PROSJEKTMANDAT FOR

PROSJEKTET «RÅDGIVNINGSTJENESTER OG KOMPETANSEHEVING»

INNENFOR PROGRAMMET «UH SIKKERHETSSATSING 2019-2022»

UNINETT PROSJEKTNUMMER: U1210018

Programleder Anders Lund, Uninett	Programeier Sigurd Eriksson, Unit

Prosjektleder TBA	Prosjekteier Tom Røtting, Uninett

ENDRINGSLOGG

Versjon	Dato	Endring	Produsent	Godkjent
0.1	05.09.19		ML	
0.2	09.09.19	Endringer ifm prosjektomfang	ML	
0.3	22.09.19	Revidert ihht kommentarer fra AL, RSN, TG og ØE	ML	
0.9	23.09.19	Siste justeringer før gjennomgang i Programstyre	ML	AL
0.9.1	03.10.19	Endringer ihht innspill fra Unit	ML, RSN	
0.9.1.1	17.10.19	Tekstlige justeringer under "Relevante tjenester" (pkt. 2 og 3)	RSN	
0.9.2	04.11.19	Endringer etter presentasjon i fagutvalget (okt) og innspill fra SE.	ML, RSN	
1.0	08.11.19	Siste versjon – vedtatt i programstyret	ML, RSN	Programstyre

UNINETT

1. BAKGRUNN

Prosjektet «Rådgivningstjenester og Kompetanseheving» er et av de tre hovedprosjektene definert under programmet «UH Sikkerhetssatsingen 2019-2022». Sikkerhetssatsingen er et tiltak med bakgrunn i «Digitaliseringsstrategien for UH-sektoren 2017-2021» fra Kunnskapsdepartementet (KD)[1].

Midler over statsbudsjettet er tildelt Unit og programmet skal gå over fire år. Av disse har Unit gjort videre tildeling til Uninett for å gjennomføre større deler av programmet. Programmet er organisert i tre hovedprosjekter, hvor Uninett har fått ansvaret for å lede to av dem:

1. Ny styringsmodell for informasjonssikkerhet og personvern (ledes av Unit)
2. Analysesenter og Responsmiljø (ledes av Uninett)
3. Rådgivingstjenester og Kompetanseheving (ledes av Uninett)

Dette dokumentet beskriver mandatet for prosjektet «Rådgivningstjenester og Kompetanseheving». Prosjektet skal utrede og anbefale hvilke tjenester som skal bidra til at institusjonene får mulighet til å bedre nivået på informasjonssikkerhet og personvern. Prosjektet skal videre foreslå en organisering og leveransemodell for hvordan disse tjenestene skal leveres til sektoren.

Mandatet for prosjektet understøttes av hovedanbefalingene som trekkes fram i tilstandsrapporten utgitt av Unit (2019)[2]. Som en del av Sikkerhetssatsingen, gjennomførte Unit kartleggingsmøter med de 21 statlig eide universitetene og høgskolene. Hensikten med kartleggingen er å få oversikt over omfanget av og systematikken i deres arbeid med informasjonssikkerhet og personvern. Rapporten kommer med klare anbefalinger på institusjonsnivå om å prioritere tiltak for kompetanseheving innenfor informasjonssikkerhet i alle virksomhetsområder og etablere en konsulent- og rådgivningstjenester for informasjonssikkerhet og personvern som kan bistå sektoren.

2. MÅL, HOVEDINNHOLD OG FORVENTEDE RESULTATER

Sikkerhetsløftet i kunnskapssektoren skal skje både gjennom forebyggende tiltak, videreutvikling og styrkning av den operative sikkerheten og sikkerhetskulturen generelt i sektoren.

Prosjektet skal etablere rådgivingstjenester for implementering og helhetlig praktisering av etablerte ledelsessystem for informasjonssikkerhet. Det skal etableres nødvendige tiltak for å heve kompetansen innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og øvrige ansatte.

[1] Tildelingsbrev fra Kunnskapsdepartement til Unit_ref.nr. 18/4768, datert 19.12.18

[2] Unit (2019): Tilstandsvurdering av informasjonssikkerhet og personvern blant de statlig eide universitetene og høgskolene

Prosjektet skal ta for seg organisering, mulighetsrom og utfordringer knyttet til sikkerhetsrådgivning i sektoren.

Prosjektet «Rådgivningstjenester og Kompetanseheving» skal konkret:

1. Etablere en fellesfunksjon i sektoren med ansvar for overordnet koordinering av rådgivningstjenester, og som bistår sektoren innen informasjonssikkerhet og personvern.
2. Kartlegge eksisterende kompetanse som kan tilgjengeliggjøres i sektoren og identifisere eksisterende tiltak for kompetanseheving som det kan være hensiktsmessig å bygge videre på. Dette skal bygge videre på allerede gjennomført kartleggingsarbeid i sektoren, for eksempel gjennomført risikovurdering (tilstandsrapporten, se under).
3. Iverksette nye tiltak for å heve kompetanse på institusjonsnivå innen informasjonssikkerhet og personvern i tråd med kartleggingen.
4. Vurdere hensiktsmessige samhandlingsarenaer for å skape forankring, brukerinvolvering, drøfting av løsninger, etc.
5. Vurdere hvordan prosjektet best mulig kan hjelpe institusjonene i arbeidet med kultur- og holdningsskapende arbeid innenfor informasjonssikkerhet og personvern

Prosjektet skal totalt sett bidra til å oppnå hovedmålet med programmet - å forbedre sektorens evne til å forebygge, oppdage og håndtere sikkerhetstrusler. Prosjektet skal i lag med de andre to prosjektene i satsingen bidra til å løfte informasjonssikkerheten i sektoren på et høyere nivå enn de nasjonale minstekravene.

Prosjektet vil benytte tilstands- og risikovurderingen som leveres av Unit hvert år for å gjøre justeringer på hvilke tjenester som bør prioriteres.

3. ANGREPSVINKEL OG METODE FOR GJENNOMFØRING – OMFANG AV ARBEIDET

Prosjektet skal i størst mulig grad benytte bestepraksis-metodikk. Prosjektet skal benytte smidig metodikk og tjenestedesign («design thinking») for utvikling av nye rådgivningstjenester og tiltak for kompetanseheving. Konkrete leveranser i prosjektet løftes etter hvert ut av programmet. Dette krever at prosjektet etablerer bærekraftige betalingsmodeller som sikrer at disse tjenester kan være selvbærende.
Pilotering og mest mulig kundeinvolvering skal benyttes.

Begge prosjektene ledet av Uninett gjennomføres i samarbeid med sikkerhetsmiljøene fra NTNU og UiO. Prosjektene skal samkjøres hvor det er hensiktsmessig, for å dra mest mulig nytte av synergien som finnes i arbeidet med utvikling av nye fellestjenester innen informasjonssikkerhet, rådgivning og kompetanseheving. Unit vil delta i prosjektet for å koordinere og sikre at behovene som er identifisert blir dekket i anbefalte løsninger, og vurdere hvordan de ulike miljøene best kan benyttes for å dekke behovene for rådgivningstjenester.

I tillegg til erfaringer fra tilstands- og risikovurderingen fra Unit skal man også gjennom prosjektet «Analysesenter og Responsmiljø» identifisere behov for tiltak innen kompetanseheving og rådgivningstjenester.

Arbeidet med kartlegging av rådgivningstjenester og tiltak for kompetanseheving vil falle inn under to fagområder:

- Operativ IKT[3]-sikkerhet og IRT[4] relatert (teknisk og operativ orientert)
  Målgruppe: Sikkerhetsmiljø/responsteam (IRT)
  Formål: Tiltakene skal bidra til å styrke kompetanse og øke evne til å effektivt håndtere sikkerhetshendelser lokalt på institusjonsnivå

- Informasjonssikkerhet og personvern (rettet mot administrasjon og ledelse)
  Målgruppe: Ledelse, ansatte og studenter
  Formål: Tiltakene skal bidra til å etablere felles metodikk og systemer for å bedre effekten av ledelsessystemer, internkontroll og rapportering på informasjonssikkerhet og personvern, som en integrert del av institusjonenes visksomhetsstyring.

Erfaringer og resultater fra tidligere arbeid i Sekretariatet for informasjonssikkerhet, etablert av Kunnskapsdepartementet og lagt til Uninett (2013-2018), danner et godt utgangspunkt for prosjektet.

Sekretariatet leverte følgende tjenester og tiltak til sektoren:

- Rammeverk og metodikk
- Risiko- og sårbarhetsvurderinger
- Sikkerhetskulturbygging
- Maler og informasjonsmateriell
- Internasjonalt samarbeid
- Drift av sikkerhetsforum
- Egne websider med informasjon

Sekretariatet dekket også leveranser innenfor bla. bistand til kontinuitets- og beredskapsplaner, revisjoner, bistand ved ledelsens gjennomgang, informasjon om trusselbildet og utvikling av dette.

4. HOVEDAKTIVITETER OG MILEPÆLSPLAN

4.1. Hovedaktiviteter for prosjektet

Prosjektet skal i første omgang kartlegge og prioritere arbeidspakkene og aktivitetene for perioden 2019-2020, med utgangspunkt i behovene som finnes i sektoren, slik beskrevet ovenfor. Behovs- og kompetansekartlegging er et utgangspunkt for å etablere veikartet for prosjektet.Følgende aktiviteter prioriteres for tidsrammen 2019-2020 (foreløpig plan):

[3] IKT = Informasjons- og KommunikasjonsTeknologi
[4] IRT = Incident Respons Team

Hovedaktivitet	NOV	DES	JAN	FEB	MAR	ABR	MAI	JUN	JUL	AUG	SEP	OKT	NOV
– Behovskartlegging													
Prioritering og etablering av tjenester													
Pilotering													
Evaluering													

Prosjektet anser følgende tjenester som relevant for sektoren, med bakgrunn i erfaringer fra Uninett gjennom Sekretariatarbeid (2013-2018) og hovedanbefalinger fra tilstandsrapporten utgitt av Unit (2019):

1) Revisjon og videreutvikling av ledelsessystem for informasjonssikkerhet: Bistå institusjonene med revisjoner av informasjonssikkerhet og personvern, og komme med forslag til nødvendige tiltak på bakgrunn av revisjoner. Omfatter vurdering av prosesser, organisering, sikkerhetstiltak og bruk av partnere og leverandører.

2) Risiko- og sårbarhetsvurdering (ROS): Bistand og kompetanseheving (kursing, gjennomføring og rapportskriving) for å bidra til at institusjonene gjennomfører regelmessige risikovurderinger. Risikovurderinger er et nødvendig grunnlag for alt forebyggende sikkerhetsarbeid, og er lovpålagt når det gjelder personopplysninger.

3) Bistand på institusjonsnivå for å skaffe oversikt over informasjonsverdier og klassifisering av informasjon (i forhold til f.eks. kritikalitet, sensitivitet, oppbevaringsperiode og avhending), inkludert digitale systemer og tjenester, slik anbefalt i tilstandsrapporten fra Unit (2019).

4) Styrke sikkerhetskompetanse lokalt på institusjonsnivå basert på det arbeidet som Uninett bidrar til. De fleste UH-institusjonene har gjennomført kurs hos Uninett om hvordan man etablerer og driver et responsteam («IRT-kurs»). Prosjektet skal vurdere behovet for oppfølging, oppfriskning og påfyll i sektoren, med spesielt fokus på interne rutiner for rapportering, avviks- og hendelseshåndtering. Dette inkluderer å innlemme en eksisterende IRT-funksjon i ledelsessystem.

5) Kontinuitets- og Beredskapsplan (KBP) for IT-infrastruktur: Bistå institusjonene i planlegging for gjenopprettelsen av normal drift i etterkant av alvorlige sikkerhetshendelser. Bidra til utarbeidelse, revisjon og testing av slike planer. «Kontinuitetsplanlegging» er påpekt som et anbefalt tiltak på institusjonsnivå i tilstandsrapporten fra Unit (2019).

6) Bistand til å utvikle og gjennomføre beredskapsøvelser på IKT - området. Tiltaket er spesifikk nevnt i årets tildelingsbrev fra KD/Unit.

4.2. Milepæler

Milepælsplanen for prosjektet blir mer detaljert etter arbeidet med veikartet er fullført. Tabellen under viser milepælene definert for 2019-2020.

	Beskrivelse	Ferdig dato	Godkjennes av
M0	Prosjektmandat godkjent	Nov 2019	Programstyre
M1	Behovskartlegging for prosjektet utført og godkjent	Feb 2020	Programstyre
M2	Prioritering og etablering av tjenester igangsatt	Mars 2020	
M3	Oppstart pilotering av tjenester	Mai 2020	

4.3. Konsekvenser for drift og forvaltning

Nye fellestjenester innen rådgivning og kompetanseheving for informasjonssikkerhet og personvern krever spesiell kompetanse og en robust organisasjon som holder informasjon, kompetanse og kursmaterialet oppdatert til enhver tid.

Kunnskapsdepartementets sektorvise responsmiljø; Uninett CERT og organisasjonen som prosjektet skal etablere som en faglig sentral rådgivningsenhet for sektoren må styrkes og bemannes i forhold til det reelle behovet for å klare å ivareta både vanlig drift og operative sikkerhetsoppgaver og forespørselen om sikkerhetsrådgivning fra sektoren.

5. ORGANISERING

Tabellen under viser deltakere i kjerneteamet:

Navn	Organisasjon/rolle	Rolle i prosjektet
TBA	Uninett Prosjektleder	Prosjektleder
Øyvind Eilertsen	Uninett Seniorrådgiver Sikkerhet	Seniorrådgiver
Tor Gjerde	Uninett Seniorrådgiver Sikkerhet	Seniorrådgiver
Nyansatt Seniorrådgiver	Uninett Seniorrådgiver Sikkerhet	Seniorrådgiver
NSD (TBA)		
Unit (TBA)		
Sektor representant (TBA)		

Kompetansemiljøet som finnes i Unit for informasjonssikkerhet og i NSD for personvern generelt vil trekkes inn i kjerneteamet.

Prosjektet skal etablere en referansegruppe som gjenspeiler bredden i sektoren. Det anbefales at referansegruppen skal bidra aktivt.

Interessentgruppen og andre samarbeidspartnere for programmet er kartlagt gjennom egen interessentanalyse.
Programstyret er premissgiveren for prosjektet. Referansegruppen etablert for prosjektet «Analysesenter og Responsmiljø» vil kunne gi verdifull input for de delene av prosjektet som omhandler operative og tekniske aspekter. Utover denne gruppen er det naturlig å involvere Fagutvalget for informasjonssikkerhet.

6. BUDSJETT

6.1. Finansiering

Kunnskapsdepartementet har gitt tilsagn om 17,5 mill. kroner årlig til Unit for etablering og gjennomføring av programmet for økt sikkerhetssatsing i UH-sektoren i fire år. Av disse er det gitt tilsagn om 12,5 mill. kroner til Uninett for å etablere og lede prosjektene som skal implementere nødvendige tiltak for å styrke informasjonssikkerheten, bl.a. etablering av sektorens analysesenter for cybersikkerhet, rådgivingstjenester og kompetanseheving innen informasjonssikkerhet og personvern. De øvrige 5 mill. kroner skal finansiere etablering og forvaltning av oppgavene og rollene i Unit.

12,5 mill. kroner tildelt Uninett fordeles mellom de to prosjektene som Uninett er ansvarlig for; «Analysesenter og responsmiljø» og «Rådgivningstjenester og Kompetanseheving».

Prosjekt	**Tilskudd** (MNOK pr år)
Ny styringsmodell (Unit)	**5,0**
Analysesenter og responsmiljø (Uninett)	**12,5**
Rådgivningstjenester og kompetanseheving (Uninett)	
Totalt årlig tilskudd	**17,5**

I tabellen under vises et grovt estimat over foreslått fordeling av tilskuddet mellom prosjektene.

Budsjett	**2019**	**2020**	**2021**	**2022**
Programadministrasjon	1	0,5	0,5	1
Analysesenter og Responsmiljø	10	8	7	7,5
Rådgivningstjenester og Kompetanseheving	**1,5**	**4**	**5**	**4**
Totalt tilskudd (NMOK)	**12,5**	**12,5**	**12,5**	**12,5**

Et mer detaljert budsjett for prosjektet blir utarbeidet etter at veikartet for prosjektet er skissert ferdig. Prosjektet er basert på smidig metodikk. Dermed er kostnadsfordelingen over år og mellom de to prosjektene som Uninett leder basert på et grovt estimat.

6.2. Planlagt forbruk

Prosjektet pådrar seg følgende kostnader: Egen ressursinnsats, konsulent og annen innleie, reise- og møtekostnader, samt arbeidsressurs fra samarbeidspartnere og andre direktekostnader.

De to første prosjektårene er det estimert et timeforbruk i underlag av 3 årsverk. Estimatet for timeforbruk innebærer fagpersoner fra både Uninett og eksterne fra samarbeidspartnere i prosjektet. Arbeidsomfanget og ressursbehovet for tidsrammen 2019-2020 blir først definert gjennom arbeidet med behovskartlegging i prosjektet.

7. KRITISKE SUKSESSFAKTORER / RISIKO

Suksessfaktor	Risikoreduserende tiltak
Konkretisering og riktig prioritering av leveransene i prosjektet i tråd med målsetninger og brukerbehov	Grundig planleggings- og veikartarbeid prioriteres, med involvering av ressurser hos Uninett og samarbeidspartnere. Veikartet for prosjektet forankres hos prosjektgruppen og godkjennes av Programstyret.
Tilgang på tilstrekkelige ressurser og spesialkompetansen	God ressursplanlegging mht veikartet. Inkludert innleie eller evt rekruttering av spesialkompetanse om nødvendig.
Tilfredsstillende fremdrift i prosjektet	God planlegging av delleveranser og aktivitetene ihht veikartet. Jevnlig statusrapportering i prosjektet for kjerneteamet og overfor Programstyret.
Tydelig roller og ansvarfordeling i prosjektet	Tydelig prosjektmandat og styringsdokumentasjon. Sikre felles forståelse blant prosjektdeltakere.
Sikre forankring av prosjektet hos interessentgruppen	Involvering og jevnlig informasjon til premissgivere og andre relevante interessenter.
Tillit og godt samarbeid blant deltakere i prosjektet	Åpen og hensynsfull kommunikasjon. Klare ansvarsforhold og gode rutiner for informasjonsformidling.

8. PROSJEKTSTYRING

Prosjektet rapporterer til Programstyret i forbindelse med styremøtene som er planlagt å avholdes minst fire ganger i året, på samme linje som de andre delprosjektene som inngår i satsingen. Minimumsrapportering skal innebære fremdrift, leveranser og økonomi. Rapportering utover denne minimumsrapportering kan avtales ved behandling av prosjektbeskrivelsen.

Programlederen deltar på styremøtene i tillegg til medlemmene i programstyret, med ansvar for rapportering om status på de tre prosjektene som programmet består i. Prosjektlederne kan også delta ved behov for statusrapportering.

Prosjektet skal ha hyppigere rapportering og kontinuerlig dialog med programlederen, minst to ganger i måned.

Prosjektgruppen og samarbeidspartnere skal avtale hyppige arbeids- og statusmøter basert på organisering av arbeidet iht veikartet for prosjektet.

Prosjektdokumentene skal lagres på programportalen opprettet på MS Sharepoint hos Uninett. Det benyttes samhandlingsverktøy (O365) der prosjektgruppen får tilgang til relevant prosjektinformasjon.