



Revisjon:	1.1	Dokumentansvarleg:	Per Erik Akerjordet
Revisjonsdato:	15.02.2008	Godkjent av:	
Godkjent dato:		Signatur:	

**MÅL OG STRATEGI
FOR
IKT-SIKKERHEIT
I
HAREID KOMMUNE**

MÅL FOR SIKKERHEIT

Hareid kommune si overordna målsetting er å yte innbyggjarane teneste med høg kvalitet og samtidig utnytte kommunen sine ressursar optimalt. Bruk av moderne informasjonsteknologi gjer det mogleg å løyse kommunale oppgåver best mogleg. Kommunen sine overordna mål ved elektronisk behandling av personopplysningar skal vere sikker og effektiv sakshandsaming

Hareid kommune sine mål med elektronisk handsaming av personopplysningar er definert gjennom følgjande sikkerheitsmål:

Hareid kommune skal sikre at kommunen sin informasjon har nødvendig grad av

- **konfidensialitet** – for at personopplysningar ikkje skal bli kjende for uvedkomande. Krav om konfidensialitet skal alltid prioriterast framfor krav om tilgjenge.
- **tilgjenge** – slik at sakshandsamar som handsamar sensitive opplysningar kan utføre pålagde arbeidsoppgåver i tillegg til at brukarane av kommunen sine teneste vert gitt den informasjon dei har behov for.
- **kvalitet i alle ledd** – informasjon under handsaminga skal ikkje verte endra ved eit uhell .

Ei spesiell målsetting med informasjonen skal være at den verkar mot tap av:

- - liv og helse
- - personleg integritet
- - truverde
- - økonomi

IKT er av stor strategisk betydning for Hareid kommune. Ei bevisst haldning til IKT kan være med på å

- **auke evna til konkurranse og service.** Dette kan ein oppnå ved å nytte dei rette systema til dei rette oppgåvene. Samstundes må ein passe på at brukarane av systema har kompetanse nok til å nytte dei.
- **skape og utvikle nye teneste til innbyggjarane i Hareid kommune.** Vi kan oppnå dette ved å satse på gode felles- og fagsystem og god tilgang på informasjon t.d. gjennom internett.
- **kvalitet i alle ledd i tenesteproduksjonen.** Gode rapporteringssystem, fagprogram og sakshandsamingsprogram er viktig for å få dette til. Tilgjenge til nødvendige system er ein føresetnad.
- **optimal handsamingstid og effektive verdiskapingsprosessar.** For å få dette til er det avgjerande å ha nødvendig kompetanse og gode nok system for rapportering og sakshandsaming.
- **forenkling i kommunikasjonsmåtar.** Dette gjeld både i forhold til politikarar, publikum og media, samt mot samfunnet elles. (t.d. Kostra-rapportering, kommunikasjon med andre kommuner, leverandørar etc.) Dette kan vi oppnå ved ei sterkare utnytting av E-post og Internett som informasjonsberar.

- **auka motivasjon internt i kommunen.** Ein kan nå dette målet ved å gjere dei nødvendige programma lett tilgjengeleg for dei tilsette, samt auke og vedlikehalde kompetansen til dei tilsette slik at dei får kjensle av å kunne nytte seg godt av dei system kommunen har.
- **Auka tilgang på informasjon til sakshandsamar, leing, publikum, politikarar etc.** Dette målet kan ein oppnå gjennom auka satsing på internett og intranett i heile kommunen

Akseptkriterier:

- Hareid kommune kan ikkje godta at brot på kritiske informasjonssystem overstig eitt pr. måned. Dette gjeld avbrot som ikkje er planlagde. Kvart avbrot skal ikkje overstige ein time utan at det vert gitt beskjed til brukarane om status og vidare framdrift.
- Informasjon om klientar skal alltid gjevast til rett person. Her vil kommunen praktisere **null toleranse**.

STRATEGIAR FOR SIKKERHEIT

IKT-strategien har som mål og gi ei oversikt over kommunen sine samla behov for maskiner, program, sikkerheitstiltak og kompetanse som kan være med å sikre at dei kommunale tenestene vert tilbodne til ein kostnadseffektiv pris basert på innbyggjarane sine behov og kvalitetskrav. IKT-strategien skal sikre prioritering mellom dei investerings-, opplærings-, og utviklingstiltak som vert gjort, og at dette skjer på eit fagleg og økonomisk godt fundert grunnlag.

IKT-strategien skal:

- *Vere leiinga sitt instrument for å styre kommunen sin bruk av IKT.*
- *Vere med på at system og utstyr som vert installert, vert effektivt utnytta, og sikra prioritering på dei områda i kommunen som gir størst nytte.*
- *Danne grunnlag for å treffe nødvendige beslutningar, planlegge og prioritere innkjøp og utvikling samt bruk, drift og vedlikehald av system og utstyr.*

SIKKERHEITSSTRATEGI I HAREID KOMMUNE, GENERELL DEL:

Kvart enkelt område i Hareid kommune har ansvar for å arbeide med informasjonssikkerheit som ein integrert del av den daglege drifta. Det er områdeleiar og avdelingsleiar som har ansvar for å sjå til at informasjonssikkerheit ved handsaming av personalopplysningar vert gjennomført.

Kommunen si sentrale IKT-avdeling er ansvarleg for at driftstekniske oppgåver i tilknytning til informasjonssystem har ei "oppetid" i samsvar med akseptkriteria i denne planen . IKT-systema er bygd opp rundt 3 soner. Ei sone med ope segment for ikkje-sensitiv informasjon som er tilgjengeleg for alle, ei lukka sone med fleire innbyrdes adskilte segment for sensitiv informasjon og ei stor DMZ-sone tilgjengeleg for alle (opa, lukka og internett).

Innanfor lukka sone vil berre brukarar som er autoriserte ha tilgjenge til sensitive

personopplysningar innanfor sitt segment. Ingen brukarar på open sone skal ha tilgang til lukka sone. Ingen sensitiv informasjon skal kunne flyte frå lukka til open sone. Det skal heller ikkje kunne flyte sensitiv informasjon mellom dei lukka segmenta i lukka sone.

Strategi knytt til organisering av informasjonssystemet:

Ansvar og mynde relatert til drift, vedlikehald og utvikling av Hareid kommune sine informasjonssystem er lagt til IKT-leiaren med dei arbeidsoppgåvene som er gitt i stillingsbeskrivelsen

Vidare oppfølging av sikkerheitsarbeidet (IKT-sikkerheitsleiing) er lagt til kommunen sin IKT-sikkerheitsleiar som i Hareid kommune er identisk med IKT-leiaren.

IKT-leiar/sikkerheitsleiar rapporterer til rådmannen.

Hareid kommune si IKT-avdeling står for den daglege drifta også av informasjonssystem som er lokalisert utanfor kommunen sine sentrale lokaler (skular, barnehagar, sjukeheim, helsesenter). Det er i tillegg utpeika lokale kontaktpersonar for informasjonssikkerheit ved desse einingane.

All bruk av informasjonssystemet skal utførast i samsvar med på førehand fastlagde rutiner. Det er den einkilde medarbeidar sitt ansvar å rapportere avvik på t.d. sikkerheit til næraste overordna og til kommunen sin sikkerheitsansvarleg.

Strategi knytt til sikkerheit for partnarar og leverandørar:

Hareid kommune sin bruk av partnarar og leverandørar vert regulert av kontrakter, der også bestemmelsar om informasjonssikkerheit går inn.

Ved valg av partnar eller leverandør vert ikkje berre pris, leveringsdyktigheit og leveranse kvalitet vurdert, men også partnaren/leverandøren si evne til å følge opp og vedlikehalde leveransen over tid.

I den grad personell hos partnar eller leverandør vert gjeve tilgang til utstyr eller program der sensitive personopplysningar vert handsama, tilgjenge til sjølve opplysningane eller til informasjon om sikring av slike opplysningar, - har kommunen oversikt over kva personell dette gjeld. Kommunen skal sørge for at dette personellet har sett seg inn i og underskrive kommunen si teieplikterklæring.

Leverandørar som skal utføre teknisk vedlikehald på utstyr/programvare i Hareid kommune sitt sentrale datarom, skal ikkje opphalde seg i dette romet utan i følgje med personell frå Hareid kommune si IKT-avdeling.

Strategi for personellsikkerheit:

Tilsette som gjennom sitt arbeid skal ha tilgang til informasjonssystemet skal ha naudsynt kunnskap om bruken av informasjonssystemet og skal tilførast naudsynt kompetanse om informasjonssikkerheit.

Tilsette skal berre få tilgang til personopplysningar i den grad det er naudsynt for at dei

skal kunne utføre det arbeid dei er tillagde i Hareid kommune.

Alle nyttilsette i Hareid kommune må sette seg inn i og skrive under erklæring om teieplikt. Ansvar for dette er lagt til Hareid kommune si Personalavdeling v/Personalleiar.

Strategi for fysisk sikkerheit:

Utstyr som vert nytta til handsaming av personopplysningar er sikra mot uautorisert tilgjenge gjennom at sakshandsamar sine lokale er avlåste.

Utstyr som vert nytta til å handsame sensitive personopplysningar er plassert saman med resten av kommunen sitt datautstyr i avlåst datarom.

Berre IKT-avdelinga sitt personell har nøklar til kommunen sitt datarom. Utstyr som går inn i sikkerheitsbarrierer mellom informasjonssystemet sine forskjellige soner er lokalisert i kommunen sitt datarom.

Terminalar og skrivarar som er knytta til lukka segment, er plassert på kontor og avdelingar som er avlåste når dei ikkje er i bruk.

Strategi for systemteknisk sikkerheit:

Hareid kommune sitt informasjonssystem er inndelt i soner som speglar skiljet mellom handsaming av sensitive (lukka sone) og "ikkje-sensitive" personopplysningar (open sone)

Dei delane av informasjonssystemet som handsamar sensitive personopplysningar, er vidare inndelte i samsvar med formålet med handsaminga av personopplysningane/tenestene kommunen leverer. Lukka sone er vidare inndelt i fleire lukka segment som ikkje kan utveksle informasjon seg imellom eller ut i opa sone.

Brukarar i lukka sone skal berre ha avgrensa tilgang til teneste i dei andre delane av kommunen sitt informasjonssystem.

Brukarar som jobbar frå heimekontor har kun tilgang til opa sone. Tilgang frå heimekontor skal konfigurert og godkjennast av IKT-avdelinga. Behovet for slik oppkobling skal vurderast nøye av den tilsette sin områdeleiar.

Strategi for dokumentsikkerheit:

Dokument som inneheld sensitive personopplysningar skal merkast "Untatt offentlegheit" og gjeldande lovheimel skal påførast både det fysiske dokumentet og den elektroniske registreringa i sak/arkiv fagsystem.

Dokument med sensitive personopplysningar vert oppbevart i avlåst arkivskap ved den enkelte avdelinga eller i sentralarkivet.

Konsekvensar ved brot på sikkerheitsreglane

Hareid kommune legg stor vekt på utvikling av sikkerheitsmål og –strategiar. Dette er eit viktig arbeid for dei krava vi stiller til informasjonssikkerheit og datadisiplin. Ein grundig planlagd og gjennomført strategi på dette feltet er ein viktig del av kommunen si verksemd.

Rådmannen føreset at den einskilde tilsette legg vekt på å etterleve dei vedtekne sikkerheitsreglane.

Brot på sikkerheitsreglane (mål og strategi) og vedtekne sikkerheitskrav, vil bli oppfatta som eit tillitsbrot mellom den tilsette og kommunen. Brot på teieplikta eller brot på bestemmelsar i kommunen sitt regelverk vil kunne gje grunnlag for disiplinære reaksjonar mot den tilsette, evt. avsked/oppseiing.

Eg er kjend med Hareid kommune si vektlegging av sikkerheitsreglar og teiepliktbestemmelsar, og stadfester med dette å ha sett meg inn i dei reglar og bestemmelsar som gjeld for Hareid kommune si IKT-sikkerheit:

Stad: Hareid Dato: 21/2-2008

B. K. K. K.
Rådmann