POLITIET
KRIPOS

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

NCIS Norway

Deres referanse:	Vår referanse:	Sted, dato
201900197-1	201900264-2	Oslo, 24. februar 2019

HØRINGSUTTALELSE – LEDELSESSYSTEM FOR SIKKERHET

Det vises til høringsbrev datert 11. januar 2019 vedrørende oppdatering av ledelsessystem for sikkerhet i politiet.

Nedenfor følger Kripos' merknader til bestemte temaer i utkastene, herunder bemerkninger til enkelte bestemmelser.

1. Merknader til *Policy for sikkerhet i politiet*

Det bør avklares hvilket forhold denne policyen skal ha til Policy for informasjonssikkerhet i politiet av 22. desember 2015.

Til punkt 3 *Politidirektørens mål for sikkerhetsarbeidet*
Etter Kripos' oppfatning bør det tydeliggjøres hva som legges i begrepet "verdier". Informasjon, samfunnskritiske funksjoner samt skjermingsverdige objekter og infrastruktur er uttrykkelig nevnt i utkastet. Etter vår oppfatning bør det avklares om andre verdier, eksempelvis materiell, kompetanse, liv og helse, omdømme, også er omfattet i denne sammenhengen.

Det bør også avklares om begrepet "ressurser" er overflødig da det er en vanlig forståelse at dette også anses som en verdi.

Når det gjelder avsnitt to, fremstår det som at informasjon må håndteres forsvarlig, effektivt og enhetlig for at den skal være beskyttet med hensyn til konfidensialitet, integritet og tilgjengelighet. Etter vår oppfatning oppnår man beskyttelse av informasjon ved å ha sikkerhetstiltak. Videre har "håndtering" mer med *bruk* av informasjon å gjøre.

I avsnitt tre bør begrepet samfunnskritiske funksjoner tydeliggjøres. Det er uklart om det siktes til utpekte KIKS-objekter eller lignende funksjoner for øvrig. Det bør videre tydelig skilles mellom ovennevnte begrep og skjermingsverdige objekter og infrastruktur som også er av samfunnskritisk art.

Kripos/

Post: Pb. 2094 Vika, 0125 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.no/kripos

Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no

Org. nr: 974 760 827

Det bør også klarlegges hvilket forhold begrepet "tilfredsstillende sikringsnivå" skal ha til sikkerhetslovens "forsvarlig sikkerhetsnivå". For å redusere uklarheter bør det så langt mulig være gjenbruk av allerede innarbeidede og predefinerte begreper. For øvrig bør det tydeliggjøres om det i utkastet legges opp til at tilfredsstillende sikringsnivå skal være en type rettslig standard i politiet.

Til punkt 4 *Prinsipper for sikkerhetsarbeidet*
Det fremgår av dette avsnittet at arbeidet med sikkerhet blant annet skal basere seg på standarden ISO 27001 *Ledelsessystemer for informasjonssikkerhet*. Det bør klargjøres om arbeidet med andre fagområder enn informasjonssikkerhet skal basere seg på standarden. For det tilfelle at standarden skal benyttes i arbeidet med de øvrige fagområdene, bemerkes det at den aktuelle standarden gjennomgående tar utgangspunkt i informasjon som en verdi. Videre er det vanskelig å se at det er hensiktsmessig kun å se hen til den i denne sammenhengen.

Til punkt 5 *Roller og ansvar*
Det fremgår av utkastet at sikkerhetsleder i Politidirektoratet utøver myndighet på politidirektørens vegne innen "forebyggende sikkerhetsarbeid og "informasjonssikkerhet". Etter vår oppfatning inngår informasjonssikkerhet i det forebyggende sikkerhetsarbeidet, og presiseringen knyttet til informasjonssikkerhet kan utelates.

Til punkt 6 *Samsvar med juridiske krav*
Da dette dokumentet er en policy for sikkerhet i politiet, så kan oversikten med fordel suppleres med SIS-loven, politiregisterforskriften, politiinstruksen, straffeprosessloven og påtaleinstruksen.

2. Merknader til *Ledelsessystem for sikkerhet*

Til punkt 5 *Ledelsessystemet for sikkerhet*
Kripos foreslår at K-1 endres til "Enhetene skal etablere og vedlikeholde ledelsessystem for sikkerhet.

Til punkt 6 *Etablering av ledelsessystemet*
I tilknytning til etableringsfasen fremgår det at gapet mellom nåsituasjon og ønsket sluttilstand beskrives. Fordi sikkerhetsarbeidet er en kontinuerlig prosess anbefales heller bruken av begrepet "ønsket tilstand" eller lignende.

Til punkt 7 *Implementering av ledelsessystemet*
Kripos slutter seg til at enhetene bør ha en risikobasert tilnærming til sikkerhetsarbeidet. Etter vår oppfatning er dette punktet i utkastet og Policy for sikkerhet i politiet punkt 4 til dels uklar, og benytter en ikke fullt ut ensartet begrepsbruk når det gjelder risikobasert tilnærming. Det vises til at begrepene *risikokartlegging, skadevurdering, verdivurdering* og *risikovurdering* omtales som separate selvstendige prosesser. Tradisjonelt er risikokartlegging, skadevurdering og verdivurdering prosesser som inngår i virksomhetens risikovurdering eller risikoanalyse[1][2][3]. Det påpekes at det riktignok er ulik praksis knyttet til hvorvidt det er risikoanalyse eller risikovurdering som defineres som den overordnede aktiviteten. En bør være restriktiv når det

[1] NSM (2016) Håndbok: Risikovurdering for sikring.
[2] Forsvarsbygg. (2016) Sikringshåndboka.
[3] Aven, T. (2006) Pålitelighets og risikoanalyse.

gjelder å avvike fra fagfeltets etablerte begrepsbruk, da dette vil kunne bidra til å skape usikkerhet blant brukere av instruksene. Eksempelvis fremgår det av punkt 7.1 at implementeringsfasen starter med "verdi og risikokartlegging". Det naturlige er her å starte med en risikovurdering, som blant annet omfatter verdivurdering og risikoanalyse. Betydningen av begrepene verdikartlegging og risikokartlegging bør for øvrig tydeliggjøres.

Det bemerkes for øvrig at det ovennevnte ikke stenger for å gi krav til skade-, verdi- og risikovurdering i egen instruks slik det pekes på i utkastet.

Til punkt 8 *Kontroll av ledelsessystemet*
I første avsnitt fremgår at kontroller gjøres gjennom egenkontroll og ved tilsyn eller revisjon. Det er grunn til å presisere hva som foretas internt og hva som gjøres av eksterne aktører. Det vises til at revisjon kan foretas som en internrevisjon eller av eksterne.

Eksemplet "mistenkelige påloggingsforsøk" i andre avsnitt foreslås endret til "forsøk på uautorisert bruk av informasjonssystemer". For øvrig retter dette eksempelet seg mot informasjonssystemer i politiet, og er i mindre grad dekkende for et ledelsessystem for sikkerhet.

3. Merknader til *Sikkerhetsroller og -ansvar*

Til punkt 5 *Organisering av arbeidet*
Kripos støtter tydeliggjøringen av at sikkerhet er et lederansvar som skal følge linjeprinsippet. Det vises til at det er linjeorganisasjonen som har størst nærhet til sine verdier, behov for sikkerhetstiltak mv.

I punkt 5.1 fremgår blant annet at alle ansatte skal rapportere "feil og mangler". Kripos er tvilende til om den naturlige språklige forståelsen av begrepet også dekker avvik, sikkerhetsbrudd og sikkerhetstruende hendelser. Det antas at formålet i denne sammenhengen er at alle ansatte skal rapportere også om dette.

Til punkt 6 *Organisatorisk tilhørighet*
Begrepet "sikkerhetsledelsen" er ikke definert fra tidligere og kan misforståes.

Til punkt 8 *Sikkerhetsorganisasjonen*
I punkt 8.1 fremgår det at sikkerhetsleder har myndighet til å utøve enhetsleders ansvar for alle fagområdene innen "forebyggende sikkerhet og informasjonssikkerhet". Etter vår oppfatning inngår informasjonssikkerhet i det forebyggende sikkerhetsarbeidet. Det fremgår videre av avsnittet at sikkerhetsleder har myndighet til å utøve enhetsleders ansvar. Språklig er det trolig bedre å omtale dette som å utøve myndighet enn å utøve ansvar, særlig fordi ansvar vanskelig kan delegeres.

Med hilsen

Vigleik Antun
ass. sjef Kripos