Rollebeskrivelse for systemeier ved Universitetet i Bergen

Generelt

Dette dokumentet beskriver arbeids- og ansvarsdelingen rundt drift, forvaltning og videreutvikling av IT-systemer ved UiB i de tilfellene der systemet har en systemeier.

Universitetsstyret behandlet i møte 20.6.2013 "Innsats for utvikling og koordinering av universitetets informasjonssystemer." (Se link på slutten av dokumentet.) Her bllir det bl.a. fastslått at det er de ulike sentraladministrativer avdelingene som har ansvar for systemene. I saksforelegget defineres systemansvar. Dette dokumentet operasjonaliserer dette ansvaret.

Rollebeskrivelsen erstatter ikke driftsavtale/"Avtale om leveranse av IT-tjenester". I noen tilfeller vil det foreligge en slik avtale i tillegg til rollebeskrivelsen.

Rollebeskrivelsen er først og fremst beregnet for systemer som er i produksjon. For systemer som er i utvikling eller under innføring, må rollebeskrivelsen sees i sammenheng med prosjektplan for utvikling/innføring av systemet.

De oppgavene som er knyttet til sikkerhet, må ses i lys av "Overordnet IKT- sikkerhetspolitikk ved UiB" fastsatt av Universitetsstyret. (Se link på slutten av dokumentet. Det er kommentert i fotnoter hvilke punkter som er direkte hentet fra "Overordnet IKT- sikkerhetspolitikk ved UiB".)

Spesifikasjon og aksept av rollebeskrivelsen

Denne rollebeskrivelsen gjelder for:	
System:	
Produksjonsstart dato:	
I drift til:	☐ Inntil videre ☐ Sluttdato:
Systemeier avdeling:	
Kontaktperson(er) hos systemeier:	
Kontaktperson(er) ved IT-avdelingen:	
Driftsleverandør:	☐ IT-avdelingen ☐ Ekstern: Kontaktperson(er) hos evt. ekstern driftsleverandør:
Merknader / unntak:	

Rollebeskrivelsen er forstått og akseptert.

Sted / dato:

Systemeier	IT-avdelingen	Evt. ekstern driftsleverandør

Arbeids- og ansvarsfordeling

	Systemeiers ansvar	ITAs ansvar
Overordnet[1]	Totalansvar for tjenesten. Ansvarlig for tjenestens funksjonelle kvalitet overfor sluttbrukerne. Ansvar for forvaltning av tjenesten.	*For systemer som ITA drifter:* – Ansvarlig for at system/applikasjon(er) kjører med tilstrekkelig tilgjengelighet og kapasitet.
Organisering, prosesser og leverandørkontakt	Sørge for at systemet håndteres etter gjeldende lover og regler.[2] Ansvarlig for at systemet oppfyller krav i lover, forskrifter o.l. Herunder også krav til personvern i henhold til Personopplysningsloven, Helseregisterloven, Helseforskningsloven m.v. Dokumentere hvilke eksterne bestemmelser og krav som er retningsgivende for informasjonssystemet.[3] Ansvarlig for avtaleverk med eventuell ekstern leverandør. (Driftsavtale, databehandleravtale o.l.) Etterleve prosesser og metoder som er etablert ved systemeier-avdeling, IT-avdelingen og UiB ellers. Forholde seg til roller og arbeidsgang som er beskrevet i evt. prosjektplan. *For systemer som utvikles/vedlikeholdes/driftes av ekstern leverandør:* – Hovedansvar for kontakt med eventuell ekstern leverandør. – Foreta bestillinger til ekstern leverandør. Bestillinger av teknisk karakter skal gjøres i forståelse med / etter godkjenning fra ITA.	Bistå og kvalitetssikre i avtaleinngåelse, forhandlinger o.l. med eventuell ekstern leverandør. Skrive og kvalitetssikre tekniske underlag, vedlegg o.l. for avtaler. Etterleve prosesser og metoder som er etablert ved systemeier-avdeling, IT-avdelingen og UiB ellers. Forholde seg til roller og arbeidsgang som er beskrevet i evt. prosjektplan. *For systemer som utvikles/vedlikeholdes/driftes av ekstern leverandør:* – Ansvar for dialog med eventuell ekstern leverandør om tekniske forhold. *For systemer som utvikles/vedlikeholdes/driftes ved UiB:* – Vurdere og godkjenne at produkter passer inn i UiBs systemportefølje og driftsmiljø.
Økonomi	Dekke alle direkte kostnader med tjenesten, så som lisenser, driftsavtale, serviceavtale, konsulentbistand, kurs/opplæring o.l. Dekke kostnaden for ITAs leveranser ihht. avtale eller prisliste når dette er avtalt.	Opplyse om kostnader, forhold som vil påvirke kostnader osv. Dekke kostnaden ved egen innsats som det ikke er avtalt at systemeier skal dekke.

[1] Jfr. "Status for og utvikling av universitetets informasjonssystemer. Juni 2013", s. 1.
[2] Jfr. "Status for og utvikling av universitetets informasjonssystemer. Juni 2013", s. 1.
[3] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 12.

	Systemeiers ansvar	**ITAs ansvar**
Utvikling, endringer, test og vedlikehold	Ansvar for utarbeidelse av kravspesifikasjoner i samarbeid med ITA. Ansvar for selv å kravsette funksjonalitet, brukergrensesnitt, arbeidsflyt o.l. Godkjenne forslag til nyutvikling. Prioritere oppgaver i samarbeid med ITA. Overordnet ansvar for test og aksept av endret funksjonalitet. Ansvarlig for akseptanse før produksjonssetting; herunder utarbeidelse av kriterier og testplan og gjennomføring av akseptansetest. Opplæring og informasjon til brukere ved ny funksjonalitet.	Vurdere forslag til nyutvikling. Skrive og kvalitetssikre utredninger og beslutningsunderlag for endringer og IKT- investeringer. Ved egenutviklete systemer: Foreta videreutvikling (i form av større og mindre endringer) på oppdrag fra systemeier. *For systemer som utvikles/vedlikeholdes av ekstern leverandør:* – Gi råd ved bestilling av nyutvikling, systemendringer, feilretting og vedlikeholdsoppgaver fra ekstern leverandør. *For systemer som ITA utvikler/vedlikeholder:* – Gjennomføre funksjonell og teknisk testing – Produksjonssetting av nye versjoner. – Endringshåndtering og implementering av mindre rettelser – Konfigurasjonsstyring.

	Systemeiers ansvar	**ITAs ansvar**
Drift	Ansvar for førstelinje brukerstøtte: Alle henvendelser om feilmeldinger, endringer o.l. går gjennom Systemeier Påse at enhetene som er involvert i drift av systemet har dokumenterte driftsprosedyrer.[4] Utarbeide egne rutiner for tilgang til det enkelte informasjonssystem.[5] Utarbeide og vedlikeholde eller tilrettelegge og tilgjengeliggjøre brukerdokumentasjon. Sørge for brukeropplæring.	Selv foreta, eller bestille fra ekstern leverandør problemløsning, feilretting, vedlikehold osv. *For systemer som ITA utvikler/vedlikeholder:* – Utarbeide og vedlikeholde system- og driftsdokumentasjon. – Sørge for tilstrekkelige overvåknings-/varslingsrutiner og -systemer. – Sørge for beskyttelse mot virus og andre former for angrep som kan påvirke systemenes stabilitet, integritet og konfidensialitet, samt rutiner for forebygging av de mest forekommende feilsituasjoner.[6] – Gjennomføre sikkerhetskopiering og tilbakelegging etter systemeiers spesifikasjoner. – Oppta og analysere hendelseslogger, i samråd med systemeiere.[7]

[4] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 8.
[5] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 9.
[6] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 8.
[7] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 8.

	Systemeiers ansvar	ITAs ansvar
Sikkerhet, data, datautveksling	Hovedansvarlig for sikkerhet knyttet til systemet, herunder ansvar for fastsetting av sikkerhetsnivået i systemene og for kontroll av at sikkerheten ivaretas, bl.a. gjennom systematiske gjennomganger (internkontroll).[8] Ansvarlig for klassifisering og sikring av informasjonen i systemet. Ansvarlig for at eventuelle personopplysninger i systemet håndteres i henhold til gjeldende lover og regler. Ansvarlig for å gjennomføre risikovurdering i samarbeid med ITA. Inkludert kritikalitetsvurdering og sårbarhetsanalyse. Ansvarlig for datainnhold i systemet, herunder datakvalitet og tilgjengeliggjøring av åpne data. Utarbeide planer og påse at det iverksettes tiltak som kan redusere avbrudd ved sikkerhetssvikt til et akseptabelt nivå. (Kontinuitetsplaner.) Det skal utføres realistiske kontroller for å verifisere effektiviteten av de tiltakene som er iverksatt.[9] Ansvarlig for å sikre at systemet og informasjon i systemet kan gjenopprettes.[10] *For systemer som driftes av ekstern leverandør:* – Ansvarlig for å vurdere behov for databehandleravtale og inngå slik der det er nødvendig.	Gi råd om sikkerhet. Vurdere og gi råd om tekniske sider ved datautveksling og integrasjon. Bidra ved risikovurdering. *For systemer som ITA utvikler/vedlikeholder:* – Implementere og ivareta sikkerhetsnivået som er valgt av systemeieren. – Utforme, implementere og drifte kontinuitetsløsning i henhold til systemeiers spesifikasjoner. Delta i realistiske kontroller av kontinuitetsløsning. – I samråd med Systemeier sikre at systemet og informasjon i systemet kan gjenopprettes.[11] – Varsle ved avvik, sikkerhetshendelser, trusler o.l. som berører systemet. – Utvikle integrasjon med andre interne eller eksterne systemer etter oppdrag fra systemeier eller andre. Herunder tilgjengeliggjøring av åpne data.

[8] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 12.
[9] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 11.
[10] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 11.
[11] Jfr. Overordnet IKT-sikkerhetspolitikk ved UiB, kap. 11.

	Systemeiers ansvar	ITAs ansvar
Kompetanseutveksling, informasjon	Forplikter seg til kompetanseutveksling med IT-avdelingen og ekstern leverandør slik at løsningen sikres en stabil og god driftssituasjon for UiB. Plikter å gjennomføre kompetansehevingstiltak i den grad det er nødvendig for å unngå personavhengigheter og sikre god forvaltning. Plikter å orientere ITA og ekstern leverandør om endringer i rutiner, organisering o.l. som kan ha betydning. Delta i UiB systemforum (hvis aktuelt; gjelder administrative fellessystemer). Innkalle til jevnlige møter med ITA.	Forplikter seg til kompetanseutveksling med systemeier og ekstern leverandør slik at løsningen sikres en stabil og god driftssituasjon for UiB. Plikter å gjennomføre kompetansehevingstiltak i den grad det er nødvendig for å unngå personavhengigheter og sikre god forvaltning. Plikter å orientere systemeier og ekstern leverandør om endringer i rutiner, organisering o.l. som kan ha betydning. Delta på jevnlige møter med systemeier.

Definisjoner:

(Slutt)bruker: Den som bruker et system/tjeneste.

Databehandleravtale: Avtale som brukes i tilfeller der behandling av personopplysninger settes ut til en annen virksomhet. Databehandleravtalen regulerer forholdet mellom eier og behandler av dataene.

Driftsavtale: Avtale som brukes i tilfeller der drift av et system settes ut til en annen virksomhet. Driftsavtalen regulerer forholdet mellom driftsleverandør og eier/bruker av systemet.

(System-)forvaltning: Ansvar for alle oppgaver knyttet til bevaring og forbedring av et system. Skilles gjerne fra de rent tekniske driftsoppgavene med å holde systemet operativt.

Integrasjon: Sammenkobling av systemer, f.eks. ved at et system mottar data fra et annet system for videre behandling.

Konfigurasjonsstyring: Prosessen med registrering og administrasjon av de ulike komponenter (maskinvare og programvare) som inngår i et system, med hensikt å visualisere og kontrollere systemets ytelse, funksjonelle og fysiske attributter.

Kontinuitet: I forbindelse med datasystemer: Systemers evne til å opprettholde vedvarende funksjonalitet og ytelse, spesielt i forbindelse med hendelser som kan forårsake avbrudd.

Personopplysninger: Opplysninger og vurderinger som kan knyttes til en enkeltperson. (Definisjon fra Lov om behandling av personopplysninger (personopplysningsloven) §2.

Produksjon: Fasen systemet er i når det brukes som normalt. Til forskjell fra utviklings- og test-fasene.

System: Generelt er et (data)system den samlingen av maskin- og programvare som brukes som en enhet eller for et avgrenset fagfelt eller formål. I dette dokumentet menes spesielt de(t) programmet/-ene som inngår i en slik enhet, omtrent det samme som en "applikasjon".

Systemeier: Den som har ansvar for et systems innhold og bruk i organisasjonen, i motsetning til driftsleverandøren, som har ansvar for den tekniske driften av systemet. Ved UiB er systemeieren øverste leder ved enheten som er ansvarlig for de enkelte systemene og løsningene.

Åpne data: Data som er gjort tilgjengelig for hele verden for fri videre bruk. Se også http://data.uib.no.

Relaterte eller nyttige dokumenter:

UiB styresak 2013-039: "Innsats for utvikling og koordinering av universitetets informasjonssystemer":
http://www.uib.no/filearchive/2013-039.pdf

"Overordnet IKT- sikkerhetspolitikk ved UiB," Fastsatt av Universitetsstyret 3.12.2009:
http://regler.app.uib.no/regler/Del-4-OEkonomi-eiendom-og-IKT/4.3-Informasjons-og-kommunikasjonsteknologi/Overordnet-IKT-sikkerhetspolitikk-ved-UiB

Uninett: "UFS136: Retningslinjer for klassifisering av informasjon":
https://www.uninett.no/webfm_send/758

Datatilsynet: "Databehandleravtale om behandling av personopplysninger" med bl.a. mal for databehandleravtale: http://www.datatilsynet.no/sikkerhet-internkontroll/databehandleravtale/

Direktoratet for samfunnssikkerhet og beredskap: "Risiko- og sårbarhetsanalyse":
http://www.dsb.no/no/Ansvarsomrader/Regional-og-kommunal-beredskap/Risiko-og-sarbarhet/Risiko--og-sarbarhetsanalyser/

Direktoratet for forvaltning og IKT: "Driftsavtalen (SSA-D). Avtale om kjøp av driftstjenester knyttet til maskinvare, infrastruktur og programvare" (Statens standardavtaler):
http://www.difi.no/artikkel/2009/11/driftsavtalen-ssa-d

Lov om behandling av personopplysninger (personopplysningsloven):
http://lovdata.no/dokument/NL/lov/2000-04-14-31

Lov om helseregistre og behandling av helseopplysninger (helseregisterloven):
lovdata.no/dokument/NL/lov/2001-05-18-24

Lov om medisinsk og helsefaglig forskning (helseforskningsloven):
http://lovdata.no/dokument/NL/lov/2008-06-20-44