UNIVERSITETET I BERGEN

Styre: Universitetsstyret **Dato:** 23.01.2020
Styresak: 16/20 **Arkivsaksnr:** 2015/11386
Møtedato: 20.02.2020

Styringsmodell for IKT

Henvisning til bakgrunnsdokumenter

- Styresak 53/19, Styringssystem for informasjonssikkerhet og personvern
- Styresak 66/19, Etatsstyringsmøte 2019. Tilbakemelding fra Kunnskapsdepartementet
- Styresak 67/19, Internrevisjonsrapport - Lokalt driftede IT-systemer
- Kunnskapsdepartementets styringsmodell for informasjonssikkerhet i høyere utdanning og forskning
- Styresak 5/20 Tildelingsbrev 2020 for Universitetet i Bergen

Saken gjelder:

I behandling av styresak 67/19 Internrevisjonsrapport - Lokalt driftede IT-systemer, ba styret om en sak om IT-governance, eller Styringsmodell for IKT, som er den termen vi velger å bruke. I denne saken legges det fram forslag til endringer i UiBs styringsmodell for IKT for bedre å ivareta UiBs institusjonelle ansvar for sin informasjonssikkerhet. Disse endringene formaliseres gjennom endringer i Styringssystem for informasjonssikkerhet og personvern.

Bakgrunnen var at internrevisjonen vurderte risikoen knyttet til lokal drift av IT-utstyr til å være middels med behov for forbedringer og at UiB har reaktive, og i dagens virkelighet, for svake styringsmekanismer relatert til IT-sikkerhet.

Endringene innebærer at UiB innfører et føre-var-prinsipp med tydelige krav om sikker drift og forvaltning av IT-systemer. IT-systemer og utstyr som skal kobles på nettverket må godkjennes. IT-avdelingen vil gjennom forhåndsgodkjenning få mulighet til i større grad å henvise systemer til UiBs skjermede datanett for forskningsinfrastruktur og tilsvarende (LabIT), UiBs løsning for sensitive data (SAFE) og andre tilpassede løsninger. Dette er i tråd med anbefalingen fra internrevisjonen.

Hovedregel vil bli at IT-avdelingen står for drift og forvaltning av systemer og plattformer opp til og med operativsystemnivå. Systemer kan driftes og forvaltes lokalt dersom man kan dokumentere at rutiner for sikker drift og forvaltning er i henhold til offentlige anbefalinger og UiBs felles regler kan etterleves.

Kunnskapsdepartementet vier informasjonssikkerhet økende oppmerksomhet og informasjonssikkerhet tas opp i den løpende styringsdialogen. Departementet og statsråden har på ulike måter tydeliggjort styrets ansvar i denne sammenhengen.

Forslag til vedtak:
Universitetsstyret vedtar endringene i Del I i Styringssystem for informasjonssikkerhet og personvern i henhold til anbefaling i saksframlegg.

Kjell Bernstrøm
universitetsdirektør

7.02.2020/Maria Lundhaug/Sidsel Storebø/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	16/20	20.02.2020	2015/11386

Styringsmodell for IKT

Bakgrunn
Informasjonssikkerhet og IT-sikkerhet er av avgjørende betydning for UiBs virksomhet, vår integritet, autonomi og vårt omdømme. Vi må sikre at våre data er til å stole på, at riktige personer har tilgang, at systemene virker som de skal og at de ivaretar krav til konfidensialitet, integritet og tilgjengelighet.

Gjennom erfaringer fra UiBs virksomhet, informasjon fra nasjonale myndigheter og annen åpen informasjon, ser vi at truslene mot informasjonssikkerheten øker. Å ivareta informasjonssikkerhet på en god måte er viktig for UiB og hele universitets- og høyskolesektoren.

Kunnskapsdepartementet har etablert et styringssystem for informasjonssikkerhet for universitets- og høyskolesektoren som helhet. I et brev fra statsråden 7. januar 2019 til institusjonene i sektoren ble det informert om modellen. I brevet tydeliggjør statsråden styrets ansvar: «Det er styrets ansvar å sette virksomheten i stand til å håndtere risikoen slik at denne er på et nivå som styret aksepterer. Jeg forventer også at håndteringen av dette viktige området integreres i den generelle virksomhetsstyringen og er tydelig forankret i styret og toppledelsen».

Departementets oppmerksomhet på området framkommer videre i tilbakemelding fra etatsstyringsmøtet 2019, der departementet «forutsetter at UiB prioriterer å etterleve gjeldende krav for informasjonssikkerhet og personvern». I tildelingsbrevet for 2020 forutsetter departementet at «UiB dimensjonerer forebyggende og konsekvensreduserende sikkerhetsarbeid i tråd med styrets risikoaksept».

UiB etablerte sitt styringssystem for informasjonssikkerhet i 2015. 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 sist 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.

Våren 2019 ble det gjennomført en internrevisjon på lokalt driftede IT-systemer på UiB (styresak 67/2019). Lokalt driftet innebærer at drift og forvaltning av systemene utføres på det enkelte institutt, i forskergrupper og andre steder utenfor IT-avdelingen. Med IT-system menes infrastruktur/utstyr og applikasjoner som behandler data i en eller annen form. Internrevisjonen vurderte risikoen knyttet til lokal drift av IT-systemer til å være middels med behov for forbedringer, og at UiB har reaktive og for svake styringsmekanismer for IT-systemer med tanke på IT-sikkerhet. Funnene i internrevisjonsrapporten bekrefter det generelle inntrykket av situasjonen på området.

Gjennom kartlegginger gjort i forbindelse med en pågående omorganiseringsprosess på IT-avdelingen, er det avdekket hvordan ukoordinerte anskaffelser av IT-systemer, gjerne med tilkoblet spesialutstyr (sensorer, måleapparater), både kan bli kostnadsdrivende, ineffektive

og sikkerhetsutfordrende. Det gjøres installasjoner og anskaffelser der UiBs sentrale IT-avdeling må drive brannslukking og opprydding i etterkant. Dette øker kostnadene og svekker IT-sikkerheten til UiB.

Styringsmodell IKT
Dagens styringsmodell 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. Vesentlige deler av UiBs IT-sikkerhet bygger dermed på at ansvaret til systemeier er forstått og ivaretatt, og står og faller på lokal kompetanse og ressurser. Vi ser at dette ikke alltid er tilstrekkelig for å ivareta UiBs informasjonsverdier og IT-sikkerhet.

I dialog med fagmiljøer avdekkes det stadig aktiviteter, oppsett og IT-utstyr som ikke oppfyller gjeldende lover, forskrifter og/eller god praksis. I utgangspunktet har ikke IT-direktør eller IT-sikkerhetsansvarlig fullmakt til å gripe inn overfor disse med mindre det er vesentlige sikkerhetshull.

I tråd med ovennevnte er det fra det institusjonelle ansvaret behov for å stramme inn på styringsmodellen. Dagens praksis med en ensidig serviceorientering har medført svekket IT-sikkerhet og økende kostnader.

Nivå på IKT-styring for å ivareta informasjonssikkerhet
Man kan foreta ulike grader av innstramming, fra å presisere ansvar med tilhørende krav til sikker drift og forvaltning, via ulike varianter av godkjenningsordninger og internkontrollregimer, til en full sentralisering av all IT-drift og forvalting på UiB med tilhørende sikkerhetsmekanismer.

Det er et krav i eForvaltningsforskriften[1] at forvaltningsorgan som UiB skal ha et styringssystem for informasjonssikkerhet bygd på anerkjente standarder. Dette gjelder hele UiBs virksomhet. UiB sitt styringssystem er basert på ISO 27001 som er den mest brukte standarden. For de mer spesifikke kontrollpunktene har UiB tatt utgangspunkt i standarden ISO 27002 for sine sentrale rutiner og praksis på området. Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet noen grunnprinsipper for IKT-sikkerhet[2]. Prinsippene omgjør kravene i ISO 27002 til noe mer forståelig og håndfast, og beskriver hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser. Digitaliseringsrundskrivet fra Kommunal- og moderniseringsdepartementet henviser til NSM sine grunnprinsipper som en anbefaling. Som forvalter av en betydelig IT-infrastruktur og stor samling av IT-systemer, må UiB bygge sine krav til sikker drift og forvaltning på disse prinsippene eller noe tilsvarende. Grunnprinsippene til NSM ansees som gode og relevante.

Det er få miljøer på UiB utenom IT-avdelingen som har kapasitet og/eller kompetanse til å følge NSMs grunnprinsipper. Det er derfor grunn til å etablere et helhetlig drifts- og forvaltningsregime for alle IT-systemer på UiB bygd på NSM sine grunnprinsipper.

UiB er en utsatt virksomhet der brudd på informasjonssikkerhet og personvern kan ha store konsekvenser. Brudd kan svekke UiBs integritet og omdømme vesentlig, usikkerhet om vi kan stole på våre forskningsdata vil være ødeleggende for forskningen i tillegg til direkte

[1] Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), §15
https://lovdata.no/dokument/SF/forskrift/2004-06-25-988
[2] https://www.nsm.stat.no/publikasjoner/andre-publikasjoner/grunnprinsipper-for-ikt-sikkerhet-1-1/

økonomiske konsekvenser gjennom tap av forskningsprosjekter, økonomisk svindel og store bøter (GDPR).

Basert på dette bør man innføre et føre var prinsipp der UiB på institusjonsnivå må sørge for sikker drift og forvaltning. Systemeier må sørge for å dokumentere at man ivaretar sikker drift og forvaltning, blant annet gjennom kompetanse og kapasitet, risikovurderinger og tiltak. I dag er det et problem at det til stadighet settes opp systemer som eksponerer UiBs data med for lav sikkerhet både med hensyn på integritet, tilgjengelighet og konfidensialitet. Derfor anbefales et føre-var prinsipp med en godkjenningsordning av systemer som skal kobles på nettet. På denne måten kan man også få oversikt over alt utstyr i tråd med internrevisjonens anbefaling.

Bedre IT-tjenester for bedre IT-sikkerhet
Omfang og kompleksitet knyttet til sikker drift og forvaltning med forhåndsgodkjenning av nye IT-systemer er krevende, og vil innebære en stor innsats fra IT-avdelingen. Samtidig vil det trolig være enda mer krevende for UiB om de enkelte fagmiljøene på egen hånd skal anskaffe, drifte og forvalte sine IT-systemer på en forsvarlig måte, med det betydelige kompetanseløftet, kapasitetsøkning og driftsregime det vil innebære. I tillegg er IKT-kompetanse i dagens arbeidsmarked vanskelig å skaffe og beholde.

I den pågående omorganiseringen av IT-avdelingen, og gjennom sentraladministrasjonens tjenesteutviklingsprosjekt, er det et mål å innrette avdelingens aktiviteter i større grad mot primærvirksomheten for å komme tettere på og bedre understøtte faglige behov. Gjennom et samarbeid med fagmiljøene vil en påse at krav til mer sentralisert drift og/eller forhåndsgodkjenning ikke hemmer den faglige aktiviteten. Ved å komme inn tidligere i prosessen, der informasjonssikkerhet og krav til forsvarlig drift settes på dagsorden, vil vi unngå dagens merarbeid knyttet til brannslukking og opprydding i etterkant.

Endringer i Styringssystem for informasjonssikkerhet og personvern (SIP)
Basert på gjennomgangen over fremmes det i denne saken forslag til endringer i SIP, styrende del. Det er to endringer, en på systemeieransvaret og krav til sikker drift og forvaltning med et føre-var prinsipp, deretter en bemyndigelse for å kunne iverksette tiltak for å følge dette opp.

Endring 1: Tydeliggjøring av systemeieransvar og krav til sikker drift
Fra internrevisjonsrapporten og oppfølging av den, ser vi at det kan være formålstjenlig å presisere at systemeieransvaret tilfaller leder ved den enheten som har anskaffet eller utviklet et system i de tilfellene der systemeieransvaret ikke er utpekt eller opplagt. Dagens formulering kan oppfattes å være litt uklar her, og det fremmes en forenkling.

For både å tydeliggjøre ansvaret til systemeier, krav til sikker drift og forvaltning og krav om godkjenning basert på føre-var, foreslås det i tillegg å omformulere resten av pkt. 4.5 og innføre et nytt punkt 4.6 som omhandler kravet til anskaffelser, sikker drift og forvaltning.

Angivelse av hvem som er systemeier er gitt i første avsnitt i pkt 4.5, der andre setning er ny. I det følgende er begge disse tatt med der nytt punkt 4.5 og 4.6 erstatter dagens 4.5:

> *4.5 Systemeieransvar*
> Systemeier er den øverste lederen ved enheten som eier systemene og er ansvarlig for de enkelte systemene innenfor enheten. Der det ikke er utpekt en systemeier, regnes leder ved den enheten 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 ansvar for å fastlegge formålet med behandlingen av personopplysninger i systemet og ivaretagelse av innebygd personvern.

4.6 Krav til anskaffelser og sikker drift og forvaltning av systemer
Ved anskaffelse eller utvikling av nye systemer har systemeier ansvar for at kravene til informasjonssikkerhet og personvern blir innfridd.

Systemeier skal sørge for sikker drift og forvaltning av systemene i henhold til lover, forskrifter, regler og øvrige bestemmelser, inkludert alle deler av UiBs styringssystem for informasjonssikkerhet og personvern.

Endring 2: Operativt ansvar for informasjonssikkerhet

For å kunne operativt iverksette tiltak basert på manglende sikker drift og forvaltning og øvrige krav, må noen bemyndiges til dette. I dagens modell kan IT-direktør iverksette tiltak og gripe inn overfor systemer med sikkerhetshull:

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.

Som tidligere vist er det behov for å innføre et føre-var prinsipp og sørge for at UiB som helhet oppfyller forskrifter og pålegg gjennom å forsterke bemyndigelsen her. Med dette formålet foreslås følgende som et nytt avsnitt etter foregående i punkt 4.4:

IT-direktør godkjenner systemer som skal kobles til og tilby tjenester på UiBs nett, basert på oppfyllelse av krav til anskaffelse og sikker drift og forvaltning. Dette omfatter også UiBs systemer som settes opp hos tredjepart. For de systemer der IT-direktør er systemeier ivaretar IT-sikkerhetsansvarlig denne oppgaven.

Formålet her er å sørge for at UiB har sikker drift og forvaltning av alle sine systemer. Formuleringen «kobles til og tilby tjenester» benyttes her for å avgrense mot ordinære PCer, mobile enheter og tilsvarende som kobler seg på UiBs nett med sikte på ordinært bruk. I de tilfellene en datamaskin eller annet IT-utstyr åpner for å besvare henvendelser fra internett lokalt eller eksternt, kommer formuleringen til anvendelse.

Universitetsdirektøren sine kommentarer

Universitetsdirektøren ser at god informasjonssikkerhet er en stadig større utfordring. Kunnskapsdepartementet har også en økende oppmerksomhet på området. God IT-sikkerhet er nødvendig for å sikre universitetets autonomi og integritet.

Lokalt og nasjonalt ser vi at det oppstår saker der institusjoners omdømme svekkes. Det er av kritisk viktighet for universitetets virksomhet å sørge for integritet i våre data. Dersom man ikke vet om man kan stole på sine forskingsdata ødelegges grunnlaget for forskningsresultatene.

Universitetsdirektøren ser at gode IT-tjenester til forskningsmiljøene er et godt tiltak også for informasjonssikkerhet. Kompetanse, kapasitet, kontinuitet og stordriftsfordeler gjennom å samle disse er et nødvendig tiltak for å kunne ivareta UiBs ansvar på institusjonsnivå.

I denne konteksten er den pågående omorganiseringen av IT-avdelingen der man i større grad skal bygge en organisering og innretning basert på verdiskapningen og aktivitetene i primærvirksomheten, et godt tiltak.

Iverksettelse og oppfølging av tiltakene i den foreliggende saken vil kunne medføre behov for organisatoriske endringer som har effekt også utenfor IT-avdelingen. Vi ser videre at lokal drift og forvaltning utenfor IT-avdelingen ofte blir utført av ansatte som har andre primæroppgaver. En vil vurdere nærmere om en sentralisering av disse oppgavene i tråd med internrevisjonsrapportens anbefaling vil medføre behov for ressurstilførsel for å gjennomføre endringene på en god måte med gode resultater. Skal UiB lykkes med å bedre informasjonssikkerheten slik beskrevet og i dagens kontekst, forutsetter det gode og sentrale IT-tjenester tilpasset primærvirksomheten.

Universitetsdirektøren anbefaler de framlagte forslagene til endringer i styringssystemet.

7.02.2020/Maria Lundhaug/Sidsel Storebø/Tore Burheim (avd. dir.)

Styringssystem for informasjonssikkerhet og personvern (SIP)

Del 1 – Styrende del

Universitetet i Bergen

Versjon 3

Innhold

1 Styringssystem for informasjonssikkerhet og personvern (SIP) 3
1.1 FORMÅL 3
1.2 BESLUTNINGSMYNDIGHET 3
1.3 VIRKEOMRÅDE 3
1.4 AKTUELLE LOVER, FORSKRIFTER OG REGLER 3
1.5 DEFINISJONER 5
2 Sikkerhetspolicy og policy for personvern 6
2.1 IDENTIFISERING AV KRITISKE VERDIER VED UIB 6
2.2 OVERORDNEDE SIKKERHETSMÅL 6
2.3 OVERORDNEDE STYRINGSMÅL FOR PERSONVERN 6
2.4 SIKKERHETSSTRATEGI 6
2.5 STRATEGI FOR PERSONVERN 7
2.6 KOMPETANSE 7
3 Risikostyring 7
4 Sikkerhetsorganisasjon, roller, ansvar og myndighet 8
4.1 BEHANDLINGSANSVARLIG FOR PERSONOPPLYSNINGER 8
4.2 OPERATIVT ANSVAR FOR BEHANDLING AV PERSONOPPLYSNINGER 8
4.3 OVERORDNET ANSVAR FOR INFORMASJONSSIKKERHET 8
4.4 OPERATIVT ANSVAR FOR INFORMASJONSSIKKERHET 8
4.5 SYSTEMEIERANSVAR 9
4.6 KONTINUITETSPLANLEGGING 9
4.7 FYSISK SIKKERHET 9
4.8 BEREDSKAP 9
4.9 ANSATTE OG STUDENTER 10

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	Sidsel Storebø
20.02.2010	3	Oppdatert etter internrevisjon 2019 og styresak 67/2019 om å øke governance/styringskontroll	Sidsel Storebø

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.
System	Infrastruktur/utstyr, applikasjoner, tjenester og løsninger som behandler data i en eller annen form.

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 godkjenner systemer som skal kobles til og tilby tjenester på UiBs nett, basert på oppfyllelse av krav til anskaffelse og sikker drift og forvaltning. Dette omfatter

også UiBs systemer som settes opp hos tredjepart. For de systemer der IT-direktør er systemeier ivaretar IT-sikkerhetsansvarlig denne oppgaven.

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 som eier systemene og er ansvarlig for de enkelte systemene innenfor enheten. Der det ikke er utpekt en systemeier, regnes leder ved den enheten 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 ansvar for å fastlegge formålet med behandlingen av personopplysninger i systemet og ivaretagelse av innebygd personvern. ~~alle sider ved forvaltningen av IT-systemene enheten har ansvar for når det gjelder utvikling, oppgradering, drift, tilgangskontroll, brukerstøtte og opplæring.~~

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.

4.6 Krav til anskaffelse og sikker drift og forvaltning av systemer

Ved anskaffelse eller utvikling av nye systemer har systemeier ansvar for at kravene til informasjonssikkerhet og personvern blir innfridd.

Systemeier skal sørge for sikker drift og forvaltning av systemene i henhold til lover, forskrifter, regler og øvrige bestemmelser, inkludert alle deler av UiBs styringssystem for informasjonssikkerhet og personvern.

~~4.6~~4.7 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~~4.8 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~~4.9 Beredskap

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

~~4.9~~4.10 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.