvis er engasjert i Sikkerhetssatsingen og i Prosjekt sikre forskningssystemer. Sikkerhetssatsingen på UiB innebærer også en styrking av andre IT-funksjoner og tjenester som er avgjørende for god informasjonssikkerhet.

UiBs styringssystem for informasjonssikkerhet og personvern rammer inn UiBs arbeid med informasjonssikkerhet. Styringssystemet består av en styrende del, en gjennomførende del og en kontrollerende del. Styrende del beskriver blant annet sikkerhetsmål, sikkerhetsstrategi og hovedelementene i organiseringen, og besluttes av universitetsstyret. Selv om UiBs styrking av sitt arbeid med informasjonssikkerhet de siste årene først og fremst berører områder regulert av gjennomførende del og kontrollerende del er det nødvendig med noen oppdateringer i omtalen av organiseringen i styrende del også. Forslag til endringene omtales senere i dette saksforelegget.

Parallelt med UiBs satsing på informasjonssikkerhet har omfanget av styringsdokumenter og krav til styring, etterlevelse og rapportering økt. Universitets og høyskolesektoren har fått en *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*[3], det er etablert en *Styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning*[4], og KD har utarbeidet et *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor*[5]. Informasjonssikkerhet, beredskap og sikkerhet har også vært omtalt i Kunnskapsdepartementets tildelingsbrev til UiB de siste årene. UiB rapporterer i tråd med styringsmodellen årlig til HK-dir om sitt arbeid med informasjonssikkerhet, og HK-dir rapporterer til KD om sine funn. Totaliteten her innebærer at styring og rapportering innen informasjonssikkerhet har fått en mer fremtredende plass i eierstyringen fra KD. Dette forholdet bør også avspeiles i styringssystemet gjennom at styret

---

[1] Se styresak *120/21 Status og tiltak informasjonssikkerhet (unntatt offentlighet)*

[2] Se styresak *28/23 Oppfølging av internrevisjon informasjonssikkerhet og GDPR (unntatt offentlighet)*

[3] https://www.regjeringen.no/no/dokumenter/f-04-20-policy-for-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning/id2769629/

[4] https://cdn.sanity.io/files/dc7vqrwe/production/a36c542197a4876f46692a71d13da8f4602fde8b.pdf?dl

[5] https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeidet-med-samfunns-sikkerhet-og-beredskap-i-kunnskapssektoren/id2512037/

trekkes inn i styringssystemet. Vi opplever at dette er i tråd med universitetsstyret tydelige oppmerksomhet på informasjonssikkerhet de siste årene.

UiBs internrevisjon gjennomførte høsten 2022 en vurdering av UiBs arbeid med informasjonssikkerhet[6]. Revisjonsrapporten etterlyste blant annet noen rollebeskrivelser og formalisering av ansvaret for andrelinje internkontroll. I tråd med øvrig praksis på UiB har fagavdelingen ansvaret for andrelinje internkontroll, uten at dette er formalisert. Grunnet kapasitetsmangel har andrelinje internkontroll innen informasjonssikkerhet primært vært ivaretatt ved funn av avvik og årlig egenrapportering. Samtidig kan man argumentere for at Prosjekt sikre forskningssystemer er et stort andrelinje internkontrolltiltak. Det er senere i dette dokumentet forslag til endringer for begge disse forholdene.

Riksrevisjonen har i 2022/2023 gjennomført en forvaltningsrevisjon av informasjonssikkerhet i forskning og la fram rapporten for Stortinget 17.januar 2024. UiB var en av virksomhetene som ble undersøkt og fikk en tilbakemelding på funn sommeren 2023. Et par av funnene omhandler Styringsdokumentet (del I) i UiBs styringssystem for informasjonssikkerhet og personvern. Riksrevisjonen påpekte at noen rollebeskrivelser og mandater knyttet til informasjonssikkerhet forelå i andre styringsdokumenter[7], men ikke i styringssystemet. Videre påpekte de noen uklarheter i veiledninger og underliggende styringsdokumenter, samt manglende formalisering av retningslinjer. Det er noe overlapp mellom internrevisjonens funn og riksrevisjonens funn.

Om UiBs styringssystem for informasjonssikkerhet og personvern

UiBs styringssystem for informasjonssikkerhet og personvern er hjemlet i forvaltningsloven med forskrift. I henhold til e-forvaltningsforskriften skal styringssystemet være bygd på anerkjente standarder. UiBs styringssystem er bygd på ISO 27001 som er den mest brukte standarden. UiB etablerte sitt styringssystem i 2015 gjennom vedtak i universitetsstyret. Systemet består av en styrende del, en gjennomførende del og en kontrollerende del. Det bygger på kontinuerlig forbedring og årlige gjennomganger med ledelsen.

Styringssystemet ble revidert våren 2019 ved at UiB integrerte personvern i det, og justerte den styrende delen til å være konsistent med GDPR-regelverket og oppdatert personvernlovgivning. Styringssystemet byttet da navn til Styringssystem for informasjonssikkerhet og personvern (SIP).

I 2020 ble styringssystemet oppdatert for å tydeliggjøre UiBs styringsmodell for IKT[8]. Styringsmodellen bygger på at alle IT-systemer har en definert systemeier og at ansvar for sikker implementering, drift og forvaltning påligger vedkommende. Systemeier er definert til å være øverste leder på den enheten som eier/anskaffer systemet med mindre det er eksplisitt utpekt andre. IT-direktør er systemeier for fellessystemer, avdelingsdirektører er systemeiere for sine respektive fagsystemer, instituttleder er normalt systemeier for lokale fagsystemer som brukes i forskning og undervisning. Instituttleder og avdelingsdirektør vil i denne modellen være systemeier for personlige datamaskiner som ansatte drifter selv. Vesentlige deler av UiBs IT-sikkerhet bygger på at ansvaret til systemeier er forstått og ivaretatt.

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.

---

[6] Se styresak 14/23 *Internrevisjonsrapport – Informasjonssikkerhet og GDPR (unntatt offentlighet)*

[7] Rollebeskrivelsene og mandatene forelå i IT-avdelingens funksjons og bemanningsplan og i IT-avdelingens beredskapsplan, men ikke i SIP.

[8] Se styresak 16/20 *Styringsmodell for IKT*

Endring 1: Oppdatering av rollebeskrivelser i sikkerhetsorganisasjonen

Riksrevisjonen påpekte at informasjonssikkerhetsleder ikke hadde en eksplisitt rollebeskrivelse i styringssystemet, men var kun beskrevet i IT-avdelingens funksjons og bemanningsplan. Rollen framkommer implisitt ulike steder i styringssystemet gjennom oppgaver og ansvar, men ingen selvstendig rollebeskrivelse. I og med styrkingen av organiseringen knyttet til informasjonssikkerhet på UiB, og den økte betydning informasjonssikkerhet har fått, er det formålstjenlig å innta rollebeskrivelsen i styringssystemet. En slik rollebeskrivelse er tatt inn i kapittel 4 *Sikkerhetsorganisasjon, roller, ansvar og myndighet*. Rollebeskrivelsen er hentet fra funksjons og bemanningsplanen til IT-avdelingen, men forenklet med vekt på relevante oppgaver og ansvar.

Informasjonssikkerhetsleder leder IT-sikkerhetsgruppen som er organisatorisk plassert i IT-avdelingen. Informasjonssikkerhetsleder leder det løpende arbeidet med informasjonssikkerhet og rapporterer til IT-direktør som har det operative ansvaret for informasjonssikkerhet på UiB. Gruppen består i dag av teknikere, jurist og en ansatt som arbeider med risikostyring. Gruppen er godt integrert med øvrig virksomhet i IT-avdelingen. Denne integrasjonen bidrar til bedre løsninger, god ressursutnyttelse, god sikkerhetskultur og kompetansedeling på tvers.

Internrevisjonen[9] gav rollen som prosjektledere for forskningsprosjekter oppmerksomhet og indikerte at manglende opplæring og struktur rundt disse ville kunne utgjøre en risiko. UiB har ikke tatt med rollebeskrivelse av prosjektleder i styringssystemets styringsdokument for ikke å skape tvil om at ansvaret for informasjonssikkerhet og personvern ligger i linjen for forskningsansvarlige, som følger faglig lederlinje. Prosjektleders oppgaver i forhold til personvern og informasjonssikkerhet er omtalt i UiBs forskningsetiske retningslinjer. Riksrevisjonen påpekte i denne sammenhengen mangelfulle retningslinjer for sensitive data som ikke er persondata. Vi vil oppdatere retningslinjene for å tydeliggjøre ansvaret knyttet til sensitive data som ikke er personsensitive, samt en gjennomgang for å søke å tydeliggjøre kategoriseringen av ulike typer data.

I tillegg til punktene over er ansvaret for opplæring i informasjonssikkerhet og personvern tydeliggjort i styringsdokumentet samt en del mindre redaksjonelle endringer.

Endring 2: IRT-team og beredskap

Riksrevisjonen etterlyste også formalisering av UiBs IRT-team i styringssystemet. Et IRT-team (Incident Response Team) er en operativ tverrfaglig vaktstyrke som trener og har et spesifikt ansvar for førstelinje deteksjon og beskyttelse i tilfelle dataangrep. Gruppen ledes av informasjonssikkerhetsleder og er primært en beredskapsgruppe. UiBs IRT-team er sammensatt av særlig kompetente ansatte på tvers av IT-avdelingen og skal dekke et adekvat teknologispekter ut fra UiBs infrastruktur og systemer. Det er viktig å påpeke at gruppens eksistens ikke bryter med ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet i UiB og IT-avdelingens beredskapsarbeid.

UiBs IRT-team har i dag sitt mandat i UiBs beredskapsplaner og er en del av UiBs beredskapsorganisasjon. Riksrevisjonen påpekte at gruppen ikke var omtalt i styringssystemet. Vi har tatt med overordnet oppdrag i styringsdokumentet sammen med en tydeligere kobling mellom UiBs sikkerhetsstyring og beredskapsplaner. IRT-teamet vil ha et

[9] Se styresak 14/23 Internrevisjonsrapport – Informasjonssikkerhet og GDPR

eksplisitt mandat som ligger i et eget vedlegg i styringssystemets gjennomførende del. Dette mandatet vil inngå både i UiBs beredskapsplaner og i styringssystemet.

IT-avdelingens beredskapsplan skal dekke vesentlig mer enn bare informasjonssikkerhet (personal, HMS, pandemi, mv) og skal i tillegg være en støttefunksjon i beredskapssituasjoner for UiBs øvrige beredskap. Det er ikke naturlig å ta med andre deler av beredskapsplanverket i styringssystemet ut over et krav om at IT-avdelingen skal ha en beredskapsorganisasjon og beredskapsplaner som dekker informasjonssikkerhetshendelser.

Endring 3: Andrelinje internkontroll

Internrevisjonsrapport behandlet i styresak 14/23 påpekte at det ikke var tydelig i UiBs styringssystem for informasjonssikkerhet og personvern, hvem som hadde ansvaret for andrelinje internkontroll innen informasjonssikkerhet. Kontrollerende del av styringssystemet (del III) gir universitetsdirektør og IT-direktør rett til å gjennomføre kontrollerende aktiviteter, men ansvaret er ikke eksplisitt omtalt. Den kontrollerende aktiviteten gjennomføres ved årlig egenrapportering fra systemeiere og ved oppfølging av enkeltmiljøer ved funn av avvik. Det er også de siste årene gjennomført sikkerhetskontroller gjennom blant annet penetrasjonstester. Prosjekt sikre forskningssystemer som ble vedtatt av universitetsstyret i 2021, kan i denne konteksten betraktes som et stort andrelinje internkontrolltiltak. Prosjektet kartlegger og gjennomgår alt som finnes av lokalt driftet utstyr og systemer på UiB, og ser på organiseringen og ressurser til IT-drift, forvaltning og sikkerhet for disse. Basert på dette identifiseres og gjennomføres nødvendige tiltak. Dette prosjektet inngår nå i UiBs sikkerhetssatsing.

I styresak 13/23 *Helhetlig internkontroll ved Universitetet i Bergen* omtales ansvaret for andrelinje internkontroll som følger:

> *«2. linje har ansvar for å gjennomføre utvalgte aktiviteter for å etterprøve at 1. linjen fungerer tilstrekkelig. De fellesadministrative avdelingene ved UIB har overordnet prosessansvar på mange områder, og 2. linjeansvaret ligger dermed til disse enhetene. Enhetene skal dokumentere prosessene og gi rådgivning og støtte innenfor sine fagområder/hovedprosesser og har ansvar for å etterprøve at prosessene har tilstrekkelig kvalitet.»* (side 3 i saksforelegget, vår understrekning her)

I tråd med vedtaket i den saken vil andrelinje internkontroll for informasjonssikkerhet legges til IT-avdelingen, og ansvaret bør da plasseres her. Med hensyn til uavhengighet gis IT-sikkerhetsleder et selvstendig ansvar til å gjennomføre sikkerhetskontroller av det som er sentralt driftet og forvaltet. Kontrollene skal gjennomføres ut fra en verdi- og risikovurdering. Formuleringer som omtaler dette ansvaret er lagt inn i informasjonssikkerhetsleders rollebeskrivelse i kapittel 4 *Sikkerhetsorganisasjon, roller, ansvar og myndighet*.

Endring 4: Årlig rapportering til styret

Informasjonssikkerhet har de siste årene fått større oppmerksomhet i både eierstyring og rapportering til Kunnskapsdepartementet. Det har også blitt viktigere i UiBs virksomhet mer generelt. På denne bakgrunn er det naturlig å trekke styret tettere på oppfølging av området. I henhold til UiBs styringssystem for informasjonssikkerhet og personvern, og i de underliggende standardene dette bygger på, skal det avlegges en årlig rapport til ledelsens gjennomgang. Denne gjennomgangen har blitt gjort med universitetsdirektør og øvrig universitetsledelse. I tråd med ønsket om å trekke styret tettere på oppfølgingen foreslås det at den rapporten legges fram til styret sammen med universitetsdirektørens kommentarer etter ledelsens gjennomgang.

Ledelsens gjennomgang gjøres normalt i løpet av januar og det er derfor naturlig at denne saken legges fram for universitetsstyret i løpet av første kvartal. Det er lagt inn formuleringer i styringssystemet i tråd med dette i kapittel *4.4 Rapportering*.

I tillegg til punktene over er det gjort det en del mindre redaksjonelle endringer.

Universitetsdirektøren sine kommentarer
Universitetet i Bergen har de siste årene gjennomført en betydelig styrking av sitt arbeid med informasjonssikkerhet. I tillegg til konkrete forbedringer, har styrkingen også resultert i mer kapasitet og en sterkere systematikk. UiBs styringssystem for informasjonssikkerhet og personvern legger strukturen og rammene for dette arbeidet.

Krav til struktur, dokumentasjon og rapportering i arbeidet med informasjonssikkerhet har økt de siste årene, og den økte kapasiteten på området gjør det mulig å formalisere og forbedre UiBs praksis. Oppdateringene som foreslås i denne saken, vil følges opp med tilsvarende oppdateringer i de øvrige delene av styringssystemet.

Riksrevisjonen la fram sin rapport om informasjonssikkerhet i forskning 17.januar 2024. Det som omhandler enkeltinstitusjoner i rapporten, er unntatt offentlighet og noe er i tillegg skjermet etter sikkerhetsloven. UiB fikk i juni 2023 en rapport med Riksrevisjonens funn hos UiB. Disse følges opp blant annet med endringene fremmet i denne saken. Riksrevisjonens innretning og deres funn hos UiB er godt i overenstemmelse med vurderingene som ligger til grunn for UiBs sikkerhetssatsing. Vi vil komme tilbake til styret med oppfølgingen i forbindelse med rapportering på sikkerhetssatsingen til universitetsstyret.

I tråd med den oppdaterte versjonen av styringssystemet vil styret få framlagt årsrapport for informasjonssikkerhet på møtet i mars samtidig med rapportering på sikkerhetssatsingen.

Universitetsdirektøren anbefaler de framlagte forslagene til endringer i styringssystemet.

24.01.2024/Jimmy Thomsen/Monica Nielsen Øen/Tore Burheim (avd. dir.)

Styringssystem for informasjonssikkerhet og personvern (SIP)

Del 1 – Styrende del

Universitetet i Bergen

Versjon 4

Forslag til Universitetsstyret 01.02.2024

Innhold

Versjonshistorikk

Dato	Versjon	Endring	Godkjent
26.11.2015	1	Første versjon vedtatt av universitetsstyret	Styresak 131/15
28.05.2019	2	Oppdatert i iht 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 xx/24

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.

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 og beslutning av styringssystemet

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 og øvrige dokumenter og vedlegg som inngår i styringssystemet.

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)
- 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.
Informasjonsverdier	Alle typer data, opplysninger og dataressurser (IT utstyr, applikasjoner, systemer, datanettverk m.m) som har betydning for UIB sin virksomhet
Personvern-konsekvensvurdering (DPIA)	Lovpålagt vurdering når det er sannsynlig at behandlingen av personopplysninger medfører høy risiko.

IRT	Incident Response Team, et eget team av ressurspersoner som er utpekt særskilt til å håndtere sikkerhetshendelser på IKT området
IKT	Informasjons- og kommunikasjonsteknologi
EduCSC	Cybersikkerhetssenteret hos SIKT, innehar rollen som sektorvist responsmiljø (SRM) for universitets og høyskolesektoren. Sektorvise responsmiljø inngår i nasjonalt rammeverk for håndtering av IKT-sikkerhetshendelser.

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 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 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).

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 hensikten 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 UiBs faglige virksomhet.	Kan sammen med universitetsdirektør beslutte retningslinjer for behandling av personopplysninger

Rolle / funksjon	Ansvar	Myndighet
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.
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 sikkerhetsprosedyrer, 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. 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.	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.

Rolle / funksjon	Ansvar	Myndighet
Informasjons-sikkerhetsleder	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 vedlikeholde beredskapsplaner for informasjonssikkerhet. Bidra til at opplæring og rådgivning innenfor informasjonssikkerhet og personvern gjennomføres.	
Systemeier	Ansvarlig for å ha nødvendige risikovurderinger, og at risikohåndtering og tiltak gjennomføres slik at gjenværende risiko er på et akseptabelt nivå. Ansvarlig for å sette sikkerhetsnivå i systemer man eier ut fra dokumentert klassifisering av informasjon og personinformasjon, samt å ha dokumentasjon på at informasjonssikkerhet og personvern ivaretas. Ansvarlig for sikker drift og forvaltning av systemene de eier i henhold til lover, forskrifter, regler og øvrige bestemmelser, inkludert SIP, i hele systemets levetid. Ansvarlig for at nødvendig opplæring tilbys og gjennomføres i tilknytning til systemer de er eier av. 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	

Rolle / funksjon	Ansvar	Myndighet
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.	

Rolle / funksjon	Ansvar	Myndighet
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 sektorvis responsmiljø i eduCSC (SIKT).	

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 skal inngå i UiBs beredskapsplaner og beredskapsorganisasjon. IT-avdelingen skal ha en beredskapsplan og en beredskapsorganisasjon med særlig ansvar for informasjonssikkerhet. Beredskapen for informasjonssikkerhet og personvern skal bygge på ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet.

Som en del av beredskapen skal det eksistere et Incident Respons Team (IRT) ved IT avdelingen for særskilt håndtering av sikkerhetshendelser. Mandat og instruks for dette er 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.