UiT Norges arktiske universitet

Rutine for oppfølging av databehandleravtaler, informasjonssikkerhet og tjenesteavtaler med leverandører

Fastsatt av:	IT-direktør	Dato:	28.11.2023
Ansvarlig enhet:	ITA-RING	Id:	
Sist endret av:	ITA-RING	Dato:	28.11.2023
Erstatter:	Ny	Arkivref.:	2023/965

Formålet med rutinen er å beskrive hvordan UiT skal gjennomføre systematisk oppfølging av databehandleravtaler, informasjonssikkerhet og tjenesteavtaler med eksterne systemleverandører. Rutinen er forankret i retningslinjer for avtaleoppfølging som eies av innkjøpsfunksjonen på ORGØK (under utarbeiding pr. 28.11.2023).

Virkeområde
Denne rutinen gjelder alle leverandørforhold der en ekstern part leverer IT-tjenester til UiT.

UiT kjøper IT-tjenester innenfor de fleste virksomhetsområdene ved universitetet. Økt bruk av såkalte «hyllevarer» er en ønsket utvikling begrunnet i de siste årenes stortingsmeldinger om IT i offentlig sektor og økt bruk av sky-baserte leveranser. Dette innebærer et skifte for UiT fra å være på gode på intern drift, forvaltning og sikkerhet, til å bli gode på oppfølging av leverandørene.

Ansvar, myndighet og oppgavefordeling
Hovedformålet er at UiT får til en systematisk oppfølging av informasjonssikkerheten i leveransene inn til universitetet. Alle IT-tjenester er eid av en enhet, og det varierer stort hvor mange deler tjenestene består av og hvor kompleks forvaltningen blir for universitetet. Det vil derfor variere hvor mange møter som gjennomføres med leverandørene og hvor omfattende disse gjennomgangene blir. Denne rutinen beskriver et minstenivå for leverandøroppfølgingen, og må sees som et supplement til den generelle merkantile avtaleoppfølgingen som gjøres av innkjøpstjenesten ved UiT.

Regelverket for offentlige anskaffelser viser ikke hvordan universitetet skal følge opp databehandleravtaler, informasjonssikkerhet og tjenesteavtaler spesifikt, men vi finner at dersom universitetet skal få dette til, så må omfanget beskrives i avtalen vi inngår med leverandøren. Forarbeidet UiT gjør i anskaffelsen og avtaleinngåelsen setter føringer for leverandøroppfølging senere.

Begreper
«IT-tjenester» er i denne rutinen et samlebegrep som omfatter IT-systemer, IT-plattformer, programvare og apper. I noen tilfeller anskaffes systemer som er enkeltstående tjenester i seg selv, i andre tilfeller er tjenestene av en blanding av flere systemer/apper. I alle tilfeller er informasjonssikkerhet viktig.

Beskrivelse
Oppfølgingsaktivitetene følger linjen.

Systemeier initierer kontakt med leverandør og gjennomfører de årlige møtene som er forhåndsavtalt, samt evt. møter UiT får behov for underveis dersom noe endres i leveransen.

Faggruppelederne holder sine systemkatalogoppføringer oppdatert via sine systemforvaltere, og rapporterer evt. mangler til seksjonsleder. Det skal være kjent i alle faggrupper og tjenestelinjer hvordan dette foregår.

Rapportene (strukturerte referater) fra leverandøroppfølgingsmøtene skal arkiveres, og det skal sendes en kopi av rapporten til **innkjøpstjenesten** ved universitetet, som har ansvaret for generell merkantil avtaleoppfølging. Innkjøpstjenesten samler rapportene i sitt *konkurransegjennomføringsverktøy* og bruker de til fremtidig leverandøroppfølging.

I leverandørmøtene skal UiT:

- Spørre etter en oppdatert liste over underleverandører, og sammenhold denne med listen i avtalen
- Spørre om informasjon om evt. endringer i lokasjon for databehandling
- Spørre leverandør om de har hatt sikkerhetsbrudd som angår våre data siden sist gjennomgang
- Sjekke hvilken kontaktinformasjon leverandøren har fått fra oss, og ved behov endre denne til å være en funksjons e-postadresse slik at vi er sikre på at vi mottar varsler om sikkerhetshendelser
- Spørre leverandøren om de har evaluert sine egne sikkerhetstiltak og gjennomført internkontroll, siden sist

UiT skal, hvor det er mulig, gå gjennom tilgjengelige *revisjonsrapporter* som flere av de største leverandørene tilbyr kundene sine. Omfanget av disse rapportene er stort, og UiT må prioritere hvilke som skal gjennomgås basert på kritikalitet og anbefalinger fra sikkerhetsmyndighetene, informasjonssikkerhetsbrudd som blir kjent i media osv.

Referanser

- Retningslinje for avtaleoppfølging for ITA, *under utarbeidelse* (Seksjon for økonomi og innkjøp, ORGØK)