BEREDSKABSSTYRELSEN

Sikkerhedspolitik for beredskabers brug af SINE

1. november 2024

CFB Center for Beredskabs-kommunikation

Center for Beredskabskommunikation
W: www.sikkerhedsnet.dk

Indhold

1. Indledning 3
2. Beredskabernes håndtering af SINE-radioer 3
3. Brugernes håndtering af SINE-radioer 3
4. Sikkerhedsansvarlig 4
5. Tavshedspligt 4
6. Informationsoverførsel 4
7. Leverandørstyring 4
8. Certificerede radioer og udstyr 5
9. Applikationer 5
10. Brug af Bluetooth-udstyr 5
11. Vedligeholdelse af SINE-udstyr 5
12. Udlån af SINE-radioer 5
13. Bortskaffelse af SINE-radioer 6
14. Håndtering af SINE-data 6
15. Patching af talegrupper 6
16. Kontrolrumsløsning 7
17. Sikkerhedsbrud 7

1. Indledning

Denne sikkerhedspolitik henvender sig til beredskabsmyndigheder og øvrige brugere af SINE[1].

Formålet med sikkerhedspolitikken 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.

Sikkerhedspolitikken 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. 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 Center for Beredskabskommunikation. Sikkerhedsmyndighederne, Politiets Efterretningstjeneste og Center for Cybersikkerhed har deltaget i risikovurderingen.

2. 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
- 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.

3. 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:

[1] Sikkerhedspolitikken er et bilag til henholdsvis '*Vejledning til Bekendtgørelse nr. 262 om tilslutning og anvendelse af radiokommunikationsnettet - for beredskaber'* samt til '*Vejledning til bekendtgørelse nr. 262 af 22. april 2008 om tilslutning til og anvendelse af det landsdækkende radiokommunikationsnet – for Andre Aktører (myndigheder og virksomheder uden tilslutningspligt, der kan tilsluttes SINE)'.* Vejledningerne kan hentes på www.sikkerhedsnet.dk.

- Må kun anvendes til tjenesteligt behov.
- Må kun fjernes fra beredskabets område, når det følger af det tjenestelige behov, herunder i forbindelse med vagt fra hjemmet.
- Må kun anvende de talegrupper, hvortil man har et operativt behov.
- Straks informere nærmeste leder samt SINE superbruger, hvis en SINE-radio er bortkommet.

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

4. 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.

5. 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.

6. 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.

7. 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.

8. Certificerede radioer og udstyr

Alle typer af radioer og udstyr, der anvendes på SINE, skal være certificeret hertil. Dette kræves bl.a. for at sikre, at radioer og udstyr lever op til de sikkerhedsmæssige krav. Der henvises til oversigter over certificerede radioer og udstyr på www.sikkerhedsnet.dk.

9. Applikationer

Applikationer skal godkendes af CFB, og supplerende kommunikationssystemer kan kun anvendes under særlige omstændigheder.

10. Brug af Bluetooth-udstyr

Beredskaberne kan anvende Bluetooth i SINE-radioer og tilbehør som fx head-sets. Både SINE-radioer og tilknyttet tilbehør, som anvendes i beredskaberne, skal som minimum understøtte Bluetooth version 4.1 eller nyere for at opretholde en høj sikkerhedsstandard. Der henvises til '*Vejledning til sikker brug af Bluetooth-garniture med SINE-radioer*' på www.sikkerhedsnet.dk.

11. 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.

12. 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.

13. Bortskaffelse af SINE-radioer

Det enkelte beredskab er ansvarlig for at sikre, at SINE-radioer, der ikke skal anvendes længere, bortskaffes på sikker vis. Herved menes, at radioernes adgang til SINE-nettet fjernes.

Procedure for bortskaffelse er som følger:

- Beredskabet tager kontakt til DBK via en SINE-superbruger for at få fjernet radioens adgang til SINE.

- DBK udleverer derudover en specifik tastekombination, som indtastes på radioen, hvorved alle krypteringsnøgler slettes.

- Radioerne sendes efterfølgende til vederlagsfri destruktion ved DBK:

  Motorola Solutions
  Sydvestvej 15
  2600 Glostrup
  Att.: Motorola Service

14. 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.

15. 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.

16. Kontrolrumsløsning

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

Beredskabsmyndighederne bør som minimum have fokus på følgende sikkerhedsforanstaltninger for deres kontrolrum:

- Fysisk og logisk adgangsstyring
- Fysisk sikkerhed
- Adskillelse af netværk (segmentering)

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

17. 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.