Tekniske forberedelser til implementering av responsløsning og trygghetsskapende teknologi

Margrethe Noraas
Kristiansand kommune / KR-IKT

Leveransen

- Utstyr hos tjenestemottaker
  - Trygghetsalarm, eLås, fall-alarm, sensorer, sporingsteknologi mm
- Teknisk driftsløsning (Saas/Skytjeneste)
  - Grensesnitt for teknisk overvåkning og drift. Benyttes av f.eks. vaktmester, teknisk helse eller IT. Tar i mot tekniske signaler fra sensorer og alarmer – viser at utstyret er aktivt og virker. Tar imot feilmelding fra utstyr
- Teknisk responsløsning (Saas/Skytjeneste)
  - Grensesnitt for kommunalt bemannet responssenter (siling og videreformidling av alarmer)
  - Grensesnitt for mobile enheter for utførende tjeneste til hjemmeboende (via responssenter eller direkte
  - Grensesnitt for utførende tjeneste på institusjon (Sykesignalanlegg)
  - Grensesnitt for mobile enheter for pårørende

Mobildekning

- Løsningen kan kreve innendørsdekning på mobilnett. Kontroller om slik dekning er tilfredsstillende i aktuelle bygg (institusjon)
- Særlig relevant dersom det er aktuelt med tale over mobilnettet for alarmer med to-veis-tale.

- (Merk at innendørsdekning på mobilnettet via wifi ikke fullt ut tilfredsstiller alle krav i løsningen).

Wifi – Trådløst nett

- Wifi er ikke del av leveransen, men leveres gjennom den enkelte kommunes egne avtaler på nettverksutstyr/it-utstyr
- Kommuner som ønsker varslingsanlegg for institusjon må på forhånd ha implementert wifi i bygget
- Wifi bør gi dekning inne på beboerrom og i ganger og fellesarealer
- Manglende wifi i institusjon kan medføre forsinkelse i leveranse av varslingsanlegg
- Dersom en ønsker å kjøre tale over wifi for alarmer med to-veis-tale, må wifi-anlegget støtte tale (prioritering etc)

Drift og beredskap - infrastruktur

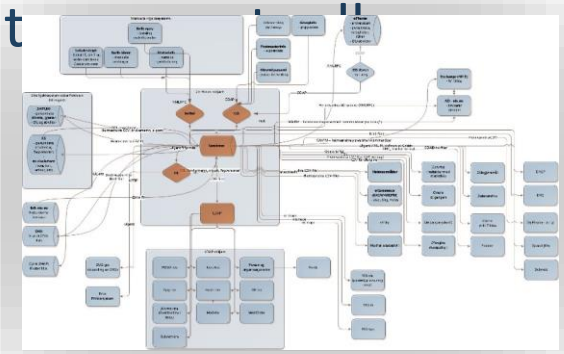
- Redundans i løsninger og høy tilgjengelighet har vært prioritert i anskaffelsen
- Varslingsanlegg på institusjon (SaaS med lokal reserveløsning som sikrer at varslingsanlegget fungerer uavhengig av internettlinjer)
- Wifi og strøm til aktuelt utstyr på institusjon kan være en usikkerhetsfaktor
- Følg opp tilgjengelighetskrav i egen involvert infrastruktur og løsninger
- Kommuner som selv har teknisk drift og overvåkning av trygghetsskapende teknologi (trygghetsalarmer etc) bør ha beredskapsrutiner som ivaretar behovet for feilhåndtering i tråd med direktoratets anbefalinger (99,9% oppetid)
- Vurder å inngå driftsavtaler for lokale servere på institusjoner (lokal server på institusjon er del av skyløsning og sikrer at varslingsanlegg fungerer uavhengig av internett)

Kritisk infrastruktur

- Vurder beredskapsrutiner knyttet til bortfall av mobilnett og annen kritisk infrastruktur med tanke på formidling av trygghetsalarmer og mobile trygghetsalarmer fra tjenestemottakere. Behov for manuelle rutiner?
- Redundans i telelinjer? Vurder mulighet for å ta imot samtaler og ringe ut via to ulike teleleverandører.
- ROS-Analyser

Integrasjoner og «datavask»

- Løsningen skal kunne benytte personalsystemet eller tilsvarende som autorativ kilde for ansatte. Hensikten med dette er å ha brukerbase kun ett sted. Den enkelte kommune må selv bidra inn i dette arbeidet for å få en strukturert brukerdatabase.
- Før etablering av nye løsninger bør data om tjenestemottakere gjennomgås og ryddes etter avtale med leverandøren og legges inn i den nye løsningen.
- Leverandøren vil integrere systemene mot sentralt integrasjonsknutepunkt (eVIK) når dette er klart. Den enkelte kommune er selv ansvarlig for å implement[illegible] endringer i EPJ sammen med sin EPJ-leverandør for integrasjon mot informasjonsknutepunktet.



Sikkerhet og kommunikasjonsløsninger

- Behov for tekniske forberedelser (trafikkruting, sikkerhet og brannmur) for at løsningen skal kunne tas i bruk, eventuelt i samarbeid med leverandøren. Gjelder sikkerhetskrav knyttet til mobile løsninger, skytjenester, autentiseringsmekanismer, kommunikasjonsløsninger, sertifikater mm.
- Behov for tekniske ressurser fra den enkelte kommune i implementeringsprosjektet
- **Etabler tidlig kontakt med egen IT-avdeling!**