



DNK faktaserie

Sikkerhetsregler for bruk av nytt digitalt nødnett

dNk
Direktoratet for nødkommunikasjon

DNK-FAKTA-0007 – versjon 1 - 29. august 2007

INNHold

1. INNLEDNING	3
2. GENERELLE BESTEMMELSER.....	4
3. ORGANISASJON	5
4. RADIOTERMINALER.....	5
5. KOMMUNIKASJONSSENTRALER	6
6. SIKKERHETSREVISJON	7

1. Innledning

1.1. Innledning

Stortinget vedtok 18. desember 2006 at et første utbyggingstrinn for nytt digitalt nødnett i Norge skal igangsettes. Utbyggingen starter i Østfoldområdet, og de første brukerne i nettet vil være de tre nødetatene brann, politi og helse.

Justis- og politidepartementets nødnettorganisasjon (JDN) inngikk 22. desember 2006 kontrakt med Siemens AS som gir Siemens et helhetsansvar for leveranse av et nødnett basert på TETRA-teknologi og tilhørende betjeningsutstyr til kommunikasjonsentraler.

Direktoratet for nødkommunikasjon (DNK) tok 1. april 2007 over ansvaret for forvaltning av kontraktene. Siemens AS overførte i april 2007 kontraktene for nødnettsprosjektet til Nokia Siemens Networks Norge AS (NSN).

Nødnettet vil benyttes til å formidle sensitive personopplysninger og tidskritiske beredskapsmeldinger og gi mulighet for overføring av sikkerhetsgradert informasjon. Dette krever at det etableres et sett med sikkerhetsbestemmelser for bruk av nødnettet som er felles for alle brukerorganisasjonene for å sikre at sikkerheten i systemet kan opprettholdes over tid.

1.2. Hensikt

Dokumentet beskriver de foreløpige sikkerhetsrutinene som er fastlagt for bruk av nødnettet. Rutinene er utarbeidet for å sikre at den sikkerheten som tilbys i nettet kan opprettholdes i nettets levetid. Sikkerhet omfatter i denne sammenheng de tre elementene tilgjengelighet, integritet og konfidensialitet.

Hensikten med dette dokumentet er å gi fremtidige abonnenter et bilde av hva slags sikkerhetsregler som vil bli fastlagt i fremtidige abonnementsvilkår. Utbygging av nødnettet er i en oppstartsfase, og det må påregnes oppdateringer til dette dokumentet.

Målgruppe for dokumentet er i første omgang fremtidige brukere av nødnettet, herunder personell tilknyttet nødetatenes kommunikasjonsentraler hvor det skal installeres utstyr i løpet av 2007. Det forutsettes at leseren har en overordnet kunnskap om hva nødnettet er, jf. St.prp.nr.30 (2006-2007) om igangsetting av første utbyggingstrinn av nytt digitalt nødnett.

Dokumentet er offentlig.

1.3. Innhold

Dette dokumentet inneholder følgende:

- Generelle bestemmelser
- Krav til organisasjon
- Krav til klargjøring og bruk av radioterminaler
- Krav til klargjøring og bruk av kommunikasjonsentraler

1.4. Definisjoner

DNK:	Direktoratet for nødkommunikasjon
Abbonent:	Formell juridisk avtalepart til DNK for mottak av utstyr og/eller tjenester i nødnettet. Dette kan for eksempel være et kommunalt AS eller et helseforetak eller direktorat.
Abbonentens representant:	Leder for en operativ enhet under abonnenten, for eksempel leder for en kommunikasjonssentral.
Systemeier:	Abbonentens oppnevnte ansvarlige person(er) for mottatt utstyr og/eller tjenester i nødnettet.
Sikkerhetsansvarlig:	Abbonentens oppnevnte ansvarlige person(er) for å ivareta pålagte sikkerhetsrutiner knyttet til mottatt utstyr og/eller tjenester.
Bruker:	Bruker av nødnettet, for eksempel bruker av en radioterminal eller operatør ved en av nødetatens kommunikasjonssentraler.
Kommunikasjonssentral:	Sentral som vil installere utstyr for å betjene nødnettet, herunder politiets operasjonssentraler, brannvesenenes 110-sentraler og helsetjenestens AMK-sentraler (Akuttmedisinske kommunikasjonssentraler), legevaktsentraler og akuttmottak ved sykehus.

2. Generelle bestemmelser

Bestemmelsene i dette dokumentet gjelder inntil dokumentet erstattes av abonnementsvilkår for bruk av nødnettet.

Deler av informasjonen om nødnettet er sikkerhetsgradert til nivå **BEGRENSET**. Eksempler på dette er detaljerte dekningskart, geografisk plassering av enkelte installasjoner m.m. I den grad abonnenten eller abonnentens representant får tilgang til slik informasjon, skal informasjonen behandles i samsvar med Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven).

Nødnettet vil i mange tilfeller bli benyttet til overføring av personopplysninger. Behandling av personopplysninger er regulert i Lov om behandling av personopplysninger (Personopplysningsloven) og Lov om helseregistre og behandling av helseopplysninger (Helseregisterloven), hvor henholdsvis § 13 og § 16 stiller krav til sikring av personopplysningene. Utfyllende bestemmelser for informasjonssikkerhet er gitt i Forskrift om behandling av personopplysninger (Personopplysningsforskriften), 2. kapittel.

3. Organisasjon

3.1. Generelt

Abonnementen skal ha et system for å ivareta sikkerhet der roller og ansvarsområder er fastlagt.

3.2. Systemeier

DNK er sentral systemeier til nødnettet. Abonnementen skal utpeke en egen systemeier, og ved behov både utpeke sentral og lokal systemeier for nødnettet. Systemeiers oppgaver vil variere, men de etterfølgende krav skal som et minimum oppfylles ved bruk av nødnettet:

Systemeier skal utpeke en sikkerhetsansvarlig for nødnettet. Sikkerhetsansvarlig skal forestå koordinering, rådgivning og kontroll av sikkerheten som abonnentens representant og den enkelte bruker er ansvarlig for.

For å begrense uvedkommendes adgang til systemet vil det være et system for kontroll av rettigheter. DNK vil ha ansvaret for den overordnede rettighetsadministrasjonen, men systemeier vil være ansvarlig for administrasjon av rettigheter innen egen organisasjon. Det påligger den enkelte bruker å oppbevare passord og PIN-koder slik at disse ikke kommer på avveie.

Det skal videre finnes rutiner for håndtering av feil, svakheter og hendelser, utilsiktede eller tilsiktede, for anvendelse av nødnettet.

3.3. Informasjon til brukere

Abonnementens representant skal sikre at brukere innen egen organisasjon er informert om de til enhver tid gjeldende sikkerhetsbestemmelsene knyttet til bruk av nettet.

4. Radioterminaler

4.1. Generelt

Det skal kun benyttes radioterminaler som er godkjent av DNK for bruk i Nødnettet. DNK vil utgi oversikter over de til enhver tid godkjente terminaler. Anskaffelse av radioterminaler skal kun gjøres over de rammeavtaler som er inngått av DNK for dette formål.

4.2. Administrasjon

Parametersetting i radioterminalene skal skje i samsvar med regler for dette (disse er under avklaring).

4.3. Programvare

Det tillates ikke at abonnentens utvikler eller får utviklet programvare for radioterminaler uten at dette er godkjent av DNK.

4.4. Fysisk sikring

Det påligger abonnentens representant å utarbeide bestemmelser for fysisk sikring av radioterminaler som er i operativ bruk. Det skal også utarbeides bestemmelser for lagring/oppbevaring av radioterminaler som ikke er i bruk.

4.5. Programvareversjon

På radioterminalene skal det kun benyttes programvareversjoner som er godkjent av DNK for bruk i nødnettet. DNK vil utgi oversikter over de til enhver tid godkjente programvareversjoner.

4.6. Tapt/ frastjålet radioterminal

Ved tap av radioterminal skal bruker umiddelbart varsle abonnentens sikkerhetsansvarlige for å få terminalen sperret for videre bruk. Det er av avgjørende betydning for sikkerheten i nettet at tapte terminaler ikke kan benyttes til uautorisert bruk. Det er derfor viktig at abonnentens representant tar hensyn til dette ved utarbeidelse av bestemmelser for fysisk sikring, ref pkt 4.4 over.

4.7. Forsendelse

Radioterminaler skal sperres for bruk i nettet (deaktiveres) før de sendes mellom forskjellige organisatoriske enheter.

4.8. Reparasjoner

Reparasjon av radioterminaler skal kun utføres over reparasjonsavtaler godkjent av DNK.

5. Kommunikasjonssentraler

Dette avsnittet gjelder kun abonnenter som har betjeningsutstyr for å betjene nødnettet fra kommunikasjonsentralen. Bestemmelsene gjelder utstyr som er tilknyttet nødnettet og berører ikke annet utstyr eller programvare på kommunikasjonsentralen.

5.1. Fysisk sikring

Det påligger abonnentens representant å utarbeide bestemmelser for fysisk sikring av kommunikasjonsentraler som er i operativ bruk. Det skal også utarbeides bestemmelser for fysisk sikring av kommunikasjonsentraler som ikke er i daglig bruk eller i døgndrift.

5.2. Konfigurasjonsendringer

Endringer i konfigurasjonen for den enkelte kommunikasjonsentral, som vil kunne påvirke nødnettets ytelse eller sikkerhet, skal godkjennes av DNK før de iverksettes.

5.3. Applikasjoner

Nye applikasjoner ved kommunikasjonsentralene som kan påvirke belastningen av nødnettet ved økt forbruk av kapasitet skal godkjennes av DNK før de tas i bruk.

5.4. Programvareversjon

Det skal kun benyttes programvareversjoner på kommunikasjonsentraler som er godkjent av DNK for bruk i nødnettet. DNK vil ha oversikter over de til enhver tid godkjente programvareversjoner.

5.5. Service/ Reparasjoner

Reparasjoner på utstyr i kommunikasjonssentralen levert av nødnettet skal kun utføres over godkjente reparasjonsavtaler.

6. Sikkerhetsrevisjon

Sikkerhetsansvarlig skal være ansvarlig for å følge opp at sikkerheten ivaretas ved jevnlig årlige sikkerhetsrevisjoner. Det skal utarbeides en egen plan for sikkerhetsrevisjoner.

Sikkerhetsrevisjonen skal:

- Kontrollere at alle nødvendige sikkerhetstiltak er innført
- Verifisere at sikkerhetstiltakene fungerer etter hensikten

Eventuelle avvik som oppdages skal rapporteres til leder for virksomheten.



Direktoratet for nødkommunikasjon

Postboks 7, Nydalen PIB, 0410 Oslo

Telefon 23 30 57 00, Telefaks 22 23 29 41

www.dinkom.no