NSMs kvalitetsordning

Hendelseshåndtering

Versjon 1.1

Gyldig fra og med 15. februar 2019

OM DOKUMENTET

Dokumentet gir bestemmelser for NSMs kvalitetsordning for bruk av tredjepart innen hendelseshåndtering.

Dokumentet er fem-delt:

1. Formålet med ordningen
2. Informasjon om søknadsprosess
3. Vilkår for deltakelse i ordningen
4. Søknadsskjema
5. Vedlegg

Innhold

Ved å fremsende søknad om å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering aksepterer søknadsstiller samtidig ordningens vilkår.

1 FORMÅLET MED ORDNINGEN

Formålet med ordningen er at virksomheter som opplever en IKT-sikkerhetshendelse skal kunne velge en leverandør av hendelseshåndteringstjenester der NSM har vurdert at leverandøren tilfredsstiller de kvalitetskrav som NSM har definert til tjenesten.

For å være søknadsberettiget må søkeren således tilby hendelseshåndteringstjenester til det åpne markedet. Leverandører som kun tilbyr hendelseshåndteringstjenester til en avgrenset kundekrets, herunder bare leverer tjenesten til virksomheter som også kjøper andre tjenester av leverandøren, faller utenfor ordningen og er ikke søknadsberettiget.

2 INFORMASJON OM SØKNADSPROSESS

2.1 Definisjoner

2.1.1 Godkjennelse/godkjent

Med bruk av ordene «godkjennelse» eller «godkjent» i dette dokumentet menes at en bedrifts/organisasjons søknad, med underliggende dokumentasjon, ved søknadstidspunktet tilfredsstiller NSMs krav til medlemskap i kvalitetsordningen for hendelseshåndtering.

2.1.2 Hendelseshåndtering (HH)

I denne ordningen defineres omfanget av HH som følgende:

HH er en prosess for å identifisere og respondere på en IKT-sikkerhetshendelse. En IKT-sikkerhetshendelse har oppstått om en aktør har eller har hatt uønsket tilgang til ett eller flere informasjonssystemer – eller det er mistanke om at noen har skaffet seg en slik uønsket tilgang - med den intensjon å skaffe tilgang på sensitiv informasjon, eller å ødelegge, skade eller endre informasjon på systemene mtp. konfidensialitet, autentisitet, integritet og/eller tilgjengelighet. HH-prosessen er en kvalitetsprosess som blant annet inneholder tiltak for å:

1. Identifisere og klassifisere hva som har skjedd, uønsket aktør og/eller skadevare, angrepsvektor og verktøy samt aktørens modus operandi
2. Kartlegge hvordan tilgangen er skaffet til veie, og omfang av aktørens eller skadevarens aktiviteter på informasjonssystemene
3. Begrense og ev. hindre videre uønsket aktivitet på systemet, samt registrere hvorledes dette utføres
4. Sikre elektroniske bevis
5. Gjenopprette normaltilstand ved informasjonssystemet
6. Utarbeide læringspunkter og anbefalte tiltak til oppdragsgiver for å øke sikkerheten
7. Rapportere omfanget av ovenstående til oppdragsgiver

2.2 Søknadsprosess

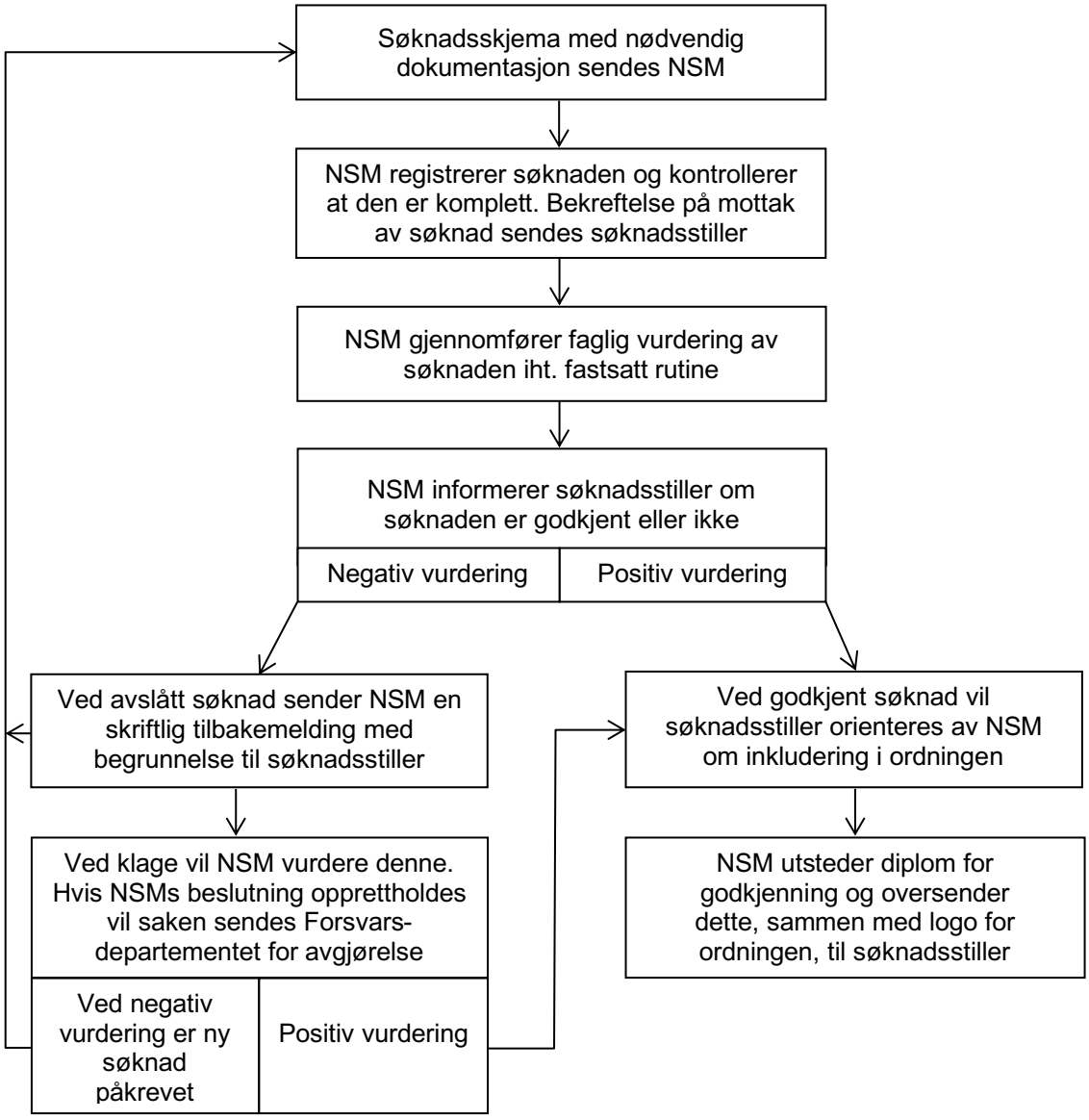
Bedrifter/organisasjoner som ønsker å søke om å bli godkjent iht. NSMs kvalitetsordning for hendelseshåndtering skal fylle ut søknadsskjemaet og sende dette til NSM. Skjemaet kan sendes som brevpost eller som e-post til følgende adresse:

Nasjonal sikkerhetsmyndighet
Postboks 814
1306 Sandvika
E-post: post@nsm.stat.no

NSM vil bekrefte mottak av søknad. NSMs evalueringsprosess er estimert å ta normalt åtte uker. NSM tar forbehold om at noe utvidet saksbehandlingstid kan forekomme. Ved godkjent søknad vil søknadsstiller bli informert om dette pr. brevpost.

En søknadsstiller som ikke får godkjent sin søknad vil bli orientert om dette pr. brevpost. NSM vil gi søknadsstiller en begrunnelse hvorfor søknaden ble avslått.

Visuell fremstilling av hovedpunkter i søknadsprosessen:



Ved å fremsende søknad om å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering aksepterer søknadsstiller samtidig ordningens vilkår.

NSMs godkjennelse er normalt gyldig i ett år. Tidspunkt for godkjennelse vil være angitt i NSMs svarbrev.

Regodkjenning gjennomføres årlig. Søknad om regodkjenning må være NSM i hende 8-12 uker før utløp av eksisterende godkjennelsesperiode. NSM vil basere en regodkjenning på:

a) Søknadsskjema område 5 og 6 med beskrivelse av oppdrag siden forrige søknad.
b) Ev. endringer fra opprinnelig søknad.

Søkere som fremsender søknad iht. alternativ b) i pkt. 3.2.1 bes merke seg dokumentasjonskrav som angitt i merknad 7 ved første gangs regodkjenning.

2.3 Klageprosess

Klager fra søker på avgjørelser fattet av NSM følger normal klagebehandling iht. lov om behandling i forvaltningssaker (forvaltningsloven).

2.4 Formelle søknadskrav

a) Søknaden skal skrives på norsk. Eksempel på sluttrapport i område 6 kan være skrevet på engelsk.
b) Områdene i søknaden kan ha sidebegrensning. Sidebegrensningen skal følges av søknadsstiller. Informasjon fra søknadsstiller utover angitt sidebegrensning vil ikke bli tatt hensyn til i evalueringen av søknaden.
c) Søknaden skal fremsendes pr. brevpost eller e-post som angitt på side 2.
d) Søknader som fremsendes pr. brevpost skal være utformet på følgende måte:
    1. Det skal fremsendes tre kopier av søknaden
    2. Søknaden fremsendes i dobbel konvolutt. Det skal ikke fremgå av ytterste konvolutt hva forsendelsen inneholder
    3. Kopiene skal ha to-sidig utskrift i A4-størrelse
    4. Skrifttype Arial, font-størrelse minimum 11, linjeskift 1,5
e) Søknader som fremsendes pr. e-post skal være utformet på følgende måte:
    1. Som pkt. 1.4.d) 4.
    2. Søknaden skal være konvertert til ikke-redigerbar PDF-fil
    3. Ved bruk av kryptering skal NSM NorCERTs offentlige PGP-nøkkel benyttes

2.5 Søknads- og medlemsgebyr

Det er ikke gebyr for å søke om å bli godkjent iht. kvalitetsordningen for hendelseshåndtering. Det er heller ikke medlemsgebyr for de bedrifter/organisasjoner som blir godkjent.

MERKNAD 1:
NSM tar forbehold om at søknads- og/eller medlemsgebyr kan bli implementert.

2.6 Evaluering

Alle søknader vil bli evaluert av NSM. For å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering må søknadsstillere oppnå følgende poengsummer:

a) Oppnå en individuell poengsum på 3 eller bedre på hvert område: 1, 2, 3, 5, 7, 8 og 9.
b) Oppnå en individuell poengsum på 5 på område 4 og 6.

MERKNAD 2:
Både 1.6. a) og 1.6. b) må være oppfylt for å få en søknad godkjent.

Hvert område vil bli bedømt iht. skjema i punktene 4.1 og 4.2.

2.7 Informasjonshåndtering

Informasjon som NSM mottar vil bli håndtert iht. lov om rett til innsyn i dokument i offentleg verksemd (offentleglova) § 13 og lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) § 13.

2.8 Revisjon av ordningen

Kvalitetsordningen innen hendelseshåndtering vil være gjenstand for revisjon av NSM for å vurdere ordningens faglige innhold og måloppnåelse. NSM tar forbehold om at ordningen vil kunne bli endret eller terminert.

3 VILKÅR FOR DELTAKELSE

Ved å fremsende søknad om å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering plikter søknadsstiller samtidig å følge nedenstående vilkår:

1. Aktiviteter opp mot kunder, og resultater av disse aktivitetene, som en godkjent bedrift/organisasjon utfører, er bedriftens/organisasjonens eget ansvar. NSM fraskriver seg ethvert ansvar for resultatet av det oppdraget som utføres.
2. Søknadsstillers utgifter dekkes i sin helhet av søknadsstilleren selv.
3. Søkers adgang til å gjøre seg kjent med sakens dokumenter vil være regulert av forvaltningsloven.
4. Søkeres rettigheter og plikter ved markedsføring *etter* å ha blitt godkjent:
    a) Logo utarbeidet av NSM for kvalitetsordningen innen hendelseshåndtering kan benyttes i markedsføringsøyemed. Kun logo utarbeidet av NSM skal benyttes til dette formålet.
    b) Følgende setning skal benytte ved muntlig/skriftlig markedsføring av å være godkjent: «X tilfredsstiller kravene iht. NSMs kvalitetsordning for hendelseshåndtering.» (X vil erstattes av godkjent søkers firmanavn).
    c) Hvis godkjennelsen omtales på bedriftens/organisasjonens hjemmeside skal det på en klar og entydig måte være en klikkbar link til NSMs hjemmeside om ordningen.
5. NSMs rettigheter og plikter:
    a) NSM vil inkludere godkjente bedrifter på en liste på NSMs hjemmeside over godkjente leverandører av hendelseshåndteringstjenester. NSM vil vise til denne listen ved forespørsler om støtte til hendelseshåndtering.
    b) NSM har som intensjon å invitere godkjente tjenesteleverandører til frivillig deltakelse i et samarbeidsforum med regelmessig møtefrekvens (halvårlig).
    c) Ordningen vil være gjenstand for årlig revisjon av NSM. Ved ev. justeringer vil godkjente leverandører få en hensiktsmessig frist til å møte endringene.
6. Godkjent bedrift/organisasjon og NSM har gjensidig informasjonsplikt overfor hverandre dersom en kunde klager på kvaliteten ved den tjenesten som leveres.
    a) Hvis klagen mottas av godkjent tjenesteleverandør skal NSM informeres om dette. Tjenesteleverandøren skal beskrive forholdet, samt ev. forslag til tiltak.
    b) Hvis NSM mottar klagen vil tjenesteleverandøren bli informert om forholdet.
    c) I begge tilfeller vil NSM kunne gå i dialog med tjenesteleverandøren for ev. videre behandling og avklaring. NSM vil vurdere ev. konsekvenser og behov for tiltak.

Ved å fremsende søknad om å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering aksepterer søknadsstiller samtidig ordningens vilkår.

7. Tjenesteleverandøren plikter å informere NSM umiddelbart om forhold som vil kunne påvirke godkjennelsen i tidsperioden denne gjelder. I dette inngår vesentlig endringer i de forhold som er lagt til grunn for NSMs godkjennelse, samt f. eks. eierskifte, personellendringer, ny forretningsstrategi, kompromittering av egne systemer etc.
8. Personelliste med rolletilhørighet og relevante kvalifikasjoner iht. søknadsskjema område 4 skal til enhver tid holdes oppdatert av bedriften/organisasjonen. Prosedyre for dette fastsettes av NSM.
9. NSM kan utføre inspeksjon av bedriften/organisasjon rettet mot forhold relevant for godkjennelsen. Ved mangelfulle forhold vil NSM sette en frist for å avklare og ev. utbedre disse.
10. NSM kan sette en frist for å avklare ev. uklare forhold ved en søknad. Svarfrist vil normalt settes til tre uker.
11. Rapportering:
    a) Aggregert rapport over gjennomførte oppdrag skal sendes NSM minimum halvårlig. Mal for rapport er angitt i pkt. 4.3.
    b) NSM anmoder om at godkjente søkere fremsender kopi av sluttrapporter til NSM etter hvert oppdrag. Disse rapportene kan om nødvendig anonymiseres. Slik rapportering vil øke NSMs situasjonsforståelse og gjennom dette bidra til økt nasjonal samfunnssikkerhet. Fremsendelse av rapporter vil videre gjøre det lettere for NSM å kunne forbedre ordningen og ev. støtte godkjente søkere.

    MERKNAD 3:
    Ved fremsendelse av rapport etter hvert oppdrag bortfaller kravet om aggregert rapportering.

12. Manglende oppfyllelse av ett eller flere av ovennevnte vilkår vil kunne føre til at NSM trekker godkjennelsen tilbake.

4 SØKNADSSKJEMA

MERKNAD 4:
NSM vil behandle all mottatt informasjon ifm. søknaden med konfidensialitet. Informasjon om/fra den enkelte søker, med unntak av nødvendig kontaktinformasjon, vil kun være tilgjengelig for ordningens saksbehandlere. Ved særskilt ønske om beskyttelse av sensitiv informasjon kan NSM kontaktes.

4.1 Informasjon om bedrift/organisasjon

4.1.1 Generelt

Navn:	
Organisasjonsnummer:	
Postadresse:	
Besøksadresse:	
Eventuelle bedriftssertifiseringer:	
Regnskap siste år er vedlagt:	(Ja/nei)

4.1.2 Kontaktperson

Oppgi navn på kontaktpersoner i bedriften/organisasjonen som NSM ved behov kan kontakte vedrørende søknaden:

	Hovedkontakt	Alternativ kontakt
Navn:		
Stilling:		
Postadresse (hvis annen adresse enn oppgitt i pkt. 3.1.1):		
Telefonnummer (kontor):		
Telefonnummer (mobil):		
E-post adresse:		

Ved å fremsende søknad om å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering aksepterer søknadsstiller samtidig ordningens vilkår.

4.1.3 Markedsføring

Oppgi kontaktinformasjon og logo til bruk på NSMs hjemmesider:

Bedriftsnavn som skal vises:	
Web-url for hendelseshåndtering:	
Telefonnummer for kontakt:	
E-post-adresse for kontakt:	
Logo vedlagt:	(Ja/nei)

Ved å fremsende søknad om å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering aksepterer søknadsstiller samtidig ordningens vilkår.

4.2 Krav

MERKNAD 5:
Dokumentasjon er påkrevet.

4.2.1 Område 1: Referanser

4.2.1.1 Formål

Dokumentere praktisk erfaring innen hendelseshåndtering (offentlig/privat sektor, internasjonale organisasjoner, ev. andre relevante kunder/oppdrag).

4.2.1.2 Bakgrunn

Punktet skal i så stor grad som mulig underbygge at søkeren har erfaring fra hendelseshåndteringsoppdrag og leverer tjenester som NSM vurderer å ha tilfredsstillende kvalitet på fagområdet. Punktet skal videre underbygge at søkeren er bevisst på kundens situasjon og miljø, og at søknadsstiller møter kundens behov.

4.2.1.3 Krav

Søknadsstiller skal fremlegge dokumentasjon på utførte oppdrag innen hendelseshåndtering. Søker kan velge å gjøre dette på én av to måter:

Alternativ a)

Søker skal som en hovedregel beskrive minimum tre, maksimalt fem hendelseshåndteringer som søkeren har gjennomført siste to år. I dokumentasjonen skal følgende inngå:

a) Navn på bedrift/organisasjon som ble støttet
b) Oppdragets tidspunkt og varighet
c) Kort beskrivelse av den tjenesten som ble levert
d) Fremgangsmåte som ble benyttet
e) Problemer som dukket opp under oppdragsløsningen, samt hvordan disse ev. ble løst
f) Kontaktperson i virksomheten som mottok tjenesten. Denne personen vil kunne bli kontaktet av NSM som en referanse for kvaliteten ved det utførte oppdraget.

Alternativ b)

Alternativt må søkeren dokumentere at alt personell som har en rolle i søkerens HH-organisasjon har relevant kompetanse fra praktisk utført arbeid innen hendelseshåndtering i sin rolle gjennomført de siste to år. Søkeren må dokumentere tre gjennomførte hendelseshåndteringer pr. aktuell rolle og person, samt kvaliteten ved disse hendelseshåndteringene. I dokumentasjonen skal følgende inngå:

a) Navn på bedrift/organisasjon som ble støttet
b) Oppdragets tidspunkt og varighet
c) Kort beskrivelse av den tjenesten som ble levert
d) Fremgangsmåte som ble benyttet
e) Problemer som dukket opp under oppdragsløsningen, samt hvordan disse ev. ble løst
f) Kontaktperson i virksomheten som mottok tjenesten. Denne personen vil kunne bli kontaktet av NSM som en referanse for kvaliteten ved det utførte oppdraget.

NSM gjør oppmerksom på at for søkere som benytter alternativ b), gjelder fremdeles krav iht. område 5 og 6 for søkers egen HH-organisasjon.

Sidebegrensning: For begge alternativ skal hver beskrivelse av en hendelseshåndtering være på maksimalt én A4-side.

MERKNAD 6:
NSM ber om at ev. erfaring fra hendelseshåndteringsoppdrag i Norge beskrives spesielt.

MERKNAD 7:
Søkere som fremsender søknad iht. alternativ b) skal ved første gangs regodkjenning fremsende dokumentasjon iht. alternativ a).

4.2.2 Område 2: Cyber-trusseletterretning

4.2.2.1 Formål

Dokumentere innsikt i og forståelse for eksisterende og potensielle cyber-trusler og -teknikker, spesielt de som blir benyttet av relevante[A] trusselaktører.

4.2.2.2 Bakgrunn

Punktet skal i så stor grad som mulig underbygge at søkeren kan demonstrere en klar forståelse for den teknikk, kapasitet og infrastruktur som aktuelle trusselaktører besitter i operasjoner mot norske virksomheter og/eller interesser. Søker skal også ha rutiner for å forsikre seg om at denne forståelsen kontinuerlig utvikles og forbedres.

4.2.2.3 Krav

Søknadsstiller skal fremlegge dokumentasjon på hvorledes søker regelmessig følger aktuelle trusselaktørers utvikling, samt de operasjoner som aktørene gjennomfører.

For å oppnå minimum poengsum på området må søknadsstiller dokumentere kunnskap om kapasiteter, teknikker og infrastrukturer som relevante trusselaktører benytter.

> MERKNAD 8:
>
> NSM vil kunne ta kontakt med søknadsstiller for å få en nærmere innsikt i søkers kunnskap om dette området.

Sidebegrensning: Beskrivelsen på området skal være på maksimalt fire A4-sider.

[A] Hva som regnes som relevante trusselaktører vil være avhengig av søkers kundemålgruppe eller fokusområde.

4.2.3 Område 3: Verktøy

4.2.3.1 Formål

Dokumentere evne til å utvikle, tilpasse og bruke verktøy og teknikker som en del av etterforskning av digitale operasjoner.

4.2.3.2 Bakgrunn

Punktet skal gi NSM en forståelse for i hvilken grad søkeren innehar intern bedriftskompetanse innen bruk av verktøy, og kompetanse til å tilpasse og ev. utvikle disse.

4.2.3.3 Krav

Søknadsstiller skal dokumentere hensiktsmessige applikasjoner som søker benytter innen hendelseshåndtering. Dette kan være:

a) Egenutviklede programmer
b) Kommersiell programvare
c) Åpen kildekode-programvare
d) Åpen kildekode/kommersiell programvare som er videreutviklet/forbedret av bedriften/organisasjonen

Verktøyene kan være innen ulike kategorier av hendelseshåndtering, f. eks:

- Digital etterforskning (forensics)
- Data-/bevisinnhenting
- Dynamisk/statisk analyse
- Nettverksanalyse
- Administrativt

Sidebegrensning: Beskrivelsen på området skal være på maksimalt to A4-sider.

4.2.4 Område 4: Prosess

4.2.4.1 Formål

Dokumentere en hensiktsmessig, repeterbar og effektiv hendelseshåndteringprosess.

MERKNAD 9:
Dette punktet krever poengsum 5 for å være bestått.

4.2.4.2 Bakgrunn

Punktet skal vise at søkeren har en dokumentert kvalitetsprosess for hendelseshåndtering.

4.2.4.3 Krav

Søknadsstiller skal dokumentere en grundig metodikk for å gjennomføre en hendelseshåndteringsprosess. NSM vil bl. a. se etter:

a) Beredskap og plan for håndtering
b) Beskrivelse av hendelseshåndteringsorganisasjonen, herunder fordeling av roller og ansvar, med faglige krav til respektive funksjoner
c) Identifisering av skadetype og omfang
d) Sikring og verifisering av beviskjeden
e) Notoritet og logging av aktivitet
f) Koordinering av aktiviteter for nødvendige mottiltak og gjenoppretting av normaltilstand
g) Rapportering
h) Evaluering og læringspunkter

Personelliste med rolletilhørighet og relevante kvalifikasjoner rapporteres til NSM som beskrevet på ordningens hjemmeside. NSM vil be om følgende opplysninger:

- Fullt navn
- Fødselsdato
- Telefonnummer kontor/telefonnummer mobil
- Tid ansatt i bedriften/organisasjonen (år)
- Rolle i bedriftens/organisasjonens hendelseshåndteringsorganisasjon
- Relevant kompetanse
- Eventuelle relevante sertifiseringer
- Språkkunnskaper (skriftlig/muntlig)

Sidebegrensning: Beskrivelsen på området skal være på maksimalt fem A4-sider. Flytdiagrammer kan legges ved i tillegg. Personelliste rapporteres separat.

4.2.5 Område 5: Beskrivelse av utført oppdrag

4.2.5.1 Formål

Beskrive en tidligere gjennomført hendelseshåndtering inkludert relevante tilhørende aktiviteter.

4.2.5.2 Bakgrunn

Basert på metodikken som søknadsstiller beskrev i område 4, skal denne beskrivelsen vise hvordan søkeren har gjennomført en komplett hendelseshåndteringsprosess. Dette omfatter tidsrommet fra søknadsstilleren første gang ble varslet, til oppdraget ble ferdigstilt og rapport utarbeidet.

4.2.5.3 Krav

Søknadsstiller skal gi en konsis oppsummering av ett tidligere oppdrag der et angrep er håndtert. Beskrivelsen skal dekke hele operasjonens forløp. Overskrifter/emner som NSM bl. a. vil se etter:

a) Navn på virksomhet (eller beskrivelse av denne hvis virksomheten må anonymiseres)
b) Hvordan initiell kontakt med virksomheten ble etablert og oppdraget ble registrert, definert og formulert
c) Analyse av situasjon og foreliggende informasjon, og hvordan forståelsen av dette ble benyttet under selve hendelseshåndteringen
d) Steg i etterforskningsprosessen og beskrivelse av verktøybruk
e) Eventuelle operative begrensninger pga. virksomhetens/informasjonssystemets art, samt tiltak iverksatt for å kompensere for dette
f) Teknisk analyse av skadevare og angrepsvektor
g) Kartlegging av omfang av eventuelle kompromitterte/eksfiltrerte data
h) Kartlegging og vurdering av aktørens fremgangsmåte, tekniske kapasitet og infrastruktur som ble benyttet i operasjonen, samt hvorledes denne informasjonen ble benyttet for å videreutvikle/oppdatere søkerens interne trusselforståelse
i) Tilbakemeldinger og rapportering til oppdragsgiver, inkludert skadeomfang og hvordan kunnskapen fra håndteringen er brukt for å sikre oppdragsgiver bedre i ettertid

MERKNAD 10:
For å tilfredsstille minimumskravet på området skal søknadsstiller på en klar måte vise bruk av hensiktsmessige analysemetoder og beskrevne prosesser. Søker skal redegjøre for valg av verktøy i hendelseshåndteringsprosessen.

Sidebegrensning: Beskrivelsen på området skal være på maksimalt fem A4-sider inkludert ev. diagrammer/flytskjema.

4.2.6 Område 6: Eksempel på sluttrapport

4.2.6.1 Formål

Dokumentere klar og konsis rapportering til både teknisk og ikke-teknisk personell etter en hendelseshåndtering.

MERKNAD 11:
- Dette punktet krever poengsum 5 for å være bestått
- Eksempel på rapport kan være skrevet på engelsk
- Omtalt virksomhet i rapporten kan om nødvendig anonymiseres

4.2.6.2 Bakgrunn

Dette punktet skal vise at søknadsstiller er i stand til å utarbeide klare og konsise rapporter til personell med ulik faglig bakgrunn i en virksomhet.

4.2.6.3 Krav

Søknadsstiller skal legge ved en kopi av en relevant rapport til en virksomhet etter en gjennomført hendelseshåndtering. NSM vil bl. a. se etter:

a) Om rapporten på en klar og konsis måte kommuniserer til personell med både teknisk og ikke-teknisk bakgrunn
b) Hvordan hendelsen kunne skje samt omfanget av denne
c) Nødvendige mottiltak/plan for å gjenopprette normaltilstand
d) Anbefalte tiltak til oppdragsgiver for å øke sikkerheten
e) Hvis relevant: resultatet av iverksatte mottiltak/plan for å gjenopprette normaltilstand

Sidebegrensning: Ikke definert.

4.2.7 Område 7: Egenbeskyttelse

4.2.7.1 Formål

Dokumentere evne til å beskytte sensitiv informasjon.

4.2.7.2 Bakgrunn

Dette punktet skal i så stor grad som mulig underbygge at søknadsstiller er i stand til å beskytte sensitiv informasjon som besittes og erverves. Det skal videre sikre at søker har gode og hensiktsmessige rutiner for å lagre/benytte skjermingsverdig informasjon, herunder bevissikring.

4.2.7.3 Krav

Søknadsstiller skal redegjøre for hvorledes sensitiv informasjon håndteres og beskyttes. I dette inngår spesielt informasjon som tilegnes ifm. kundeoppdrag. NSM vil bl. a. se etter følgende:

a) Hvordan digitale bevis og fysiske media håndteres og beskyttes, herunder relevante verktøy som benyttes
b) Intern sikkerhet, herunder:
    1. Sikkerhetsfaglig kompetanse
    2. Sikkerhetsorganisasjon
    3. Sikkerhetsrutiner
    4. Fasiliteter, herunder:
        i. Lokaler
        ii. Informasjonssystemer
        iii. Lagring/oppbevaring
        iv. Mulighet for sikker kommunikasjon
c) Relevante sertifiseringer av organisasjon og personell
d) Planer for å håndtere interne sikkerhetshendelser er øvet

Sidebegrensning: Beskrivelsen på området skal være på maksimalt tre A4-sider.

4.2.8 Område 8: Læringssløyfe

4.2.8.1 Formål

Dokumentere hvordan situasjonsforståelsen av cyber-trusler, teknikker og/eller verktøy brukes til å forbedre arbeidsmetodikk, samt beskyttelse av egne systemer og nettverk.

4.2.8.2 Bakgrunn

Dette punktet skal vise at søknadsstiller har etablerte rutiner for kontinuerlig oppdatering av risikovurdering, sikkerhetsrutiner, prosesser og verktøy. Dette skal gjøre at søkerens operative aktiviteter har redusert sannsynlighet for kompromittering.

4.2.8.3 Krav

For å møte minimumskravet må søknadsstiller kunne dokumentere hvordan bedriftens/organisasjonens cyber-trusselvurdering medvirker til en grundig arbeidsmetodikk, samt hvordan verktøy og teknikker brukes for å forhindre kompromittering av informasjon i egen organisasjon.

Sidebegrensning: Beskrivelsen på området skal være på maksimalt én A4-side.

4.2.9 Område 9: Robusthet

4.2.9.1 Formål

Dokumentere evnen til å opprettholde operasjoner, forretningsvirksomhet og operative informasjonssystemer over tid.

4.2.9.2 Bakgrunn

Dette punktet skal i så stor grad som mulig underbygge at søknadsstiller kan:

a) Støtte en virksomhet kontinuerlig over tid
b) Begrense sannsynligheten for at negativ publisitet rammer samarbeidende parter
c) Opprettholde konfidensialitet og tilgjengelighet
d) Utføre effektiv håndtering av media og er bevisst på konsekvensen av publisering av informasjon

4.2.9.3 Krav

For å møte minimumskravet skal søknadsstiller dokumentere at det foreligger planer som bidrar til å opprettholde operasjoner, forretningsvirksomhet og operative informasjonssystemer over tid. NSM vil spesielt se etter en robust organisering, tydelige roller og ansvarsfordeling, samt planer og kapasitet til mediehåndtering.

Sidebegrensning: Beskrivelsen på området skal være på maksimalt én A4-side.

5 VEDLEGG

5.1 Poengbeskrivelse

Under evalueringen av en søknad vil alle områdene tildeles en poengsum fra 0-5. Tabellen under indikerer forventet nivå for hver poengsum.

Poengsum	Beskrivelse
5	**Særdeles tilfredsstillende** Søknadsstiller dokumenterer i betydelig grad større forståelse, evne, erfaring, teknisk kompetanse, ressurser, ekspertise, innovasjon, ledelse og tjenesteleveranse enn det som er å anse som tilfredsstillende.
4	**Meget tilfredsstillende** Søknadsstiller dokumenterer større forståelse, evne, erfaring, teknisk kompetanse, ressurser, ekspertise, innovasjon, ledelse og tjenesteleveranse enn det som er å anse som tilfredsstillende.
3	**Tilfredsstillende** Søknadsstiller dokumenterer relevant forståelse, evne, erfaring, teknisk kompetanse, ressurser, ekspertise, innovasjon, ledelse og tjenesteleveranse for å møte relevante krav.
2	**Nokså tilfredsstillende** Søknadsstiller opererer på et grunnleggende nivå. Dokumentert effektiv metodikk og hensiktsmessige verktøy mot cyber-trusler er ikke tilstrekkelig for å møte relevante krav.
1	**Lite tilfredsstillende** Det mangler informasjon for å dokumentere at søknadsstilleren tilfredsstiller kravet, eller har metodikk og kapasitet til å levere tjenesten.
0	**Ikke tilfredsstillende** Dokumentasjon er fraværende.

5.2 Oppsummering av krav til poengsum

Område	Krav
1. Referanser.	3
2. Cyber-trusseletterretning.	3
3. Verktøy.	3
4. Prosess.	5
5. Beskrivelse av utført oppdrag.	3
6. Eksempel på sluttrapport.	5
7. Egenbeskyttelse.	3
8. Læringssløyfe.	3
9. Robusthet.	3

5.3 Mal rapporteringsskjema på aggregert nivå

Aggregerte rapporter defineres utfra punktene under. Aggregert rapport skal bruke engelsk språk. Foreløpig har vi ingen formelle krav til formatet på rapporteringen, men setter pris på om rapporteringen kommer i rent tekstformat. Aggregert rapport vil være gjenstand for revisjon, og vi vil jobbe for å få til en mer automatisert innrapportering, trolig basert på STIX/TAXII.

Følgende felter skal rapporteres per hendelse:

5.3.1 Tidslinje

Her ønskes tidspunkt for flest mulig av feltene som er definert under. Som et minimum må startdato og sluttdato for hendelseshåndteringen, samt første fiendtlige observasjon og eventuell dato for kompromittering være angitt (Incident_Opened, Incident_Closed, First_Malicius_Action og Initial_Compromise). Tidspunkt angis ihht NS-ISO 8601 (dvs YYYY-MM-DD eventuelt YYYY-MM-DD hh:mm:ss+hh). Det er ønskelig at eventuelle klokkeslett angis med tidssone (eksempelvis +01 for norsk vintertid og +02 for norsk sommertid).

Mulige felter her er:

First_Malicious_Action	The First_Malicious_Action field specifies the time that the first malicious action related to this Incident occured.
Initial_Compromise	The Initial_Compromise field specifies the time that the initial compromise occured for this Incident.
First_Data_Exfiltration	The First_Data_Exfiltration field specifies the first time at which non-public data was taken from the victim environment
Incident_Discovery	The Incident_Discovery field specifies the first time at which the organization learned the incident had occurred.
Incident_Opened	The Incident_Opened field specifies the time at which the Incident was officially opened.
Containment_Achieved	The Containment_Achieved field specifies the first time at which the incident is contained (e.g., the “bleeding is stopped”).
Restoration_Achieved	The Restoration_Achieved field specifies the first time at which the incident's assets are restored (e.g., fully functional)”.
Incident_Reported	The Incident_Reported field specifies the time at which the Incident was reported.
Incident_Closed	The Incident_Closed field specifies the time at which the Incident was officially closed.

5.3.2 Målsektor

Hvilken sektor tilhører virksomheten hvor hendelseshåndteringsoppdraget ble utført.

Mulige verdier listet i tabellen under.

Target sector	Overordnet department
Finance	Finansdepartementet
Defence	Forsvarsdepartementet
Government	Generelt offentlig forvaltning (ev Komunal- og moderniseringsdepartementet)
Health and Care Sevices	Helse- og omsorgsdepartementet
Trade, Industry and Fisheries	Nærings- og fiskeridepartementet
Justice	Justis- og beredskapsdepartementet
Culture	Kulturdepartementet
Climate and Environment	Klima- og miljødepartementet
Petroleum and Energy	Olje- og energidepartementet
Space (Aerospace/Aviation)	Nærings- og fiskeridepartementet
Transport and Communications	Samferdselsdepartementet
Education	Kunnskapsdepartementet
Agriculture and Food	Landbruks- og matdepartementet

5.3.3 Klassifisering av hendelse

Klassifisering ihht taxonomi fra eCSIRT.net-prosjektet. ”Incident Class” er obligatorisk, ”Incident Type” er ønskelig.

Incident Class (obligatorisk)	Incident Type (valgfritt, men ønskelig)	Beskrivelse/eksempler
Abusive Content	Spam	Or ‘unsolicited bulk e-mail’, meaning that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having identical content
	Harassment	Discrediting or discriminating against somebody (ie, cyberstalking)
	Child/sexual/violence/...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Scanning	Attacks that send requests to a system to discover weak points. This also includes some kinds of testing

Information Gathering		processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, …).
	Sniffing	Observing and recording network traffic (wiretapping)
	Social engineering	Gathering information from a human being in a non-technical way (eg, lies, tricks, bribes, or threats)
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (eg, buffer overflow, backdoors, cross side scripting, etc).
	Login attempts	Multiple login attempts (guessing / cracking of passwords, brute force)
	New attack signature	An attempt using an unknown exploit
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by unauthorized local access.
	Unprivileged account compromise	
	Application compromise	
Availability	DoS	In this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYN- a. PING- flooding or e-mail bombing (DDoS: TFN, Trinity, etc.). However, availability can also be affected by local actions (destruction, disruption of power supply, etc).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (eg, the use of e-mail to participate in illegal profit chain letters or pyramid schemes)
	Copyright	Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez)
	Masquerade	Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

5.3.4 Innplassering i Cyber Kill Chain

Hvor i Cyber Kill Chain kjeden ble det kartlagt aktivitet. Her kan det være flere oppdaget aktivitet på flere nivåer, og mulige verdier er: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Action on Target.

5.3.5 Navn på trusselaktør

Hvis angrepet er attribuert ønsker vi navnet på trusselaktør. Her forventer vi navn som kan knyttes til åpne rapporter.

5.3.6 Verktøy

Eventuelle verktøy som ble oppdaget brukt under angrepet.

5.3.7 Indikatorer

Her ønsker vi alle identifiserte ”Indicators of Compromise” (IoC) og ”Indicators of Attack” med eventuell kontekst.

Indikatortyper kan være f.eks:

Malicious E-mail	Indicator describes suspected malicious e-mail (phishing, spear phishing, infected, etc.).
IP Watchlist	Indicator describes a set of suspected malicious IP addresses or IP blocks.
File Hash Watchlist	Indicator describes a set of hashes for suspected malicious files.
Domain Watchlist	Indicator describes a set of suspected malicious domains.
URL Watchlist	Indicator describes a set of suspected malicious URLS.
Malware Artifacts	Indicator describes the effects of suspected malware.
C2	Indicator describes suspected command and control activity or static indications.
Anonymization	Indicator describes suspected anonymization techniques (Proxy, TOR, VPN, etc.).
Exfiltration	Indicator describes suspected exfiltration techniques or behavior.
Host Characteristics	Indicator describes suspected malicious host characteristics.
Compromised PKI Certificate	Indicator describes a compromised PKI Certificate.
Login Name	Indicator describes a compromised Login Name.
IMEI Watchlist	Indicator describes a watchlist for IMEI (handset) identifiers.
IMSI Watchlist	Indicator describes a watchlist for IMSI (SIM card) identifiers.

5.3.8 Kontekst

Eventuell utfyllende kontekst.

Ved å fremsende søknad om å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering aksepterer søknadsstiller samtidig ordningens vilkår.

5.4 Eksempel på aggregert rapport

```
Incident 1


Incident_Opened=2016-03-22
Incident_Closed=2016-03-30
First_Malicious_Action=2016-01-16 08:32:22+01
Initial_Compromise=2016-01-16 08:55:41+01
Target_Sector=Government
Incident_Class=Intrusions
Incident_Type= Unprivileged account compromise
Cyber_Kill_Chain= Delivery, Exploitation, Installation, Command and
Control, Action on Target
Threat_Actor=sofacy
Tools=CORESHELL, AZZY


Indicator_Type=Malicious E-mail
Indicator_Value=from:andy@anom.com, subject:Meeting at conference
Indicator_Context=Subject and sender of the initial spearfishing
email


Incicator_Type=C2
Indictor_Value=10.0.0.1


Context=”Further description”
```