**// AVTALE – BILAG**

**Arbeids- og velferdsdirektoratet**

**v/IT avdelingen**

**Avtale om Managed security service**

**Kontrakt 20-6572**

**Bilag 1 Kundens kravspesifikasjon**

Innholdsfortegnelse

[1 Formålet med anskaffelsen 3](#_Toc51151312)

[1.1 Innledning 3](#_Toc51151313)

[1.2 Begrepsliste 3](#_Toc51151314)

[2 Overordnet beskrivelse av leveransen 3](#_Toc51151315)

[2.1 Omfang og beskrivelse 3](#_Toc51151316)

[2.2 Servicehåndbok 4](#_Toc51151317)

[3 Forklaring til kravspesifikasjonen 4](#_Toc51151318)

[3.1 Innledning 4](#_Toc51151319)

[3.2 Prioritering av krav 5](#_Toc51151320)

[3.3 Besvarelse av krav 5](#_Toc51151321)

[4 Generelle krav for hele tjenesteavtalen 6](#_Toc51151322)

[4.1 Krav til sikkerhetsklarering og taushetsplikt 6](#_Toc51151323)

[4.1.1 9.1 6](#_Toc51151324)

[4.1.2 9.2 6](#_Toc51151325)

[4.1.3 6](#_Toc51151326)

[4.2 24/7 SOC tjenester (Security Operations Centre) 6](#_Toc51151327)

[4.2.1 Krav til tjenester for sikkerhetsovervåking, hendelseshåndtering og varsling 24/7. 6](#_Toc51151328)

[4.2.2 Krav til tjenester for hendelsesrapportering. 6](#_Toc51151329)

[4.2.3 Krav til loggovervåkingstjenester (IaaS, PaaS, SaaS, on-premise, multicloud) 7](#_Toc51151330)

[4.3 Operational services (en del av SOC) 7](#_Toc51151331)

[4.3.1 Krav til IPS/IDS tjenester 7](#_Toc51151332)

[4.3.2 Krav til SIEM tjeneste 7](#_Toc51151333)

[4.3.3 Krav til Endpoint Detection and Response (EDR) 7](#_Toc51151334)

[4.3.4 Krav til Email security 7](#_Toc51151335)

[4.3.5 Krav til Cloud access security broker (CASB) 7](#_Toc51151336)

[4.3.6 Krav til Web application firewall (WAF) 8](#_Toc51151337)

[4.3.7 Krav til Continuous Vulnerability Monitoring (Sårbarhetsanalyse) 8](#_Toc51151338)

[4.4 Incident Response Team (IRT) 8](#_Toc51151339)

[4.4.1 Krav til konsulentbistand og beredskap i forbindelse med håndtering og analyse av sikkerhetshendelser (Incident Response Team – IRT). 8](#_Toc51151340)

[4.5 Kompetanse til innføring av nye tjenester 8](#_Toc51151341)

[4.5.1 Krav til konsulentbistand ved innføring av nye eller endring av eksisterende sikkerhetsovervåkingssystemer, samt generell rådgivning innenfor avtaleområdet. 8](#_Toc51151342)

[4.6 Krav til forretningsmessig satsningsområde innen sikkerhetsovervåkning 9](#_Toc51151343)

[4.6.1 9](#_Toc51151344)

[4.6.2 9](#_Toc51151345)

[4.6.3 9](#_Toc51151346)

**Bilag 1: Kundens kravspesifikasjon**

# Formålet med anskaffelsen

## Innledning

NAV IT skal anskaffe en avtale for sikkerhetsovervåking av IKT-tjenestene. IKT-tjenestene omfatter NAVs totale infrastruktur fra datasenter til klienter.

Avtalen skal dekke behov for sikkerhetsovervåking av dagens og fremtidens IKT-tjenester i NAV. NAV IT ønsker gjennom dialog med leverandører å komme frem til en best mulig tilpasset løsning, som også kan videreutvikles i samarbeid med leverandøren i avtaleperioden.

NAV ønsker at anskaffelsen resulterer i følgende effekter:

• monitorering og korrelering av sikkerhetsalarmer 24/7/365 med hensyn på å avdekke sikkerhetshendelser og varsle disse

• sørge for sikkerhet og kontinuitet i NAVs tjenester gjennom proaktiv filtrering og blokkering av potensielt skadelig innhold

• synliggjøre trusselbildet gjennom periodiske rapporter for å kunne ta bedre avgjørelser og iverksette nødvendige tiltak

• ivareta sikkerhetsovervåking og aktiv trafikkregulering/blokkering av sikkerhetstrusler for eksisterende og fremtidige løsninger i NAV

• gi NAV rask tilgang på spisskompetanse for bistand ved større sikkerhetshendelser.

## Begrepsliste

NAV planlegger at vi sammen med deltakerne i dialogen skal komme frem til en begrepsliste som forklarer viktige begreper som skal benyttes ved utførelsen av tjenesten

# Overordnet beskrivelse av leveransen

## Omfang og beskrivelse

Kommende endringer i NAVs systemer og infrastruktur vil påvirke kjøp på avtalen. Anskaffelsen omfatter utfasing av gammel IPS -løsning, og innfasing av en ny tjeneste for sikkerhetsovervåkning.

Avtalen inkluderer anskaffelse, drift og vedlikehold av løsninger for sikkerhetsovervåking av Kundens systemer samt aktiv blokkering av sikkerhetstrusler mot Kundens systemer. Følgende områder er inkludert:

* 24/7 SOC tjenester (Security Operations Centre)
  + Tjenester for sikkerhetsovervåking, hendelseshåndtering og varsling 24/7.
  + Tjenester for hendelsesrapportering.
  + Loggovervåkingstjenester (IaaS, PaaS, SaaS, on-premise, multicloud)
* Operational services (en del av SOC)
  + IPS/IDS tjenester
  + SIEM tjeneste
  + Endpoint Detection and Response (EDR)
  + Email security
  + Cloud access security broker (CASB)
  + Web application firewall (WAF)
  + Continuous Vulnerability Monitoring (Sårbarhetsanalyse)
* Incident Response Team (IRT)
  + Konsulentbistand og beredskap i forbindelse med håndtering og analyse av sikkerhetshendelser (Incident Response Team – IRT).
* Kompetanse til innføring av nye tjenester
  + Konsulentbistand ved innføring av nye eller endring av eksisterende sikkerhetsovervåkingssystemer, samt generell rådgivning innenfor avtaleområdet.

## Servicehåndbok

I tilknytning til avtalen skal det etableres en Servicehåndbok. Denne skal inneholde detaljert beskrivelse av felles rutiner, grensesnitt og roller mellom Leverandøren og Kunden, og regulere hvordan disse skal ajourholdes og forvaltes.

Alle rutiner, grensesnitt og roller som er en konsekvens av kravene som stilles i dette bilaget, vil bli generelt beskrevet under angjeldende kapittel/punkt. Den detaljerte beskrivelse av de samme rutiner, grensesnitt og roller skal innarbeides i Servicehåndboka.

Innholdet i Servicehåndboka skal kunne endres ved enighet mellom partene i statusmøter, uten å måtte gjøre endringer i avtalen. I tilfelle uoverensstemmelser mellom Avtalen og Servicehåndboka, vil Avtalens tekst alltid være gjeldende.

Leverandøren har ansvar for at siste versjon av Servicehåndboka til enhver tid ligger tilgjengelig i Kundeportalen.

# Forklaring til kravspesifikasjonen

## Innledning

Ved kunngjøring av konkurransen har oppdragsgiver utformet et utgangspunkt for den kravspesifikasjonen som skal gjelde i konkurransen (dette dokumentet). I dialogfasen skal oppdragsgiver, sammen med leverandørene, komme frem til den endelige kravspesifikasjonen for konkurransen. Den kunngjorte kravspesifikasjonen vil dermed bli utviklet og endret i dialogen med leverandørene.

De kravene som er merket som A-krav i dette dokumentets punkt 4, er å anse som minimumskrav for det som skal inngå i tjenesten. Disse kravene vil ikke bli endret som følge av dialogen. Dialogen mellom partene vil imidlertid kunne medføre at det tilføres ytterligere A-krav som skal gjelde i konkurransen, samt V-krav som vil være gjenstand for evaluering.

## Prioritering av krav

Kravene er gitt en prioritet ut fra følgende system:

A - Absolutt og ufravikelig krav

V - Viktig krav

## Besvarelse av krav

Kravspesifikasjonen er bygget opp i tabeller som vist nedenfor:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  |  | V |  | X |

***<Leverandørens utfyllende kommentar til krav ......>***

Kravspesifikasjonen skal besvares på følgende måte:

|  |  |
| --- | --- |
| **Felt** | **Besvares som beskrevet** |
| Nr. | Kundens identifikasjon av kravet. *Skal ikke endres*. |
| Krav til Leverandør | Kundens beskrivelse av kravet. *Skal ikke endres*. |
| Prioritet (A/V) | Kundens prioritering av kravet. Se 3.1. *Skal ikke endres*. |
| Svar (J/N) | Leverandøren skal her svare om kravet kan oppfylles eller ikke.  Dersom kravet oppfylles i sin helhet i den på nåværende tidspunkt tilgjengelige versjon som Leverandøren vil tilby, svares <J>.  Dersom kravet bare delvis oppfylles eller vil bli oppfylt i en senere versjon, svares <N>. Leverandøren kan i dette tilfellet beskrive på hvilken måte kravet delvis oppfylles eller vil bli oppfylt. Leverandøren skal da krysse av i feltet ’Utfyllende kommentar’ med uthevet skrifttype som vist: <X>. |
| Utfyllende kommentar | Når dette feltet er krysset av med en <X>, skal Leverandøren gi en utfyllende kommentar i anvist område under kravtabellen, se nedenfor. Dersom Leverandøren selv ønsker å gi utfyllende kommentarer, skal feltet krysses av med en uthevet <X> som beskrevet ovenfor. |
| <Leverandøren...> | Dette angir området hvor Leverandøren skal gi sine utfyllende kommentarer. Kommentarene skal skrives med uthevet skrift. Dersom Leverandøren selv velger å gi utfyllende kommentarer, skal Leverandøren legge disse inn på tilsvarende måte. Dette området må da komme rett etter angjeldende tabell, og henvise til punktet |

# Generelle krav for hele tjenesteavtalen

## Krav til sikkerhetsklarering og taushetsplikt

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet (A/V) | Svar  (J/N) | Utfyllende  kommentar |
| 4.1.1 | Ansatte hos Leverandør som jobber mot NAV eller har innsyn i tjenestene og dermed kjennskap til tjenesteleveransene skal kunne sikkerhetsklarereres på nivå HEMMELIG, jf. Sikkerhetsloven. §5-3 | A |  |  |
| 4.1.2 | Ansatte hos Leverandøren med inngående kjennskap til tjenesteleveransene skal undertegne Kundens taushetserklæring. | A |  |  |
| 4.1.3 | Alle tjenester som leveres skal være lokalisert innenfor EU/EØS. | A |  |  |

## 24/7 SOC tjenester (Security Operations Centre)

### Krav til tjenester for sikkerhetsovervåking, hendelseshåndtering og varsling 24/7.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal ha en organisasjon og et sikkerhetsovervåkingssenter som leverer tilbudte tjenester samt drift/vedlikehold av eventuelt kundeplassert utstyr og programvare 24 timer i døgnet, 365 dager i året. | A |  |  |
|  | Dialogen med sikkerhetsovervåkningssenteret, både skriftlig og muntlig, skal hovedsakelig foregå på norsk så sant dette er praktisk mulig | A |  |  |
|  | Leverandøren skal sørge for kontinuerlige trussel vurderinger rettet mot det norske markedet.  Beskriv hvordan leverandøren holder seg oppdatert på den norske trusselsituasjonen. | A |  | X |
|  | Leverandørens primære SOC skal ligge i Norge. | A |  |  |
|  | Leverandørens SOC skal være redundant, backup SOC kan være etablert i Norden. | A |  |  |
|  | Leverandørens SOC tjenester skal lagre data i Norden | A |  |  |

### Krav til tjenester for hendelsesrapportering.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandør skal levere periodiske hendelsesrapporter. Rapportene skal som minimum utarbeides pr mnd, kvartalsvis og år. | A |  |  |

### Krav til loggovervåkingstjenester (IaaS, PaaS, SaaS, on-premise, multicloud)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal levere tjeneste for overvåkning av logger i kundens IaaS, PaaS, SaaS og On-premise - miljø | A |  |  |

## Operational services (en del av SOC)

### Krav til IPS/IDS tjenester

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal levere IPS eller tilsvarende tjeneste. | A |  |  |
|  | |  | | --- | | Leverandøren skal levere IDS eller tilsvarende tjeneste. | | A |  |  |

### Krav til SIEM tjeneste

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal levere en SIEM tjeneste | A |  |  |

### Krav til Endpoint Detection and Response (EDR)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal levere en EDR tjeneste | A |  |  |

### Krav til Email security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal levere tjeneste for å sikre kundens e-postsystem | A |  |  |

### Krav til Cloud access security broker (CASB)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandør skal levere en CASB tjeneste | A |  |  |

### 

### Krav til Web application firewall (WAF)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal levere en WAF tjeneste | A |  |  |

### Krav til Continuous Vulnerability Monitoring (Sårbarhetsanalyse)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal levere en tjeneste for Continuous Vulnerability Monitoring | A |  |  |

## Incident Response Team (IRT)

### Krav til konsulentbistand og beredskap i forbindelse med håndtering og analyse av sikkerhetshendelser (Incident Response Team – IRT).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal tilby en incident response tjeneste (IRT) | A |  | X |

## Kompetanse til innføring av nye tjenester

### Krav til konsulentbistand ved innføring av nye eller endring av eksisterende sikkerhetsovervåkingssystemer, samt generell rådgivning innenfor avtaleområdet.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet  (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Leverandøren skal tilby konsulenttjenester innenfor avtaleområdet. | A |  |  |

## 

## Krav til forretningsmessig satsningsområde innen sikkerhetsovervåkning

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Krav | Prioritet (A/V) | Svar  (J/N) | Utfyllende  kommentar |
|  | Gi en kort beskrivelse av Leverandørens nåværende posisjon i markedet innenfor området som omfattes av avtalen. | V |  | X |
|  | Beskriv kort hvilke planer Leverandøren har for å videreutvikle tjenestene i tråd med utviklingen i markedet. | V |  | X |
|  | Beskriv kort hvilke kompetansehevende tiltak Leverandøren har for ansatte. | V |  | X |