Informasjonssikkerhet

Hefte 1

Ansatte og sikkerhetskultur

Melhus er en mangfoldig kommune
der det skal være mulig å være modig

MELHUS
kommune

Innhold

Revisjonsliste

Dato	Versjon	Skrevet av	Endring i forhold til forrige versjon
26.07.2013	1.0	Rodo	Ny utgave, sikkerhetshåndboken delt I 3 utgaver
05.11.2013	1.1	Rodo	Godkjent av rådmannen
20.02.2014	1.2.	Rodo	2.5.2.6 Passordbeskyttelse av skjermsparer
25.08.2017	2.0	Rodo/Gewo	Periodisk gjennomgang med en del endringer

1.0 Om sikkerhetshåndboken

Sikkerhetshåndboken utgjør 3 hefter som basis for Melhus kommunes styringssystem for informasjonssikkerhet. Systemet bygger på et felles grunnlag for informasjonssikkerhet med særlig vekt på behandling av personopplysninger i henhold til lover, forskrifter og retningslinjer. Styringssystemet bidrar til å sikre et felles nivå på informasjonssikkerhet på tvers av virksomhetene i kommunen, og gir felles føringer for kommunens ansatte, eksterne brukere, borgere og samarbeidspartnere.

Sikkerhetshåndboken er delt inn i 3 hefter:

- **Ansatte og sikkerhetskultur** (for alle ansatte)
- **Policy, regelverk, rutiner og prosedyrer** (for ledere)
- **IT-løsning – drift** (for IKT-ansatte og sikkerhetsansvarlig)

Målgruppen for dette dokumentet er brukere av Melhus kommune sitt IKT-utstyr.

Formålet med styringssystemet for informasjonssikkerhet er å sikre at all behandling av personopplysninger og annen informasjon i Melhus kommune samt bruk av IT-hjelpemidler, skjer innenfor fastsatte krav. Dette er krav til tilgjengelighet, konfidensialitet, integritet og sporbarhet. Krav i henhold til lover og forskrifter, samt inngåtte avtaler og interne krav i Melhus kommune.

Styringssystemet for informasjonssikkerhet er utformet med basis i de veiledninger som Datatilsynet har publisert på www.datatilsynet.no, særlig veiledningene om internkontroll som ble publisert november 20018. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

1.1 Hva er informasjonssikkerhet?

Informasjonssikkerhet er tiltak for å beskytte informasjon, herunder personopplysninger, som behandles av et informasjonssystem. Informasjonssikkerhet dreier seg om å håndtere risiko relatert til informasjonsverdier.

Beskyttelse av informasjon innebærer sikring av informasjonens:

- tilgjengelighet (for rett person, til rett tid, i rett form og på rett sted)
- integritet (at informasjonen er korrekt og ikke forfalsket eller ødelagt eller feilaktig)
- konfidensialitet (at informasjonen sikres mot uvedkommende innsyn, herunder utilsiktet utlevering)
- robusthet (at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser).

I tillegg må det sikres at **særskilte** (sensitive) **kategorier av** personopplysninger behandles på en korrekt måte.

Personopplysningsloven definerer særskilte kategorier av personopplysninger som opplysninger om:

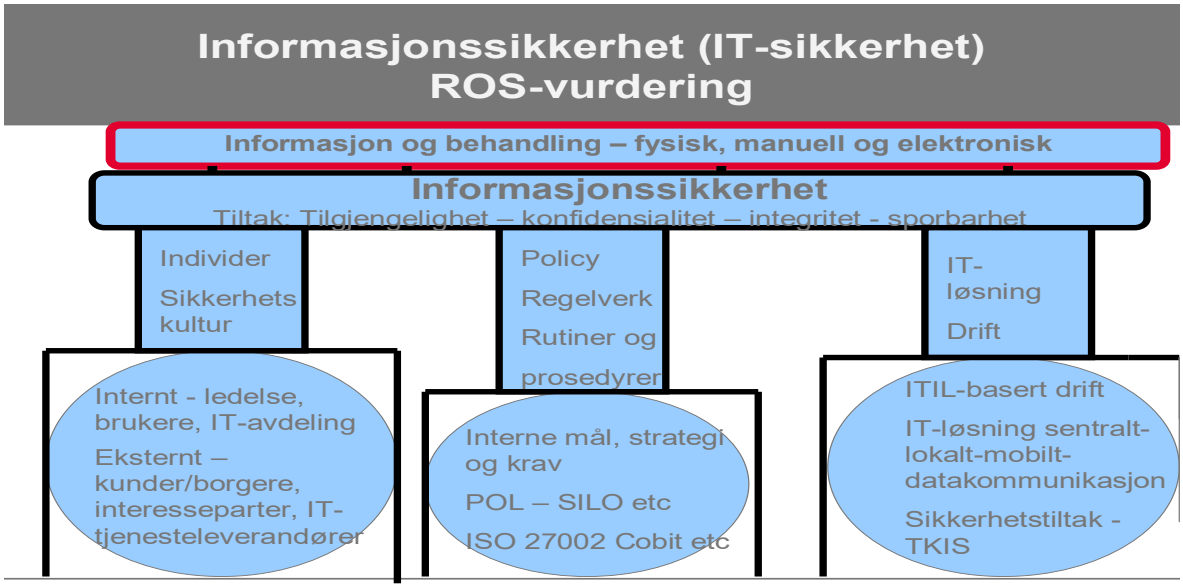
- Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
- At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- Helseforhold
- Seksuelle forhold

- Medlemskap i fagforeninger
- Biometriske data
- Genetiske opplysninger

Tiltak og virkemidler som benyttes for å beskytte informasjon som lagres, behandles og kommuniseres i IKT-systemer kalles ofte IT-sikkerhet. I dette dokument benytter vi begrepet IT-sikkerhet synonymt med informasjonssikkerhet.

Lov- og regelverket krever at Melhus kommune har gjennomført planlagte og systematiske tiltak for å oppnå tilstrekkelig informasjonssikkerhet, at tiltakene er dokumentert og at gjennomføringen følges opp.

Styringssystemet dekker følgende områder som er illustrert på tegningen nedenfor:



2.0 Sikkerhetsregler ved bruk av IKT-tjenester

Denne instruksen beskriver retningslinjer for bruk av IKT i Melhus kommune. Instruksen gjelder for alle ansatte, konsulenter og vikarer.

2.1 Viktige punkter for bedre informasjonssikkerhet

1. Overhold taushetsplikten.
2. Personopplysninger skal ikke være tilgjengelig for eller bli kjent for uautorisert personell eller uvedkommende internt eller eksternt.
3. Bidra til at du får tilstrekkelig opplæring i rutiner og regelverk, i bruk av it-verktøy og i informasjonssikkerhet.
4. Vær bevisst når du registrerer, behandler, lagrer og formidler personopplysninger.
5. Beskytt passordene dine, jf. pkt. 2.5.3.
6. Administratorrettigheter for å legge inn ny programvare fås ved henvendelse til IKT-enheten.
7. Vær på vakt: Ekstern e-post og vedlegg kan inneholde virus og annet uønsket innhold.
8. Særskilte kategorier personopplysninger skal kun lagres på sikker sone.
9. Ikke last ned programmer eller informasjon som bryter lisensbestemmelser eller copyright eller som har et innhold du ikke kjenner.
10. Meld fra om brudd på bestemmelsene om informasjonssikkerhet og andre avvik.

11. Lagring av private bilder, film og musikkfiler krever stor lagringsplass og kan hindre nødvendig sikkerhetskopiering. Det gis derfor ikke anledning til lagring av slike filer.

Du finner råd om sikkerhet ved bruk av IT på:
www.nettvett.no/ - Post- og teletilsynet
www.datatilsynet.no - Datatilsynet
www.norsis.no/ - Norsk senter for informasjonssikring

2.2 Taushetsplikt

Ansatte, vikarer og eksterne konsulenter som skal gis tilgang til kommunens IKT-systemer, skal undertegne denne instruksen samt underskrive taushetserklæring.

2.3 Opplæring

1. Før du får tilgang til de aktuelle IKT-systemene, skal du i samarbeid med nærmeste leder bidra til at du har fått tilstrekkelig opplæring i rutiner og regelverk, i bruk av IKT-systemer og i informasjonssikkerhet.
2. Du er selv ansvarlig for å følge de regler som gjelder for bruk av de forskjellige IKT-systemene i Melhus kommune.
3. Behandling av beskyttelsesverdig informasjon skal skje i henhold til reglene i dette dokumentet og i samsvar med gjeldende lov- og regelverk.

2.4 IKT-drift i Melhus kommune

Informasjon om IKT-drift i Melhus kommune er beskrevet på kommunens intranettsider. Her informeres om, driftstider, planlagte driftsavbrudd etc.

2.5 De viktigste sikkerhetstiltakene i IKT-løsningen

2.5.1 Kompetanse i IKT-enheten og hos samarbeidspartnere

Drift av IKT-systemer utføres av kvalifisert personell i IKT-enheten og/eller i nært samarbeid med samarbeidspartnere. Alle samarbeidspartnere må autoriseres før tilgang til IKT-utstyr blir gitt.

IKT-enheten benytter et supportsystem hvor alle driftshendelser, support og oppgaver blir loggført.

2.5.2 Brukeradministrasjon

1. Du får tildelt brukernavn og førstegangs passord av IKT-enheten for pålogging til Melhus kommunes domene. Passord for tilgang til andre fagsystemer opprettes om nødvendig av ansvarlig for de respektive fagsystemer.
2. Det er ikke tillatt å opprette fellesbruker eller dele passord.
3. Når arbeidsplassen forlates i korte perioder skal datamaskinen låses (windowstast+L). Maskinen skal også være satt opp med automatisk passordbeskyttet skjermsparer (låseskjerm), med aktivering etter 15 minutters inaktivitet.
4. Nettbrett tilknyttet MD-nett (mobile device) er oppsatt med autolås etter 15 minutter. Unntak kan gjøres etter en konkret vurdering ved særskilte behov.
5. Du skal alltid logge ut før du overlater maskinen til andre.

2.5.3 Passord

1. Passord er strengt personlig og skal ikke oppgis til eller lånes ut til andre. Dette er et personlig ansvar.

2. Velg et passord som er lett å huske men som likevel ikke lett lar seg knytte til brukeren.
3. Passordet skal bestå av en kombinasjon av store og små bokstaver og tall/tegn og være på minst 8 tegn. Det anbefales å bruke en setning.
4. Passordet har en varighet på inntil 12 måneder. Siste 5 passord kan ikke gjenbrukes.
5. Dersom du har mistanke om at passordet har blitt kjent av uvedkommende, skal passordet byttes og hendelsen rapporteres til nærmeste leder snarest mulig som et avvik, jf pkt. 4.1.

2.5.4 Totrinns pålogging for tilgang utenfor kommunens lokaler

Kommunens ansatte har tilgang dokumenter og informasjon gjennom Office 365 og Teams. Gjelder også på privat utsyr og for mobile enheter. Enkelte av kommunens saksbehandling- og fagsystem kan under gitte forutsetninger også benyttes utenfor kommunens lokaler.

For å sikre autorisert tilgang benytter Melhus kommune løsning for totrinns pålogging. Dette innebærer adgangskontroll i form av kombinasjoner av brukernavn, passord og sikkerhetskode fra sekundær autentiseringsløsning.

Totrinns pålogging kalles også totrinns verifiseiring, tofaktor autentisering eller multifaktor autentisering. Det er en tjeneste som gjør at du i tillegg til passord trenger flere godkjenningsmekanismer for å bevise din identitet. Det kan være at du får tilsendt en kode på SMS, bankens kodebrikke eller at du bruker en kode-app eller autentiseringsapp.

For å få tilgang til e-post, teams og dokumenter i Melhus kommune, kan du velge å bruke Microsoft Authenticator App eller engangskode på SMS. Du vil ikke trenge å få varsel/engangskode når du sitter på jobb. Dette gjør at hvis noen får tak i passordet ditt og prøver å logge inn som deg, så må denne personen også ha tilgang til din totrinns pålogging.

2.5.4 Nettverk oppdelt i soner

Soner benyttes som et grunnleggende prinsipp i sikkerhetsarkitekturen. En sone utgjør en del av et informasjonssystem og deles for eksempel opp etter behov for skjerming av ulike personopplysninger. For å begrense tilgangen til personopplysninger, er det i Melhus kommune benyttet følgende soner:

• Sikker sone; **hvor sensitive personopplysninger behandles (ved behov opprettes flere sikrede soner i virksomheten, for eksempel dersom dette bedre understøtter taushetsplikt). Den enkelte sikrede sone er teknisk atskilt fra resten av det interne nettverk og eventuelle andre sikrede soner, foruten mot eksterne nettverk.**

2.5.5.2 Sikker sone

I sikkerhetsmålene går det bl.a. fram:

«Den fysiske sikkerhet ved Melhus kommune skal hindre at uautoriserte får adgang til lokaler der beskyttelsesverdig informasjon og sensitive personopplysninger lagres og behandles.»

Fjernoppkobling på sikker sone må kun foretas i omgivelser som er skjermet for uautorisert adgang.

• **Intern sone**; hvor "ikke-sensitive" personopplysninger behandles. Denne kan også omfatte andre opplysninger i virksomheten som ikke skal eksponeres eksternt.

2.5.6 PC, smarttelefon, nettbrett, lagringsmedier og annet portabelt utstyr

1. PC, smarttelefon, nettbrett, lagringsmedier og annet portabelt utstyr skal konfigureres av IKT-enheten. Dette oppsettet skal ikke endres av bruker.
2. Sensitiv informasjon skal ikke lagres på bærbar PC, Smarttelefon eller annet portabelt utstyr. Sensitiv informasjon skal kun lagres på sikker sone.
3. Den enkelte bruker er ansvarlig for å håndtere bærbar PC og andre enheter på en forsvarlig måte. La aldri bærbar PC, smarttelefon eller annet bærbart utstyr ligge uten tilsyn.
4. Ved evt. tap av utstyr nevnt i dette punktet må det umiddelbart meldes avvik til IKT-enheten og nærmeste leder. Ved tap av smarttelefon må IKT-enheten varsles for å sperre telefonen og slette lagret informasjon.
5. Dersom vi får forespørsel fra utenforstående om utskrift m.m. fra minnepenn, må pennen skannes for evt. infeksjoner. Se dokumentet «Minnepinner» under fanen Relatert.

2.5.7 Installasjon/destruksjon av programvare og maskinvare

1. Dersom du har behov for ytterligere lisensiert eller annen programvare, ta kontakt med IKT-enheten for å få midlertidig administrasjonsrettighet.
2. All maskinvare og lagringsmedia/harddisk skal være registrert hos IKT-enheten. Dersom dette mangler, skal IKT-enheten varsles.
3. Disker, utstyr som inneholder harddisker og annet lagringsmateriale (f.eks. minnebrikker, backuptape etc.), skal leveres til IKT-enheten for forsvarlig destruksjon.

2.5.8 Privat/personlig utstyr

1. Beskyttelsesverdig informasjon fra Melhus kommune tillates ikke lagret på privat/hjemme-PC. Privat og personlig utstyr tillates ikke brukt i Melhus kommunes nettverk: Gjester/elever* kan ved behov få tilgang til kommunens gjestenett.

2. Det er kun IKT-enheten som kan iverksette arbeid som utføres av eksternt personell på informasjonssystemer og utstyr.

2.5.9 Fysisk adgang og sikring av bygninger

Dersom du mister nøkkel/nøkkelkort, meld umiddelbart fra til nærmeste leder. Ansatte som slutter eller går ut i permisjon, skal levere tilbake nøkkel/nøkkelkort.

2.5.10 Reparasjon, service og vedlikehold

Alle feil eller mistanker om feil i informasjonssystemer (både maskinvare og programvare) skal rapporteres til IKT-enheten snarest mulig.

2.5.11 Sikkerhetskopiering

1. For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på servere i Melhus kommunes nett.
2. For PC som benyttes i forbindelse med reiser og hjemmearbeid, må oppdatering mot servere i nettet gjøres regelmessig, spesielt dersom andre er avhengig av informasjonen.
3. Ved behov for gjenoppretting av sikkerhetskopiert informasjon, meld sak til support.

2.5.12 Dokumentasjon

Alle installasjoner, endringer og lignende hva gjelder IKT-systemer skal dokumenteres og det skal føres endringslogg. Det er krav til at alle installasjoner skal evalueres opp mot de til enhver tid gjeldene sikkerhetsbestemmelser.

3.0 Internett og media

3.1 Internett

2. Det er ikke tillatt å laste ned utuktig materiale, opphavsrettslig beskyttet materiale (f.eks. musikk, filmer og programvare) eller annet som er i strid med lovverket.
3. Eksterne tjenester for fildeling(f.eks. dropbox) tillates ikke på grunn av sikkerhetsrisiko knyttet til disse tjenestene.
5. Melhus kommune har anledning til å logge informasjon om trafikk på Internett og via e-post for å sikre alminnelig drift samt for sporing ved eventuelle interne eller eksterne sikkerhetsbrudd.
6. Det er ikke tillatt å forsøke å forbigå sikkerhetsmekanismer beskrevet i denne sikkerhetsinstruks, for eksempel ved å skjule ikke-tillatte tjenester gjennom andre tjenester.

3.2 Publisering av informasjon

Dokumenter som er unntatt offentlighet eller som inneholder sensitive personopplysninger eller fødselsnummer skal ikke publiseres. Dokumenter som omhandler mer private forhold, begrenses av personopplysningsloven når det gjelder hva kommunen kan publisere.

Avvik fra disse bestemmelsene rapporteres til nærmeste overordnede og rapporteres som et avvik, jf. pkt. 4.1.

3.3 Publisering av bilder

Det finnes i dag ingen spesifikke lover som gjelder offentliggjøring av bilder på Internett. Selve publiseringen vil imidlertid falle inn under åndsverkloven § 45c.

Ved publisering av bilder, spesielt mindreårige, skal Datatilsynets klare normer for publisering av bilder følges. Informasjon om disse normene finnes på hjemmesiden til Datatilsynet:

https://www.datatilsynet.no/rettigheter-og-plikter/internett-og-apper/bilder-pa-nett/bilder-av-barn/

3.4 Bruk av sosiale medier

I kommunens Etiske retningslinjer punkt 3, Hensynet til menneskeverdet, går følgende fram:

Folkevalgte og medarbeidere skal behandle brukere, kollegaer og andre de kommer i kontakt med gjennom sitt arbeid eller arbeidsrelaterte aktiviteter, med høflighet og respekt. Medarbeidere og folkevalgte må ikke opptre på en måte som kan krenke menneskeverdet.

Dette gjelder også ved bruk av sosiale medier som elektroniske møtesteder.

3.5 Kontakt med media

Det er kun Rådmannen eller den hun/han gir ansvaret til, som har myndighet til å uttale seg til presse eller andre media i forbindelse med saker som gjelder IT-sikkerhet, sikkerhetsbrudd eller større hendelser.

3.6 Muntlig informasjon, papirdokumenter

Utlån av saker eller andre dokumenter med sensitiv informasjon skal skje via den person som er ansvarlig for oppbevaringen, slik at lånet blir registrert.

Utskrifter på felles skrivere skal ikke ligge tilgjengelig for uvedkommende. Fortrolige utskrifter skal skrives ut med sikret utskrift. Med sikret utskrift menes her at utskriften er passordbeskyttet/Follow me print og ikke kan skrives ut før ansvarlig person identifiserer seg med personlig pinkode eller lignende på skriveren. Fortrolige datautskrifter og dokumenter skal aldri kastes i papirkurv, men først makuleres.

3.7 E-post/kalender

1. All kommunal e-post (innkommende og utgående) skal gå gjennom kommunens e-post løsning. Det er ikke tillatt å laste ned og lagre e-post fra andre operatører (f.eks. privat e-post). Kommunens e-post skal ikke lastes ned på privat IKT-utstyr, men kan kun leses via nettleser (Webmail) for lisensierte brukere.
2. Dersom e-post må benyttes for overføring av beskyttelsesverdig informasjon, skal informasjonen sendes som kryptert vedlegg til e-post med godkjent. krypteringsprogram.
3. Brukere er selv ansvarlig for å vurdere hva som er arkivverdig e-post.

Den enkelte skal bruke elektronisk post med tilstrekkelig aktsomhet. Elektronisk post må, forutsatt at den ikke er kryptert, betraktes å være relativt lett tilgjengelig for uvedkommende.

- Mottatt E-post som inneholder sensitive opplysninger skal ikke distribueres videre, kommenteres eller besvares.
- I den grad det er sendt e-post med sensitivt innhold til Melhus kommune, skal meldingen raskest mulig skrives ut og registreres som sak. Opprinnelig melding (og eventuelle kopier av denne) skal slettes og avsender informeres.
- Vedlegg til e-post skal ikke åpnes, med mindre forsendelsen kommer fra en avsender det er rimelig å forvente ønsker saklig kontakt
- E-post er først forsvarlig slettet når de er slettet fra e-postsystemets «slettede elementer».

4. Sensitive personopplysninger skal ikke ligge i kalenderen.

4.0 Avvik eller sikkerhetsbrudd

4.1 Avviksbehandling

Meld straks fra til nærmeste leder via avvikssystemet i EQS dersom du oppdager sikkerhetsbrudd eller hendelser som kan ha betydning for sikkerheten. Viser for øvrig til avviksprosedyre i EQS.

Alle *avvik* som skyldes brudd på datasikkerheten skal meldes til Datatilsynet. Unntak fra dette gjelder hvis det er usannsynlig at avviket medfører en *risiko* for enkeltpersoners rettigheter eller personvern.

Avviksmelding skal leveres Datatilsynet innen 72 timer..

4.2 Snoking

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger uten at det er begrunnet i hjemmel i lov eller forskrift. Likeså tillates det ikke snoking i dokumenter som ikke er relatert til eget arbeid.

4.3 Reaksjoner ved brudd

Konsekvenser for ansatte som har forårsaket brudd på sikkerhetsreglene, vil bli vurdert i hvert enkelt tilfelle og kan ved alvorlige brudd få konsekvenser for ansettelsesforholdet.

Dersom brukere har prosjektspesifikke behov som avviker fra denne instruks, skal det sendes en anmodning til virksomhetsleder.

4.4. Personvernombud

Melhus kommune har eget personvernombud som skal påse at kommunen behandler personopplysninger etter bestemmelser i personopplysningsloven og personopplysningsforskriften.

5.0 Underskrift

Sikkerhetsinstruksen er lest og forstått: