Gáivuona suohkan
Kåfjord kommune
Kaivuonon komuuni

SIKKERHETSHÅNDBOK

for

INFORMASJONSSIKKERHET OG PERSONVERN
i
Kåfjord kommune

m/sikkerhetsmål og sikkerhetsstrategi

November 2022

INNLEDNING

Sikkerhetshåndboken fastlegger Kåfjord kommunes krav til beskyttelse av personopplysninger og øvrige opplysninger som samles inn, lagres, bearbeides, overføres og formidles så vel manuelt som elektronisk.
Denne håndboken finnes også i kommunens ***kvalitetssystem***.

Håndboken utgjør et felles rammeverk for det praktiske arbeid med informasjonssikkerhet og personvern i kommunen, og skal benyttes

- *for at de respektive tjenestesteder i kommunen skal kunne oppnå et nødvendig og riktig sikkerhetsnivå i sin daglige drift*
- *for å skape en felles sikkerhetskultur gjennom nødvendig opplæring og økt forståelse av behovet for informasjonssikkerhet*
- *for å etterleve kravene til informasjonssikkerhet og personvern i Personopplysningsloven, som også inkluderer EU's/EØS' Forordning om personvern, GDPR (General Data Protection Regulation), Helseregisterloven inkl Normen for informasjonssikkerhet, Helse-informasjonssikkerhetsforskriften, Lov om Barnevern, Opplæringsloven og annet relevant lovverk og sikkerhetsprinsippene i ISO 27001-standarden*

Den enkelte leder vil være ansvarlig for at relevant innhold i denne håndboken gjøres kjent blant sine respektive medarbeidere – og at beskrevne, nødvendige tiltak blir iverksatt og fulgt opp.

INNHOLDSFORTEGNELSE

INNLEDNING 2

1. KÅFJORD KOMMUNES SIKKERHETSPOLITIKK 5

1.1 Hvorfor informasjonssikkerhet og personvern i Kåfjord kommune? 5

1.2 Sikkerhetsmål 6

1.3 Sikkerhetsstrategi 7

1.3.1 Organisering 8
1.3.2 Partnere og leverandører 9
1.3.3 Personellsikkerhet 9
1.3.4 Fysisk sikkerhet 9
1.3.5 Systemteknisk sikkerhet 9
1.3.6 Dokumentsikkerhet 10

2 LOVER, FORSKRIFTER M.M. 11

2.1 Lover, forskrifter og bestemmelser 11

SIKKERHETSHÅNDBOK FOR KÅFJORD KOMMUNE 13

3 ORGANISATORISK SIKRING 13

3.1 Ansvar for sikkerheten 13

3.1.1 Kommunedirektøren 13
3.1.2 Sikkerhetsansvarlig 13
3.1.3 Autorisasjonsansvarlig 14
3.1.4 Medarbeidere 14

3.2 Administrative og driftsmessige sikringstiltak 14

3.2.1 Systemplanlegging og -anskaffelse 14
3.2.2 Drift av kommunens IT-systemer 15
3.2.3 Avvikshåndtering og forbedringsordning i kommunen 15
3.2.4 Egenkontroll 16
3.2.5 Ledelsens gjennomgang 16
3.2.6 Avbrudds- og beredskapsplan 16
3.2.7 Utskrifter/dokumenter, kopiering og makulering 17
3.2.8 Sikkerhet og orden på det enkelte kontor 17

3.3 Personellsikkerhet 18

3.3.1 Etiske regler 18
3.3.2 Fast ansatt personell og vikarer med tidsbegrenset arbeid 18
3.3.3 Konsulenter og leverandører av IT-tjenester 19
3.3.4 Servicepersonell (teknikere, håndverkere, rengjøringspersonell etc) 19
3.3.5 Besøkende 19
3.3.6 Taushetsplikt 19
3.3.7 Brudd på reglement/arbeidsavtaler 20

4 SYSTEMTEKNISK SIKRING 20

4.1 Sikkerhetskopiering og oppbevaring av kopier 20

4.2 Aktivitetslogging 20

4.3 Sikringstiltak mot datavirus, spam, hacking etc. 20

4.4 Destruksjon/sletting av sensitive data 21

4.5 Logisk tilgangskontroll 21

4.5.1 Brukeridentifikasjon/autentisering 21

4.5.2 Autorisasjonskontroll 21

4.6 Nettverkssikkerhet og rutiner for bruk av epost i kommunen 22

4.6.1 Rutiner for bruk av e-post 22

VEDLEGG 1 – Viktige sikkerhetsregler *Feil! Bokmerke er ikke definert.*

1. KÅFJORD KOMMUNES SIKKERHETSPOLITIKK

1.1 Hvorfor informasjonssikkerhet og personvern i Kåfjord kommune?

Kommunens økende bruk av data-/informasjonsteknologi (IT) medfører økende teknologisk avhengighet og sårbarhet, dvs. at IT-systemer og -opplysninger må være tilgjengelige når de ansatte har behov for dem. Dette stiller igjen krav til fysiske, system-/IT-tekniske og organisatoriske tiltak for å sikre denne tilgjengeligheten.

Et hovedkrav til kommunens behandling av personopplysninger og andre, viktige opplysninger, er etterlevelse av pålagte regulatoriske bestemmelser, herunder Personopplysningsloven (POL) m/GDPR-forordningen (General Data Protection Regulation), Helseregisterloven, Barnevernloven, Opplærings-loven, Normen for informasjonssikkerhet og i Helseinformasjonssikkerhetsforskriften.

Mulige svakheter (trusler) knyttet til kommunens informasjonssikkerhet og personvern kan bl.a. skyldes interne forhold i kommunen (medarbeidere/utstyr/rutiner, uklare avtaler, manglende opplæring etc.) eller eksterne faktorer.

De eksterne truslene er bl.a. knyttet til ulike konsekvenser som følge av økt bruk av nettverks- og skytjenester etc., mens de interne forhold bør fortsatt vies størst oppmerksomhet bl.a. ved at for liten sikkerhetsforståelse internt kan utgjøre en større trussel enn eksterne forhold.

Konsekvenser ved dårlig eller utilfredsstillende informasjonssikkerhet og personvern i kommunen:

- dersom IT-systemene skulle bli utilgjengelige over tid (for eksempel mer enn én dag) på grunn av feil på nettverk, strømproblemer, tekniske problemer med utstyr, feil i data-systemene, brann etc., vil viktige arbeids- og beslutningsprosesser kunne stoppe opp - med forsinkelser og lav effektivitet som resultat

- eventuelle feil på informasjon/data vil kunne svekke beslutningskvaliteten og bidra til spredning av feilaktig informasjon - med mulige konsekvenser for kommunens interne og eksterne brukere – og for kommunen som sådan

- upålitelig informasjonsbehandling som følge av for dårlig tilgangskontroll, rutinefeil, driftsstans, at viktig/sensitiv personinformasjon/øvrig informasjon kommer på avveie, osv. kan medføre erstatningsansvar og dessuten skade brukernes og omgivelsenes tiltro til kommunen

God informasjonssikkerhet og godt personvern blir derved en stadig viktigere forutsetning for at Kåfjord kommune skal kunne fungere tilfredsstillende og troverdig: hver enkelt medarbeider i kommunen har sin del av ansvaret for dette.

1.2 Sikkerhetsmål

Kåfjord kommune har som sikkerhetsmål at **rett informasjon til rette vedkommende til rett tid** for å sikre forsvarlige tjenester til kommunens innbyggere og brukere. Dette innebærer at informasjonen må sikres tilfredsstillende

- **konfidensialitet** – slik at sensitive person-/klientopplysninger ikke blir kjent for uvedkommende, dvs. at kun autorisert personell skal ha tilgang til slike opplysninger; slik tilgang skal også være sporbar/kontrollerbar

- **tilgjengelighet** – slik at alle medarbeidere med tjenstlig behov skal kunne utføre pålagte oppgaver, samtidig som brukerne av kommunens tjenester – inkl. pasienter og øvrige innbyggere - gis tilfredsstillende service og informasjon.

- **integritet** – slik at opplysningene ikke utilsiktet eller uautorisert endres ved behandling. Det skal være sporbart hvem som har foretatt registreringer, endringer, rettinger og slettinger av opplysninger

- **kvalitet** – slik at sensitive helse- og personopplysninger kan henføres til riktig, identifiserbar person, at de registreres i henhold til avtalte regler og rutiner og at opplysningene er fullstendige, dvs. et resultat av autoriserte handlinger

Sikkerhetsarbeidet i kommunen skal omfatte både **fysiske**, **systemtekniske** og **organisatoriske** sikkerhetsforhold.

- **Fysisk sikring** innebærer i nødvendig grad å sikre kommunens tjenestesteder mot uautorisert adgang, tyveri, brann etc.

- **Systemteknisk sikring** innebærer å sikre teknologikomponentene (IT-utstyr, kommunikasjonslinjer og –utstyr/-løsninger, programvare osv.) og informasjonen (registre etc.) ved hjelp av program- og/eller maskintekniske sikkerhetsmekanismer/-barrierer

- **Organisatorisk sikring** fokuserer på det menneskelige element og det ansvar ledere og medarbeidere har i sikkerhetssammenheng. Sikringstiltakene kan være knyttet til administrative rutiner som ansvars- og arbeidsdeling, opplæring/motivasjon, kontrollrutiner, osv.

- formålet med hver behandling av helse-/personopplysninger i kommunen er å yte forsvarlig helsehjelp og tjenester knyttet til all helse- og omsorgsrelatert klientbehandling, barnevern, oppvekst, sosialytelser, osv.

- sikkerhetsarbeidet skal ivareta hensynet til helse, miljø og sikkerhet og relevante lover og forskrifter, herunder POL inkl GDPR-forordningen (se mer om denne i pkt 2.2)

- sikkerhetsarbeidet skal rette særlig oppmerksomhet mot interne trusler/svakheter

- sikkerhetstiltakene skal beskytte investeringer i teknisk utstyr og innsamlede data mot feil, uhell, tyveri, etc.

- sikkerhetstiltakene skal forebygge uautorisert innsyn i IT-systemer/data og annen ikke-offentlig informasjon

- sikkerhetstiltakene skal redusere konsekvensene og snarest sikre betryggende gjenoppretting til normalsituasjon etter eventuelle feil og uhell - også eventuelle lengre driftsavbrudd/katastrofer

- sikkerhetstiltakene skal sørge for at alle ledere og medarbeidere i kommunen får nødvendig opplæring i alle sikkerhetsrelaterte forhold

1.3 Sikkerhetsstrategi

Informasjonssikkerhet og personvern i Kåfjord kommune er et lederansvar, men den enkelte medarbeider har et selvstendig ansvar for å følge vedtatte regler og vise aktsomhet i sitt daglige arbeid.

Kommunen skal ha et bevisst forhold til den risiko som gjelder ved elektronisk behandling av person-/klientopplysninger og annen viktig/sensitiv informasjon.

Kommunen er underlagt krav til informasjonssikkerhet og personvern i POL m/GDPR-forordningen, i Helseregisterloven, Normen for informasjonssikkerhet og Helseinformasjonssikkerhetsforskriften, og er i tillegg underlagt krav om profesjonsbestemt taushetsplikt bl.a. etter Forvaltningsloven, Opplæringsloven, Barnevernloven, Lov om Innkreving av skatter og avgifter, Arkivloven, Sosialtjenesteloven og Helsepersonelloven.
All behandling av personopplysninger skal være i samsvar med disse krav og lover.

Ved behandling av sensitive personopplysninger skal kravet til konfidensialitet ikke vike til fordel for kravet til tilgjengelighet.

Denne håndboken med diverse vedlegg og kommunens øvrige rutiner for bl.a. håndtering av avvik, omhandler de grunnleggende prinsipper og rutiner knyttet til informasjonssikkerhet og personvern i kommunen, dvs. styrende (f.eks. retningslinjer), gjennomførende (f.eks. etablerte rutiner) og kontrollerende (f.eks. gjennom evalueringer).

Omfanget av gjennomførende og kontrollerende rutiner i kommunen vår må vurderes i sammenheng med risikoen for de registrertes rettigheter ved behandling av personopplysninger; avgjørende her er altså ikke mulig risiko knyttet til kommunens verdier ved slik behandling.

Disse rutiner og prinsipper er i overensstemmelse med kravene til internkontroll i POL inkl. GDPR og annet relevant, nasjonalt sikkerhetsregelverk, og skal sikre at personvernet og sikkerhetsarbeidet for øvrig i kommunen blir en kontinuerlig prosess - ivaretatt på en systematisk og dokumentert måte.

Internkontroll representerer kommunens kvalitetssystem, styringssystem eller ledelsessystem for etterlevelse av regelverk. Internkontroll er med andre ord **ledelsens** verktøy for å kunne ivareta sitt ansvar og etterleve lover og forskrifter inkl. personvernregelverket, og **medarbeidernes** verktøy for å kunne utføre sine oppgaver på en forsvarlig og sikker måte.

Tiltak knyttet til kommunens internkontroll skal forbedres, dokumenteres og oppdateres ved behov.

Kåfjord kommune skal som behandlingsansvarlig virksomhet i overensstemmelse med kravene i Personopplysningslovens (POL) GDPR-forordning, spesielt artikkel 30, registrere **protokoller over behandlingsaktiviteter** som utføres under vårt ansvar; herunder behandling av opplysninger knyttet til kommunens barneverntjeneste, helse-/omsorgstjeneste, skole-/oppvekst-tjeneste, osv.

Norske kommuner utfører i all hovedsak de samme behandlinger og vil derfor ha behandlingsprotokoller med tilnærmet samme innhold; antallet slike protokoller vil ligge på mellom 150 og 200 i de fleste kommuner i landet.

Innholdet i disse protokoller vil ifølge GDPR-artikkel 30 nr 1 bl.a. være knyttet til

- Formålet med behandlingen
- Behandlingsgrunnlag, lovreferanse etc.
- Kategorier av registrerte
- Kategorier av opplysninger i behandlingen
- Hvem opplysningene deles med
- Hvor opplysningene innhentes fra
- Hvor opplysningene lagres
- Hvor lenge opplysningene lagres

Ved kommende forvaltningsrevisjoner og ved kontrolltilsyn fra Datatilsynet vil det bli økt fokus på kravet til registrering av behandlingsprotokoller. Kåfjord kommune vil benytte kvalitetssystemet Compilo for å registrere, administrere og oppdatere de nødvendige behandlingsprotokoller. Det vil være viktig at dette arbeidet prioriteres, og at de respektive tjenesteledere med sine avdelinger engasjerer seg her – med NorIKT som en teknisk og koordinerende støttefunksjon

1.3.1 Organisering

Kommunedirektør har det overordnede ansvar (behandlingsansvaret) for informasjonssikkerheten og personvernet i kommunen.

Overordnet operativt ansvar for disse områdene er tillagt sikkerhetsansvarlig; Avdelingsleder for Servicekontoret og Arkivleder.
Denne funksjonen skal videreutvikle og overvåke arbeidet med informasjonssikkerhet og personvern i kommunen. I forhold til personvern, skal det også etableres rutiner som sikrer at personvernombudet på riktig måte og til rett tid involveres i relevante problemstillinger som gjelder vern av personopplysninger.

Den enkelte virksomhetsleder har i tillegg et selvstendig ansvar for gjennomføring av sikringstiltak og oppfølging knyttet til kommunens arbeid med disse områdene.

Kommunens informasjonssystem (dvs. den totale IT-løsning) skal konfigureres og dokumenteres slik at tilfredsstillende informasjonssikkerhet og personvern oppnås.

Bruk av IT-systemene skal skje i overensstemmelse med fastlagte rutiner og retningslinjer, og det er den enkelte medarbeiders ansvar å rapportere eventuelle avvik, f.eks. sikkerhetsbrudd, til nærmeste overordnede.

1.3.2 Partnere og leverandører

Kommunens bruk av leverandører og eventuelle partnere skal reguleres av skriftlige kontrakter, hvor det også skal inngå bestemmelser om informasjonssikkerhet og personvern.

Kommunens krav til informasjonssikkerhet og personvern ved ulike leveranser vil kommunen dokumentere i en egen Kravspesifikasjon for sikkerhet (KSS). Denne vil bl.a. inneholde krav til rutiner for logging for kontroller av ulike feilsituasjoner ved mistanke om uautorisert tilgang, etc. I KSS skal det også tydeliggjøres hva aktuelt IT-system/-utstyr skal benyttes til, hvilke krav i relevant lovverk som må etterleves, osv.

Kommunen skal ha tilgang til sikkerhetspolicy hos relevante leverandører og partnere og skal jevnlig forsikre seg om at denne policy gir tilfredsstillende informasjonssikkerhet og personvern. Leverandør og partnere som har avgitt nødvendige erklæringer (herunder om taushetsplikt) og inngått nødvendige avtaler med kommunen, skal kunne utføre avtalt, tidsbestemt fjernbetjent vedlikehold og oppgraderingsarbeid på kommunens IT-systemer.

1.3.3 Personellsikkerhet

Alle medarbeidere som har tjenstlig tilgang til IT-systemene skal ha nødvendige autorisasjoner for slik tilgang, og skal ha tilstrekkelig kunnskap om bruken av de respektive systemer og om kravene til informasjonssikkerhet og personvern i kommunen.

Medarbeidere skal kun gis tilgang til sensitive personopplysninger i den grad dette er nødvendig for å utføre pålagte oppgaver, og alle medarbeidere skal være informert om den taushetsplikt som gjelder. Kompetansehevende tiltak for å redusere kritisk avhengighet av nøkkelpersonell skal prioriteres.

1.3.4 Fysisk sikkerhet

Det skal treffes tiltak på kommunens tjenestesteder for å sikre mot uautorisert adgang til lokaler som ikke er åpne for publikum.

Utstyr for behandling av person-/klientopplysninger og annen informasjon, som ikke skal være tilgjengelig for uautorisert personell, skal være tilfredsstillende sikret mot fysisk adgang fra uvedkommende.

1.3.5 Systemteknisk sikkerhet

Kommunens IT-systemer skal inneholde mekanismer for logisk tilgangskontroll for å sikre at kun godkjente (autoriserte) brukere har tilgang til systemene.

IT-behandling i avdelinger der det behandles sensitive person-/ klientopplysninger, skal være beskyttet mot innsyn fra ikke-autorisert personell.

Eksterne oppkoblinger skal kun skje i overensstemmelse med kommunens IKT-avdeling; dette omfatter også eventuell oppkobling av hjemmekontor og bruk av bærbart/mobilt datautstyr.

Ved salg, kassering eller annen avhending av IT-utstyr skal det foretas forsvarlig (nødvendig) sletting av data; IKT-avdelingen har ansvaret for at dette håndteres på tilfredsstillende måte.

1.3.6 Dokumentsikkerhet

Rutiner for bruk av kommunens IT-systemer og annen informasjon av betydning for sikkerheten og personvernet, skal i nødvendig grad dokumenteres og være tilgjengelige på intranettet; kopier av slik dokumentasjon skal i tillegg oppbevares på annet sikkert sted ('fjernlager').

Detaljerte beskrivelser av kommunens sikringstiltak og rapporter fra risikovurderinger og eventuelle andre egenkontroller, sikkerhetsrevisjoner og ledelsens oppfølging skal unntas offentlighet.

Kommunens sikkerhetspolitikk er godkjent den 05.12. 2022

Trond Arne Hoe
Kommunedirektør Kåfjord kommune

Gáivuona suohkan
Kåfjord kommune
Kaivuonon komuuni
Suohkandirektevra
Kommunedirektør

2 LOVER, FORSKRIFTER M.M.

2.1 Lover, forskrifter og bestemmelser

For kommunens informasjonssikkerhet gjelder en rekke lover og bestemmelser som bl.a. tar sikte på å hindre at noen uten lovlig hjemmel får tilgang til personopplysninger, herunder opplysninger underlagt meldeplikt eller øvrige informasjoner unntatt offentlighet. Alle berørte ledere og medarbeidere skal gjøres kjent med og følge det til enhver tid gjeldende lovverk.

Følgende lover og bestemmelser har relevans for så vel dokument- som databehandling i Kåfjord kommune:

- **Personopplysningsloven (POL)** gjeldende fra 20.juli 2018 inkl GDPR-forordningen. Se punktet nedenfor.

- **EU/EØS-forordningen GDPR** om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. I praksis erstatter GDPR de tidligere forskriftene til Personopplysningsloven i vårt land. I pkt 2.2. gis en nærmere orientering om GDPR

- § 15 i **Lov om helseregistre og behandling av helseopplysninger** (Helseregisterloven) av 5. april 2001 og **Helsepersonelloven** og **Pasient- og brukerrettighetsloven** vedrørende bl.a. behandling av klient-/pasientdata og taushetsplikt for helsepersonell

- **Normen for informasjonssikkerhet** fra 28. juni 2006 med senere endringer - ref www.normen.no

- **Helseinformasjonssikkerhetsforskriften** (http://www.lovdata.no/for/sf/ho/xo-20110624-0628.html

- **Helse- og omsorgstjenesteloven,** §6-7 i **Lov om barnevern** og §18-4 i **Lov om folketrygd** omhandler alle kravet om taushetsplikt

- **Kommuneloven**

- **Opplæringsloven**

- **Lov om innkreving av skatter og avgifter**

- **Lov om vergemål for umyndige**

- **Arbeidsmiljøloven**

- **Forvaltningsloven** av 10. februar 1967 inneholder bl.a. saksbehandlingsregler for forvaltningen, herunder regler om habilitet for saksbehandlere. Denne loven inneholder også regler om taushetsplikt (§§13-13e), om informasjons- og veiledningsplikt, om varsling og innsyn og om klager og omgjøring av enkeltvedtak

- **Offentleglova** inneholder bestemmelser om i hvilken grad forvaltningens saksdokumenter skal være tilgjengelige for offentligheten. Hovedregelen er at dokumentene er tilgjengelige, hvis ikke denne loven eller andre lover bestemmer noe annet. Offentlighetsloven har også en bestemmelse som sier at selv om forvaltningen kan hindre offentlig innsyn, skal det vurderes om dokumentene allikevel skal gjøres tilgjengelige hvis det kommer en forespørsel; dette kalles meroffentlighet

- **Lov om opphavsrett (Åndsverkloven)** av 12.5.1961, jfr. EU's direktiv om rettslig beskyttelse av edb-program

- **Lov om elektronisk (digital) signatur**

- **Straffeloven**, der bl.a. §121 omhandler kravet til taushetsplikt for bl.a. kommunalt ansatte

- **Forskrift om revisjon** av 13.01.93, spesielt § 11.2

- **Forskrift om internkontroll - Helse, Miljø, Sikkerhet (HMS)**

- **Lov om arkiv** av 4.12.1992 og tilhørende forskrifter

- **Sikkerhetsloven** av 20. mars 1998, omhandler opplysninger som er av betydning for rikets selvstendighet og sikkerhet, dvs skjermingsverdig informasjon. Loven gjelder alle forvaltningsorgan, herunder kommuner. Loven er rettet mot å hindre at konfidensielle opplysninger kommer på avveie – ved bruk av nødvendig/aktuell sikkerhetsgrad. Loven omfatter også sikring av IT-systemer og datanett som må underlegges sikkerhetsgradering. Loven erstatter det tidligere Datasikkerhetsdirektivet. Følgende sikkerhetsgrader benyttes:

    - STRENGT HEMMELIG
    - HEMMELIG
    - KONFIDENSIELT
    - BEGRENSET

Øvrige bestemmelser:

- **Personalreglementet for Kåfjord kommune**
- **Arkivplan for kommunen**
- **Anskaffelsesreglementet for kommunen**
- **Kommunens IKT-strategi**
- **Kommunens Kvalitetssystem**

SIKKERHETSHÅNDBOK FOR KÅFJORD KOMMUNE

3 ORGANISATORISK SIKRING

3.1 Ansvar for sikkerheten

Kommunedirektør Trond Arne Hoe har det overordnede ansvar (behandlingsansvaret) for informasjonssikkerheten og personvernet i kommunen.

Overordnet operativt ansvar for disse områdene – som kommunens sikkerhetsansvarlig - er tildelt avdelingsleder for Servicekontoret og Arkivleder Greta S Larsen; ref her også pkt 3.1.2.

3.1.1 Kommunedirektøren

Kommunedirektøren plikter å ha tilfredsstillende kunnskap om bl.a. Personopplysningsloven og Helseregisterloven og har i sikkerhetssammenheng det overordnede ansvaret for:

- å etablere tiltak for **internkontroll** for informasjonssikkerhet og personvern innen alle tjenesteenheter i kommunen
- å påse at det ved behov foretas vurdering av sikkerhetsbehov og gjennomføring av nødvendige sikringstiltak i tråd med lover/forskrifter og eget sikkerhetsregelverk
- at det operative ansvaret for informasjonssikkerheten og personvernet er definert og tilrettelagt
- at forholdene legges til rette på en slik måte at alle ledere kan ivareta sitt sikkerhetsansvar
- at forholdene legges slik til rette at alle medarbeidere får den nødvendige sikkerhetsforståelse og –kunnskap, slik at de kan ivareta sitt personlige sikkerhetsansvar
- at kommunen følger opp at personvernombudets arbeid blir respektert, etterlevd og fulgt opp

3.1.2 Sikkerhetsansvarlig

Det sentrale sikkerhetsansvaret i kommunen innebærer bl.a. følgende ansvar/oppgaver:

- skal sørge for at kommunens internkontrollsystem følges opp og etterleves av alle ledere
- skal i samarbeid med kommunedirektøren sørge for at alle behandlinger av personopplysninger i kommunen blir registrerte i såkalte **behandlingsprotokoller**; kommunen vil benytte verktøyet Compilo til dette arbeidet
- skal påse at det foretas nødvendig sikkerhetsopplæring i alle enheter og avdelinger
- skal påse at **virksomhetsenhetene** vurderer konsekvensene for personvernet **før** behandlingen av personopplysninger starter (eks et nytt IT-system) ved å gjennomføre en DPIA - Data Protection Impact Assessment. Etter at dette er gjort, skal personvernombudet se gjennom/vurdere og godkjenne denne – **før** behandling settes i gang
- skal påse at det ved behov gjennomføres nødvendige risikovurderinger og eventuelt andre egenkontroller

3.1.3 Autorisasjonsansvarlig

Autorisasjonsansvarlig er den person som har fullmakt til å bestemme hvilke medarbeidere som skal ha hvilke tilgangsrettigheter til de respektive IT-systemer og registre. Dette ansvaret er lagt på ledernivå. Autorisasjonsansvarlig skal bl.a. sørge for

- autorisasjon til IT-systemene, dvs. bestemme og registrere hvilke rettigheter medarbeidere skal ha med hensyn til å kunne registrere, oppdatere og lese informasjon i de respektive IT-system
- kontroll med at ingen uvedkommende får tilgang til IT-systemer og data (uvedkommende kan i denne sammenheng også være egne ansatte)
- å melde ut brukere ved arbeidsopphør evt. stillingsendringer
- at lovpålagte krav etterleves for de respektive IT-systemer og personopplysninger

Tilgangsrettigheter tildeles via autorisasjonsskjema; som ikke er gyldige uten skriftlig signatur fra autorisasjonsansvarlig. IKT-avdelingen sørger for tilgang til nettverk og servere, mens de respektive autorisasjonsansvarlige oppretter (og endrer/sletter) tilganger til fagsystemene.

3.1.4 Medarbeidere

Alle ansatte og innleide medarbeidere i kommunen skal overholde vedtatte instrukser og bestemmelser. Et effektivt sikkerhetsarbeid er avhengig av alle medarbeideres lojale holdning og aktive engasjement. Alle medarbeidere skal derfor:

- forstå viktigheten av sikkerhet i forbindelse med eget arbeid
- praktisere og etterleve vedtatte sikkerhetsbestemmelser og -tiltak
- være ansvarlig for kvaliteten på det arbeid de utfører
- forstå konsekvensen ved eventuelle brudd på taushets- og sikkerhetsbestemmelsene

Den enkelte leder har ansvaret for å følge opp at medarbeiderne får den nødvendige kunnskap og informasjon om data-/informasjonssikkerhet.

3.2 Administrative og driftsmessige sikringstiltak

3.2.1 Systemplanlegging og -anskaffelse

I forbindelse med anskaffelse av nye IT-systemer skal det utarbeides en kravspesifikasjon for sikkerhet (KSS); denne bør bl.a. inneholde krav til innebygget personvern, krav til rutiner for logging av ulike feilsituasjoner, ved mistanke om uautorisert tilgang, etc. Kommunen er oppmerksom på at ikke alle leverandører tester ut sine respektive systemer/applikasjoner like godt, og har spesifisert dette tydelig i sine avtaler. Datatilsynet nevner dette som et økende problem og ber også behandlingsansvarlig virksomhet stresse dette ansvaret spesielt overfor de aktuelle leverandører i forbindelse med anskaffelse av nye systemer/applikasjoner.
Først når akseptansetest er godkjent av ansvarlig leder/autorisasjonsansvarlig i samarbeid med NorIKT, kan systemet settes i drift.

3.2.2 Drift av kommunens IT-systemer

NorIKT as har ansvaret for driften av kommunens IT-systemer, herunder bl.a.:

- installasjon, overvåking og drift av IT-systemer, IT-utstyr og nettverk i nødvendig samarbeid med aktuelle leverandører
- vurdering og implementering av nødvendige fysiske, organisatoriske og systemtekniske sikkerhetstiltak, herunder backup-rutiner, beredskapsrutiner, dataviruskontroller, nett-verkssikkerhet/kryptering, kapasitet/ redundans på nettverk, konfigurasjonsstyring, osv.
- brukerstøtte ved ulike feilsituasjoner
- oppfølging av responstider og eventuelle problemer knyttet til dette
- nødvendig sikring av PC-er, annet mobilt datautstyr og -enheter, datanettverk, servere og øvrig, relevant IT-utstyr som er plassert i kommunens lokaler
- påse at IT-systemene med tilhørende infrastruktur tilfredsstiller relevante sikkerhets- og kvalitetsmessige krav i lover og forskrifter
- informasjon og opplæring/brukerstøtte knyttet til kommunens IT-systemer og sikkerhet
- etablering og oppfølging/kontroll av autorisasjons- og tilgangskontroll-rutiner i samarbeid med de respektive system-/autorisasjonsansvarlige
- etablering av nødvendige planer for avbrudds-/beredskap for kommunens IT-systemer
- informasjon og opplæring knyttet til datarelaterte sikkerhetsforhold i kommunen

3.2.3 Avvikshåndtering og forbedringsordning i kommunen

Personvernbrudd/-avvik representerer et brudd på kommunens sikkerhet som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

GDPR-artikkel 33 og 34 beskriver hvordan den behandlingsansvarlige skal håndtere personvernavvik.
Etter artikkel 33 nr. 5 skal den behandlingsansvarlige
«dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det»
Videre må den behandlingsansvarlige etter artikkel 33 nr. 1
«senest 72 timer etter å ha fått kjennskap til det, melde bruddet til Datatilsynet, med mindre bruddet sannsynligvis **ikke** vil medføre en risiko for fysiske personers rettigheter og friheter»
Videre følger det av artikkel 34 nr. 1 at
«Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en **høy risiko for fysiske personers rettigheter og friheter**, skal den behandlingsansvarlige uten ugrunnet opphold underrette den **registrerte** om bruddet».

Kommunen skal også ha rutiner for rapportering, registrering og oppfølging av **øvrige** feil/mangler, dvs. **avvik** som oppstår (IT-relaterte, HMS-relaterte etc.), inklusive forslag til konkrete forbedringer.

Dette innebærer at kommunen må sikre at personvernavvik og øvrige avvik både avdekkes, dokumenteres og håndteres i samsvar med personvern-bestemmelsene og øvrige rutiner og bestemmelser, hvilket igjen krever at kommunen må ha et avvikssystem som dekker håndteringen av alle typer avvik.

Avviksrutinene i kommunen må tydeliggjøres overfor alle ledere og ansatte for øvrig, da flere avvik som rapporteres gjelder driftsrelaterte feil etc. som blir rettet raskt, men som ikke blir ajourført/meldt som løst i avvikssystemet. Kommunen bør derfor utarbeide eksempler på hvilke feil etc. som bør meldes som avvik – og hvilke som **ikke** skal rapporteres her. Dette vil både gi en bedre, mer effektiv og riktigere avviksrapportering – og en større respekt for avvikssystemet i hele organisasjonen.

Ved eventuelle kritiske feil, mangler eller avvik skal strakstiltak som reduserer og forebygger skadevirkninger vurderes.

Håndteringen av avvik og forbedringsordningen i kjølvannet av dette, må brukes konstruktivt og ikke bidra til å 'henge' ut medarbeidere. Rapporter som gjelder medarbeidere, bør alltid anonymiseres i forhold til de informasjoner som legges ut på intranettet.

Avvikshåndteringen inklusive forbedringsordningen skal motivere til at kommunen **lærer** av de feil og avvik som oppstår, **korrigerer** de feil og uønskede hendelser som inntreffer, og **forbedrer** organisasjonen og rutinene for å **redusere** antallet feil og avvik.

3.2.4 Egenkontroll

Kommunen skal minst årlig gjennomføre egenkontroll av at rutiner for håndtering av personopplysninger og for informasjonssikkerhetstiltak er i bruk og fungerer etter hensikten ved alle tjenestesteder.
Sikkerhetsansvarlig sørger for at egenkontrollskjema blir oppdatert etter Ledelsens gjennomgang og forøvrig ved behov som følge av avviks- og endringshåndtering.

3.2.5 Ledelsens gjennomgang

Kommunens ledelse skal jevnlig – og helst årlig – gjennomgå sikkerhetsmål og sikkerhetsstrategi for å vurdere ledelsens beslutninger opp mot kommunens behov for informasjonsteknologi og informasjonssikkerhet. Resultat fra sikkerhetsrevisjoner og egenkontroller vil danne en viktig del av grunnlaget for slike gjennomganger.

3.2.6 Avbrudds- og beredskapsplan

Det er en økende avhengighet av at IT-systemene i kommunen er tilgjengelige for brukerne når de trenger dem; selv korte avbrudd vil for enkelte brukergrupper innebære store ulemper/problemer. Årsakene til avbrudd kan skyldes feil på datautstyr og i datasystemer, brudd i datakommunikasjon (eksterne/interne årsaker), brann/branntilløp, strømavbrudd, etc.

For å håndtere eventuelle feil i nettverk, datasystemer og lokalt og desentralt datautstyr så raskt og riktig som mulig, skal kommunen i samarbeid med NorIKT snarest utarbeide en plan over hvordan mulige feil -/avbrudds-situasjoner skal håndteres best mulig. Dette inkluderer med andre ord også beredskapsløsninger i NorIKT. Tiltak knyttet til dette skal sikre at kommunens brukere normalt vil ha IT-tilgang kort tid etter avbrudd.

I tillegg til tekniske, IT-relaterte tiltak, vil kommunen i beredskapssituasjoner også være helt avhengig av at organisasjonen for øvrig - som viktige ledd i kommunens totale beredskapsløsning - reagerer raskt og riktig; herunder

- at det er etablert klare ansvarsforhold og organisering i en alvorlig avbruddssituasjon, herunder et katastrofe-/beredskapsteam
- at ledere/medarbeidere er kjent med og tilgjengelige for å håndtere ulike avbruddssituasjoner er så raskt og riktig som mulig
- at det er etablert klare regler/instrukser for strakstiltak og aksjonering dersom ulike feil-/avbruddssituasjoner skulle oppstå:

    - brann, vannlekkasje, etc.
    - tekniske uhell/avbrudd
    - strømstans/overspenning
    - sensitive data på avveie, presseoppslag
    - innbrudd/hærverk/sabotasje

3.2.7 Utskrifter/dokumenter, kopiering og makulering

Kommunen er i gang med å ta i bruk skrivere med sikker print-funksjon, dvs at den som skal aktivere sin egen skriverkø (normalt) må stå fysisk ved skriveren og taste eget passord evt. bruke kort her – og stå ved skriveren til utskrift er ferdig. Der slike skrivere er tatt i bruk, vil vi (sterkt) anbefale at passord-autentisering etc. på skriver **ikke** kan/bør velges bort. Sikker print vil representere et svært viktig sikkerhetstiltak og gi et 'løft' ift god sikkerhet på tjenestestedene. Det vil også redusere behovet for antallet skrivere i kommunen og muliggjøre plassering i sentrale områder der også uvedkommende, besøkende etc. tidvis kan passere; det skal jo **ikke** ligge uavhentede utskrifter her. Vi vil imidlertid anbefale at det på tjenestesteder der det tidvis kan være store – og sensitive – print-filer, bør vurderes å beholde en av de 'lokale' skrivere – på innelåst rom. Ett eksempel her er i barnevernsavdelingen.

3.2.8 Sikkerhet og orden på det enkelte kontor

Den enkelte medarbeider i kommunen har selv ansvaret for sikkerheten på eget kontor/egen arbeidsplass.

Dette forutsetter igjen

- at passord etc. beskyttes (dette er den enkelte ansattes egen sikkerhetsnøkkel)
- at PC/tynn klient slås av etter endt arbeidsdag – at viktige dokumenter etc ikke ligger åpent tilgjengelige
- at fortrolige dokumenter ikke kastes i papirkurv, men makuleres
- at kontordør – der dette er mulig - avlåses når kontoret ikke er bemannet; dette gjelder spesielt på steder der det foregår behandling av sensitiv informasjon at uvedkommende ikke har adgang til kontorlokaler når eget personell ikke er tilstede

3.3 Personellsikkerhet

3.3.1 Etiske regler

Kommunen legger stor vekt på redelighet, ærlighet og åpenhet i all sin virksomhet.

Alle ansatte har et selvstendig etisk ansvar for egne handlinger, og skal ta avstand fra enhver uetisk forvaltningspraksis; eksempler på dette kan være:

- handlinger som krenker noens rettsvern
- handlinger som tilgodeser noen på en uberettiget måte

Alle ansatte plikter å overholde de etiske regler som gjelder i kommunen:

All informasjon som gis i forbindelse med virksomhet for kommunen, skal være korrekt og pålitelig og ikke med hensikt gis tvetydig formulering. Ansatte og folkevalgte skal opptre profesjonelt og med respekt og representere kommunen på en god måte både internt og eksternt.

Kollegaer:
Alle ansatte skal ta sin del av ansvaret for et godt og inkluderende arbeidsmiljø og behandle hverandre med respekt. Det forventes at det ikke snakkes nedsettende om kollegaer som ikke er til stede og kan svare for seg. Mobbing og trakassering er ikke tillatt på noe nivå.

Innbyggere/ brukere:
Innbyggere og brukere skal møtes med respekt og høflighet. Ansatte skal opptre profesjonelt overfor brukere, og legge vekt på forsvarlig saksbehandling og sikre partenes rett til å uttale seg.

3.3.2 Fast ansatt personell og vikarer med tidsbegrenset arbeid

Medarbeidere på alle nivåer skal gjennomgå behovstilpasset opplæring i bruk av IT og i informasjonssikkerhet.

Samtlige medarbeidere skal som et minimum gis en orientering om kommunens sikkerhetsmål og retningslinjer for informasjonssikkerhet.
Kompetansehevende tiltak for å redusere kritisk avhengighet av nøkkelpersonell bør prioriteres.

Autorisasjonsansvarlig skal vurdere hvilke autorisasjoner, dvs tilgangsrettigheter vedkommende skal ha til de(t) respektive IT-system. Autorisasjonsansvarlig skal selv kunne legge inn nødvendige tilgangsrettigheter etc. i de respektive IT-systemene/applikasjonene. NorIKT tildeler brukeridenter, passord osv.
Ved ansettelsesopphør skal tilgangsrettigheter, passord etc slettes umiddelbart. Nøkler og eventuelle andre kommunale eiendeler skal innleveres. Ved endring av stilling etc. skal også tilgangsrettighetene vurderes endret. Ansvaret for dette ligger hos nærmeste leder.

3.3.3 Konsulenter og leverandører av IT-tjenester

Alle eksterne rådgivere, konsulenter og leverandører av IT-tjenester til kommunen, skal før arbeid tar til ha regulert sin tjenestetilknytning med et kontraktsforhold; dette skal også omfatte krav til taushetsplikt.
For konsulenter etc. som vil kunne få tilgang til sensitive personopplysninger, stilles det ekstra krav til konfidensiell behandling av slike opplysninger. Innleide medarbeidere og samarbeidspartnere skal ha tilgang til opplysninger etter 'need to know'-prinsippet og det bør i ettertid være mulig å foreta kontroller av at ingen eksterne brukere har gått ut over sine tidsavgrensede tilgangsmuligheter og –rettigheter – bl.a. gjennom stikkprøvekontroller. At slike kontroller kan bli foretatt, bør i forkant opplyses til alle aktuelle leverandører.

3.3.4 Servicepersonell (teknikere, håndverkere, rengjøringspersonell etc)

Servicepersonell som ikke er ansatt, men som engasjeres av kommunen, f.eks.

- håndverkere
- elektrikere
- evt. rengjøringspersonell

skal også følge kommunens sikkerhetsbestemmelser i sitt arbeid for kommunen.
Uten visse regler og en viss kontroll vil risikoen for at informasjoner kan komme på avveie og muligheter for tyveri etc. øke.
Det bør derfor være et overordnet prinsipp at innleid personell ikke har adgang til lokaler, utstyr og informasjoner, når ansatte selv ikke er tilstede.

3.3.5 Besøkende

Kommunens ulike enheter og lokaler er i hovedsak lett tilgjengelige; dette representerer på mange måter en god, nødvendig og positiv løsning både for ansatte, besøkende/ publikum og klienter/brukere. Samtidig behandles og lagres det informasjon i kommunen som hverken skal eller bør være tilgjengelig for uvedkommende personell. Tilsvarende gjelder datautstyr og annet utstyr.

For å sikre følsomme data, dokumenter og utstyr i nødvendig grad mot uvedkommende/ besøkende, bør derfor aktuelle kontorer på steder der uvedkommende vil kunne oppholde seg uten nødvendig kontroll, avlåses når de ikke er bemannet – også ved kortere fravær som lunsjpauser etc. Kopirom og rekvisita rom etc. bør også skjermes/sikres tilsvarende.

3.3.6 Taushetsplikt

Ved ansettelse i fast stilling eller vikariat i kommunen skal arbeidstaker undertegne arbeidsavtale, hvor ett eksemplar går til arbeidstaker og ett til arbeidsgiver; som del av arbeidsavtalen inngår også taushetserklæring.

Overholdelse av taushetsplikten er spesielt viktig i tilfeller der det vil kunne være til skade for en person dersom opplysninger om personen kommer uvedkommende i hende.
Med skade menes her problemer med hensyn til personlig integritet, helse, omdømme, rettigheter, osv.
Det er straffbart å bryte denne taushetsplikten etter straffelovens §121; straffen kan være bøter eller fengsel inntil 6 måneder.

Taushetsplikten gjelder også etter at ansettelsesforholdet har opphørt. Kommunen har utarbeidet skjema for dette og som begge parter signerer. Tilsvarende gjelder for innleide konsulenter, håndverkere etc.

3.3.7 Brudd på reglement/arbeidsavtaler

Sikkerheten i kommunen er en svært viktig del av ansvaret til hver enkelt arbeidstaker, og begrensningen av risiko for feil, uhell, dårlig kvalitet, osv. er nært knyttet til den enkeltes holdning og årvåkenhet, samt praktisering av gjeldende sikkerhetsbestemmelser.

For å beskytte kommunens informasjoner og øvrige verdier er det derfor av største viktighet at alle medarbeidere utviser aktsomhet i sitt arbeid.

Eventuelle brudd på disse bestemmelser skal meddeles nærmeste overordnede; slike brudd kan også få konsekvenser for arbeidstakers ansettelsesforhold i kommunen.

4 SYSTEMTEKNISK SIKRING

4.1 Sikkerhetskopiering og oppbevaring av kopier

Sikkerhetskopiering (back-up) av kommunens data foretas av NorIKT, som også kontrollerer at sikkerhetskopieringen er riktig utført, og at alle data er lagt over på back-up. De skal også teste restore, dvs. at kopierte data er korrekte og kan benyttes ved eventuelle behov for senere rekonstruksjon etc.

Det er ikke tillatt lagret personsensitiv informasjon på den enkelte brukers PC/bærbare PC, mobiltelefon eller USB minnebrikke - dersom det ikke er installert krypteringsløsninger eller gode passord-løsninger benyttes for å sikre dette.

4.2 Aktivitetslogging

IT-systemene som benyttes i kommunen bør inneholde funksjoner for logging av aktiviteter i den utstrekning dette ansees nødvendig for å kunne forebygge, oppdage og redusere skade som følge av eventuelle misbruk og feil. For IT-systemer der det foregår behandling av sensitive personopplysninger skal det foretas slik logging; dette kravet skal inngå i avtalene med de respektive leverandører ved anskaffelse av nye systemer/applikasjoner.
Det er autorisasjonsansvarlig som i samarbeid med NorIKT skal vurdere behovet for logging, etablere rutiner for dette og foreta nødvendig kontroll i ettertid.
Eksempler på relevante aktiviteter som kan/bør logges:

- inn-/utlogging
- transaksjoner, sletting av data, endring av kodeverk og nøkkeldata

4.3 Sikringstiltak mot datavirus, spam, hacking etc.

NorIKT har ansvaret for nødvendig sikring av servere og nettverk inkl. mobilt datautstyr i Kåfjord kommune. Det foretas skanning av evt. datavirus og annet 'ondsinnet' programvare av all ekstern e-post til og fra kommunen på egen e-mailserver og automatisk oppdatering og 'utrulling' av antivirus-

program til servere og klienter. Bruk av tynne klienter i kommunen innebærer at datavirus etc. normalt ikke kan ramme disse 'klientene'.
På kommunens egne bærbare PCer etc. skal det være installert nødvendig kontroll mot bl.a. datavirus og spam.
Dersom bruker oppdager eller får mistanke om datavirus, skal NorIKT kontaktes umiddelbart – og datautstyr skal ikke benyttes før dette er klarert. Den enkelte bruker skal som en generell regel være spesielt oppmerksomme på e-poster fra ukjente avsendere eller e-poster som 'tilsynelatende' virker å være fra seriøse avsendere/leverandører; sjekk dette spesielt og kontakt NorIKT snarest hvis du er usikker og før du evt. vurderer å åpne slike mailer!

4.4 Destruksjon/sletting av sensitive data

Ved salg eller kassering av datautstyr – eller at ny bruker skal overta 'din' PC etc. - skal NorIKT sjekke at alle data på harddisk slettes på en forsvarlig måte.
Ved disk-krasj, skal disker som inneholder følsomme data, destrueres evt. leveres til forbrenning. Datalagringsmedier skal makuleres evt. leveres til forbrenning. USB minne- pinner, harddisker fra kopimaskiner, evt. mobiltelefoner etc. med sensitive opplysninger skal behandles på tilsvarende måte.

- Harddisker som flyttes mellom soner eller som inneholder sensitive personopplysninger og skal gjenbrukes, overskrives enten med software etc. eller Killdisk. (www.killdisk.com); begge disse metoder er godkjente av Datatilsynet.

NorIKT har ansvaret for disse rutiner.

4.5 Logisk tilgangskontroll

Tilgangskontroll-rutinene skal sikre at informasjoner kun er tilgjengelig for autorisert personell og at de ikke utilsiktet kan leses, endres eller slettes ved konvertering, behandling, lagring, utskrift eller distribusjon.
Alle IT-system i Kåfjord kommune er underlagt logisk tilgangskontroll, og skal omfatte nødvendig brukeridentifikasjon, autentisering og autorisasjonskontroll. NorIKT har ansvaret for rutinene knyttet til den IT-tekniske tilgangskontrollen, mens kontroller i forhold til fagsystemene skal foretas av de respektive systemansvarlige/autorisasjonsansvarlige.

4.5.1 Brukeridentifikasjon/autentisering

Hver enkelt IT-bruker skal som hovedregel tildeles en unik kode for identifikasjon i forbindelse med pålogging til PC, server og nettverk.
Bruker skal logge seg ut eller 'legge ned' skjermbildet når han/hun forlater arbeidsplassen. Passord evt. strengere autentisering må benyttes for å aktivere skjermbildet.

4.5.2 Autorisasjonskontroll

Autorisasjon inkl. nødvendige passord innebærer en godkjenning for å tildele de respektive brukere tilgang til de IT-systemer/applikasjoner og informasjon de trenger for å kunne utføre sine oppgaver ('need to know').
Autorisasjonen (eller autorisasjonsprofilen) skal angi hvilke IT-systemer, programrutiner og dataelementer vedkommende bruker har lovlig tilgang til, og hvilke operasjoner (lese, skrive, oppdatere, osv.) brukeren har lov til å utføre.

Tilsvarende rutiner gjelder for å unngå at brukerne kan utføre rutiner og operasjoner de ikke er autorisert for. Det skal i ettertid kunne foretas stikkprøvebaserte kontroller for å sikre at eventuelle forsøk på misbruk av tildelte autorisasjoner blir avdekket.

Det er kommunens respektive system-/autorisasjonsansvarlige som – evt. i samarbeid med NorIKT - tildeler brukerne slike tilgangsrettigheter.
Ved ansettelsesopphør skal rettighetene til vedkommende bruker slettes snarest.

4.6 Nettverkssikkerhet og rutiner for bruk av epost i kommunen

4.6.1 Rutiner for bruk av e-post

- e-post kan fritt brukes til meldinger som ikke inneholder sensitive/taushetsbelagte opplysninger (eks. beskjeder, meldinger, arbeidsutkast til saksdokument, møteinnkallinger, osv.)
- det er ikke tillatt å sende sensitiv informasjon via e-post med mindre vedleggene krypteres (se nedenfor siste kulepunkt)
- vær skeptisk til e-postsendinger spesielt fra ukjente avsendere (spam etc.): slike vedlegg skal ikke åpnes! Ved eventuelle datavirus-/spam-'angrep' eller ved mistanke om dette, skal datautstyr ikke benyttes før NorIKT har foretatt nødvendige undersøkelser

Brukerne i kommunen er bevisste på at de ikke skal sende e-post-meldinger med sensitive, personidentifiserbare opplysninger; dette er selvsagt mulig å gjøre i selve tekstfeltet i meldingen. Tidvis vil det allikevel kunne være situasjoner som nødvendiggjør at epost med sensitivt innhold (selv om kommunen benytter KS SvarINN/SvarUT-løsning – se neste punkt nedenfor) må sendes til en autorisert mottaker. Dette kan gjøres på en sikker måte ved å sende et kryptert word-dokument som vedlegg til mailen. Dette gjøres i Word under fil-informasjon, deretter Beskytt dokument og Kryptér med passord, som må gjentas én gang. Mailen sendes så med word-dokumentet som vedlegg til rette mottaker, men vedkommende får ikke åpnet den uten å taste passordet filen er generert med. Av sikkerhetshensyn sendes passordet i egen e-post evt. på sms etc. for å sikre at det kun er rette mottaker som kan åpne det krypterte dokumentet. I selve mailteksten refereres det til vedlegget uten å angi sensitiv tekst her

KS SvarUT og SvarINN-tjenestene benyttes gjennom kommunens post- og saksbehandlingssystem Acos Websak. Når et brev ekspederes ut herfra, sendes det elektronisk gjennom KS SvarUT til autorisert bruker, som mottar brevet i sin Digipost-'kasse' eller e-Boks avhengig av hvem mottaker har valgt som sin digitale postkasse. For å få åpnet dette brevet, må bruker autentisere seg gjennom eget passord + 'brikke' (2-faktorautentisering). Barnevern, NAV og Helse bruker også SvarUT via sine respektive fagsystem ved kommunikasjon mot autoriserte mottakere; det fungerer svært bra! Kommunen bruker Grafisk Digital AS ved utsending av fysisk post for de som ikke har elektronisk postkasse, eller ikke åpner den elektronisk innen 3 dager etter mottak. KS SvarINN kommer til 'importsentralen' i Acos Websak og fordeles deretter videre til saksbehandlere. Kommunen er også dyktig og bevisst i forhold til å sikre eposter med sensitivt innhold; her benyttes aktiv kryptering i Outlook; dette liker vi svært godt og viser at medarbeidere inkl. ledere er kommet langt i forhold til sikkerhetsbevissthet og til det å etablere gode, sikre rutiner inklusive et godt personvern. Mottaker av krypterte e-poster må bruke 2-faktorautentisering for å få åpnet aktuell epost.

Personvern og data-/informasjonssikkerhet i Kåfjord kommune er også MITT ansvar som medarbeider

1. Jeg er selv ansvarlig for kvaliteten på mitt eget arbeid i kommunen

2. Jeg har selv ansvar for å sikre sensitiv informasjon ved oppkobling mot usikre internettforbindelser på reiser, i kurssammenheng osv. NorIKT vil utarbeide veiledning om nødvendig sikring i slike sammenhenger

3. Passord, kodebrikker/kort etc. for ulike tilganger til IT-systemer, nettverk og IT-utstyr, som jeg er autorisert bruker av, er mine personlige 'sikkerhetsnøkler' og skal holdes utilgjengelige for andre medarbeidere – og øvrige

4. Jeg sørger for at uvedkommende ikke ser skjermbilder med fortrolig informasjon – og logger ut og slår av tynnklient/PC og skjerm, når jeg forlater arbeidsplass, møterom.

5. Jeg lar ikke fortrolige papirer/utskrifter ligge åpent tilgjengelig

6. Jeg kaster ikke fortrolige dokumenter eller minnebrikker i papirkurv, men makulerer disse i henhold til kommunens instruks for dette

7. Epost og -vedlegg fra ukjente avsendere og som jeg ikke kjenner innholdet av, skal IKKE åpnes. Er jeg i tvil, skal NorIKT kontaktes

8. Jeg laster ikke ned programvare som ikke har gyldige lisenser

9. Jeg hindrer uvedkommende i å få adgang til lokaler i kommunen hvor datautstyr, skrivere og fortrolige dokumenter er plassert

10. Jeg snakker ikke om følsomme, virksomhets-/personrelaterte saker til uvedkommende

11. Jeg er årvåken i det daglige arbeid - og sier ifra om noe unormalt oppdages

12. Jeg skal vise respekt for andre personers livssyn og nasjonalitet, og de skal ikke forulempes eller fornærmes; dette gjelder også ved bruk av sosiale medier

13. Jeg er klar over at jeg ved bruk av internett og sosiale medier er en synlig representant for kommunen og at jeg setter spor på de nettsteder jeg besøker