RIGSPOLITIET

CFB Center for Beredskabs-kommunikation

Udkast

Sikkerhedspolitik for beredskabers brug af SINE

Indledning
Formålet med denne sikkerhedspolitik er at sikre, at opbevaring, brug og vedligeholdelse af SINE-udstyr og informationer herom håndteres på en sikkerhedsmæssigt hensigtsmæssig måde, således at uautoriserede personer ikke kan få adgang til SINE eller kan påvirke driften heraf.

Denne sikkerhedspolitik skal ses som en formalisering af de sikkerhedskrav for brug og håndtering af SINE-udstyr og informationer, som allerede gælder efter gældende lovgivning og best practice på området, herunder navnlig persondataforordningen, retshåndhævelsesloven og ISO27001, som er den statsligt anvendte standard inden for informationssikkerhed. Sikkerhedspolitikken er et supplement til beredskabernes egne retningslinjer for tavshedspligt, fortrolighed m.v.

Sikkerhedskravene udspringer endvidere af en risikovurdering, som er udarbejdet for SINE af Rigspolitiets Center for Beredskabskommunikation. Sikkerhedsmyndighederne Politiets Efterretningstjeneste og Center for Cybersikkerhed har deltaget i risikovurderingen.

Beredskabernes håndtering af SINE-radioer
For at sikre SINE mod uautoriseret adgang er det vigtigt, at de enkelte beredskaber har implementeret sikkerhedsforanstaltninger for at forhindre bortkomst af SINE-radioer.

Beredskaberne skal som minimum have følgende sikkerhedsforanstaltninger:

- Opdateret overblik over alle SINE-radioer
- Regelmæssige optællinger af SINE-radioer
- SINE-radioer skal opbevares utilgængeligt for uvedkommende personer
- SINE-radioer uden opsyn skal låses inde
- Hvis en radio er bortkommet, skal Dansk Beredskabskommunikation A/S straks underrettes

Herudover er det enkelte beredskab ansvarlig for, at brugerne løbende bliver informeret om korrekt håndtering af SINE-udstyr, herunder ved udlevering af denne sikkerhedspolitik.

Brugernes håndtering af SINE-radioer
For at sikre SINE mod uautoriseret adgang, er det vigtigt at de enkelte beredskabers brugere håndterer SINE-radioer hensigtsmæssigt.

Brugere af SINE-radioer skal som minimum overholde nedenstående sikkerhedsforanstaltninger:

- Må kun anvendes til tjenesteligt behov
- Må kun fjernes fra beredskabets område til tjenestelige opgaver
- Må kun anvende de talegrupper, hvortil man har et operativt behov
- Straks informere nærmeste leder, hvis en SINE-radio er bortkommet

Brugerne skal endvidere søge at minimere risikoen for, at uvedkommende kan lytte med på radiokommunikationen, eksempelvis som følge af unødigt høj lydindstilling, dog således at hensynet til brugernes kommunikationsmæssige behov og løsningen af beredskabsopgaverne til enhver tid prioriteres.

I tilfælde af anvendelse af SINE-radioer uden tjenesteligt formål, f.eks. i fritiden eller ved uautoriseret aflytning af skadestedssæt, bør ansættelsesmyndigheden overveje, om overtrædelsen skal have ansættelsesretlige konsekvenser. I tilfælde af gentagne overtrædelser eller overtrædelser af særlig grov karakter bør ansættelsesmyndigheden endvidere overveje, om der er grundlag for at indgive en politianmeldelse.

Sikkerhedsansvarlig
Det enkelte beredskab bør udpege en sikkerhedsansvarlig, som har til opgave at strukturere og koordinere beredskabets processer til sikring af, at denne sikkerhedspolitik overholdes.

Tavshedspligt
Medarbejdere med adgang til følsomme informationer om SINE, og som ikke er omfattet af reglerne om tavshedspligt for offentligt ansatte, bør underskrive en NDA (fortrolighedserklæring) for at sikre, at informationer om SINE ikke havner hos uautoriserede personer.

Dette gælder både medarbejdere, konsulenter og underleverandører som får kendskab til følsomme informationer om SINE.

Informationsoverførsel
For at sikre at informationer om SINE ikke kommer uautoriserede personer i hænde, skal al kritisk information omkring SINE beskyttes, når informationen overføres, eks. gennem benyttelse af krypteret mail.

Eksempler på kritisk information kan være, men er ikke begrænset til: Information for at få adgang til SINE (passwords, krypteringsnøgler og lign.), IP numre til ICCS'er, numre på talegrupper og fleetmaps.

Leverandørstyring
Det enkelte beredskab er ansvarlig for, at dennes leverandører behandler informationer omkring SINE på forsvarlig vis.

Dette gøres gennem styring af leverandørydelsen, hvor man f.eks. kan anvende anerkendt best practice for at opnå en struktureret og helhedsorienteret tilgang til leverandørstyringsopgaven.

Vedligeholdelse af SINE-udstyr
Den enkelte beredskabsmyndighed er ansvarlig for, at dennes SINE-udstyr løbende bliver vedligeholdt og udskiftet efter behov, således at det til enhver tid vil kunne anvendes ved en større hændelse.

Udlån af SINE-radioer
I det omfang et beredskab udlåner sine SINE-radioer til en aktør på baggrund af en beredskabsfaglig indstilling, jf. vejledningens punkt 4.4, er det det pågældende beredskabs ansvar at sikre, at de udlånte SINE-radioer anvendes til de aftalte formål, samt at låneorganisationen lever op til de stillede krav for anvendelsen af SINE.

SINE-radioer må kun udlånes, hvis låneorganisationen har et behov for beredskabskommunikation.

Ved udlån af SINE-radioer, skal man som minimum sørge for følgende foranstaltninger:

- Overblik over de udlånte SINE-radioer
- Instruks for tilladt brug af de udlånte SINE-radioer
- Uddannelse i brug af de udlånte SINE-radioer
- Kontrol med tilbagelevering af de udlånte SINE-radioer

Såfremt en indstillet aktør evt. selv måtte have finansieret SINE-radioer, som anvendes i forbindelse med en beredskabsfaglig indstilling, vil det indstillende beredskab ligeledes være ansvarlig for, at aktøren anvender SINE-radioerne til de aftalte formål og lever op til de stillede krav for anvendelsen af SINE. Det indstillende beredskab skal desuden sørge for, at der sker en tilsvarende overholdelse af ovennævnte foranstaltninger, herunder at SINE-radioerne afmeldes i nettet, når den beredskabsfaglige indstilling bringes til ophør.

Ved mistanke om uretmæssig brug eller misbrug af SINE-radioerne, skal Center for Beredskabskommunikation og Dansk Beredskabskommunikation A/S underrettes hurtigst muligt.

Håndtering af SINE-data
Ved opbevaring af data fra SINE (f.eks. optagelse af talekommunikation eller positioneringsdata) er det beredskab, der opbevarer pågældende data, selvstændigt ansvarlig for, at dette sker i henhold til gældende lovgivning, herunder navnlig persondataforordningen og retshåndhævelsesloven.

Patching af talegrupper
Beredskabsmyndighederne skal i så stort omfang som muligt anvende skadestedssæt og assistance-skadestedssæt og minimere patching af talegrupper på tværs af VPN nummerstrukturen.

Har man stadig et behov for at patche talegrupper på tværs af VPN afgrænsninger, skal man være opmærksom på at skille talegrupperne ad, når behovet for patching af talegrupper ikke længere er til stede.

Certificering
Kun udstyr, som er certificeret af Center for Beredskabskommunikation, må anvendes på SINE. Det er det enkelte beredskabs ansvar at sikre, at udstyr, der anvendes, er certificeret til anvendelse på SINE.

Kontrolrumsløsning
For at sikre mod uautoriseret adgang til SINE, er det vigtigt at beredskabernes kontrolrum er tilfredsstillende sikret.

Beredskabsmyndighederne skal som minimum have følgende sikkerhedsforanstaltninger for deres kontrolrum:

- Fysisk og logisk adgangsstyring
- Fysisk sikkerhed
- Netværkssegmentering

Det enkelte beredskab bør have udarbejdet en beredskabsplan for fortsættelse af de operative opgaver uden et fungerende kontrolrum.

Sikkerhedsbrud
Ved mistanke om brud på sikkerheden skal beredskabet hurtigst muligt kontakte Center for Beredskabskommunikation og Dansk Beredskabskommunikation A/S, så eventuelle yderligere konsekvenser kan forebygges.