Retningslinje for informasjonssikkerhet i leverandørforhold

Type dokument	Retningslinje
Forvaltes av	Leder av IT-avdelingen
Godkjent av	Direktør for Organisasjon og infrastruktur
Gjelder fra	12.06.2023
Neste revisjon	12.06.2025
Unntatt offentlighet	Nei
Referanse ISO	ISO27002:2022 5.10,5.19,5.20
Referanse NSMs grunnprinsipper for IKT-sikkerhet	1.3.3c, 2.1.4
Referanse LOV/Regel	Eforvaltningsforskriften
Referanse interne dokumenter	Politikk for informasjonssikkerhet

1. Formål

Formålet med denne retningslinjen er å sikre at NTNUs leverandører ivaretar NTNUs informasjonsverdier og ikke påfører NTNU risiko for brudd på informasjonssikkerheten, dvs. sikre informasjon ut ifra krav om konfidensialitet, integritet og tilgjengelighet.

2. Gjelder for

"Retningslinje for informasjonssikkerhet i leverandørforhold" gjelder for alle innkjøpere og alle med oppfølgingsansvar i leverandørforhold.

3. Overordnede prinsipper

a. Kravene til informasjonssikkerhet slik de fremkommer i NTNUs «politikk for informasjonssikkerhet» med underliggende retningslinjer og rutiner, skal gjelde for eksterne leverandører.
b. Eksterne leverandører skal få tilstrekkelig opplæring i NTNUs krav til informasjonssikkerhet idet de gis fysisk eller logisk tilgang til IKT-infrastruktur som benyttes til å aksessere, transportere eller lagre informasjonsverdier som er klassifisert som Intern, Fortrolig eller Strengt Fortrolig. NTNUs IKT-infrastruktur omfatter alt utstyr, digital informasjon, informasjonssystemer og tjenester som benyttes til informasjonsbehandling og kommunikasjon.
c. Eksterne skal undertegne tilgangsavtale før de gis fysisk eller logisk tilgang til IKT-infrastruktur som benyttes til å aksessere, transportere eller lagre informasjonsverdier som er klassifisert som Intern, Fortrolig eller Strengt Fortrolig.
d. NTNU skal til enhver tid ha en oppdatert leverandørliste i et arkivsystem.
e. NTNU skal ha rutiner for forvaltning av leverandøravtaler. Leveransene skal regelmessig evalueres og revideres for å ivareta kravene til informasjonssikkerhet.

4. Krav til dokumentasjon og forvaltning

4.1. Dokumentasjonskrav

Leverandørliste skal inneholde:

a. leverandørens navn
b. leverandørens kontaktpunkt for gjennomføring av avtalen
c. NTNUs kontaktpunkt for gjennomføring av avtalen
d. avtalens varighet
e. lenke til avtalen, inklusive eventuelle endringer etter kontraktsinngåelse
f. oversikt over hvilke leveranseområder avtalen dekker
g. hvilke tilganger leverandøren har til NTNUs IKT-infrastruktur og/eller informasjonsverdier
h. hvilket klassifiseringsnivå på informasjon leverandøren er gitt tilgang til
i. om leverandøren behandler personopplysninger på vegne av NTNU, og om det er inngått skriftlig databehandleravtale (med lenke til en eventuell avtale)
j. om tjenestene fra leverandøren ansees som kritiske for at NTNUs IKT-infrastruktur skal være operativ
k. at det er gjennomført en risikovurdering dersom data som inneholder personopplysninger skal overføres til og/eller leverandør skal gis tilgang til slike data i løpet av avtaleperioden

4.2. Leverandørforvaltning

Følgende informasjon skal inngå:

a. en fordeling av roller og ansvar i avtaleforvaltningen
b. informasjonsflyten mellom rollene
c. nødvendige kontrollpunkter som kan verifisere at kravene til konfidensialitet, integritet og tilgjengelighet (KIT) er ivaretatt av leverandøren
d. hvordan samarbeidet med leverandøren skal utøves ved en alvorlig hendelse [1] eller en krise[2]
e. det skal følges opp at all informasjon og eiendeler leveres tilbake eller slettes ved terminering av avtale

5. Roller og ansvar

5.1. Leder av Økonomiavdelingen

a. er ansvarlig for at NTNU har en oversikt over leverandøravtaler som kan påvirke informasjonssikkerheten
b. er ansvarlig for at NTNU har en rutine for leverandørforvaltning

5.2. Leder av HR- og HMS-avdelingen

a. er ansvarlig for at ledere og ansatte er kjent med, og har tilstrekkelig kompetanse, til å ivareta sitt ansvar i henhold til denne retningslinjen.

5.3. Leder av IT-avdelingen

a. skal konsulteres ved endringer i retningslinjen

[1] Retningslinje for hendelseshåndtering og krisehåndtering
[2] Politikk for beredskap ved NTNU

5.4. Systemeier

a. er ansvarlig for at alle nødvendig avtaler med eksterne leverandører foreligger herunder databehandleravtale hvis relevant

5.5. Systemforvalter

a. er ansvarlig for å følge opp systemeiers interesser iht avtalen(es) innhold er ivaretatt overfor leverandøren(e)
b. skal foreta interne og eksterne bestillinger iht kontrakt(er) ved behov.
c. skal varsle systemeier om behov for endringer i kontrakt(er)

5.6. Linjeleder

a. skal sørge for tilstrekkelig opplæring i samarbeid med IT-avdelingen og HR-HMS-avdelingen og undertegning av alle nødvendige avtaler
b. skal vurdere og bestille nødvendige tilganger