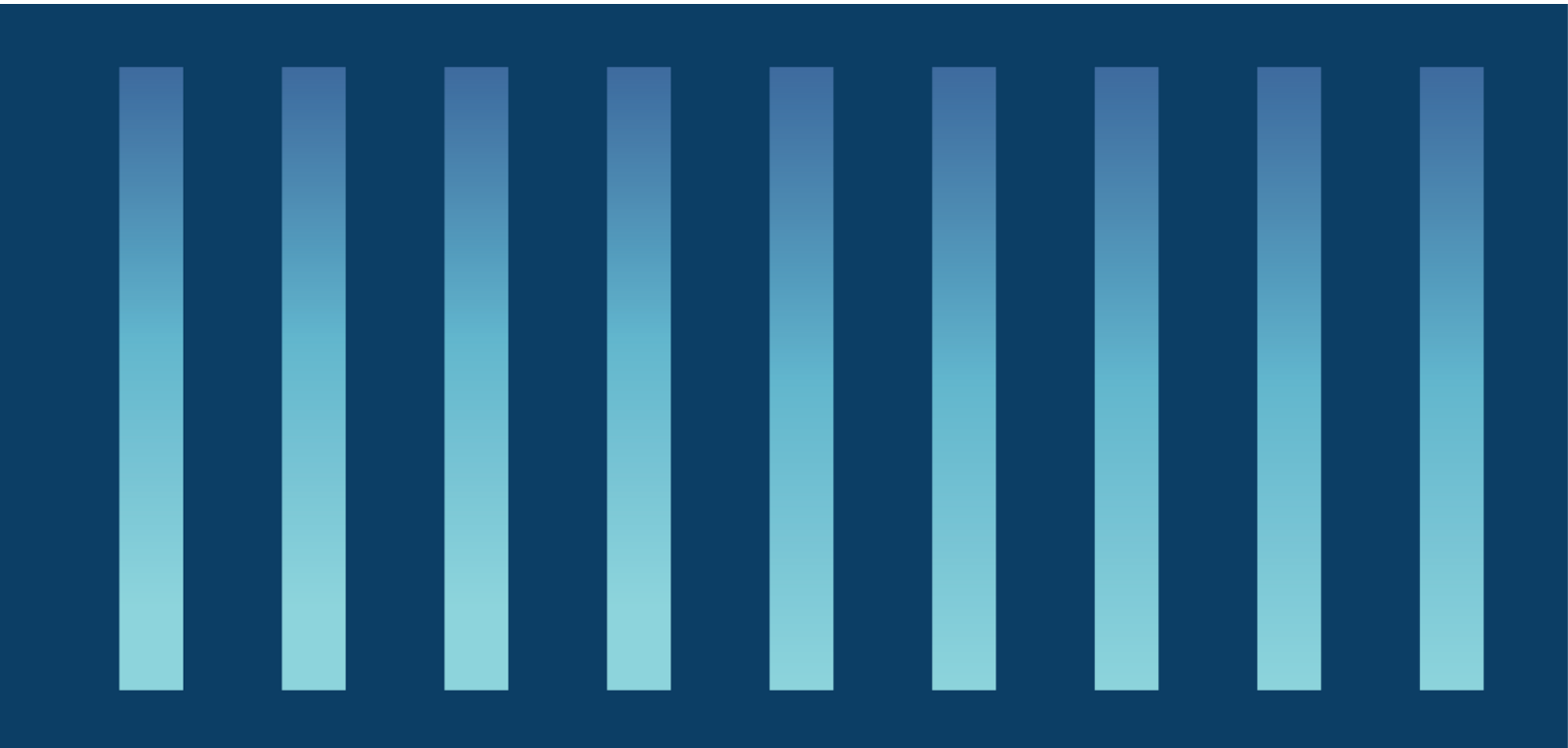
NASJONAL
SIKKERHETSMYNDIGHET

Søknads- og kravdokument

NSMs kvalitetsordning for Hendelseshåndtering

Gyldig fra og med 20. april 2023

Versjon: 2.0



Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). NSM skal gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid.

Sikkerhetsloven med tilhørende forskrifter trådte i kraft 1. januar 2019. Loven skal bidra til å forebygge, avdekke og motvirke tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

INNHOLD

Om dokumentet

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

Dokumenthistorikk

Dato publisert	Versjon	Beskrivelse
15. august 2016	1.0	Første versjon publisert.
20. desember 2018	1.1	Punkt 1 «Formålet med ordningen» tatt inn.
18. februar 2019	1.2	Rettet feil ved punktnummerering i versjon 1.1.
	2.0	Revidert versjon av versjon 1.2. Følgende endringer er gjort: • Ny mal. • Varigheten for en godkjenning er endret fra ett til to år. • Pkt. 4.1.3 «Operativt kontaktpunkt» er tatt inn. • Språklige presiseringer. • Departement ved klage er endret til Justis- og beredskapsdepartementet. • Karakterkrav 0-5 er erstattet av prosentvis poengsum i forbindelse med evaluering av søknaden. • Under område 1 «Referanser» er det presisert at det kun er mulig å benytte alternativ b) én gang som grunnlag for godkjent søknad. • Område 10 «Kompetanse og kompetanseutvikling» er tatt inn. • Mal for rapportering er tilpasset «Rammeverk for håndtering av IKT-hendelser» og bedre presisert. • Datoer for halvårlig rapportering er lagt til.
12. august 2019	2.0	• Endret betegnelse fra NSM NorCERT til Nasjonalt cybersikkerhetssenter (NCSS).
2. september 2019	2.0	• Endret betegnelse forkortelsen på Nasjonalt cybersikkerhetssenter fra NCSS til NCSC. • Endret e-post-adresse for NSM i pkt. 2.2 fra post@nsm.stat.no til postmottak@nsm.no.

14. januar 2020	2.0	Krav til referanser fra nye hendelser ved regodkjenning i pkt. 2.4.
29. januar 2020	2.0	Foreslåtte endringer fra Juridisk seksjon lagt inn.
20. april 2023	2.0	• Språklige presiseringer. • Pkt. 4.2.6.3 er tydeliggjort. • Oppdatert navn for enkelte departementer.

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 norske 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.

Ordningen er ment å kvalitetssikre søkerens kapasitet til å utføre hendelseshåndtering, og vurderer ikke dag-til-dag sikkerhetsovervåkning eller driftsoppgaver. Langtids Managed Security Service Provider- (MSSP) og Security Operation Centre-avtaler (SOC) faller for eksempel ikke inn under ordningen.

2. Informasjon om søknadsprosessen

2.1. Definisjoner

2.1.1. Godkjenning / godkjent

Med bruk av ordene «godkjenning» 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

I denne ordningen defineres omfanget av hendelseshåndtering som følgende:

Hendelseshåndtering 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. Hendelseshåndtering--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 eventuelt 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 til:

Nasjonal sikkerhetsmyndighet
Postboks 814
1306 Sandvika

Søknaden kan også oversendes NSM pr. e-post til **postmottak@nsm.no**. Dersom virksomheten av ulike årsaker ønsker å kryptere søknaden kan denne krypteres med Nasjonalt cybersikkerhetssenter (NCSC) sin offentlige PGP-nøkkel.

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 søker bli informert om dette pr. brevpost.

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

En søker som ikke får godkjent sin søknad kan tidligst fremsende ny søknad etter 6 måneder.

2.3. Godkjenningens varighet

NSMs godkjenning er normalt gyldig i to år. Tidspunkt for godkjenning vil være angitt i NSMs svarbrev.

2.4. Regodkjenning – prosedyre og omfang

Regodkjenning gjennomføres hvert annet år. Søknad om regodkjenning må være NSM i hende 8-12 uker før utløp av eksisterende godkjenningsperiode.

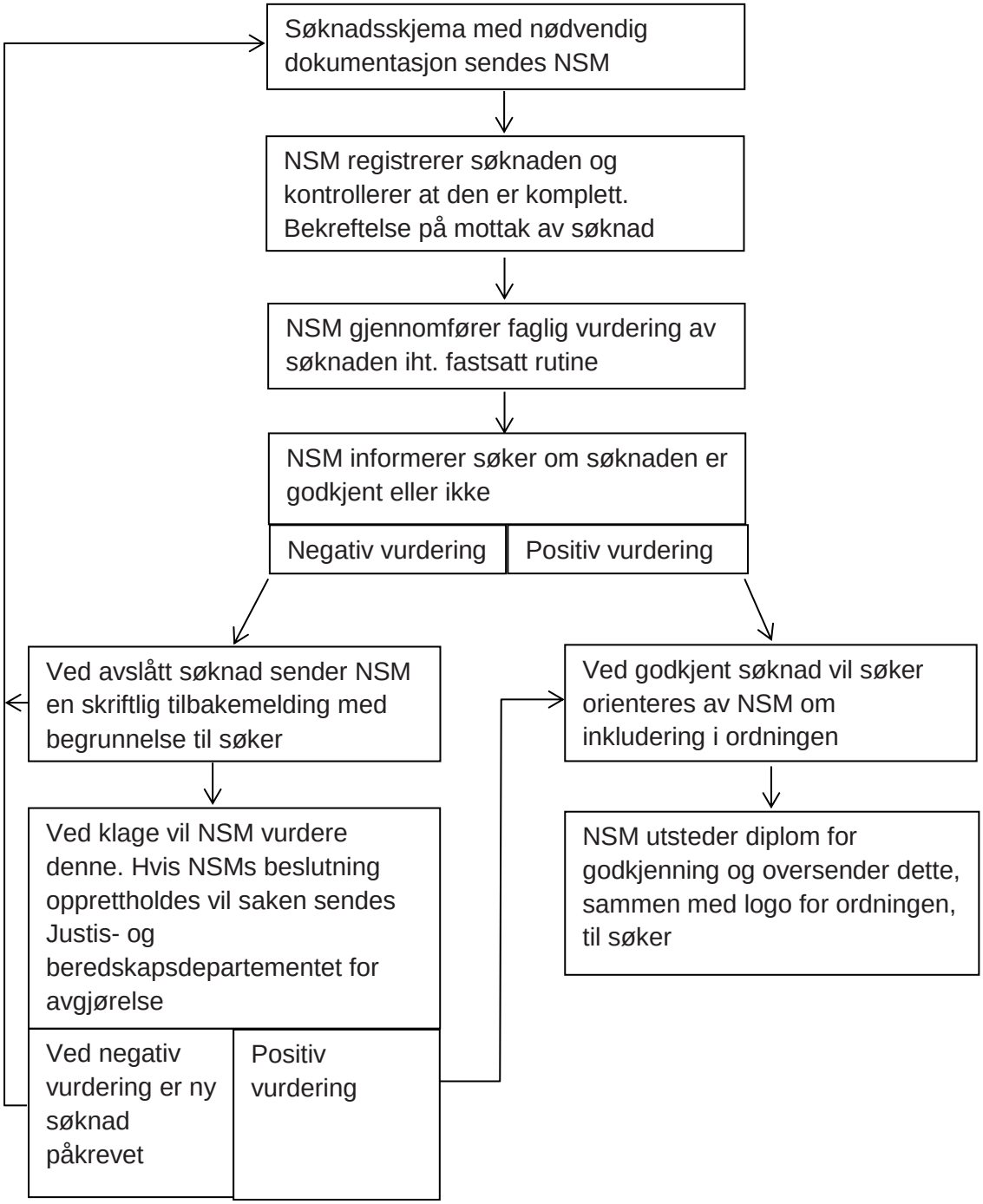
Hvis søker under forrige evalueringsrunde ble forespurt ytterligere informasjon skal søker ved regodkjenning sende ny fullstendig søknad der denne informasjonen er inkludert. Dersom dette ikke er tilfelle behøver søkeren kun sende følgende områder til NSM:

a) Søknadsskjema område 5 og 6 med beskrivelse av oppdrag utført i Norge siden forrige søknad.
b) Eventuelle endringer fra opprinnelig søknad.

c) Minst to referanser etter gjennomførte oppdrag siden forrige søknad.
d) Søkere som benyttet alternativ b) i område 1 ved opprinnelig søknad må sende dokumentasjon iht. alternativ a) i område 1 ved søknad om regodkjenning.

Manglende oppfyllelse av ovennevnte prosedyre og krav vil kunne føre til at NSM trekker godkjenningen tilbake.

Visuell fremstilling av søknadsprosessen:



2.5. Klageprosess

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

2.6. 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 søker. Informasjon fra søker utover angitt sidebegrensning vil ikke bli tatt hensyn til i evalueringen av søknaden.
c) Søknaden skal sendes pr. brevpost eller e-post som angitt under pkt. 2.2.
d) Søknader som sendes pr. brevpost skal være utformet på følgende måte:
    1. Det skal sendes tre kopier av søknaden.
    2. Søknaden sendes i dobbel konvolutt. Det skal ikke fremgå av ytterste konvolutt hva forsendelsen inneholder.
    3. Kopiene skal ha tosidig utskrift i A4-størrelse.
e) Skrifttype Arial, font-størrelse minimum 11, linjeskift 1,5. Søknader som sendes pr. e-post skal være utformet på følgende måte:
    1. Som pkt. 2.6. d) 4.
    2. Søknaden skal være konvertert til ikke-redigerbar PDF-fil.
    3. Ved bruk av kryptering skal NCSCs offentlige PGP-nøkkel benyttes.

2.7. 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.

2.8. Evaluering

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

- Minimum 50% poengsum på hvert av områdene 1, 2, 3, 5, 7, 8, 9 og 10.
- Minimum 80% poengsum på hvert av områdene 4 og 6.

2.9. 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.

2.10. 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 sende søknad om å bli inkludert i NSMs kvalitetsordning for hendelseshåndtering plikter søker samtidig å følge nedenstående vilkår:

1. Aktiviteter opp mot kunder, og resultater av disse aktivitetene, som en godkjent virksomhet utfører, er virksomhetens eget ansvar. NSM fraskriver seg ethvert ansvar for resultatet av det oppdraget som utføres.
2. Søkers utgifter dekkes i sin helhet av søkeren 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 benyttes ved muntlig/skriftlig markedsføring av å være godkjent: «X tilfredsstiller kravene iht. NSMs kvalitetsordning for hendelseshåndtering.» (X erstattes av godkjent søkers firmanavn).
    c) Hvis godkjenningen omtales på virksomhetens 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 virksomheter 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 virksomheter til frivillig deltakelse i et samarbeidsforum med regelmessig møtefrekvens (halvårlig).
    c) Ordningen vil være gjenstand for årlig revisjon av NSM. Ved eventuelle justeringer vil godkjente leverandører få en hensiktsmessig frist til å møte endringene.
6. Godkjente virksomheter 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 eventuelle 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 eventuell videre behandling og avklaring. NSM vil vurdere eventuelle konsekvenser og behov for tiltak.

7. Tjenesteleverandøren plikter å informere NSM umiddelbart om forhold som vil kunne påvirke godkjenningen i tidsperioden denne gjelder. I dette inngår vesentlig endringer i de forhold som er lagt til grunn for NSMs godkjenning, samt for eksempel 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 virksomheten. Denne listen skal kunne forevises NSM ved forespørsel.
9. NSM kan utføre inspeksjon av virksomheter rettet mot forhold relevant for godkjenningen. Under en inspeksjon kan NSM kreve å få tilgang til dokumentasjon som er relevant for godkjennelsen. Ved mangelfulle forhold vil NSM sette en frist for avklaring og eventuell utbedring av disse.
10. NSM kan sette en frist for å avklare eventuelle uklare forhold ved en søknad. Svarfrist vil normalt settes til tre uker.
11. Rapportering:
    a) En samlet rapport over gjennomførte oppdrag skal sendes NSM minimum halvårlig. Mal for rapport er angitt i del 5 til dette dokumentet. Ved halvårlig rapportering er frist for rapportering hhv 15. april og 15. oktober.
    b) NSM anmoder om at godkjente søkere sender 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. Sendelse av rapporter vil videre gjøre det lettere for NSM å kunne forbedre ordningen og eventuelt støtte godkjente søkere.

MERKNAD 2:
Ved sendelse av rapport etter hvert oppdrag bortfaller kravet om samlet rapportering.

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

4. Søknadsskjema

NSM vil behandle all mottatt informasjon i forbindelse med 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 virksomheten

4.1.1. Generelt

Navn:	
Organisasjonsnummer:	
Postadresse:	
Besøksadresse:	
Eventuelle virksomhetssertifiseringer:	
Regnskap siste år er vedlagt:	(Ja/nei)
Kundemålgruppe og fokusområde for leveranse av hendelseshåndtering -tjenester:	

4.1.2. Kontaktperson

Oppgi navn på kontaktpersoner i virksomheten 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:		

4.1.3. Operativt kontaktpunkt

Oppgi et felles operativt kontaktpunkt ved virksomheten som NSM ved behov kan kontakte vedrørende operative henvendelser:

Telefonnummer:	
E-post adresse:	
PGP-fingerprint:	

4.1.4. 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)

4.2. Krav

4.2.1. Område 1: Referanser

4.2.1.1. Formål

Dokumentere praktisk erfaring innen hendelseshåndtering (offentlig/privat sektor, internasjonale organisasjoner, eventuelt 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 søker møter kundens behov.

4.2.1.3. Krav

Søker skal fremlegge dokumentasjon på utførte oppdrag innen hendelseshåndtering.

Søker kan velge å gjøre dette på én av to måter der alternativ a) er hovedregelen:

Alternativ a)

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

a) Navn på virksomheten 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 eventuelt 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 hendelseshåndteringsorganisasjon 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 virksomheten 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 eventuelt 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 hendelseshåndteringsorganisasjon.

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

MERKNAD 3:
NSM ber spesielt om at eventuell erfaring fra hendelseshåndteringsoppdrag i Norge beskrives.

MERKNAD 4:
Alternativ b) kan kun benyttes som grunnlag for godkjent søknad én gang. Søkere som sender søknad iht. alternativ b) skal ved første gangs regodkjenning sende 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 trusselaktører. Hva som regnes som relevante trusselaktører vil være avhengig av søkers kundemålgruppe og fokusområde.

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 relevante 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

Søker 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 søker dokumentere kunnskap om kapasiteter, teknikker og infrastrukturer for minst to navngitte relevante trusselaktører.

> MERKNAD 5:
> NSM vil kunne ta kontakt med søker for å få en nærmere innsikt i søkers kunnskap om dette området.

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

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 kompetanse innen bruk av verktøy, og kompetanse til å tilpasse og eventuelt utvikle disse.

4.2.3.3. Krav

Søker 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 virksomheten.

Verktøyene kan være innen ulike kategorier av hendelseshåndtering, for eksempel:

- 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 6:
Dette punktet krever minimum 80% poengsum 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

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

a) Beskrivelse av rutiner for oppstart, for eksempel:
    1. Utrykning
    2. Kartlegging av systemer og eventuelle begrensninger
    3. Kommunikasjon.
b) Beredskap og plan for håndtering.
c) Beskrivelse av hendelseshåndtering-organisasjonen, herunder fordeling av roller og ansvar.
d) Identifisering av skadetype og omfang.
e) Sikring og verifisering av beviskjeden.
f) Notoritet og logging av aktivitet.
g) Eventuelt teknisk utstyr som medbringes ved utrykning.
h) Koordinering av aktiviteter for nødvendige mottiltak og gjenoppretting av normaltilstand.
i) Rapportering.
j) Evaluering og læringspunkter.

Personelliste ved søknadstidspunktet med rolletilhørighet og relevante kvalifikasjoner rapporteres til NSM som egen liste. NSM ber om følgende opplysninger:

- Fullt navn.
- Fødselsdato.
- Telefonnummer kontor/telefonnummer mobil.
- Tid ansatt i virksomheten (år).
- Rolle i virksomhetens 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 søker beskrev i område 4, skal denne beskrivelsen vise hvordan søkeren har gjennomført en komplett hendelseshåndteringsprosess. Dette omfatter tidsrommet fra søkeren første gang ble varslet, til oppdraget ble ferdigstilt og sluttrapport utarbeidet.

4.2.5.3. Krav

Søker 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, samt sammensetting av hendelseshåndteringsteam.
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) Beskrivelse av loggføring.
f) Eventuelle operative begrensninger pga. virksomhetens/informasjonssystemets art, samt tiltak iverksatt for å kompensere for dette.
g) Teknisk analyse av skadevare og angrepsvektor.
h) Kartlegging av omfang av eventuelle kompromitterte/eksfiltrerte data.
i) 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.
j) Beskrivelse av tiltak for skadebegrensning og gjenopprettelse av normal drift.
k) Tilbakemeldinger og rapportering til oppdragsgiver, inkludert skadeomfang og hvordan kunnskapen fra håndteringen er brukt for å sikre oppdragsgiver bedre i ettertid.

MERKNAD 7:
For å tilfredsstille minimumskravet på området skal søker på en klar måte vise bruk av hensiktsmessige analysemetoder og beskrevne prosesser. Søker skal redegjøre for valg av verktøy og rollefordeling i hendelseshåndteringsprosessen.

Sidebegrensning: Beskrivelsen på området skal være på maksimalt fem A4-sider inkludert eventuelle 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 ett utført hendelseshåndteringsoppdrag i Norge.

MERKNAD 8:

- Dette punktet krever minimum 80% poengsum for å være bestått.
- Rapporten kan være skrevet på engelsk.
- Om nødvendig kan omtalt virksomhet anonymiseres i rapporten.

4.2.6.2. Bakgrunn

Dette punktet skal vise at søker er i stand til å utarbeide klare og konsise rapporter til personell med ulik faglig bakgrunn i en virksomhet. En sluttrapport er et dokument som er ment å gi en dekkende oversikt av hele hendelseshåndteringen. Rapporten er ofte rettet mot både ledelse og teknisk personell.

4.2.6.3. Krav

Søker skal legge ved en kopi av en reell rapport som ble levert til en virksomhet i Norge etter 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) Beskrivelse av hendelseshåndteringen. Skal inkludere en tydelig tidslinje med søkers aktiviteter hos kunden i håndteringen av hendelsen. Er dette i form av en logg e.l. kan denne sendes som vedlegg.
c) Beskrivelse av eventuelle operative eller tekniske problemer/begrensninger.
d) Hvordan hendelsen kunne skje samt omfanget av denne.
e) Nødvendige mottiltak/plan for å gjenopprette normaltilstand og eventuelle resultater/konsekvenser av disse.
f) Anbefalte tiltak til oppdragsgiver for å øke sikkerheten.
g) Oversikt over relevante tekniske funn.

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 søker 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

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

a) Hvordan digitale bevis og fysiske media dokumenteres og håndteres, 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) Sertifiseringer relevant for egenbeskyttelse av organisasjon og personell.
d) Planer for å håndtere interne sikkerhetshendelser.
e) Relevant øvelsesaktivitet.

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 søker 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 søker kunne dokumentere hvordan organisasjonen nyttiggjør seg av informasjon og erfaringer fra hendelseshåndteringer. NSM vil bl. a. se etter hvordan denne erfaringen brukes praktisk til:

a) Oppdatering av interne opplæringsprogram/interne kurs.
b) Oppdateringer av deteksjonskapabilitet.
c) Oppdatering av trusselbildet.
d) Oppdatering av egenbeskyttelse.
e) Valg av verktøy.
f) Revisjon av relevante prosesser.

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

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 søker 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 søker 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.

4.2.10. Område 10: Kompetanse og kompetanseutvikling

4.2.10.1. Formål

Dokumentere at søkeren har utdannings- og kompetansekrav, samt utdanningsplaner knyttet opp mot rollene i hendelseshåndteringsprosessen.

4.2.10.2. Bakgrunn

Dette punktet skal vise at søker har spesifikke kompetanse- og erfaringskrav knyttet til de ulike rollene i hendelseshåndteringsprosessen, samt planer for å vedlikeholde og videreutvikle kompetanse og erfaring.

4.2.10.3. Krav

For å møte minimumskravet må søker kunne dokumentere hvilke spesifikke kurs, utdanninger og/eller eventuell realkompetanse som kreves i de forskjellige rollene i hendelseshåndteringsprosessen.

Søkeren må videre dokumentere planer for vedlikehold og videreutvikling av kompetansen hos hendelseshåndteringspersonellet.

> MERKNAD 9:
> NSM vil ikke gjøre vurderinger av de spesifikke kurs/utdanninger som søkeren omtaler under dette området. NSM vil dog vurdere om søkeren har gjennomtenkte og realistiske utdannings- og kompetansekrav samt utdanningsplaner for det personellet som er knyttet opp mot rollene i hendelseshåndteringsprosessen.

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

5. Mal for samlet rapportering

Samlet rapport defineres utfra punktene under. Samlet rapport skal bruke engelsk språk. Foreløpig har vi ingen formelle krav til formatet på rapporteringen, men det må være maskinlesbart (csv, JSON, XML…). Samlet rapport vil være gjenstand for revisjon, og vi jobber med å få til en mer automatisert innrapportering eller felles delingsplatform.

Følgende felter skal rapporteres per hendelse:

5.1. 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.

5.2. Målsektor

Hvilken sektor tilhører virksomheten hvor hendelseshåndteringsoppdraget ble utført.

Bruk «Target_Sector» som overskrift/navn på feltet. Mulige verdier listet i tabellen under.

Målsektor (Target_Sector)	**Overordnet departement**
Finance	Finansdepartementet
Defence	Forsvarsdepartementet
Government	Generell offentlig forvaltning (ev. Kommunal- og distriktsdepartementet)
Health and Care Sevices	Helse- og omsorgsdepartementet
Trade, Industry and Fisheries	Nærings- og fiskeridepartementet
Justice	Justis- og beredskapsdepartementet
Culture	Kultur- og likestillingsdepartementet
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. Klassifisering av hendelse

Klassifisering er samme som beskrevet i NSMs «Rammeverk for håndtering av IKT-sikkerhetshendelser» og er en forenklet versjon av taxonomi fra eCSIRT.net-prosjektet. Bruk «Incident_Class» som navn på feltet. Mulige verdier er A til G ihht følgende tabell:

Klassifisering (Incident_Class)	**Beskrivelse/eksempler**
A. Uautorisert tilgang til informasjon (Information Content Security)	Vellykket uautorisert tilgang til informasjon eller funksjoner på systemer eller tjenester. Resultatet kan være kompromittering av konfidensialitet, integritet og/eller tilgjengelighet. Dette dekker også tilgang til informasjon under overføring.
B. Kompromittering (Intrusions)	Vellykket uautorisert tilgang til system eller tjeneste. Ingen tegn til aktivitet på målet.
C. Forsøk på kompromittering (Intrusion Attempts)	Forsøk på kompromittering av systemer eller tjenester ved for eksempel å lure autorisasjonssystemet, gjette passord, utnytte sårbarheter i systemet eller feil i oppsett. Mye brukt

	metode er også å lure legitime brukere til å starte skadelig programvare på interne systemer.
D. Tjenestenekt (Availability)	I denne typen angrep blir systemet bombardert med så mye trafikk at tjenester går ned eller blir mindre responsive.
E. Svindel (Fraud)	Bruk av ressurser for å tjene penger, for eksempel misbruk av domenenavn eller epostadresser. Salg eller installasjon av materiale beskyttet av copyright. Bruk av andres identitet.
F. Rekognosering / informasjonsinnsamling (Information Gathering)	Informasjonsinnsamling om målet via for eksempel åpne kilder, skanning av nettverksinfrastruktur og tjenester som er åpne mot Internett, sniffing på nettverkstrafikk, sosiale nettverk eller direkte kontakt for eksempel via telefon.
G. Støtende innhold (Abusive Content)	Spam eller reklame fra parter som ikke har innhentet tillatelse til utsendelse. Plaging, trusler eller forfølgelse via digitale kanaler. Distribusjon av barnepornografi eller forherligelse av vold.

5.4. Kategorisering av mål

Mål refererer til hvem som er utsatt for en hendelse og hvor hendelsen inntreffer. Navn på feltet er «Target_Type», og mulige verdier er 1 til 7 etter følgende tabell:

Kategori (Target_Type)	**Beskrivelse**
1. Tverrsektorielt (GNF)	Virksomheter fra flere sektorer er involvert. Grunnleggende nasjonale funksjoner er rammet.
2. Sektor (GNF)	Flere virksomheter fra samme sektor er involvert. Grunnleggende nasjonale funksjoner er rammet.
3. Virksomhet (GNF)	Kun en involvert virksomhet. Grunnleggende nasjonale funksjoner er rammet.
4. Tverrsektorielt	Som tverrsektorielt ovenfor men uten å ramme GNF.

5. Sektor	Som sektor ovenfor men uten å ramme GNF.
6. Virksomhet	Som virksomhet ovenfor men uten å ramme GNF.
7. Privatperson	En/flere privatpersoner, uten spesiell knytning til virksomhet.

Klassifisering av hendelse og kategorisering trekkes sammen i rapporteringen. Bruk da «Incident_Class+Target_type» som feltnavn. For eksempel kan da en kompromittering (B) i en virksomhet uten å ramme GNF (6) da skrives som «B6».

5.5. 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. Feltnavn er «Cyber_Kill_Chain» og mulige verdier er: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Action on Target.

5.6. Navn på trusselaktør

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

5.7. Verktøy

Eventuelle verktøy som ble oppdaget brukt under angrepet. Feltnavn «Tools».

5.8. Indikatorer

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

Feltnavn som brukes er «Indicator_Type» og mulige verdier listes i tabellen under. I tillegg brukes «Indicator_Value» og «Indicator_Context» for å beskrive indikatoren.

Type (Indicator_Type)	**Beskrivelse**

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.

5.9. Kontekst

Eventuell utfyllende kontekst. Feltnavn «Context».

5.10. Eksempel på rapportert hendelse i samlerapport

```
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+Target_type=B6
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”
```

Nasjonal

sikkerhetsmyndighet

Postboks 814

1306 Sandvika