SIKKERHETSSTRATEGI

Formål:
Beskrive overordnede regler for sikkerhetsstrategi i Namsos kommune.

Ansvar:
Ansvar er dokumentert i NAKSO.4.03 Sikkerhetsorganisasjon.

1. Informasjonssystemet

All bruk av informasjonssystemet skal skje i forhold til fastlagte prosedyrer og rutiner. Den enkelte databehandler har ansvar for å rapportere avvik, ved f. eks. brudd på rutiner, feil på teknisk utstyr, feil i autorisasjon eller sikkerhetsbrudd. Rapportering skjer til nærmeste overordnede og til informasjonssikkerhetsansvarlig.
Kun utstyr og programvare som eies eller driftes av Namsos kommune, kan inngå i informasjonssystemet. Det skal være utarbeidet konfigurasjonskart som beskriver kommunens informasjonssystem.

2. Samarbeidende virksomheter

Partnere og leverandører skal velges ut fra betraktninger om leverings- og service – dyktighet over tid, produktvurdering og pris. I tillegg skal partnere og leverandørers sikkerhetssystem legges til grunn ved vurderingen.
Forholdet mellom Namsos kommune og partnere/leverandører skal kontraktfestes, og i den grad partner/leverandør har personell som gies tilgang til kommunens informasjonssystem, skal kommunen ha oversikt over dette personellet. Personell fra partnere og leverandører som gies tilgang til Namsos kommunes informasjonssystem skal skrive under taushetserklæring til Namsos kommune.
Namsos kommunes sikkerhet dokumenteres overfor samarbeidende virksomheter med NAKSO.5.13.03 Skjema - Sikkerhetserklæring. Samarbeidende virksomheter skal dokumentere egen sikkerhet overfor Namsos kommune.

3. Personellsikkerhet

Personell som har tilgang til informasjonssystemet skal motta opplæring som gjør dem i stand til å bruke systemet på en sikker måte, og til å ivareta kravet om sikker informasjonsbehandling.
Alt personell som har tilgang til informasjon som er taushetsbelagt, skal skrive under på NAKSO-7.9.07 Taushetsplikt. Alt personell som kan bruker systemet til elektronisk post og Internet skal signere samtykke til at arbeidsgiver skal kunne spore kilde ved ureglementert bruk.
NAKSO.5.6.01 Sikkerhetsinstruks skal følges.

4. Fysisk sikkerhet

Lokaler og utstyr som blir benyttet for behandling av personopplysninger, og dokumenter som inneholder personopplysninger, skal sikres mot uautorisert adgang. Dette gjelder også installasjoner som inngår i kommunens informasjonssystem, som lagringsmedier og kommunikasjonssystemer.
Rutiner for fysisk sikkerhet skal følges.

5. Systemteknisk sikkerhet

Kommunens informasjonssystem er inndelt i soner, som skiller mellom ekstern informasjon, intern informasjon og sensitive personopplysninger. De områder hvor sensitive personopplysninger behandles, er delt inn i samsvar med formålet med behandlingen av personopplysningene.
Kommunen har "delt løsning", som muliggjør at informasjon fra de ulike soner kan leses på samme maskin. Dette krever særlig aktpågivenhet fra driftsenheten i forhold til brannmurer, konfigurasjon, kommunikasjon og nettverksløsninger. Det skal foreligge eget konfigurasjonskart for brannmurene mellom eksterne og interne soner.

6. Dokumentsikkerhet

Dokumenter, eller medier som inneholder personopplysninger (disketter, cd'er, kassetter og lignende), skal være merket på en måte som gjør at disse blir behandlet i tråd med fastsatte rutiner om oppbevaring av personopplysninger, jfr. kvalitetssystemets prosedyre for post, journal og arkiv – føring.

7. Risikovurdering

Det skal føres oversikt personopplysninger som behandles. Oversikten skal benyttes som grunnlag for gjennomføring av risikovurdering.
Med risikovurdering menes en systematisk gjennomgang av forskjellige risikoforhold, bedømme sannsynligheten for at de skal inntreffe og en vurdering av de konsekvenser det vil få om hendelsen inntreffer.

Risikovurdering skal foretas i forhold til den behandlingsansvarliges kriterier for akseptert risiko og de sikkerhetstiltak som er iverksatt. *Akseptert risiko* er hvor grensen for produktet av sannsynlighet og konsekvens overskrider det Namsos kommune, representert ved behandlingsansvarlig, tolererer, jfr. målsetting.

Risikovurdering gjennomføres i hht. "*Rutine for risikovurdering*"

8. Sikkerhetsrevisjon

Det skal gjennomføres periodisk kontroll med virksomhetens arbeid i forhold til informasjonssikkerhet og arbeid med personopplysninger.
Formålet er at kommunens plan for informasjonssikkerhet ved behandling av personopplysninger med tilhørende rutiner etterleves.
Sikkerhetsrevisjonen vil være et viktig bidrag i forbindelse med ledelsens gjennomgang(pkt.9).
Sikkerhetsrevisjon skal gjennomføres minst én gang årlig.
Sikkerhetsrevisjon utføres i hht. NAKSO.5.3.01 Sikkerhetsrevisjon

9. Avvik

Bruk av informasjonssystemet som er i strid med fastlagte rutiner skal behandles som avvik. Jfr. rutine for avviksbehandling.

10. Organisering

Ansvar og myndighet i forbindelse med bruk av informasjonssystemet er beskrevet i NAKSO.4.03 Sikkerhetsorganisasjon, delegasjonsreglementet og stillingsbeskrivelsene.

11. Ledelsens gjennomgang

Ledelsen skal årlig gjennomgå sikkerhetsmål, strategi og organisering av informasjonssystemet. I forbindelse med dette, har man i Namsos kommune utarbeidet en sikkerhetsorganisasjon NAKSO.4.03 Sikkerhetsorganisasjon. Kommunens *sikkerhetsutvalg* og *virksomhetsleder*, skal møtes én gang pr. år for å foreta ledelsens gjennomgang. Gjennomgangen skal bygge på

- resultater/rapporter fra egenkontroller og kontroller utført av offentlig myndighet
- endringer som har betydning for drift av informasjonssystemet eller for informasjonssikkerheten, som:
    - endringer i offentlige sikkerhetskrav
    - endringer i de personopplysninger virksomheten skal behandle
    - endringer i trusselbildet fra gjennomførte risikoanalyser
    - behov for endringer av informasjonssystemet, som følge av endret bruk eller ny funksjonalitet

Ledelsens gjennomgang skal gjennomføres i første kvartal hvert år, slik at evt. beslutninger med økonomisk konsekvens kan innarbeides i kommunens økonomiplan og budsjetter.

Det skal utarbeides *Rapport fra ledelsens gjennomgang*.