Arkivsak 16/775-1 11.2.16

MIDT-TELEMARK

Plan for informasjonssikkerhet i Midt-Telemarkkommunene

Bø, Nome og Sauherad

Anne Fredriksen

02.11.2012

Revidert av Bø kommune – desember 2015

Plan for informasjonssikkerhet er Midt-Telemarkkommunene sitt internkontrollsystem som skal sikre at virksomhetene i kommunene behandler personopplysninger lovlig, sikkert og forsvarlig.

Alle virksomheter	INTERNKONTROLL HMS	1. versjon: 02.11.2012 Utarbeidet av: Midt-Telemarkrådet Godkjent av: AMU Bø, AMU Nome, AMU Sauherad 2. versjon: Desember 2015 Godkjent av AMU Bø: Side 1 av 86
	Sikkerhetsplan for Midt-Telemarkkommunene	

Innhold ..... **Feil! Bokmerke er ikke definert.**

Ansvars- og samarbeidsforhold	RAMMEBETINGELSER • Om Midt-Telemarkkommunene • Forholdet til kommunen og forholdet mellom kommunene • Forholdet mellom kommunene og driftsleverandør
Formål og begrunnelse	• Systemet skal skape tillit hos brukerne gjennom forståelse og aksept og dokumentere at informasjon blir behandlet i henhold til lovverket og kommunale krav • Samordning: Gjøre det lettere å dele erfaringer og oppnå bedre kontroll med endringer og gjøre kommunene mindre sårbare i forhold til kapasitet og kompetanse ved fravær
Sikkerhetsstrategi	• Mål og virkemidler for informasjonssikkerhet
Sikkerhetsorganisasjon	• Organisering og roller i sikkerhetsarbeidet
Definisjoner	• Definisjoner på begreper brukt i informasjonssikkerhetssystemet og i regionale dokumenter knyttet til IKT
Sentrale lover og forskrifter	• Henvisninger til sentrale forskrifter med kort beskrivelse av relevante paragrafer
Normer og standarder	• Henvisninger til aktuelle normer og standarder.

Autorisasjon og tilgangsstyring **Passord** **Avhending og kassering** **Bruk av datautstyr** **Fysisk sikring** **Hendelseslogging**	SIKKERHETSPROSEDYRER Prosedyrer for informasjonssikkerhet skal: • vareta hensynet til informasjonssikkerhet og relevante lover og forskrifter • rette oppmerksomhet mot sikkerhetsutfordringer og trusler/svakheter • sørge for at sikkerhetstiltakene er basert på kvalifiserte begrunnelser • beskytte investeringer og innsamlede data mot feil, uhell, tyveri, osv. • skape bevisstgjøring, erfaring og kunnskap om informasjonssikkerheten • sørge for registreringer og oppfølging av sikkerhetshendelser, -brudd og -svakheter
Sikkerhetshendelser, -brudd og svakheter **Meldeplikt, Oversikt over behandlinger** **Innsyn, retting og sletting** **Risikovurdering** **Samarbeidsparter og leverandører** **Sikkerhetskopiering** **Sikring mot ondsinnet programvare** **Innsyn i ansattes e-post og personlige kataloger**	Ansvaret framgår av prosedyrene og gjelder for • Rådmenn • Regionrådssekretær • Faste ansatte • Innleid arbeidskraft • Driftsleverandør • Andre tjenesteleverandører • Prosjektledere og -deltakere  *Alle som behandler informasjon er ansvarlig for sikkerhet og kvalitet i eget utført arbeid.*

IT Beredskapsplan **Sikkerhetsrevisjon virksomhet** **Sikkerhetsrevisjon kommune** **Ledelsens gjennomgang** **Endringsstyring** **Etablering og styring av dokumenter**	STØTTEPROSEDYRER • redusere konsekvenser og sikre snarlig drift etter uhell, feil og katastrofer • sikre effektiv egenkontroll av informasjonssikkerhetssystemet • sikre tilgang på korrekt, oppdatert og tilstrekkelig systemdokumentasjon • dele informasjon, erfaringer og krav med brukere og samarbeidspartnere • sikre kontroll med endringer - IT-systemer og sikkerhetstjenester - i organisasjon, kontrakter, arbeidsmetoder og lignende - som følge av registrerte hendelser og resultater fra revisjoner og risikovurderinger

1.1 Ansvars- og samarbeidsforhold

Formål

Formålet med denne prosedyren er å beskrive ansvars og samarbeidsforhold innen informasjonssikkerhet i Midt-Telemarkkommunene.

Om Midt-Telemarkrådet

1. Arbeider for felles interesser overfor fylkeskommunene, fylkesmannen, stat og næringsliv.
2. Arbeide for samordning og effektivisering av den kommunale tjenesteytingen.
3. Arbeide for utvikling av næringsliv og kulturliv i regionen.
4. Profilere regionen som ett attraktivt boområde og arbeidsmarked.
5. Arbeide for bærekraftig utvikling i regionen i tråd med Fredrikstaderklæringen.

Arbeidet i Midt-Telemarkrådet baserer seg på en generell Viljeserklæring om samarbeidet. Erklæringen godkjennes av de tre kommunestyrene, og stadfestes av Midt-Telemarktinget i starten på hver kommunestyreperiode

Forholdet mellom Midt-Telemarkrådet og kommunene

Kommunene er behandlingsansvarlige, dvs. de som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jamfør Personopplysningslovens (POL) § 2. Kommunen har ansvaret for at opplysninger behandles i henhold til de kravene som POL oppstiller.

I forholdet til Nome og Sauherad kommune er Midt-Telemark IKT (MT-IKT) databehandler når avdelingen står ansvarlig for driften av ett eller flere systemer. Bø kommune er vertskommune for MT-IKT

Forholdet mellom Midt-Telemarkkommunene og leverandørene

Leverandøren er databehandler, dvs. den som behandler personopplysninger på vegne av den behandlingsansvarlige, jamfør. POL § 2, nr. 5 og helseregisterlovens § 2 nr. 9. Databehandler skal behandle personopplysninger i henhold til (databehandler) avtale med den behandlingsansvarlige.

Behandlingsansvarlige kan sette strengere krav enn hva som følger av POL, men ikke avtale vilkår som er i strid med kravene som POL stadfester, jamfør Datatilsynets veileder om databehandleravtaler.

Leverandører som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i personopplysningslovens kapittel 2. Det betyr at avtalen bør inneholde bestemmelser om

- avvikshåndtering og tilgangskontroll

- kontrollmekanismer for loggføring
- taushetsplikt,
- sikkerhetsrevisjoner,
- fysiske sikringstiltak,
- hvordan rutiner og liknende skal dokumenteres og
- oversikt over personell hos partene som skal ha tilgang til personopplysninger

Dette er i overensstemmelse med Datatilsynets veileder om databehandleravtaler.

Personopplysningsforskriftens § 2-8, 3. punktum: Autorisert bruk av informasjonssystemet skal registreres. Forskriften § 2-15 (sikkerhet hos andre virksomheter), 3. punktum: Leverandører som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i dette kapittelet (dvs. kapittel 2, herunder § 2-8).

Forholdet mellom kommunene

Når en kommune håndterer en tjeneste på vegne av en eller flere av de andre kommunene i samarbeidet, må de aktuelle kommunene klarlegge om dette betyr at det kun er denne kommunen som har behandlingsansvaret, jamfør POL § 2 nr. 4. Hvis dette er tilfellet, er det kun én melding fra denne kommunen som er nødvendig. Dersom hver kommune er behandlingsansvarlig, men har delegert funksjonen til en annen kommune skal hver av kommunene sende melding.

1.2 Informasjonssikkerhetssystemet – Formål og begrunnelse

Hvem gjelder informasjonssikkerhetssystemet for?

Informasjonssikkerhetssystemet for Midt-Telemark kommunene gjelder for:

1. Alle ansatte og politikere (politisk nivå)
2. Konsulenter
3. IKT Infrastruktur
4. Brukere av mobiltelefoner, datamaskiner
5. Alle som behandler (lese, dele, endre, søke, flytte) informasjon i kommunen eller på vegne av kommunen
6. Alle som får eller kan få tilgang til eller informasjon, fysisk eller gjennom data
7. Alle som omfattes av bestemmelsene og unntakene i Offentlighetsloven (registrerte, innbyggere)
8. Innbyggere

Begrunnelser for å etablere og vedlikeholde et system for informasjonssikkerhet

- Sikre at sensitive eller fortrolig informasjon ikke kommer uvedkommende i hende
- Sikre at kommunene har tilgang til nødvendig informasjon om innbyggere, ansatte, brukere
- God forvaltning av opplysningene som kommunene registrerer og arkiverer
- Sikre rutiner for internkontroll
- Krav fra offentlige myndigheter

Begrunnelse for felles infrastruktur og fagsystemer for to, flere eller alle kommunene

Et felles system for informasjonssikkerhet i Midt-Telemark gir:

- Stordriftsfordel med felles systemer, utvikling, implementering og vedlikehold
- Profesjonalitet og kvalitet
- Kommunene samarbeider i økende grad om felles løsninger og tjenester.
- Krav til samkjørt informasjonssikkerhet ivaretas lettest med felles system
- Lettere å holde systemet levende, felles opplæring
- Ajourhold og vedlikehold
- Dele informasjon og erfaringer med hverandre
- Gjøre kommunene mindre sårbare i forhold til kapasitet og kompetanse ved fravær eller tap av arbeidskraft

Andre grunner for felles informasjonssikkerhetssystem
Service og sikkerhet overfor innbyggere

Et tydelig og velfungerende system skal sammen med gode holdninger og praksis hos medarbeiderne skape tillit overfor medarbeidere, politikere og brukere av kommunenes tjenester i forhold til hvordan informasjon blir behandlet i kommunene

Kontroll

Sikre at informasjon blir behandlet i henhold til kravene om konfidensialitet, integritet og tilgjengelighet.
Sikre krav fra offentlige myndigheter.
Sikre kontroll med personopplysninger.
Sikre at all informasjon blir behandlet innenfor relevante lover og forskrifter.
Sikre kontroll med endringer i IT-systemer, herunder, funksjonalitet, oppgradering og vedlikehold.
Sikre kontroll med endringer i tjenesteleveranser (konsulenter, driftsleverandører, leverandører av fagsystemer, revisorer, renhold, osv.) og rammebetingelser.

1.3 Informasjonssikkerhetsstrategi

Mål for informasjonssikkerhet

Midt-Telemarkkommunene presenterer rett informasjon til rett tid og sted, det betyr at

1. Arbeid med informasjonssikkerhet skal inngå som en integrert del av kommunenes tjenesteproduksjon
2. Innbyggerne skal til enhver tid ha tilgang til korrekt og nødvendig informasjon i henhold til tjenesteyting fra kommunene
3. Sensitive eller fortrolige opplysninger skal kun være tilgjengelig for autorisert personell
4. Aktiviteten i Midt-Telemarkkommunene skal kunne gjenopptas raskest mulig etter sikkerhetshendelser og -brudd.
5. Medarbeidere skal ha tillit til at personlig informasjon blir ivaretatt på en tilfredsstillende måte fra ansettelse til fratredelse også der vedkommende ikke kan forsvare sine interesser.
6. Medarbeidere skal ha tillit til at informasjonssikkerhet er forankret hos rådmenn og i kommunenes ledelse.
7. Medarbeiderne skal ha faglige forutsetninger, myndighet og motivasjon til å kunne ivareta sitt ansvar i behandlingen av informasjon
8. All informasjon skal behandles i henhold til krav om opplysningsplikt, konfidensialitet, tilgjengelighet, integritet, pålitelighet og disposisjonsrett (iht. åndsverkloven).
9. Systemet skal tilfredsstille Datatilsynets kriterier for et fullverdig internkontrollsystem.

Ansvar for informasjonssikkerhet

1. Rådmannen har det overordnede og juridiske ansvaret for informasjonssikkerheten i kommunen som er delegert videre til sikkerhetsansvarlig i hver kommune
2. Informasjonssikkerhetsarbeidet i Midt-Telemarkkommunene skal være basert på klare ansvarsforhold og roller for alle medarbeidere og er et lederansvar.
3. Alle som behandler informasjon på vegne av kommunene er ansvarlig for sikkerheten i eget utført arbeid.

Virkemidler

1. Sikkerhetsarbeidet i Midt-Telemarkkommunene skal være basert på ett regionalt samordnet sikkerhetssystem som er lett tilgjengelig og som er tilrettelagt for å kunne sikre riktig, tilstrekkelig og enhetlig informasjon.
2. Informasjonssikkerheten skal omfatte systemtekniske, fysiske og organisatoriske sikkerhetsforhold.

3. Midt-Telemarkkommunene skal arbeide i henhold til anbefalt teknisk sikkerhetsarkitektur fra Datatilsynet.
4. Sikkerhetssystemet skal være basert på resultater fra dokumenterte risikovurderinger. Systemet er laget for både å forebygge og korrigere sikkerhetshendelser, -brudd og –svakheter.
5. Sikkerhetssystemet skal legge til rette for at ansatte kan fremme forslag til forebyggende eller korrigerende tiltak og sikre at de får tilbakemelding.
6. Midt-Telemarkkommunene skal legge til rette for kompetanseoppbygging for medarbeidere og samarbeidspartnere knyttet til informasjonssikkerhet.
7. Fysiske forhold skal være slik at de ivaretar kravene til informasjonssikkerhet.
8. Medarbeidere som registrerer eller observerer sikkerhetshendelser, -brudd og/eller -svakheter melder fra i henhold til retningslinjer for avviksbehandling.
9. Sikkerhetssystemet skal ivareta hensynet til relevante lover og forskrifter om informasjonssikkerhet.
10. Midt-Telemarkkommunene skal stille det samme kravet til informasjonssikkerhet overfor sine samarbeidspartnere som til seg selv.
11. Midt-Telemarkkommunene skal ha kunnskap om sikkerhetsstrategien hos leverandører og forsikre seg om at den gir tilfredsstillende informasjonssikkerhet.
12. Midt-Telemarkkommunene skal ha beredskapsplan som reduserer konsekvensene og snarest sikre betryggende gjenoppretting til normalsituasjon etter eventuelle feil og uhell (inkludert driftsavbrudd og katastrofer).
13. Periodiske gjennomganger skal sørge for at systemet fortsatt er hensiktsmessig og virker effektivt. Gjennomgåelsen omfatter å bedømme muligheter for forbedringer/behov for endringer.

1.4 Sikkerhetsorganisasjon

Formål

Prosedyren skal sikre at ansvar og roller er fordelt og beskrevet slik at sikkerheten kan ivaretas på en hensiktsmessig måte, og i samsvar med krav gitt i lov og forskrift.

Omfang

Prosedyren skal beskrive og regulere ansvaret for personvern og informasjonssikkerhet i kommunene og det regionale koordinerende leddet.

Prosedyren skal også beskrive ansvarsområdet til de forskjellige rollene i sikkerhetsorganisasjonen.

Beskrivelse - Roller

Roller i kommunene:

- Behandlingsansvarlig
- Daglig ansvarlig
- Personvern- og sikkerhetsansvarlig
- Driftsansvarlig
- Systemeier
- Systemansvarlig
- Bruker

Roller på regionalt nivå:

- Databehandler
- Koordineringsansvarlig
- Driftsansvarlig

Behandlingsansvarlig

Rådmann i hver kommune

- Bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
- Behandlingsansvarlig har ansvaret for at alle sider ved behandlingen skjer i overensstemmelse med lov og forskrift.
- Den behandlingsansvarliges daglige plikter ivaretas normalt av leder for den virksomheten der behandlingen foregår.

Daglig ansvarlig

I Bø kommune: einingsleiarar og andre medlemmer av RUL - se «Definisjoner 1.5»

- Gjennomføre risikovurdering.
- Bestemme tilgang til informasjon og funksjonalitet for brukere.
- Sørge for at all påkrevet dokumentasjon foreligger.
- Sørge for at det finnes et opplæringstilbud med fokus på rutiner og informasjonssikkerhet.
- Kontrollere jevnlig at gjeldende driftsrutiner blir fulgt og at nødvendig dokumentasjon foreligger.
- Ta stilling til og følge opp meldte avvik i henhold til prosedyre for avviksbehandling.
- Minimum årlig å gjennomføre prosedyre for sikkerhetsrevisjon.

Systemeier

I Bø kommune: Kommunalsjefene, IKT og leverandør.

- Daglig ansvar for å oppfylle plikter som behandlingsansvarlig på vegne av rådmannen jf. Personopplysningsloven og retningslinjer for IKT-sikkerhet.
- Overordnet ansvar for å gi brukere nødvendig opplæring i systemet.

- Oppfølging av økonomi knyttet til bruk og videreutvikling av systemet.
- Skal utnevne systemansvarlig.
- Ansvar for å inngå eventuelle databehandleravtaler.
- Gi melding til Datatilsynet.

Systemansvarlig

I Bø kommune: IKT og Informasjonssikkerhetsansvarlig for punkt merket med *

- Kontaktperson mot driftsorganisasjonen
- Vedlikehold og tilpasninger av systemet.
- Etablere og dokumentere system for vedlikehold og tildeling av brukertilganger.
- Etablere og dokumentere rutiner som er nødvendige i forhold til bruk av systemet.
- Bistå med testing og godkjenning ved oppgradering og ny funksjonalitet.
- Bistå driftsorganisasjonen ved behov for feilretting/feilsøking.
- Kontaktperson mot leverandørens brukerstøtte om bruken av systemet.
- Melde inn til driftsorganisasjonen og/eller leverandør behov for utvikling av systemet.*
- Deltaker i interkommunal faggruppe.
- Gjøre seg kjent med avtale med leverandør, spesielt med hensyn til vilkår for å benytte leverandørens brukerstøtte.

Personvern- og sikkerhetsansvarlig

I Bø kommune: Personalsjef og MTR – prosjektleder for punkt merket med *

- Godkjenne større endringer av infrastrukturen og programvaren.
- A ajourholde oversikt over kommunens informasjonssystemer med IKT drift, systemeiere og systemansvarlige.*
- Ansvar for at administrasjonen utøver sitt ansvarlig for fysisk sikkerhet, personell og sikkerhet og dokumentsikkerhet.
- Utføre ikke anmeldte inspeksjoner på natt- eller dagtid på kontorer, møterom og andre lokaler han/hun finner grunn til å inspisere.
- Motta og følge opp gjennomførte sikkerhetsrevisjoner fra systemeiere/virksomhetsledere.
- Årlig å gjennomføre og følge opp ledelsens gjennomgang i henhold til fastlagt prosedyre.

Brukere

I Bø kommune: Alle ansatte.

- Pliktig til å sette seg inn i og følge gjeldende rutiner for bruken av informasjonssystemet.
- Melde avvik

Databehandler

I Bø kommune: pr. i dag ukjent.

- Databehandlere skal ivareta ansvar og oppgaver innen informasjonssikkerhet i samsvar med lov, forskrift og databehandleravtaler.

Koordineringsansvarlig

I Bø kommune: pr. i dag ukjent.

Koordineringsansvarlig er den som på Midt-Telemarkkommunenes vegne koordinerer informasjonssikkerhetsarbeidet i regionen. Koordineringsansvarlig skal:

- Ta initiativ ift det overordnede informasjonssikkerhetsarbeidet i regionen.
- Holde regionens felles internkontrollsystem for informasjonssikkerhet ajour i forhold til de krav som settes i lov, forskrift og regionale vedtak.
- Forestå praktisk arbeid rundt endringsstyring av regional IK- informasjonssikkerhet.
- Være pådriver for at det etableres tilfredsstillende internkontroll for regionens og kommunenes fagsystemer.
- Være ressursperson og pådriver for kompetanseutvikling innen informasjonssikkerhet i regionen.
- Planlegge sikkerhetsrevisjoner på tvers av kommunene.
- Bistå kommunene med å arrangere et sikkerhetsforum for systemeiere, systemansvarlige og driftsansvarlige.

Driftsansvarlig

I Bø kommune: Leder for Midt-Telemark IKT

- Melde avvik
- Innhente godkjennelse fra systemeier før større tekniske endringer utføres.
- Etterleve gjeldende tekniske og administrative driftsrutiner.

1.5 Definisjoner

Definisjoner i Personopplysningslov og -forskrift

1) Personopplysning

Opplysninger og vurderinger som kan knyttes til en enkeltperson.

2) Behandling av personopplysninger

Enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

3) Personregister
Registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen.

4) Behandlingsansvarlig
Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
Behandlingsansvarlig i kommunene er rådmann som er delegert videre til sikkerhetsansvarlig i hver kommune.

5) Databehandler
Den som behandler personopplysninger på vegne av den behandlingsansvarlige.

6) Registrert
Den som en personopplysning kan knyttes til.

7) Samtykke
En frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv.

8) Sensitive personopplysninger
Opplysninger om

a) Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning.

b) At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling.

c) Helseforhold.

d) Seksuelle forhold.

e) Medlemskap i fagforeninger.

9) Konfidensialitet
Sikkerhet for at kun autoriserte personer får tilgang til følsom eller gradert informasjon, og at det på forhånd er foretatt en gyldig identifisering og autentisering av personen. En av tre egenskaper for informasjonssikkerhet sammen med integritet og tilgjengelighet. (NORsis)

10) Integritet
Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter.

Regionens definisjoner

Ledelse

Kommunene er organisert med forskjellige nivå og med noe forskjellige betegnelser.

Kommunale ekvivalenter fremgår av tabellen.

Region	Bø	Nome	Sauherad
Ledernivå 1	Rådmann	Rådmann	Rådmann
Ledernivå 1	Kommunalsjefene	Etatsledere	Rådmannens ledergruppe
Ledernivå 2	Ledere i RUL (Rådmannens utvidede ledergruppe)	Avdelingsledere	Enhetsledere
Ledernivå 3	Avdelingsledere	Avdelingsledere	Avdelingsledere

Systemeier

Den som er ansvarlig for et fagområde som utfører en behandling, eller benytter et datasystem. Vil som oftest være leder på nivå 1 eller 2, øverste leder for den virksomheten/de virksomhetene som bruker systemet (kan være leverandør, kommunalsjef, IKT etc.).

Systemansvarlig

Kontaktpunkt hos systemeier mot IKT-tjenesteleverandør. Har faglig ansvar for bruk og administrasjon av applikasjonen, med grunndata, tilgangskontroll og andre sentrale funksjoner (Prosjektleder – MTR laget i 2013/2014 en liste over systemansvarlig – listen ligg vedlagt)

Superbruker

En bruker som hjelper andre brukere samt bistår med kommunikasjon med Service Desk og andre funksjoner hos IT-leverandøren. Superbrukere bistår ofte både med opplæring og håndtering av hendelser. (Prosjektleder – MTR laget i 2013/2014 en liste over superbrukere – listen ligg vedlagt)

Driftsansvarlig

Den funksjonen som har ansvar for at applikasjon er teknisk ajour og fungerer som forutsatt, i seg selv og i relasjon til omgivelsene.

Dokumenteier

Den som godkjenner dokumenter i internkontrollsystemet (i denne sammenheng – IK Informasjonssikkerhet)

Dokumentansvarlig

Den som utarbeider og ajourfører dokumenter i internkontrollsystemet (i denne sammenheng – IK Informasjonssikkerhet)

Driftsleverandør

Ekstern part som leverer driftstjenester til region eller en eller flere kommuner i regionen. *Kan også være kommune som leverer tjeneste til annen kommune*

Fagsystemleverandør

Ekstern part som leverer applikasjon til region eller en eller flere kommuner i regionen.

Informasjonssikkerhet

Iverksettelse av planlagte og systematiske sikringstiltak for å sikre tilfredsstillende konfidensialitet, tilgjengelighet, integritet og sporbarhet*, spesielt knyttet til behandlingen av sensitive personopplysninger for kommunene og der behandlingen helt eller delvis skjer med elektroniske hjelpemidler.*

Informasjonssikkerhet omfatter både fysiske, organisatoriske og systemtekniske sikkerhetsforhold.

Internkontroll

Systematiske tiltak som skal sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og vedlikeholdes i samsvar med krav fastsatt i eller i medhold av lovgivningen på det aktuelle området, i dette tilfelle personopplysningslovgivningen.

Risiko

I hvilken grad en uønsket hendelse kan inntreffe, sannsynligheten for at den inntreffer og konsekvenser som følge av at hendelsen inntreffer.

Risiko = Sannsynlighet x konsekvens.

Et mulig tilfelle som kan forårsake en skade, tap eller virke inn på evnen til å oppnå mål. En risiko måles ved sannsynligheten for at en trussel inntreffer, sårbarheten til denne trusselens eiendel og påvirkningen den vil ha hvis den oppstår. (ITIL-def. av risiko)

Risikovurdering

Risikovurderingen er i denne sammenheng relatert til informasjonssikkerhet, herunder risiko ved behandling eller håndtering av:

- Personopplysninger i henhold til Personopplysningsloven med forskrift og aktuell særlovgivning.
- Informasjon som er underlagt sikkerhetsgradering i henhold til Sikkerhetsloven med forskrifter.
- Annen informasjon som av ulike årsaker er å betrakte som fortrolig i et begrenset (for eksempel under saksbehandling) eller ubegrenset tidsrom.
- Informasjons- og opplysningsplikter i henhold til lovverket og aktuell særlovgivning.

Risikovurderinger er et egnet grunnlag ved:

- Etablering av sikkerhetsregelverk (informasjonssikkerhet).
- Vurdering av konsekvenser ved endringer som har eller vil kunne ha betydning for informasjonssikkerheten.

- Utarbeidelse av beredskapsplaner for informasjonssikkerhet.

ROS-analyser

ROS-analyser omhandles ikke i systemet for informasjonssikkerhet. Begrepet er beskrevet for å kunne presisere forskjellen på en ROS-analyse og en begrenset risikovurdering.

ROS-analyse: Kartlegge risiko og sårbarhet som kan ramme større grupper av publikum eller også mindre grupper dersom risikoen er høy for dem det angår. ROS-analyser er et egnet grunnlag ved

- Utarbeidelse av kommunale planer (kommuneplan, handlingsprogram med økonomiplan, diverse sektorplaner samt årsbudsjett).
- Utarbeidelse av kriseplaner, herunder kartlegging av risiko og sårbarhet i kommunen som kan ramme større grupper av publikum eller også mindre grupper dersom risikoen er høy for de det angår innenfor områdene naturskade, trafikkulykker, brann, forurensning, kraftforsyning, telekommunikasjon og innenfor evt. andre områder hvor man finner behov for det.
- Planlegging av infrastruktur, bebyggelse og viktige samfunnsfunksjoner for å vurdere sikkerhet og beredskap i forbindelse med lokalisering, utforming og utrustning.

Sikkerhetsprosedyrer

Dokumenterte framgangsmåter som beskriver hvordan Midt-Telemarkkommunene skal oppfylle og etterleve sikkerhetskrav. Hjelpemidler som for eksempel skjemaer, programvare og/eller detaljerte spesifikasjoner (f.eks. systemdokumentasjon) kan være en del av en prosedyre. Ansvaret for, og myndigheten til å gjennomføre prosedyren, og til å bruke hjelpemidlene framgår av prosedyren.

Sikkerhetsrevisjon

En systematisk og uavhengig undersøkelse som skal framskaffe opplysninger og observasjoner, og bedømme dem objektivt for å bestemme i hvilken grad de er i samsvar med krav fastsatt i eller i medhold av aktuelle lover med forskrifter, og i samsvar med andre sentrale eller interne bestemmelser vedrørende informasjonssikkerhet.

Revisjonen sammenligner faktisk bruk av informasjonssystemet (program, data og IT-utstyr/-infrastruktur m/nettverk) med de retningslinjene som er besluttet.

Ifølge Personopplysningsloven med forskrifter skal slike revisjoner gjennomføres jevnlig og minst hver 18. måned.

Revisjoner kan gjennomføres internt eller eksternt. En revisjonsgruppe i regionen kan gjennomføre eksterne revisjoner for kommunene.

Tjenesteleverandør

En organisasjon som tilfører tjenester til en eller fler interne eller eksterne kunder.
Tjenesteleverandøren brukes ofte som kortform for IT-tjenesteleverandør.

Privat e-post og meldinger

E-post og meldinger med innhold av privat art, slik som e-post og meldinger til personlige kontakter, hilsener, til og fra fagforening, tillitsvalgte og helsetjeneste.

Se også virksomhetsrelatert e-post og meldinger.

Virksomhetsrelatert e-post og meldinger

E-post og meldinger knyttet til gjennomføring av arbeidsoppgaver.

Elektronisk meldingsutveksling

Ved elektronisk meldingsutveksling sendes informasjonen ved hjelp av meldinger fra ett fagsystem til ett annet, og kommunikasjonspartnerne får dermed kun akkurat den informasjonen avsender har sendt.

Autentisering

Prosessen hvor en bruker må vise sin identitet for å kunne få tilgang til IT-systemer og data.

Autorisasjon

Betegnelse på prosessen med å gi, eller nekte, en bruker adgang til IT-systemer og data/registre. Autorisasjonen angir hvilke IT-systemer, programrutiner og dataelementer den respektive brukeren har tilgang til og hvilke operasjoner (lese, skrive, oppdatere, slette osv.) brukeren har lov til å utføre.

Hendelsesregistrering

Registrering av hendelser i et informasjonssystem, bl.a. med sikte på å forebygge, avdekke og hindre gjentagelse av sikkerhetsbrudd.

Elektronisk pasientjournal (EPJ)

Elektronisk ført samling eller sammenstilling av nedtegnede/registrerte opplysninger om en pasient i forbindelse med helsehjelp, se også helsepersonelloven § 40, første ledd, og forskrift om pasientjournal § 3 a). Dette inkluderer både somatisk og psykiatrisk journal o.a., hver for seg eller samlet.

Virksomhetskritiske systemer

I Midt-Telemarkkommunene er følgende systemer å regne som virksomhetskritiske:

- Nettverk og katalogsystemer
- Gruppevare/E-post
- Økonomisystem
- Lønnssystem
- Fagsystem PO
- Fagsystem legevakt

- Fagsystem fastlege
- Elektronisk meldingsutveksling (Helsenett)
- Kommunens hjemmeside og intranett
- Telefonsentraler

1.6 Sentrale lover og forskrifter

Innledning

For Midt-Telemarkkommunenes informasjonssikkerhet gjelder en rekke lover og bestemmelser som blant annet tar sikte på å hindre at noen uten lovlig hjemmel får tilgang til personopplysninger, herunder opplysninger som er underlagt meldeplikt eller øvrige informasjoner som er unntatt offentlighet.

Alle berørte ledere og medarbeidere i kommunene skal gjøres kjent med, og følge til enhver tid gjeldende lovverket.

Følgende lover og bestemmelser har relevans for informasjonssikkerheten i Midt-Telemarkkommunene:

Personopplysningsloven (POL)

Formålet med loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

Loven gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler og annen behandling (innsamling, lagring, sammenstilling, analyser og vurderinger mv) av personopplysninger når disse inngår eller skal inngå i et personregister. Elektroniske hjelpemidler kan være dataregistre, enkeltstående logger, e-postforsendelser, elektroniske adgangskontroller, elektroniske sensorer, videoopptak, elektronisk tekstbehandling og telefonsystem når dette automatisk registrerer og lagrer tidspunkt og telefonnummer for samtaler og ansatte kan knyttes til de enkelte telefoner.

POL setter krav til: Hvilke opplysninger som kan behandles, måten opplysningene behandles på, partsrettigheter som samtykke, reservasjon, varsling, innsyn og retting av gale opplysninger, konsesjon og meldeplikt samt saksbehandling i Datatilsynet og Personvernnemnda.

Hovedregel: Personopplysninger kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller at et av kravene i POL § 8 er oppfylt.

Samtykke må være basert på vedkommende sin kunnskap om forhold og konsekvens. Formål: Person-opplysninger må bare nyttes til angitt og begrunnet formål. Opplysningene må være tilstrekkelig og relevante for formålet og ikke bli benyttet til andre formål på senere tidspunkt. Opplysningene må være korrekte og oppdaterte og ikke lagres lenger enn det som er nødvendig ut fra formålet.

Styringssystem: Behandling av personopplysninger skal være underlagt dokumenterte systemer for informasjonssikkerhet og internkontroll (§§ 13-14).

Personopplysningsforskriften (POF)

Forskriften omhandler blant annet hvilke sikkerhetsløsninger som må iverksettes av databehandler (vedrørende behandlingsansvarlig og databehandler i forholdet; kommunene og leverandører).

Sikkerhetsbestemmelsene i forskriftens kapittel om informasjonssikkerhet: §§ 2-1 – 2-16.

Helseregisterloven

Loven skal bidra til å gi helsetjenesten og helseforvaltningen informasjon og kunnskap uten å krenke personvernet, slik at helsehjelp kan gis på en forsvarlig og effektiv måte. Helseregisterloven bygger på de samme hovedprinsippene som POL.

Loven gjelder for helseforvaltningen og helsetjenesten i privat og offentlig sektor ved behandling av helse- og personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler og annen behandling av slike opplysninger når disse inngår eller skal inngå i et register.

Forhold til andre lover: Loven må ses i sammenheng med andre lover og forskrifter, bl.a. POL (regler for behandling av helse- og personopplysninger), POF (informasjonssikkerhet og internkontroll), e-signaturloven og e-forvaltningsforskriften (krav til elektronisk signatur, kommunikasjon og langtidslagring, osv.), pasientrettighetsloven (samtykke, innsynsrett med unntak), helsepersonelloven (taushetsplikt, innsynsrett, utlevering av helseopplysninger ved sammenstilling av opplysninger i flere helseregistre, retting og sletting av helseopplysninger), lov om helsetjenesten i kommunene (behandling av helse- og personopplysninger), og sikkerhetsloven med forskrifter (unntak fra bestemmelser ut fra hensynet til rikets sikkerhet).

Lov om helsetjenesten i kommunene

Viktige bestemmelser om informasjonssikkerhet i loven: Opplysningsplikt til berørte fagmyndigheter om forhold som vedrører arbeidsmiljøloven, produktkontrolloven, forurensningsloven og genteknologiloven; opplysningsplikt til personer som trenger helsehjelp; krav om at kommunen skal innhente politiattest fra helsepersonell (§ 3-1); krav til behandling av personopplysninger (jamfør POL's hovedregler om samtykke og formål); meldings- og opplysningsplikt til kommunestyret ("for den som planlegger eller iverksetter virksomhet som etter sin art kan ha innvirkning på helsen, eller

endring i slik virksomhet.”); opplysningsplikt til tilsynsmyndighet; taushetsplikt (etter forvaltningsloven).

Forhold til andre lover: Loven må ses i sammenheng med andre lover og forskrifter, bl.a. POL, (regler for behandling av helse- og personopplysninger), POF (internkontrollsystemer), helsepersonelloven (innhenting av politiattest i samsvar med helsepersonellovens § 20 a.), forvaltningsloven (lovens regler om klage samt taushetsplikt), kommuneloven (delegering til et interkommunalt organ eller til en annen kommune).

Kommuneloven

§ 27 omhandler interkommunalt samarbeid.

Forvaltningsloven

Loven inneholder bl.a. saksbehandlingsregler for forvaltningen, herunder regler om habilitet for saksbehandlere og andre som har med saken eller saksbehandleren å gjøre. Denne loven inneholder også regler om taushetsplikt (§§13-13e), om informasjons- og veiledningsplikt, om varsling og innsyn og om klager og omgjøring av enkeltvedtak.

E-forvaltningsforskriften

Formålet: Forskriftens formål er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen.

Gjelder for: Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller i medhold av lov.

Forskriften gir mange regler av overordnet karakter. Det er opp til forvaltningsorganet selv å lage nødvendige prosedyrer for bl.a. anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata m.v. knyttet til sertifikater, sikring av aktuelle brukermiljøer som benytter sikkerhetstjenester, tiltak ved mistanke om tap eller misbruk og behandling av personopplysninger og taushetsbelagt informasjon.

Forskriftens kapittel 4 gir bestemmelser om forvaltningsorganets informasjonsplikt til ansatte og brukere (§ 15 og 19), krav til innhenting og samtykke fra ansatte ved bruk av elektronisk signatur (§ 16), forvaltningsansattes bruk av forvaltningsorganets informasjonssystem (§ 18) og restriksjoner på bruk av sertifikat m.v. (§ 17).

Offentlighetsloven

Loven 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)

Aktuelle paragrafer: § 39h som gir hjemmel for nødvendig eksemplarframstilling av og for å framstille sikkerhetskopi av et program. § 39i som regulerer forhold der brukeren skal utvikle et program hvis formål er å fungere sammen med et annet program som vedkommende har rett til å bruke. § 43: Bestemmelsene i denne paragrafen er utarbeidet for å verne vesentlig investering, og for å verne arbeidsinnsats som ikke er av skapende art. Bestemmelsen gir vern mot eksemplarframstilling og spredning. Kapittel 6, § 53a gir forbud mot å omgå effektive tekniske beskyttelsessystemer. For tekniske innretninger til beskyttelse av et datamaskinprogram gjelder det som er bestemt i § 53c. § 53b har bestemmelser som tar hensyn til de negative virkningene som tekniske beskyttelsessystemer kan ha for lovlige brukerinteresser. Bestemmelsene i denne paragrafen gjelder ikke for datamaskinprogrammer. § 54d: Forbud mot å fjerne elektronisk rettighetsinformasjon.

Straffeloven

Herunder § 48a (straffansvar for foretak), og lovparagrafer som naturlig kommer til anvendelse ved brudd på informasjonssikkerheten, herunder datainnbrudd og ulovlig spredning av tilgangsdata (§§ 145 og 145b), avlytting (§ 145a), databedrageri og utroskap (§§ 270-271 – bedrageri og data-bedrageri, § 275-276 – utroskap), forfalskning av dokumenter og informasjon som er lagret og behandlet elektronisk (§ 179 – dokumentfalsk, §§ 182-183), skadeverk på data, datautstyr og IT-infrastruktur (§ 291-292), spionasje (§§ 294, 405a, 139), underslag og tyveri av løsøregjenstander – datautstyr (§§ 255, 256, 257, 258), ulovlig bruk av datakraft (§261), informasjonsheleri (§ 317), taushetsplikt i arbeidet for statlig eller kommunalt organ (§ 121).

Forskrift om revisjon

Spesielt § 11.2.

Forskrift om internkontroll

Lov om arkiv

Lov med av 4.12.1992 og tilhørende forskrifter.

Sikkerhetsloven

Loven omhandler opplysninger som er av betydning for rikets selvstendighet og sikkerhet, dvs. skjermingsverdig informasjon.

Loven gjelder for alle forvaltningsorgan, herunder kommuner. Loven er rettet mot å hindre at konfidensielle opplysninger kommer på avveie – ved bruk av nødvendig/aktuell sikkerhetsgrad. Slik sikker-hetsgradering skal ikke skje i større utstrekning enn strengt nødvendig, og det skal ikke brukes høyere sikkerhetsgrad enn nødvendig. Loven omfatter også sikring av IKT-systemer og datanett som må underlegges sikkerhetsgradering. Loven erstatter det tidligere Datasikkerhetsdirektivet fra Forsvarets Overkommando/Sikkerhetsstaben.

Følgende sikkerhetsgrader benyttes:

- STRENGT HEMMELIG
- HEMMELIG
- KONFIDENSIELT
- BEGRENSET

2.1 Autorisasjon og tilgangsstyring

Formål

Prosedyren skal sikre at informasjoner kun er tilgjengelig for autorisert personell og at det ikke utilsiktet kan leses, endres eller slettes ved konvertering, behandling, lagring, utskrift eller distribusjon.

Omfang

Prosedyren omfatter administrasjon av brukerrettigheter og gjelder for *ansatte,* IT-avdeling, driftsleverandør, konsulenter og fagsystemleverandører.

Beskrivelse

Brukeridentifikasjon

Hver bruker skal tildeles en unik kode for identifikasjon i forbindelse med pålogging til PC, server og nettverk. Tildelingen administreres i AD.

Det skal ikke brukes felles brukerprofiler i fagsystemer. Brukernavn er personlig og kritisk viktig for hendelsesregistrering.

Passordregler

Brukere autentiserer seg i systemet med brukernavn og passord. Regler og forhold rundt passord er beskrevet i egen prosedyre.

Innmelding

- Ansvarlig leder (nivå 1 – 3) fyller ut og signerer innmeldingsskjema. Normalt gjøres dette så snart medarbeideren har akseptert stillingen.
    - Innmeldingen baseres på en nøye gjennomgang av hvilke fagsystemer den ansatte har behov for å ha tilgang til, samt hvilke rettigheter vedkommende skal ha i ulike fagsystemer.

- IT-avdelingen:
    - Kontrollerer at innmeldingen kommer fra person som har myndighet til å melde inn brukere.
    - Registre nyansatte i AD.
    - Gir tilgang til basisprogrammene.
    - Melder til Systemansvarlige hvem som skal ha hvilke tilganger i fagsystemer, ut fra verdiene i innmeldingsskjemaet.

Endring

- Ansvarlig leder (nivå 1 – 3) fyller ut og signerer endringsskjema.
- IT-avdelingen:
  - Kontrollerer at innmeldingen kommer fra person som har myndighet til å melde inn brukere.
  - Gir tilgang til basisprogrammene.
  - Melder til Systemansvarlige hvem som skal ha hvilke tilganger i fagsystemer, ut fra verdiene i innmeldingsskjemaet/skjemaene.

Utmelding

- Ansvarlig leder (nivå 1 – 3):
  - Fyller ut og signerer utmeldingsskjema.
  - Går, sammen med brukeren, gjennom brukerkataloger og e-post, og legger aktuelle kataloger og filer på et sted der andre kan få tilgang. Aktuelle e-poster sendes videre.

- IT-avdelingen:
  - Kontrollerer at utmeldingen kommer fra person som har myndighet til å melde ut brukere.
  - Tar bort tilganger i programvare.
  - Melder til Systemansvarlige hvem som skal slettes fra hvilke tilganger i fagsystemer, ut fra verdiene i utmeldingsskjemaet.
  - Deaktiverer brukerkonto fra fratredelsestidspunkt.
  - Sletter brukerkonto tre måneder etter fratredelse.

3. Systemansvarlig
   - Ta bort tilganger.

Flytting mellom avdelinger

- Håndteres i prinsippet som ut- og innmelding.

Drifts- og systemleverandører

1. IT-avdelingen er ansvarlig for å gi tilgang for drifts- og systemleverandører ved behov.
2. IT-avdelingen er ansvarlig for å kontrollere at det foreligger databehandleravtale før tilganger åpnes.
3. Konti for leverandørene er utilgjengelig inntil det foreligger et behov. Passordreglene er de samme som ved tildeling av brukerrettigheter.
4. Drifts- og fagsystemleverandører skal sørge for at det foreligger tilgangslister over personell fra drifts- og fagsystemleverandører som har tilgang til nettverk og systemer.
   Dersom IT-avdelingen eller andre registrerer at en leverandør har vært inne på en

brukerkonto uten først å ha fått tillatelse, skal dette behandles som en sikkerhetshendelse (se egne retningslinjer).

Avvik

1. Feil ved tildeling av rettigheter, for eksempel ved at en bruker utilsiktet blir tildelt rettigheter til et fellesområde i en sikret sone, skal registreres og behandles som en sikkerhetshendelse (se prosedyre: 2.8 Sikkerhetshendelser, - brudd og svakheter).

Årlig kontroll

- Det skal årlig gjennomføres en kontroll for å sikre at kun autoriserte brukere har tilgang til fagsystemet.

Bruk av arbeidsstasjoner

1. Bruker skal kun logge seg inn på systemet fra en stasjon om gangen. Brukere med dual login er unntak.
2. Bruker skal kun logge seg inn fra stasjon som er klarert for innlogging.
3. Dersom andre skal overta egen arbeidsstasjon skal det logges ut før vedkommende overtar.
4. Det er forbudt å la andre midlertidig benytte arbeidsstasjonen når en selv er logget inn. Gjestebruker skal benyttes.
5. Forlates kontoret skal det logges ut, eller passordbeskyttet skjermblanker skal aktiveres.

2.2 Passord

Formål

Hindre uautorisert tilgang til informasjonssystemene og de opplysninger som er lagret der.

Omfang

Prosedyren gjelder

- Alle ansatte i Midt-Telemarkkommunene.
- Regler for bruk, behandling og oppbygging av passord.

Beskrivelse

Generelt om passord:

- Manuelt tildelt passord skal endres til et passord kun brukeren kjenner.
- Passordet skal lages slik at det ikke er gjenkjennbart.
- Det anbefales at man bruker samme passord til alle fagapplikasjoner.
- Passord skal endres hvert år. Dette skal fremtvinges ved automatikk i påloggingen.
- Konto sperres etter 5 mislykkede påloggingen.
- Det skal legges til rette for "single sign-on" (innlogging i hovedsystem gir direkte tilgang til fagsystemer).

Brukerens håndtering av passord

- Passordet skal aldri deles med andre.
- Dersom det anses nødvendig å låne ut passordet til en annen bruker eller til administrator for å kunne utføre eller fullføre en oppgave, skal passordet endres umiddelbart etter at hensikten med utlånet er oppnådd.
- Har andre fått kjennskap til passordet, må det endres umiddelbart.
- Passordet bør ikke skrives ned. Dersom passordet blir notert, skal det oppbevares på en slik måte at ingen andre får tilgang.
- Brukeren skal ikke benytte samme passord privat og i jobbsammenheng.

Oppbygging av passord – gode passordregler

- Passordet skal bestå av minimum 12 tegn.
- Bruk gjerne en setning.
- Bytt gjerne skrivemåten med et ord til hvordan du uttaler det – skriv dialekt.
- Passordet bør inneholde kombinasjon av tall og store og små bokstaver.

- Passordet bør inneholde minst et spesialtegn # ¤ % & / () = ? eller mellomrom
- Bytt bokstaver med tall, for eksempel:
  Bruk **0** i stedet for **o**, **1** i stedet for **i**, **5** i stedet for **s**, **6** i stedet for **b**, **9** i stedet for **g**
- Bytt bokstaver med tegn, for eksempel:
  Bruk **#** i stedet for **h**, **@** i stedet for **a**, **&** i stedet for **og**, **(** i stedet for **c**

Ting du bør unngå:

- Passord skal ikke inneholde egne initialer, eget navn eller fødselsdato, navn på familiemedlemmer, avdelingsnavn.
- Ikke bruk årets årstall.
- Ikke bruk enkeltord som finnes i ordlister.
- Ikke bruk passord basert på brukernavn.
- Ikke bruk navn på kjente personer, titler på kjente bøker, sanger eller filmer.
- Ikke bruk tallmønster som asdfg (plasseringsrekkefølge på tastaturet) eller 12345.

2.3 Avhending og kassering av brukt IT-utstyr

Formål

- Forhindre at sensitive personopplysninger, interne dokumenter eller gradert informasjon utilsiktet tilfaller uvedkommende.
- Sørge for å ajourføre utstyrslister og sørge for at de er tilgjengelige for andre behov, for eksempel i forbindelse med en beredskapssituasjon.
- Sikre miljømessig riktig avfallsbehandling.

Omfang

Prosedyren gjelder for Midt-Telemarkkommunene og leverandører. Den skal sikre at **alt** brukt datautstyr skal leveres inn til destruksjon og resirkulering.

Beskrivelse

Innlevering

Alt brukt datautstyr leveres til Midt-Telemark IKT (MT IKT). Det er brukeren som er ansvarlig for å levere inn utstyret.

Det kan, i forbindelse med større arbeider, gjøres avtale om henting.

Harddisker og andre elektroniske lagringsmedier

IT-avdelingen skal ta harddisker og elektroniske lagringsmedia ut av brukt utstyr som skal kasseres og gjenvinnes.

- Det skal ikke under noen omstendighet sendes lagringsmedier som inneholder sensitiv informasjon ut av områder som ikke er under kontroll av kommunen.
  - Ved reklamasjon på harddisk, skal leverandøren garantere skriftlig at program og dokumenter på innlevert harddisk slettes.
- Kassering av harddisker:
  - Dokumenter på harddisker som skal kasseres, skal slettes med programvare som er godkjent.

- Harddisken skal merkes med tidspunkt for når den er tatt ut av produksjon, sted og utførende person.
- Det skal holdes oversikt over lagrede harddisker som er kassert.

- Innholdet på minnepenner skal rutinemessig slettes. Minnepenner skal ikke brukes til permanent lagring eller sikkerhetskopiering.
- CD/DVD-plater som er tatt ut av produksjon skal klippes i minst 4 deler eller avmagnetiseres.
- Taper som ikke er i bruk skal makuleres med avmagnetisering.
- Disketter som inneholder sensitiv informasjon skal klippes i minst 8 deler.
- Plater, taper og disketter bør samles inn og sendes MT IKT for makulering og gjenvinning.

Gjenbruk av IT-utstyr

- All gjenbruk av IT-utstyr skal godkjennes av leder for MT-IKT.
- Gjenbruk av harddisker:
  - Dokumenter på harddisker som skal gjenbrukes, skal slettes med programvare som er godkjent av sikkerhetsansvarlig.
  - Det skal holdes oversikt over lagrede harddisker for gjenbruk.

Gjenvinning

- Alt kassert IT-utstyr skal returneres gjennom miljøgodkjent returordning for slikt utstyr.
- Utstyret samles i egen kurv og leveres ekstern leverandør.

2.4 Bruk av datautstyr, databehandling

Formål

Denne prosedyren skal beskrive generelle krav til informasjonssikkerhet ved bruk av datautstyr i Midt-Telemarkkommunene. Den skal leses av alle medarbeidere, som ved signatur skal bekrefte at de:

- Har lest og forstått prosedyren.
- Vil følge de regler og krav som er beskrevet i prosedyren.
- Er kjent med at brudd på prosedyren vil medføre reaksjon og i graverende tilfeller anmeldelse.

Omfang

Denne prosedyren beskriver retningslinjer for bruk av IKT i Midt-Telemarkkommunene. Prosedyren gjelder for alle ledere og medarbeidere, og for annet personell som gjør arbeid eller hospiterer i kommunene. Gjennom underskrift på taushetserklæringen bekrefter alle at de har satt seg inn i dokumentet, og de øvrige informasjonssikkerhetsdokumenter. Samt at de vil forholde seg deretter, og at de er kjent med at det vil bli reagert på brudd på bestemmelsene.

Beskrivelse

Bruk av informasjonssystemer i Midt-Telemark kommunene

Generelt

Dokumenter som inneholder beskyttelsesverdige opplysninger som kan skade enkeltindivider, kun, hvis de blir kjent av uvedkommende, skal graderes, merkes og håndteres i henhold til gjeldende regler.

Kommunenes informasjonssystemer er beregnet for jobbrelaterte formål. Privat bruk, f.eks. e-post og private filer tillates i begrenset omfang, så lenge det ikke påvirker jobbrelaterte oppgaver. Privat e-post mottatt på jobbadresse skal legges i mappe for privat.

Midt-Telemarkkommunene har i utgangspunktet ikke anledning til innsyn i privat e-post eller filer. Unntak gjelder, om virksomheten har behov for virksomhetsrelatert informasjon. Det er etablert en egen rutine for slikt innsyn.

All jobbrelatert informasjon som ikke håndteres av fagsystemer skal lagres på avdelings- eller prosjektområdene på filservere. Hjemmekatalogen skal primært brukes for privat informasjon som den enkelte ønsker å ta vare på.

Ledere er ansvarlige for at medarbeidere har tilgangsrettigheter i samsvar med stilling og arbeidsoppgaver. Det er ledere som melder inn, endrer og melder medarbeidere ut av IT-systemene. Dette gjøres iht. egen prosedyre for autorisasjon og tilgangskontroll.

Opplæring

Før du får tilgang til de aktuelle informasjonssystemene, skal du ha gjennomgått nødvendig opplæring.

Du er selv ansvarlig for å følge de regler som gjelder for bruk av de forskjellige informasjonssystemene, og for behandling av beskyttelsesverdig informasjon i henhold til gjeldende regler.

Brukernavn, passord og skjermsparer

Du får tildelt brukernavn og førstegangs passord av Midt-Telemark IKT (MT-IKT).

Brukernavnet som blir gitt og passord er strengt personlig. Passordet skal ikke oppgis til eller lånes ut til andre, eller ligge tilgjengelig for andre. Dette er et personlig ansvar.

Bestemmelser og veiledninger om passord finner du i egen prosedyre.

Datamaskinen skal som hovedregel låses når arbeidsplassen forlates i kortere eller lengre perioder. Maskinen skal også være satt opp med automatisk skjermsparer med aktivering etter 15 minutters inaktivitet.

Du skal alltid logge ut før du overlater maskinen til andre.

Oppdatering av antivirusprogram og operativsystem

- Antivirusprogram oppdateres automatisk ved innlogging. Servere oppdateres hver time.
- Operativsystemet oppdateres automatisk for sikkerhetskritiske oppdateringer ved innlogging og en gang om natten.
- Oppdateringer som ikke er kritiske, må godtas av den enkelte bruker.
- Bærbar jobb-PC må kobles opp mot det kommunale nettverket regelmessig for å få nødvendig sikkerhetsoppdateringer, minimum 1 gang per måned.

Skrivere og utskrifter

- Utskrifter skal fjernes fra skriveren så snart utskriftsjobben er ferdig.
- Skrivere knyttet til sikret sone bør stå på rom med tilgangskontroll og ved utskrift av sensitive opplysninger skal det brukes sikker utskrift.

Internett

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. Tjenester for ulovlig fildeling og piratkopiering tillates ikke. Ressurskrevende tjenester, eksempelvis radiolytting og TV/video-streaming, skal begrenses for ikke å påvirke jobbrelatert trafikk i nettet på en negativ måte.

Midt-Telemarkkommunene har anledning til å logge informasjon om internett- og e-posttrafikk for å sikre alminnelig drift, samt for sporing ved eventuelle sikkerhetsbrudd.

Det er ikke tillatt å forsøke å forbigå sikkerhetsmekanismer beskrevet i denne sikkerhetsinstruks, for eksempel ved å skjule ikke-tillatte tjenester gjennom andre tjenester.

E-post

- All jobbrelatert e-post (innkommende og utgående) skal gå gjennom MT-IKT sin e-post løsning.
- Dersom e-post må benyttes for overføring av beskyttelsesverdig informasjon, skal informasjonen sendes som kryptert vedlegg til e-post med godkjent krypteringsprogram.
- Brukere er selv ansvarlig for å vurdere hva som er beskyttelsesverdig. Arkivverdig e-post skal journalføres.

Sosiale media

- Ansatte i Midt-Telemarkkommunene må være beviste på hva som deles på sosiale medier. Ansatte vil alltid være en representant for kommunene, i større eller mindre grad.

Mobile enheter (Mobiltelefon, nettbrett, PC, PDA osv.)

- Stasjonære og mobile enheter er i utgangspunktet konfigurert av MT-IKT. Dette oppsettet skal ikke endres av bruker.

- Beskyttelsesverdig informasjon skal ikke lagres på mobile enheter.
- Bærbar jobb-PC kan benyttes i forbindelse med jobb på reiser og hjemme. Jobb-PC skal ikke benyttes til annet enn jobbrelaterte oppgaver.
- Den enkelte bruker er ansvarlig for å håndtere bærbare PC'er og andre enheter med informasjon i henhold til informasjonens klassifisering.
- La aldri bærbar PC, nettbrett, PDA eller annet bærbart utstyr ligge synlig uten tilsyn.

Mobile enheter på fjernaksess

- Mange forskjellige mobile enheter kan koples til kommunenes nettverk ved hjelp av VPN, VDI og andre eksterne påloggingsmuligheter.
- Det skal kun benyttes løsninger for ekstern pålogging til kommunenes nettverk, som er satt opp og levert av MT-IKT.
- Brukerne er ansvarlige for sikkerhet ved bruk av eksterne nettverk, og i forhold til hvor en sitter og jobber på fjernaksess. Innsyn og skjerming er sentrale tema, og sikkerheten skal ivaretas.

Webmail

Outlook Web Access er en fullskala kopi av Outlook som kan aksessere fra hvilken som helst datamaskin med internett kobling. Med dette følger også ett ansvar, offentlig e-post kan inneholde mye sensitive opplysninger som er unntatt offentligheten.

- Ved pålogging på Outlook Web Access får man to valg, offentlig eller privat datamaskin. Det er meget viktig at man velger riktig her.
- Vedlegg må ikke lagres lokalt på eksterne maskiner og ved bruk av offentlige maskiner vil vedlegg bli åpnet i ett program som kun tillater lesing.
- Det er viktig at epost ikke leses når det er mennesker i nærheten som kan se/kopiere informasjonen.

Sikkerhetskopiering

For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på, eventuelt kopieres til, servere i Midt-Telemarkkommunenes nett. For jobb-PC som benyttes i forbindelse med reiser og hjemmearbeid, må oppdatering mot servere gjøres regelmessig, spesielt dersom andre er avhengig av informasjonen og den ligger lokalt på PC-en.

Ved behov for gjenoppretting av sikkerhetskopiert informasjon, kontakt MT-IKT.

Installasjon av programvare og maskinvare

- Det skal ikke benyttes programvare som avviker fra lisensavtaler.
- All programvare på maskinen skal godkjennes av MT -IKT. Dette gjelder både stasjonære og mobile enheter.
- Dersom du har behov for ytterligere lisensiert programvare, ta kontakt med MT-IKT.
- All maskinvare og lagringsmedia/harddisk skal være registrert hos MT-IKT, dersom dette mangler skal MT-IKT varsles.

Modem-/bredbåndstilknytninger

Ekstern tilkopling mot kommunenes nett tillates kun etter godkjenning fra MT-IKT og kun med programvare som er godkjent og satt opp av konsulenter derfra.

Private enheter
Jobbrelaterte person- og fortrolige opplysninger skal ikke lagres på private enheter.

Reparasjon, service og vedlikehold
Alle feil eller mistanker om feil i informasjonssystemet (både maskinvare og programvare) skal rapporteres til MT-IKT snarest mulig.

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

Håndtering av informasjon og fysiske medier

Håndtering
Fysiske dokumenter (papirer) og lagringsmedia som CD, DVD, disketter, minnepinner med mer skal behandles iht. de aktuelle lovbestemmelsene som arkivlov offentlighetslov og beskyttelsesforskriften tilsier.

Kassering av medier
Disker, lagringsmedia og utstyr som inneholder harddisker og annet lagringsmateriale (f.eks. minnebrikker, backuptaper) skal kasseres etter rutine for avhending og kassering av lagringsmedia.

Fysisk adgang

Adgangskort
Dersom du mister nøkkel/inngangsbrikke, meld umiddelbart fra til kommunens ansvarlige for nøkkel/nøkkelkort.

Ansatte som slutter eller går ut i permisjon, skal levere nøkkel/inngangsbrikke tilbake til administrasjonen.

Besøkende
Den som mottar besøk, er ansvarlig for at besøkende:

- Hentes og følges tilbake av den som mottar besøket.
- Ikke oppholder seg i kommunenes lokaler uten i følge av en av de ansatte.

Personellsikkerhet

Sikkerhetsinstruks og taushetserklæring

Ansatte, konsulenter og vikarer skal rette seg etter bestemmelsene i dette dokumentet og underskrive taushetserklæring.

Konsekvenser ved brudd på retningslinjene

Konsekvenser for ansatte som har forårsaket brudd på sikkerhetsreglene, vil bli vurdert i hvert enkelt tilfelle og kan ved alvorlige brudd føre til oppsigelse/avskjed. Det er verdt å merke seg at brudd på taushetsplikt har en strafferamme på to år.

Rapportering og avvik

Rapportering av sikkerhetsbrudd/hendelser

Meld straks fra til personvern- og sikkerhetsansvarlig dersom du oppdager sikkerhetsbrudd eller hendelser som kan ha betydning for sikkerheten.

Dersom det oppdages virus/orm/trojaner på minnepinne/diskett/Cd-rom, skal MT-IKT varsles og minnepinne/diskett/Cd-rom leveres MT-IKT umiddelbart.

Avvikshåndtering

Avvik på denne instruks skal håndteres i henhold til avviksprosedyre og skal varsles til personvern- og sikkerhetsansvarlig umiddelbart.

Dersom brukere har prosjektspesifikke behov som avviker fra denne prosedyren, skal leder på nivå 1 eller 2 sende en anmodning til personvern- og sikkerhetsansvarlig.

2.5 Bruk av nettbrett og smarttelefoner

Formål

Denne prosedyren skal beskrive generelle krav til informasjonssikkerhet ved bruk av nettbrett og smarttelefon i Midt-Telemarkkommunene.

Omfang

Prosedyren gjelder for alle ledere og medarbeidere som bruker nettbrett eller smarttelefon i sitt arbeid for Midt-Telemarkkommunene.

Beskrivelse

Generelt

Denne prosedyren beskriver retningslinjer for bruk av nettbrett og smarttelefon i Midt-Telemarkkommunene.

For generell bruk av disse enhetene vises det til **2.4 Bruk av datautstyr, databehandling.**

Med i den digitale hverdagen kommer muligheten for å lese e-post på mobiler og lesebrett.

Dette er også ett behov for enkelte brukere i Midt-Telemarkkommunene, og med den nylig utførte oppgraderingen til Exchange Server 2010 er sikkerheten godt i varetatt og tjenesten kan tas i bruk. I første omgang er dette et tilbud til administrative ledere og ansatte med behov for kontinuerlig tilgjengelighet.

Med dette følger også ett ansvar. Offentlig e-post inneholder ofte sensitive opplysninger som er unntatt offentligheten. Derfor er det ekstra viktig at sikkerheten står i fokus.

Retningslinjer for bruk av nettbrett er:

- Enheten må beskyttes med skjermpassord og dette skal aktiveres automatisk etter 2 minutter inaktivitet.
- Enheten må beskyttes av PIN-kode for SIM-kort.
- Innkjøp og grunnoppsett utføres av MT-IKT. Enheten skal registreres i sentralt systemverktøy hos MT-IKT.
- Installasjon av applikasjoner skal samstemme med liste med ”godkjente” applikasjoner utarbeidet av personalavdelingene i de tre kommunene i samarbeid med MT-IKT.
- Bruk av ekstern tjeneste for lagring og deling av dokumenter på internett knyttet opp mot det kommunale nettverket er ikke lov.
- Sensitive data skal ikke lagres på enheten.
- Eksempler på sensitive informasjon:
- Personopplysninger
    - o Virksomhetskritisk informasjon.
    - o Informasjon unntatt offentligheten.
    - o Informasjon underlagt sikkerhetsloven eller beskyttelsesinstruksen.
- Om enheten blir tapt meld fra snarest på telefon til MT-IKT: 35 05 92 50 slik at innholdet blir fjernslettet.
- MT-IKT tar ingen sikkerhetskopi av nettbrett per i dag.

Retningslinjer for bruk av e-post på mobil/nettbrett

- E-postmappen vil kun inneholde e-post fra de siste 14 dager.
- Vedlegg kan leses på enheten, men ikke lagres.

- Telefonen låses etter 3 min inaktivitet, brukeren må selv legge inn en kode på 6 siffer eller passord når e-post blir aktivert på enheten.
- Om enheten blir tapt må den slettes. Dette kan gjøres via Outlook Web Access eller ved å kontakte MT-IKT.

Beskrivelse av sletting

Trykk på **Alternativer** (øverst på høyre side) og deretter **Vis alle alternativer** i listen der.
Velg **Telefon** i meny til venstre.
Velg riktig mobil/nettbrett i listen og deretter trykk på **Tøm enhet** .

2.6 Fysisk sikring

Formål

Prosedyren skal sikre uautorisert adgang til objekter og utstyr benyttet til behandling av informasjon, særlig behandling av sensitive personopplysninger, eller at de ikke er tilgjengelig når liv og helse står på spill.

Prosedyren skal sikre utstyr mot andre påvirkninger som vil være i stand til å sette informasjons- og kommunikasjonssystemer ut av drift eller hindre normal drift.

Prosedyren skal sikre tilgang til objekter for Nødetater.

Omfang

Alle virksomheter skal ha tiltak for å hindre at uautoriserte får fysisk adgang til informasjon som for disse normalt sett skal være utilgjengelig.

Behandlingsansvarlig skal sørge for at egne lokaler og utstyr er forsvarlig sikret.

Adgang til lokaler og utstyr hvor personopplysninger behandles skal kontrolleres. Virksomheten må vurdere behovet for å innføre fysisk områdeinndeling av lokaler. Denne sikringen kan gjennomføres ved bruk av adgangskontroll til lokaler eller bruk av spesielle sikringsmekanismer knyttet til bruk av selve utstyret.

Den fysiske sikringen er en vesentlig del av det totale sikkerhetskonseptet.

Tiltakene for fysisk sikring av områder, objekter og utstyr skal være tilpasset virksomhetens størrelse og hvor det behandles informasjon.

Tilgang og rutiner for nødetater skal beskrives.

Beskrivelse

Fysisk sikring av informasjonssystemer i Midt-Telemarkkommunene

Generelt

Beskrivelsene nedenfor er eksempler på tiltak som kan gjennomføres for å hindre uautorisert adgang til utstyr. For å sikre at tiltakene er tilpasset den enkelte virksomhets behov og trusselbilde, bør alle de ulike områdene som er beskrevet i denne prosedyren vurderes og tiltak identifiseres gjennom en risikovurdering.

Brudd på den fysiske sikkerheten til områder og utstyr vil øke faren for at uvedkommende får tilgang til elektronisk lagrede personopplysninger, virksomhetssensitiv eller gradert informasjon. Det er et samspill mellom tiltak for den fysiske sikringen og tiltak som er iverksatt for elektronisk sikring. Tiltakene er gjensidig avhengig av hverandre for at en skal kunne oppnå tilfredsstillende sikring av helse- og personopplysninger.

Nr.	Aktivitet/Beskrivelse	Henvisninger
1	**Risikovurdering** a) Risikovurderingen må ta utgangspunkt i de konkrete fysiske arealene som skal sikres mot uautorisert adgang. b) Risikovurderingen bør belyse behov for å definere arealene i ulike soner, ut fra virksomhetens størrelse. En sonemodell for fysisk adgang til helse- og personopplysninger for interne og eksterne kan defineres slik: – Åpen sone: Arealer hvor publikum har fri adgang, korridorer, venterom, fellesarealer, områder med alminnelig ferdsel – Indre sone: Åpne arbeidsplasser, arealer beregnet kun for medarbeidere i virksomheten, evt. publikum i følge med medarbeidere. – Sikker sone: Areal hvor kun spesielt godkjente medarbeidere har adgang, og hvor publikum ikke skal ha adgang, datarom, rom med nettverk, servere og kommunikasjonsutstyr. c) For mindre virksomheter der soneinndeling ikke er mulig må risikovurderingen belyse risiko for adgang til informasjon innen det aktuelle arealet	Se skjema iht. vernerunde: «Risikovurdering – personvernomsyn – med forslag til tiltak».

2	**Nøkler/adgangskort** a) Identifiser områder og rom hvor utstyr med helse- og personopplysninger er plassert b) Det skal foreligge en oversikt over hvem som har tjenstlige behov for adgang til aktuelle områder og rom. Adgang til dedikerte rom med driftsutstyr (servere og utstyr) skal kun gis til personell med absolutt behov for adgang. Generelt skal adgang i størst mulig grad begrenses. c) Det skal foreligge en kvitteringsliste for tildeling av nøkler/adgangskort. Alle som får utlevert og leverer inn nøkler/adgangskort skal kvittere med navn, sted og dato for utleveringen/ innleveringen. Listen bør revideres årlig, evt. hyppigere når adgangene ofte endres.	Se adgangsplan/nøkkelplan Se nøkkelliste
3	**Adgang til driftsutstyr (data- og kommunikasjonsrom)** **Sikkerhetstiltak skal hindre at annet enn autorisert personell får adgang til slikt utstyr** a) Mindre virksomhet: Servere og annet nettverksutstyr skal oppbevares i låst skap eller rom med sylinderlås. Dersom det benyttes et skap, skal dette skrus fast til veggen eller gulvet. Skapet skal ikke plasseres i resepsjonen/publikumsområde. Resepsjon/publikumsområde skal heller ikke benyttes som rom for oppbevaring av utstyret. b) Større virksomhet: Alle servere og annet nettverksutstyr skal oppbevares i et eget datarom, fortrinnsvis med kodelås. Det skal også være installert et system for varsling av innbrudd, som skal være tilkoplet kodelåsen. Andre alarmtiltak for sikring som brann- vann og temperatur skal knyttes opp mot alarmsystemet. Systemet skal varsle en ansvarlig for	Kommuner

	datarommet, alternativt vaktsentral. c) Adgang til data- og serverrom bør registreres. F.eks. kan det føres en oversikt, hvor alle besøk registreres med navn, leverandør, oppdragsbeskrivelse, dato, tid for inn og ut, og servicemedarbeiderens signatur. d) Adgang og rutiner for nødetater beskrives for hvert objekt. e) Skrivere og arbeidsstasjoner som er plassert i tilknytning til fellesområder skal fysisk sikres slik at uvedkommende ikke får adgang til informasjon.	• Brann: Slukkemidler, tilgangsmuligheter. Kontaktperson • Politi: Tilgangsmuligheter + alternative. Kommunikasjonsmidler. Risikoområder. Kontaktperson • Ambulanse: Risikoområder, transportmåter. Energiverk/Montører: Må beskrives hvordan disse får tilgang til Strømtavler. Frakopling av strøm. Tilkopling av ekstern strøm. Kontaktperson.
4	**Bærbart utstyr og hjemmekontor** Bærbart utstyr omfatter papir, PC, bærbare lagringsmedier, nettbrett og mobiltelefoner. a) Utstyr skal sikres slik at uvedkommende ikke på noen måte kan tilegne seg utstyr eller informasjon som er lagret på dette under transport, oppbevaring og bruk av dette. b) Utstyr som behandler helse- og personopplysninger skal inkluderes i virksomhetens arbeid med informasjonssikkerhet, herunder risikovurderinger, adgangsregulering, fysisk sikring og prosedyrer for bruk, på linje med andre informasjonssystemer.	Se også kapittel 2.17 «Sikring av mobilt utstyr utenfor virksomheten». og Normen Faktaark 18 – Sikring av bærbart utstyr. Normen Faktaark 29 – Hjemmekontor.
5	**Medisinsk teknisk utstyr** a) Teknisk utstyr som behandler helse- og personopplysninger skal inkluderes i virksomhetens arbeid med informasjonssikkerhet, herunder risikovurderinger, adgangsregulering, fysisk sikring	

	og prosedyrer for bruk, på linje med andre informasjonssystemer.	Diktafoner, telefonsvarere
6	**Besøkende** a) Besøkende skal normalt ledsages i åpen sone. Ledsaging er et absolutt krav i indre og sikret sone. **Besøk utenom ordinær arbeidstid skal begrenses.** Dette innebærer følgende: a) Områder der sensitive personopplysninger behandles skal være kontrollert av adgangskontroll-system. b) Tildelte adgangsrettigheter skal begrenses til det som er nødvendig ut fra tjenstlig behov, og skal alltid fjernes når arbeidsforholdet opphører c) Besøkende skal alltid følges av medarbeider som er autorisert for adgang til området, og skal aldri etterlates alene i slike områder.	

Adgangskort

Tapte nøkkel/inngangsbrikke, meldes umiddelbart fra til administrasjonen eller sikkerhetsansvarlig.

Ansatte som slutter eller går ut i permisjon, skal levere nøkkel/inngangsbrikke tilbake til administrasjonen.

Adgang til utstyr

Ved bruk av mekanismer for sikring av adgang til utstyr for behandling av sensitive personopplysninger, skal mulig bruk av utstyret begrenses til de som har tjenstlig behov for dette.
Det utstyret som benyttes ved behandling av sensitive personopplysninger (arbeidsstasjoner og skrivere, kopimaskiner, telefaks etc.) må innrettes slik at tilgangen begrenses til de som har tjenstlig behov. Dette gjennomføres ved bruk av betryggende rutiner og teknisk sikring for å hindre uautorisert bruk at utstyret, samt egnede tiltak mot innsyn.

Rapportering og avvik

Meld straks fra til sikkerhetsansvarlig dersom du oppdager sikkerhetsbrudd eller hendelser som kan ha umiddelbar betydning for sikkerheten. Deretter meldes forholdet iht. **2.8 «Prosedyre for Sikkerhetshendelser, brudd og svakheter».**

Spesielle prosjekter

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

2.7 Hendelseslogging og oppbevaring

Formål

Prosedyren skal sikre at Midt-Telemarkkommunene registrerer og lagrer aktivitet i IT-systemer og andre systemer hvor det er krav til hendelsesregistrering.

Omfang

Prosedyren gjelder for alle systemer i Midt-Telemarkkommunene med krav til hendelsesregistrering, uavhengig av hvem som drifter dem.

Beskrivelse

Prosedyre for hendelsesregistrering

a) Databehandlingsansvarlig skal påse at det etableres prosedyrer som sikrer at hendelsesregistrering etableres. Leder nivå 1 skal følge opp at prosedyrene etterfølges.
b) Prosedyren skal

- Ta hensyn til at hendelsesregistrering kan innebære en ny behandling av personopplysninger som kan være meldepliktig. Meldeplikten gjelder ikke om behandlingen har som formål
    - å administrere systemet, eller
    - å avdekke/oppklare brudd på sikkerheten i edb-systemet.
- Ivareta kravet om at hendelsesregistrene skal kunne sammenholdes med autorisasjonsregister og tilstedeværelsesregister.
- Ivareta kravet om at hendelsesregistrene skal analyseres slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke.
- Ivareta kravet om at Datatilsynet skal varsles dersom det har blitt foretatt en uautorisert utlevering av eller tilgang til helse- og personopplysninger.

Hendelsesregistrering skal etableres for

- Tilgang til behandlingsrettede helseregistre og fagsystemer
  - All tilgang til og autorisert bruk av behandlingsrettede helseregistre og fagsystemer.
  - Alle forsøk på uautorisert bruk av behandlingsrettede helseregistre og fagsystemer.
  - All bruk av nødrettstilgang med begrunnelse.

a) Infrastruktur
- Sikkerhetsrelevante hendelser i sikkerhetsbarrierer (for eksempel brannmur og ruter) slik som:
  - Alle forsøk på ulovlig tilgang både internt og eksternt.
  - Alle brudd på regler som forbyr trafikk.
  - Alle brudd på regler som slipper inn lovlig trafikk fra eksterne tilknytninger.
  - Alle forsøk på uautorisert bruk av nettverksoperativsystemer.

Hendelsesregisteret skal som minimum inneholde

a) For autorisert bruk:
- Entydig identifikator for den autoriserte brukeren (Se Autorisasjonsregister).
- Rollen den autoriserte brukeren har ved tilgangen.
- Virksomhetstilhørighet for den autoriserte brukeren (vanligvis virksomhet eller databehandler).
- Organisatorisk tilhørighet til den som er autorisert (avdelingsnavn eller avdelingskode er normalt tilstrekkelig). Kan være lik virksomhetstilhørighet om virksomheten ikke har avdelingsstruktur.
- Hvilken type opplysninger det er gitt tilgang til.
- Grunnlaget for tilgangen (for eksempel helsehjelp, nødrettstilgang, administrativ bruk).
- Tidspunkt og varighet for tilgangen (dato og klokkeslett).
- Begrunnelse ved bruk av nødrettstilgang.
- Ved fjernaksess fra leverandør:
  - Informasjon om hvem som er tildelt autorisasjon.
  - Til hvilken rolle autorisasjonen er tildelt.
  - Formålet med autorisasjonen.
  - Tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt.
  - Informasjon om hvilken virksomhet den autoriserte er knyttet til.

b) For forsøk på uautorisert bruk:
- Brukeridentiteten som ble benyttet.
- Tidspunkt (dato og klokkeslett).
- IP-adresse eller annen identifikasjon av PC/arbeidsstasjon som ble benyttet (for eksempel MAC-adresse eller NAT-adresse).

Sikring og oppbevaring av hendelsesregister

a) Hendelsesregistrene skal sikres mot innsyn, endring og sletting av uautorisert personell.
b) Hendelsesregistre skal oppbevares i minimum 2 år.

Hendelsesregisteret som bevis

c) Hendelsesregister som skal benyttes som bevis bør speilkopieres til annet medium før analyser gjennomføres.
d) Speilkopieringen bør gjennomføres under tilsyn av 2 eller flere personer.
e) Det bør opprettes en skriftlig protokoll for speilkopieringen som sier hva som er gjort. Protokollen skal signeres av de som var tilstede og oppbevares sammen med det registrerte avviket.

Bruk av hendelsesregisteret

f) Elektroniske hendelsesregistre skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd på regelverket (se også Helseregisterloven § 13a og Helsepersonelloven § 21 a.)
g) For manuelt førte hendelsesregistre skal virksomheten etablere prosedyrer for tilfredsstillende analyse av registrene.
h) Dersom brudd avdekkes skal personalmessige reaksjoner iverksettes
i) Dersom personalmessige reaksjoner ikke har nødvendig effekt over tid, dvs. det er gjentatt tilgang av flere personer som ikke er autorisert, skal nødvendige tekniske tiltak iverksettes.
j) All bruk av nødrettstilgang skal dokumenteres og hvert enkelt tilfelle skal følges opp som et avvik for å påse at begrunnelse er relevant.
k) Ved brudd på regler ved tilkobling til nett utenfor virksomheten skal kanalen stenges inntil ny sikker løsning er etablert.
l) Ved brudd på regler om logisk skille mellom Internett og nettverk der helse- og personopplysninger behandles skal regelbruddet behandles som avvik og personalmessige konsekvenser vurderes.
m) Ved brudd på regler om at sensitive personopplysninger ikke skal utleveres ved hjelp av epost skal regelbruddet behandles som avvik og personalmessige konsekvenser vurderes.

Sletting av hendelsesregistre

n) Dersom oppføringer i hendelsesregistre kan knyttes til enkeltpersoner, skal hendelsesregistrene slettes når de sikkerhetsmessige formål er oppfylt, men først etter 2 år.

2.8 Sikkerhetshendelser, -brudd og svakheter

Formål

Hensikten med prosedyren er å etablere oversikt over forhold som utfordrer og truer informasjonssikkerheten i Midt-Telemarkkommunene slik at det kan treffes nødvendige tiltak for å rette opp feil og gjenopprette nødvendig sikkerhet i informasjonssystemene.

Omfang

Prosedyren gjelder

- Hvordan melding av sikkerhetshendelser, brudd og svakheter innarbeides i kommunene og leverandørenes eksisterende avvikshåndteringssystemer.
- Hvordan data generert gjennom disse systemene behandles på regionsnivå.

Beskrivelse

Melding av sikkerhetshendelser, -brudd og svakheter følger den enkelte kommunes generelle avvikshåndteringssystem. Ved avviksmeldingen legges utfylt hms-skjema "Melding og tiltaksskjema ".

Når meldingen er sluttbehandlet i kommunens linjeorganisasjon sendes kopi til Personvern og sikkerhetsansvarlig som sammenfatter hendelser, brudd og svakheter på kommunenivå.

Personvern og sikkerhetsansvarlig rapporterer til Koordineringsansvarlig som sammenfatter for regionen som helhet. Forslag til tekniske regionstiltak fremmes til MT-IKT, i tråd med støtteprosedyre for Endringsstyring og forslag til organisatoriske tiltak fremmes rådmannsgruppen i Midt-Telemark.

2.9 Meldeplikt – prosedyre

Formål

Sørge for meldeplikt overholdes for systemer som er meldepliktige i henhold til Personopplysningsloven.

Omfang

Prosedyren gjelder

Prosedyren gjelder for de tre kommunene i Midt-Telemark og omhandler meldeplikt etter Personopplysningsloven.

Beskrivelse

Opplysninger som er underlagt Personopplysningslovens (POL) meldeplikt skal behandles i sikret nett/sikre soner. Dette gjelder tilgang til datasystemer og fysisk adgang til områder der det blir behandlet sensitive personopplysninger.

Meldepliktig funksjon

Behandlingsansvarlig er ansvarlig for at det blir sendt inn melding til Datatilsynet i henhold til prosedyren. Systemeier er ansvarlig for å melde via Datatilsynets hjemmesider: http://www.datatilsynet.no/templates/article____204.aspx.

Kvitteringen fra datatilsynet fungerer som dokumentasjon på at meldeplikten er oppfylt. Kvitteringen journalføres. Se generelle kommentarer til registrering.

Meldefrekvens

Det skal sendes inn en ny melding når:

- Det blir en ny juridisk person som står som behandlingsansvarlig.
- Formålet med meldingen blir endret.
- Etter tre år skal det alltid sendes ny melding.

Oversikt

Meldinger skal fremgå i dokumentet 3.6 «Informasjonssikkerhet ved virksomhet/avdeling 'Meldeplikt - Oversikt over behandlinger'» som skal arkiveres i sak/arkivsystemet for hver kommune og oppdateres årlig.

2.10 Innsyn, retting og sletting

Formål

Hensikten med denne prosedyren er:

- Å sikre at registrerte får innsyn i de personopplysninger de har krav på.
- At feilaktige helse- og personopplysninger blir rettet.
- At mangler ikke får betydning for den personen det gjelder.
- At helse- og personopplysninger oppbevares og slettes slik lover og forskrifter tilsier.

Omfang

Prosedyren omfatter krav til og gjennomføring av innsyn, retting og sletting av helseopplysninger og andre sensitive personopplysninger.

Prosedyren gjelder for alle behandlinger i Midt-Telemarkkommunene.

Beskrivelse

Innsyn i personopplysninger

Rett til innsyn i personopplysninger:

Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:

a) Navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,
c) formålet med behandlingen,
d) beskrivelser av hvilke typer personopplysninger som behandles,
e) hvor opplysningene er hentet fra, og
f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om

a) Hvilke opplysninger om den registrerte som behandles, og
b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i første ledd bokstav a – f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser.

Retten til informasjon etter annet og tredje ledd gjelder ikke dersom personopplysningene behandles utelukkende for historiske, statistiske eller vitenskapelige formål og behandlingen ikke får noen direkte betydning for den registrerte.

Om innsynet

- Frist for å svare registrerte er 30 dager.
- Når kravet gjelder innsyn i journal, skal dette anmerkes i journalen.
- Innsyn etter personopplysningsloven og helseregisterloven er alltid gratis. Det er ikke adgang til å dekke noen form for utgift knyttet til bruk av innsynsrettigheter.
- Innsynet skal skje konkret mot en bestemt behandling.
- Barn over 16 år har selvstendig innsynsrett i sin journal på lik linje med myndige. Barn mellom 12 og 16 år har en viss grad av innsynsrett, men må vurderes nærmere ut fra barnets alder og modenhet og omstendighetene forøvrig.
- Vedkommende trenger ikke å begrunne sitt krav.
- Før innsyn kan gis må unntakslisten nedenfor konfereres.

Innsynets form:

- Om innsynet gjelder helse- og personopplysninger skal innsynet alltid skje ved personlig fremmøte ved framvisning av gyldig legitimasjon.
- Ber den registrerte om skriftlig orientering skal det i etterkant av personlig oppmøte sendes et personlig brev. Det er ikke anledning til å benytte e-post.

Innsyn i journal kan ikke gis om:

Det er påtrengende nødvendig for å hindre fare for liv eller alvorlig helseskade for den registrerte selv, eller innsyn er klart utilrådelig av hensyn til personer som står den registrerte nær.

Pasientjournal:

Om innsyn nektes må presis henvisning til unntakshjemmelen beskrives. Av hensyn til en åpen dialog skal vedkommende gjøres kjent med at vedkommende kan klage til Helsetilsynet i fylke.

Retting og sletting av helse- og personopplysninger

Retting

- Dersom det er registrert helse- eller personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal de rettes av eget tiltak eller på begjæring fra den registrerte.
- Rettingen skal gjøres ved at de feilaktige opplysningene markeres og suppleres med korrekte opplysninger.

Sletting

Vurdering for oppbevaring av helse og personopplysninger:

- Virksomheten skal ikke lagre helse og personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven, regnskapsloven (10 år) eller annen lovgivning, skal de slettes.
- Personopplysninger kan lagres etter at formålet er oppfylt for historiske, statistiske eller vitenskapelige formål. Dette gjelder bare om samfunnets interesse i at opplysningene lagres, klart overstiger personvernulempene. I så fall skal virksomheten sørge for at opplysningene ikke oppbevares på måter som gjør det mulig å identifisere den registrerte lenger enn nødvendig.

Spesielt om oppbevaring og sletting av pasientjournaler:

- Pasientjournalene skal oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem

- Journalene skal oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem. Hvis ikke journalopplysningene deretter skal bevares i henhold til arkivloven eller annen lovgivning, skal de slettes, Deponering bør ikke skje før det er gått minst 10 år etter siste innføring i journalen

2.11 Risikovurdering

Formål

Hensikten med denne prosedyren er å gi en metodikk for gjennomføring og dokumentasjon av en fullstendig risikovurdering innen informasjonssikkerhet i Midt-Telemarkkommunene.

Beskrivelse

Midt-Telemarkkommunene har tatt i bruk en metode for risikokartlegging og vurdering som ligger i HMS-systemet. Denne metode skal brukes som årlige vurderingen av informasjonssikkerhet samtidig med den årlige HMS- gjennomgangen. Denne metoden skal også benyttes i andre situasjoner hvor risikovurdering av informasjonssikkerheten er nødvendig.

Rettledning for bruk av metoden – Bø kommune:

http://www.bo.kommune.no/Handlers/fh.ashx?MId1=1535&FilId=2034

Skjema for risikovurdering – Bø kommune:

http://www.bo.kommune.no/Handlers/fh.ashx?MId1=1536&FilId=2045

2.12 Samarbeidsparter, leverandører

Formål

Hensikten med denne planen er å sikre at samarbeidspartnere og leverandører oppfyller kravene til informasjonssikkerhet som er fastsatt gjennom lov og forskrift, Midt-Telemarkkommunenes sikkerhetsplan samt Midt-Telemarkkommunenes kontraktsmessige forpliktelser.

Omfang

Prosedyren regulerer sikkerhetsmessige forpliktelser mellom Midt-Telemarkkommunene og samarbeidspartnere som i ulik grad vil kunne påvirke informasjonssikkerheten i Midt-telemarkkommunene. Prosedyren gjelder for leverandører av produkter og tjenester knyttet til:

- Driftsleveranse (driftsleverandør).
- Databehandling: Leveranser som kan innebære tilgang til personopplysninger for at den behandlingsansvarlige (kommunene) kan gjennomføre sine rettslige plikter eller rettigheter.
- Utvikling av Midt-Telemarkkommunenes sikkerhetsprosedyrer.
- Eventuelle andre produkter og tjenester som kan ha betydning for informasjonssikkerheten.

Beskrivelse

Krav til samarbeidspartnere

Driftsansvarlig har ansvar for at bruken av samarbeidspartnere og leverandører blir regulert gjennom skriftlige kontrakter inklusive bestemmelser om informasjonssikkerhet. Omfanget og kravene i kontraktene skal være tilpasset leverandørenes/samarbeidspartnernes produkter og tjenester. Det skal tas hensyn til at kontraktene oppfyller kravene til informasjonssikkerhet som er fastsatt i særlovgivning, Midt-Telemarkkommunenes sikkerhetsregelverk og kontraktsmessige forpliktelser.

Vurdering, godkjenning og valg av samarbeidspartnere

Driftsansvarlig har ansvar for vurdering og valg av samarbeidspartnere. Vurdering av sikkerhetskrav til en løsning er beskrevet i prosedyren Sikkerhet ved anskaffelse. Ved vurdering av leverandøren i skal det i tillegg legges vekt på:

- Virksomhetens sikkerhetsstrategi og evt. sikkerhetssystem/sikkerhetsregelverk.
- Resultat fra sikkerhetsrevisjoner
- Virksomhetens referanser og omtaler i markedet.

Kontrakter med leverandører

Krav til informasjonssikkerhet i kontrakter skal vurderes ut fra hvilket sikkerhetsansvar som påhviler den respektive samarbeidspartneren gjennom dens produkter og tjenester.

Kontrakter skal inneholde nødvendige krav til informasjonssikkerhet, sikkerhets og taushetserklæringer for leverandører og personell involvert i leveransen.

Normalt skal dette dekkes gjennom en databehandleravtale som vedlegg til kontrakten.

2.13 Sikkerhet ved anskaffelse

Gjennomføringsansvar: Alle som gjennomfører IT-anskaffelser i Midt-Telemarkkommunene kan bruke denne prosedyren som rettesnor.

Formål

Hensikten med denne planen er:

- Danne grunnlag for felles forståelse mellom leverandører og Midt-Telemarkkommunene om sikkerhetskravene til IT-systemet, leveransen og tilhørende tjenester.
- Forebygge sikkerhetshendelser og -brudd i implementerings- og driftsfasen.
- Være utgangspunkt for etablering/endring av eksisterende sikkerhetsdokumentasjon.
- Grunnlag for senere sikkerhetsevaluering av IT-systemet og -leverandøren og for gjennomføring av sikkerhetsrevisjoner knyttet til systemet.

Omfang

Prosedyren kan brukes som rettesnor for alle som gjennomfører IT-anskaffelser i Midt-Telemarkkommunene.

Prosedyren skal sikre at krav til informasjonssikkerhet ivaretas ved anskaffelsen, og omfatter:

1. Sikkerhetsvurdering
2. Sikkerhetskrav
3. Sikkerhetstiltak
4. Sikkerhetstesting og kontroll
5. Håndtering av avvik

Hvert trinn er beskrevet på følgende måte:

1. Formål: Beskrivelse av hvorfor fasen blir benyttet i modellen.
2. Forutsetninger: Fasens input.
   Beslutningsgrunnlag: Ønsker, krav, behov, mål, planer, budsjetter, osv.

   Henvisning til og evt. beskrivelse av hvilket regelverk og hvilke rammebetingelser som ligger til grunn og som vil være bestemmende for framgangsmåter og for konklusjonene/beslutningene: Relevante lover/forskrifter, rammebetingelser for Midt -

Telemarkkommunene (krav/mål, retningslinjer, forpliktelser) og andre individuelle forutsetninger i kommunene.

3. Forventede resultater: Fasens output (en del av neste fases input).
4. Aktiviteter: Beskrivelse av alle aktivitetene.

Trinn 1: Sikkerhetsvurdering

Formål

- Identifisere og beskrive faktorer som vil være avgjørende for sikkerhetsvurderingen ved oppgradering eller innføring av IT-systemer for Midt-Telemarkkommunene.
- Foreta en sikkerhetsvurdering basert på disse faktorene.
- Skape aksept og forståelse for sikkerhetsvurderingen i prosjektorganisasjonen.
- Grunnlag for etablering av sikkerhetskrav.

Forutsetninger

Fasens input:

- Prosjektbeskrivelse med mål, planer og budsjettramme.
- IT-systemets omfang: Maskiner, tilleggsutstyr/-funksjonaliteter, program, komponenter.

Faktorer som vil være avgjørende for sikkerhetsvurderingen og som vil danne grunnlag for sikkerhetskravene:

1. IT-systemets virkeområde (sikkerhetsløsninger, infrastruktur, fagsystemer, eller annet) og formålet med anskaffelsen.
2. IT-systemets omfang.
3. Systemmiljøet i Midt-Telemark.
4. Klassifisering av informasjonen som skal behandles i fagsystemet:
   - Offentlig tilgjengelig
   - Personsensitiv
   - Fortrolig
   - Evt. behov for sikkerhetsgradering i henhold til sikkerhetsloven
5. Fagsystem og dets anvendelsesområde, herunder bruk av:
   - Stasjonære tjenester.
   - Mobile tjenester.
   - Elektronisk meldingsutveksling.
   - Elektroniske signaturer.
6. Organisering av tjenestene i fellessystemet:
   - Separate tjenester.

- Fellestjenester mellom et utvalg av eierkommunene.

7. Eksterne forbindelser og fjerntilgang til systemet.
8. Samordning mot lokale aktiviteter og andre fagsystemer.
9. Kommunenes sårbarhet for driftsforstyrrelser og -stans i IT-systemet.

Forventede resultater – fasens output

- "Sikkerhetsvurdering" - Dokumentert grunnlag for etablering av sikkerhetskrav.

Aktiviteter

- Identifisere, beskrive og prioritere faktorer som er avgjørende for sikkerhetsvurderingen og utarbeide en sikkerhetsvurdering på bakgrunn av dette.
- Underbygge eller eventuelt endre prosjektets mål

Trinn 2: Sikkerhetskrav

Formål

- Etablere sikkerhetskravene i forbindelse med anskaffelse, implementering og bruk av IT-systemer med utgangspunkt i sikkerhetsvurderingen.
- Grunnlag for etablering av sikkerhetstiltak overfor fag-/systemleverandør i forbinndelse med implementering av systemet.

Forutsetninger

Fasens input:

- Sikkerhetsvurdering.
- IT-systemets omfang gitt i prosjektvurderingen, prosjektmandatet eller forslag til kravspesifikasjon.

Regelverk og rammebetingelser:

- Lover og forskrifter som vil være retningsgivende for sikkerhetskravene til den informasjonen som skal behandles i systemet.

Med bakgrunn i sikkerhetsvurderingen, skal prosjektgruppa vurdere sikkerhetskrav i forbindelse med anskaffelse, implementering og bruk. Dette gjelder innenfor:

1. Kontraktsvilkår
2. Dokumentasjonskrav til leveransen
3. Systemtekniske sikkerhetskrav
4. Interne sikkerhetsforhold

Kontraktsvilkår:

- Sikkerhetskrav i kontrakter (se Krav til Samarbeidspartnere og leverandører).
- Leverandørens ansvar og rolle i prosjektet.
- Spesifisering av eventuelle tilleggsytelser (bistand ved innkjøring av system, konvertering av data fra tidligere systemer, osv.).
- Support og fastsettelse av tjenestenivå, f.eks. telefonveiledning, feilretting via nett, service på brukersted, tilkallingstid, tilgjengelighet (døgntider og ukedager).
- Programservicens omfang: Feilretting, oppgraderinger til nye versjoner (forbedringer og nye funksjonaliteter), tilpasninger til nye generelle krav i lovverk.
- Leverandøren skal gjøres kjent med Midt-Telemarkkommunenes rutiner for tildeling av rettigheter ved oppgraderinger, endringer eller feilretting.

Dokumentasjonskrav til leveransen:

- Komponentspesifikasjon: Klar og entydig definering av alle komponenter.
- Avvik mellom spesifikasjon og tilbud: Leverandøren skal klargjøre på hvilke punkter Midt-Telemarkkommunenes sikkerhetskrav, kravspesifikasjoner til funksjonalitet og/ eller formålsbeskrivelse ikke blir dekket av den løsningen som leverandøren kan tilby og som partene har blitt enige om.
- Installasjon av programvare: Leverandøren skal kunne vise til dokumenterte prosedyrer for å kontrollere installasjon av programvare i serverparken, herunder prosedyrer for testing og beskyttelse av data for systemtesting
- Endringsstyring: Leverandøren skal kunne vise til dokumenterte prosedyrer for endringsstyring slik at alle planlagte systemendringer blir kontrollert på en måte som vil sikre at de ikke svekker sikkerheten til det aktuelle systemet eller driftsmiljøet.
- Prosjektrapportering: Leverandøren kan avvike fra Midt-Telemarkkommunenes rapporteringsrutiner dersom han kan vise til egne rutiner som kan godkjennes.
- Brukerveiledninger og opplæringsplaner: Norsk brukerveiledning og opplæringsplan.

Systemtekniske sikkerhetskrav

- Evt. krav til integrasjon mot tilstøtende applikasjoner/fagsystemer (fra Trinn 1, pkt. 8).
- Sikkerhetskrav til løsninger for kryptert datakommunikasjon og elektroniske signaturer:
    - Dokumentasjon av sertifikatpolicy
    - Leverandøren skal dokumentere at nøkkeladministrasjon er basert på et avtalt sett med standarder, prosedyrer og sikre metoder.
    - Leverandøren skal klarlegge hvilke kryptografiske teknikker som anvendes:
        - Passord
        - Asymmetrisk (elektroniske signaturer)
        - Symmetrisk

- Leverandøren skal oppgi nøkkellengden for ulike kryptografiske systemer og forskjellige applikasjoner som omfattes av leveransen. Ved generering av kvalifiserte elektroniske sertifikater til offentlig sektor, skal det benyttes en nøkkellengde på minst 1024 bit.
- Leverandøren (utvikleren) skal, hvis mulig, forelegge en erklæring om i hvilken grad alle nøkkelmulighetene som ligger i de genererte nøkkellengdene blir utnyttet for hver nøkkel.

- Tekniske spesifikasjoner og integrasjon mot andre systemer:
  - I henhold til Kravspesifikasjon for PKI i offentlig sektor.
  - Leverandøren skal dokumentere at elektroniske signaturer blir generert i henhold til kravene i Kravspesifikasjon for PKI i offentlig sektor, og at de er kvalifiserte i henhold til e-signaturloven med forskrift.
- Funksjoner for logging av aktiviteter.

Interne sikkerhetskrav

I forbindelse med implementering og bruk av systemet, bør arbeidsgruppen, med utgangspunkt i sikkerhetsvurderingen, klarlegge følgende sikkerhetskrav:

- Bruk av felles tjenester: Det skal foreligge kommunale avtaler som regulerer forholdene mellom kommunene og tilgang til de ulike databasene ved innføring av felles fagsystemer med felles tjenester.
- Eventuelle krav til systemdokumentasjon og prosedyrer (oppdatering av sikkerhetshåndbok).
- Soneplassering (sikret eller intern).
- Autorisering av personell for tilgangsrettigheter.
- Aktivitetslogging og krav til registrering og oppbevaring av logger.
- Oppbevaring av sikkerhetskopier.
- Bruk av e-post.
- Krav om meldeplikt
- Avhending av utstyr.
- Behandling av sikkerhetsgradert informasjon: Henvisning til egne veiledninger fra Nasjonal Sikkerhetsmyndighet

Forventede resultater – fasens output

- Sikkerhetskrav i forbindelse med anskaffelse, implementering og bruk av felles IT-systemer i Midt – Telemarkkommunene.
- Grunnlag for sikkerhetstiltak i trinn 3.
- Eventuelle endringer i omfang eller presisering av mål.

Aktiviteter

- Fastsettelse av sikkerhetsmessige kontraktsvilkår.
- Utarbeidelse av dokumentasjon av sikkerhet ved leveransen.
- Fastsettelse av systemtekniske sikkerhetskrav.

- Fastsettelse av interne sikkerhetsforhold.
- Godkjenning av sikkerhetskravene.
- Klarlegging og godkjenning av eventuelle endringer i omfang eller mål

Referanser

- Sikkerhetssystem: Sentrale lover og forskrifter
- Sikkerhetssystem: Nettverks- og IT-sikkerhetsarkitektur
- Sikkerhetsprosedyrer: Krav til samarbeidspartnere og leverandører
- Sikkerhetsprosedyrer: Autorisasjon og tilgangsrettigheter
- Sikkerhetsprosedyrer: Hendelseslogg
- Sikkerhetsprosedyrer: Sikkerhetskopiering og oppbevaring av kopier
- Sikkerhetsprosedyrer: Avhending av brukt, kassert utstyr

Trinn 3: Sikkerhetstiltak

Formål

- Beskrivelse av hvordan sikkerhetskravene skal gjennomføres i kontraktgjennomgåelsen med leverandør og i implementeringen av systemet.
- Klarlegge behovet for og omfanget av sikkerhetstesting og kontroll (se Trinn 4).
- Sørge for å etablere eller oppdatere/endre sikkerhetsdokumentasjon som følge av sikkerhetskravene:
  - Sikkerhetssystemet eller sikkerhetsprosedyrer.
  - Registreringer: Kontrakter og sikkerhetsavtaler, autorisasjon og rettigheter, passordoversikter, nettverks- og sikkerhetsarkitektur, utstyr og komponentoversikt, etc.

Forutsetninger

Fasens input:

- IT-systemets omfang.
- Sikkerhetskrav fra Trinn 2.
- Leverandørens prosedyrer for testing (se Trinn 4).

Regelverk og rammebetingelser:

- Sentrale lover og forskrifter.
- Sikkerhetshåndbok.
- Endringsstyring – Evaluering og oppdatering.

Forventede resultater – fasens output

- Oppdaterte registreringer i sikkerhetssystemet.

- Eventuelle oppdateringer eller endringer i sikkerhetshåndbok.
- Grunnlag for gjennomgåelse av sikkerhetskravene i kontrakten med leverandør.

Aktiviteter

- Utarbeidelse av sikkerhetstiltak basert på sikkerhetskravene i Trinn 2.
- Godkjenning av sikkerhetstiltakene.

Referanser

- Sikkerhetssystemet: Sentrale lover og forskrifter
- Støtteprosedyrer: Endringsstyring – Evaluering og oppfølging

Trinn 4: Sikkerhetstesting og kontroll

Formål

- Testing av implementerte sikkerhetstiltak ved behov i godkjenningsperioden.

Forutsetninger

Fasens input:

- IT-systemets omfang.
- Sikkerhetstiltak fra Trinn 3.

Rammebetingelser:

Prosedyre for sikkerhetstesting og kontroll skal benyttes ved utarbeidelse av testbeskrivelse og gjennomføring av sikkerhetstesting og kontroll av IT-systemer.

Forventede resultater – fasens output

Evaluerte sikkerhetstiltak med angivelse av eventuelle avvik.

Aktiviteter

- Testing av sikkerhetstiltak.
- Godkjenning av sikkerhetstiltakene basert på testresultatene.

Referanser

- Sikkerhetsprosedyre: Sikkerhetstesting og kontroll
- NS-ISO 27002

Trinn 5: Håndtering av avvik fra Trinn 4

Formål

- Beskrive og vurdere de sikkerhetsmessige konsekvensene av hvert avvik.
- Beskrive og gjennomføre kompenserende tiltak inntil den gjenværende risikoen er akseptabel.

Forutsetninger

Fasens input:

- Registrerte avvik fra Trinn 4og tidligere faser.
- Se også prosedyre for Risikovurderinger.

Forventede resultater – fasens output

- Godkjenning av anskaffelse og implementering.

Aktiviteter

- Gjennomføring av risikovurdering på bakgrunn av registrerte avvik.
- Fastsettelse av akseptabel risiko.
- Gjennomføring av korrigerende tiltak

Referanser

Sikkerhetsprosedyre: Sikkerhetsrevisjoner og Risikovurdering

2.14 Sikkerhetskopiering

Formål

Hensikten med denne planen er å sikre at informasjon kan gjenopprettes om den skulle gå tapt som følge av bl.a.:

- Feil i utstyr eller programvare
- Utilsiktet sletting av bruker
- Tilsiktet ødeleggelse/hærverk
- Tap/tyveri av utstyr

Omfang

Midt-Telemarkkommunene skal ta sikkerhetskopi av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting til normal bruk.

Beskrivelse

Data som skal sikkerhetskopieres

Generelt gjelder følgende:

- Det skal tas sikkerhetskopi av helse- og personopplysninger
- Det skal tas sikkerhetskopi av annen informasjon som er nødvendig for gjenoppretting av normal bruk. For eksempel: systemdata som kontinuerlig endres, databasekonfigurasjoner, databaser over brukerkontoer, operativsystemer, ulike fagapplikasjoner og støttesystemer

Vurdering av data for sikkerhetskopiering:

- Hvilke data det skal tas sikkerhetskopi av og hvor ofte det skal sikkerhetskopieres, bør være basert på resultatene av en risikovurdering (se Risikovurderinger)

- Som en del av en risikovurdering skal det gjøres en klassifisering av de mest kritiske systemer med helse- og personopplysninger. Klassifiseringen bør fungere som et grunnlag for å utforme prosedyrer for hvordan og hvor ofte sikkerhetskopieringen skal gjennomføres. F.eks. er det viktigere at det jevnlig tas sikkerhetskopi av data i elektronisk pasientjournal (EPJ) enn av data i ekstern webserver (se Faktaark 4 - Kartlegging og klassifisering av systemer i henhold til kritikalitet i forhold til behov for tilgjengelighet)

Vurdere type sikkerhetskopi

- Full kopi: Kopi av alle data slik de er lagret på lagringsmediet på det aktuelle tidspunkt
- Inkrementell kopi: Kopi av alle data som er endret siden siste kopi

Vurdere frekvens på sikkerhetskopi

Intervallet for de ulike typer sikkerhetskopier kan variere avhengig av hvor ofte data/filer endres, og vil i hvert enkelt tilfelle være en avveining mellom:

- Tiden det tar å gjennomføre en sikkerhetskopi (dette øker proporsjonalt med datamengden det tas kopi av).
- Forbruk av lagringsenheter for sikkerhetskopiering (øker også proporsjonalt med datamengden det tas kopi av).
- Mengden av informasjon som går tapt om systemet krasjer rett før en sikkerhetskopi tas.
- Tiden det tar å gjøre en gjenoppretting.

Merking av sikkerhetskopi

- Lagringsenheten som benyttes til sikkerhetskopieringen må merkes tydelig slik at det er enkelt å finne frem til hvilken kopi som dataene er lagret på. Sikkerhetskopien kan f.eks.

merkes med følgende informasjon: dato, innhold (for eksempel system, server, disk) og type kopi (full eller inkrementell kopi).

- I større lagringsmiljøer, hvor alle lagringsenheter behandles likt (for eksempel roboter), er det ikke nødvendig med merking utover det som følger lagringsløsningen.

Planlegge gjennomføring av sikkerhetskopiering

Det finnes en rekke systemer som automatisk tar sikkerhetskopi av de aktuelle data.

Diskuter evt. med leverandøren av det aktuelle systemet hva (kataloger, filer, database mv.) det skal tas sikkerhetskopier av.

Kvalitetssikre sikkerhetskopieringen

For å verifisere at det faktisk er utført en komplett og korrekt sikkerhetskopi må hendelsesregisteret som viser sikkerhetskopieringsaktiviteten kontrolleres daglig. Ved feil må korrigerende tiltak iverksettes.

Ved etablering av ny prosedyre for sikkerhetskopiering anbefales det å kontrollere at sikkerhetskopien faktisk inneholder data som kan tilbakekopieres.

Oppbevaring av sikkerhetskopi

- Sikkerhetskopier skal oppbevares i tyveri- og brann- og varmesikkert safe/skap. Kopiene skal oppbevares på et annet sted enn de originale data.
- I større lagringsmiljøer, hvor alle lagringsenheter behandles likt (for eksempel roboter) og lagringsløsningen er fysisk sikret og adskilt fra de originale data, er det ikke nødvendig med oppbevaring i tyveri- og brannsikker safe/skap.
- Det anbefales at en sikkerhetskopi fraktes ukentlig ut av lokalene og oppbevares eksternt.

Gjenoppretting av sikkerhetskopi

Det skal jevnlig foretas test av at sikkerhetskopiene er korrekte og kan tilbakeføres. Det er viktig at virksomheten sørger for å ha denne kompetansen tilgjengelig, internt eller eksternt.

Utrangering av lagringsmedier

Sikkerhetskopien skal destrueres på en slik måte at innholdet ikke kan fremhentes. Se egen prosedyre for avhending og kassering.

2.15 Sikring mot ondsinnet programvare

Formål

Prosedyren skal sikre at kommunale IT-systemer, servere og datamaskiner er tilfredsstillende sikret mot ondsinnet programvare.

Omfang

Midt-Telemarkkommunene skal iverksette tiltak for å hindre ondsinnet programvare med tanke på om det:

- Tas i bruk usikre nettverk og tjenester.
- Tas i bruk sikrede nettverk og tjenester.
- Tas i bruk andre tilkoblingsløsninger som muliggjør overføring av ondsinnet programvare.

Beskrivelse

Beskyttelse av teknisk løsning

- Arbeidsstasjoner skal kontrolleres ved pålogging eller kontinuerlig hvis de ikke skrus av.
- Bærbart datautstyr skal kontrolleres før det kobles til andre nettverk enn gjestenettverk. Dette er en meget aktuell problemstilling fordi signaturfiler hentes på det lokale nettverket ved tilkobling til nettverket. Krav til oppdaterte signaturfiler avhenger av hvordan det bærbare utstyret er benyttet når det ikke er knyttet til nettverket. Tillates tilkobling til andre nettverk, bruk av lagringsenheter, minnepinner, CD, med mer, må dette ivaretas.
- Alle sentrale tjenestemaskiner (servere) skal kontrolleres kontinuerlig.
- Fjernaksessløsninger skal ha beskyttelsestiltak både hos leverandør og i virksomheten.
- E-post skal hentes inn til nettverket gjennom e-postfiltre, og ikke automatisk sendes inn i nettverket.
- Ekstern kommunikasjon skal ha deteksjon av forsøk på angrep.
- Medisinsk teknisk utstyr og tilhørende servere og arbeidsstasjoner skal ha beskyttelse mot ondsinnet programvare på lik linje med annet datautstyr dersom hensiktsmessig og mulig.
- Annet utstyr som kan inneholde ondsinnet programvare (f.eks. mobiltelefoner og minnepinner) skal kontrolleres ved tilkobling til nettverk.
- Beskyttelsestiltakene skal konfigureres slik at bruker ikke kan overstyre kontrollen.

Oppdatering av signaturfiler

- Signaturfiler skal hentes inn på en sikker måte for deretter rutinemessig å bli distribuert til klientene.

Kontroll av filer og medier

- Alle medier som kobles til arbeidsstasjon eller server (CD, minnepinner, lagringsenheter, med mere) skal kontrolleres før filer overføres.
- Filer og vedlegg til ekstern Internett-e-post som legges i karantene krever manuell oppheving av karantene.
- Sikkerhetskopi skal kontrolleres for å sikre at kopi ikke inneholder ondsinnet programvare.
- Nedlastning av oppdateringer fra Internett skal kontrolleres. Det anbefales at slik nedlastning til sikret sone gjøres gjennom en egen filsluse.
- Overføring fra filer fra/til supportleverandør (fjernaksess) til/fra virksomheten skal være kontrollert på tilfredsstillende måte. Det er avsender som har ansvaret for denne kontrollen.

Oversikter hos kommuner og driftsleverandører

MT-IKT og eventuell driftsleverandører skal utarbeide oversikter over antivirusprogramvare, hvor den er installert og hvordan den oppdateres.

2.16 Innsyn i e-post og personlige kataloger

Formål

Hensikten med denne planen er å gi retningslinjer for innsyn når arbeidsgiver har rett til innsyn og for å sikre arbeidstakerens rettigheter.

Omfang

Prosedyren gjelder alt innsyn i den ansattes epostkasse, personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr. Dersom utstyr er stilt til arbeidstakers disposisjon utelukkende for privat bruk, gjelder ikke reglene om arbeidsgivers innsynsrett etter personopplysningsforskriften, og dekkes følgelig ikke i prosedyren.

Innledning

Med epostkasse mv. menes e-post, personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr.

Arbeidsgiver har rett til å foreta innsyn i to ulike situasjoner:

1. Når innsyn er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten. Et eksempel på dette er den ansattes fravær (sykemelding, permisjon, dødsfall, mv.).
2. Når innsyn er begrunnet ved mistanke om at arbeidstakers bruk av epostkassen mv. medfører grovt brudd på de plikter som følger av arbeidsforholdet (for eksempel lovbrudd, brudd på arbeidsavtalen eller interne prosedyrer mv.), eller kan gi grunnlag for oppsigelse eller avskjed.

Innsyn som er nødvendig for å ivareta den daglige driften

Innsyn som er nødvendig for å ivareta den daglige driften eller andre berettigede interesser

Generelt

a) Ved lengre tids fravær bør virksomheten, for å redusere behovet for innsyn, gjøre epostkassen inaktiv. Det anbefales at arbeidsgiver pålegger den ansatte å bruke fraværsassistenten med informasjon om hvilken epostkasse som skal benyttes for virksomhetsrelatert e-post.
b) For å redusere behovet for innsyn i den enkelte arbeidstakers epostkasse mv. anbefales det avdelingsvis eller felles epostkasser og områder til virksomhetsrelatert informasjon.
c) Reglene for innsyn gjelder også opplysninger som den ansatte har slettet, men som finnes lagret på sikkerhetskopier eller lignende som arbeidsgiver har tilgang til.
d) Reglene for innsyn gjelder både overfor nåværende og tidligere arbeidstakere samt andre som utfører, eller har utført, arbeid for arbeidsgiver.

Forberedelse

a) Det er arbeidsgiver som beslutter innsyn etter en konkret helhetsvurdering. Relevante momenter vil kunne være:
   - Betydningen av arbeidstakerens fravær.
   - Den ansatte har på tross av skriftlig pålegg ikke sørget for videresending av e-post eller svar med opplysninger om hvor virksomhetsrelatert e-post skal sendes.
   - Det er god grunn til å tro at det er innkommet virksomhetsrelatert e-post og at behandlingen av denne av hensyn til virksomhetens drift ikke kan vente. Lengden på arbeidstakerens fravær vil være et moment i totalvurderingen.

   Hvis opplysningene kan fremskaffes med andre og mindre inngripende midler er det ikke grunnlag for innsyn. Virksomheten må vurdere den ansattes behov for personvern opp mot arbeidsgivers behov for å ivareta daglig drift mv.
b) Dersom arbeidsgiver vurderer at innsyn er nødvendig, skal arbeidsgiver beskrive formålet med innsynet.
c) Arbeidstaker skal så langt som mulig varsles og få anledning til å uttale seg før arbeidsgiver gjennomfører innsyn. I varselet skal arbeidsgiver begrunne hvorfor vilkårene for innsyns anses å være oppfylt og orientere om arbeidstakers rettigheter.
d) Ved innsyn uten forutgående varsel skal arbeidstaker gis skriftlig underretning om dette så snart innsynet er gjennomført.
e) Arbeidstaker skal så langt som mulig gis anledning til å være til stede under innsynet og har rett til å la seg bistå av tillitsvalgt eller en annen representant.

Gjennomføring

a) Epostkassen mv. gjøres tilgjengelig av en systemadministrator.
b) Innsynet skal i størst mulig grad utføres ved å benytte emnefeltet i e-poster, navn på konkrete dokumenter etc.

c) Dersom innsynet viser at det ikke foreligger dokumentasjon som arbeidsgiver har rett til innsyn i, skal epostkassen mv. og dokumenter i denne straks lukkes. Eventuelle kopier eller utskrifter som er tatt i forbindelse med innsynet skal slettes.

d) Relevant virksomhetsrelatert e-post kan videresendes til en annen epostkasse i virksomheten. Før videresending skal e-posten skrives ut slik at det er dokumentasjon av den opprinnelige e-posten. Dokumenter fra innsyn i personlig område kan kopieres til eksternt lagringsmedium (for eksempel minnepinne) og bør også skrives ut. Utskriften skal oppbevares sammen med dokumentasjon fra innsynet.

e) Ved innsynet skal e-postmeldinger ikke besvares fra den ansattes epostkasse. Svar til avsender skal skje på annen måte Når innsynet er avsluttet skal lese- og skriverettigheter settes tilbake til de opprinnelige innstillingene av systemadministrator.

f) Innsyn må gjennomføres på en slik måte at dataene så langt som mulig ikke endres og at frembrakte opplysninger kan etterprøves.

Dokumentasjon av innsynet

a) For å sikre etterprøvbarhet skal innsynet dokumenteres i et referat. I referatet skal det inngå:
- At vilkårene for innsyn er oppfylte.
- Hvorfor innsynet er foretatt (formål).
- Hvem som fattet beslutningen.
- Hvem som var til stede, og hvor innsynet ble gjennomført.
- Klokkeslett for gjennomføring, start- og stopptidspunkt.
- Resultatet og hvilken metode for innsyn som ble benyttet.
- Signatur fra alle som var til stede.
- Avhengig av innsynets art og formål skal referatet inneholde:
  - Hvilke e-poster som ble åpnet med angivelse av avsender, dato, klokkeslett og temafelt.
  - Hvilke e-poster som ble skrevet ut og/eller videresendt.
  - Hvilke filer det ble søkt etter.
  - Hvilke filer som eventuelt ble åpnet.
  - Hvilke filer som eventuelt ble kopiert.
  - Hvilke filer som ble skrevet ut.
  - Resultatet av innsynet (hvilke funn ble gjort mv.).

b) Dokumentasjonen av innsynet skal arkiveres.

c) Den ansatte skal ha skriftlig underretning så snart innsynet er gjennomfør dersom innsynet er foretatt uten forutgående varsel. Dette kan gjøres ved å oversende referatet.

Innsyn ved begrunnet mistanke om grovt brudd

Innsyn ved begrunnet mistanke om grovt brudd på de plikter som følger av arbeidsforholdet, eller som kan gi grunnlag for oppsigelse eller avskjed

Generelt om innsyn

a) Reglene for innsyn gjelder også opplysninger som den ansatte har slettet, men som finnes lagret på sikkerhetskopier eller lignende som arbeidsgiver har tilgang til.
b) Reglene for innsyn gjelder både overfor nåværende og tidligere arbeidstakere, samt andre som utfører, eller har utført, arbeid for arbeidsgiver.

Forberedelse

a) Det er arbeidsgiver som beslutter innsyn ved begrunnet mistanke om at arbeidstakers bruk av epostkassen mv. medfører grovt brudd på de plikter som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed. Relevante momenter vil kunne være:
    - Det foreligger begrunnet mistanke om at arbeidstaker benytter epostkassen mv. til straffbare handlinger (for eksempel tyveri, underslag, ulovlig behandling av helse- og personopplysninger, trakassering av kolleger)
    - Det foreligger begrunnet mistanke om at arbeidstaker sender ut spam, ondsinnet programvare eller e-post med annet skadelig innhold

    Det er imidlertid viktig å merke seg at mottak av e-post med illojalt innhold ikke gir grunnlag for innsyn, da dette ligger utenfor arbeidstakers kontroll.
    Det er et vilkår for innsyn at handlingen den ansatte mistenkes for må være så alvorlig at den gir grunnlag for avslutning av arbeidsforholdet
b) Dersom arbeidsgiver vurderer at innsyn er nødvendig, skal arbeidsgiver beskrive formålet med innsynet
c) Arbeidstaker skal så langt som mulig varsles og få anledning til å uttale seg før arbeidsgiver gjennomfører innsyn. I varselet skal arbeidsgiver begrunne hvorfor vilkårene for innsyns anses å være oppfylt og orientere om arbeidstakers rettigheter.
d) Ved innsyn uten forutgående varsel skal arbeidstaker gis skriftlig underretning om dette så snart innsynet er gjennomført.
e) Arbeidstaker skal så langt som mulig gis anledning til å være til stede under innsynet og har rett til å la seg bistå tillitsvalgt eller en annen representant.
f) Det er unntak fra den ansattes rett til å være tilstede under åpning og rett til å bli varslet om innsynet (jf. personopplysningsloven § 23 - Unntak fra retten til informasjon).

Gjennomføring av innsyn

a) Epostkassen mv. gjøres tilgjengelig av en systemadministrator
b) Aktuelle data bør speilkopieres. Slik speilkopi vil gi trygghet både for arbeidsgiver og arbeidstaker ved at det vil være mulig å påvise eventuelle endringer av informasjonen. Dette gjelder både endringer foretatt av arbeidstaker etter at arbeidsgiver informerte om innsynet, og eventuelle endringer foretatt ifm. gjennomføring av innsynet. Virksomheten anbefales å gjennomføre speilkopieringen med profesjonell bistand.
c) Ved behov for sikring av bevis skal det tas ytterligere en speilkopi som oppbevares av virksomheten selv eller hos en tredje part (for eksempel hos en advokat).
d) Innsynet bør foregå på speilkopien.
e) Innsynet skal i størst mulig grad utføres ved å benytte emnefeltet i e-poster, navn på
f) Konkrete dokumenter etc. Ved innsynet skal e-postmeldinger ikke besvares fra den ansattes epostkasse. Svar til avsender skal skje på annen måte.

g) Dersom innsynet viser at det ikke foreligger dokumentasjon som arbeidsgiver har rett til innsyn i, skal epostkassen mv. og dokumenter i denne straks lukkes. Eventuelle kopier eller utskrifter som er tatt i forbindelse med innsynet skal makuleres
h) Om innsynet ikke foregår på speilkopi skal lese- og skriverettigheter settes tilbake til de opprinnelige innstillingene av systemadministrator når innsynet er avsluttet
i) Innsyn må gjennomføres på en slik måte at dataene så langt som mulig ikke endres og at frembrakte opplysninger kan etterprøves.

Dokumentasjon av innsynet

a) For å sikre etterprøvbarhet skal innsynet dokumenteres i et referat. I referatet skal det inngå:
   - At vilkårene for innsyn er oppfylte..
   - Hvorfor innsynet er foretatt (formål).
   - Hvem som fattet beslutningen.
   - Hvem som var til stede, og hvor innsynet ble gjennomført.
   - Klokkeslett for gjennomføring, start- og stopptidspunkt.
   - Resultatet og hvilken metode for innsyn som ble benyttet.
   - Om det ble tatt speilkopi(er) og hvor speilkopien(e) oppbevares.
   - Hvem som har tilgang til eventuell(e) speilkopi(er).
   - Signatur fra alle som var til stede.
   - Avhengig av innsynets art og formål skal referatet inneholde:
     - Hvilke e-poster som ble åpnet med angivelse av avsender, dato, klokkeslett og temafelt.
     - Hvilke e-poster som ble skrevet ut og/eller videresendt.
     - Hvilke filer det ble søkt etter.
     - Hvilke filer som eventuelt ble åpnet.
     - Hvilke filer som eventuelt ble kopier.t
     - Hvilke filer som ble skrevet ut.
     - Resultatet av innsynet (hvilke funn ble gjort mv.).

b) Dokumentasjonen av innsynet skal arkiveres.
c) Den ansatte skal ha skriftlig underretning så snart innsynet er gjennomfør dersom innsynet er foretatt uten forutgående varsel. Dette kan gjøres ved å oversende referatet.

2.17 Sikring av mobilt utstyr utenfor virksomheten

Formål

Sikre konfidensialitet, integritet og tilgjengelighet for helse- og personopplysninger som registreres, endres og lagres på mobilt utstyr.

Omfang

Prosedyren gjelder for Midt-Telemarkkommunene og omfatter alle typer mobilt utstyr; bærbar PC, PDA, mobiltelefon, digitalt kamera og video som brukes av ansatte i tjeneste utenfor virksomheten (for eksempel hjemmetjeneste).

Beskrivelse

Innledning

Virksomhetens leder skal beslutte bruk av mobilt utstyr.

IKT-ansvarlig skal påse at det blir etablert teknisk løsning og utarbeide de nødvendige prosedyrer som skal ivareta kravet til sikkerhet.

Bestemme bruksområder for mobilt utstyr

a) Avgjøre ved hvilke tjenester utenfor virksomheten mobilt utstyr skal benyttes; besøkstjenester, hjemmetjeneste, legevakt, akuttmedisinske tjenester, osv.

b) Avgjøre om mobilt utstyr skal benyttes til:
- Motta helse- og personopplysninger fra sentrale systemer.
- Mellomlagre helse- og personopplysninger.
- Bearbeide helse- og personopplysninger.
- Overføre helse og personopplysninger til annet utstyr.
- Overføre helse- og personopplysninger til sentrale systemer.
- Utføre administrative funksjoner (for eksempel avtalebok).

c) Avgjøre hvilken type informasjon mobilt utstyr skal benyttes til:
- Tekst
- Tale/lyd
- Bilder
- Video
- Strukturert datafangst via strekkode, rfid eller annen dedikert teknologi.

Bestemme tekniske sikkerhetsregler

a) Fastsette nivå for akseptabel risiko. Virksomheten skal vurdere hva som er nødvendige sikringsmekanismer i forhold til den faktiske bruken; omfang av data på utstyret, sletteprosedyrer, sannsynligheten for at utstyret kommer på avveie, muligheten for 3. part å få innsyn, hvor lett det er å identifisere enkeltpersoner, osv.

b) Gjennomføre risikovurdering av bruk av mobilt utstyr.

c) Prioritere tiltak som ivaretar forholdsmessig sikring.

Etablere tekniske sikkerhetstiltak

a) Innføre relevante tekniske tiltak

- Kryptering av lagringsmedium eller data.
- Autorisasjon og autentisering.
- Sikkerhetsnivå 4 for autentisering ved pålogging til sentrale systemer som inneholder helseopplysninger.
- Fjerne funksjoner / tjenester som ikke skal benyttes om dette er mulig. Alternativt må slike tiltak avtales med bruker.
- Antivirusprogram.
- Sikker datakommunikasjon inklusive behandling av bilder og film med hensyn til SMS og MMS.

Etablere prosedyrer for bruk av mobilt utstyr

a) Opplæring i bruk av mobilt utstyr slik at bruker er fortrolig med hvordan det skal brukes.

b) Utlevering og innlevering av mobilt utstyr slik at behandlingsansvarlig har god kontroll med hvem som benytter mobilt utstyr til hva.

c) Sikker oppbevaring. Utstyret transporteres fra virksomhet til pasient / bruker og kan utsettes for tyveri, tap og ødeleggelse.

d) Regler for registrering, endring, retting og sletting av helse- og personopplysninger på mobilt utstyr.

e) Regler for overføring av helse- og personopplysninger til/fra sentrale systemer. Slik overføring anbefales utført på kontoret/arbeidsplassen til den enkelte og ikke fra hjemmekontor.

f) Brukeravtale. Det skal her presiseres at dette er dedikert utstyr til definerte oppgaver og skal ikke benyttes til annet enn predefinerte oppgaver.

g) Avhende eller overføre mobilt utstyr til annen bruker, herunder sletting av data.

2.18 Kommunikasjon over åpne nettverk

Formål

Å ivareta tilfredsstillende sikkerhet ved elektronisk kommunikasjon av helse- og personopplysninger over åpne nett.

Omfang

Prosedyren gjelder Midt-Telemarkkommunene og leverandører.

Bakgrunn

De fleste kommunikasjonsnett er i utgangspunktet åpne nett, for eksempel Internett eller usikrede trådløse nettverk. Informasjon som sendes i slike nett kan leses av de som får tilgang. Ved bruk av kryptering, sikker autentisering mv. vil informasjonen blir sikret mot uautorisert tilgang.
Norsk Helsenett er et åpent nett og må sikres på samme måte som andre åpne nett.

Ved etablering av løsninger for kommunikasjon over åpne nett skal det gjennomføres en risikovurdering.

Beskrivelse

Autentisering av kommunikasjonspartner

Ved kommunikasjon mellom to parter over et åpent nett er det viktig at partene, på en sikker måte, kan autentisere seg for hverandre. Sikker autentisering er viktig for å verifisere at kommunikasjonsparten faktisk er den som den utgir seg for å være. Dette kan for eksempel gjøres ved å bruke PKI og virksomhetssertifikater.

Autentisering av personer/brukere

Ved autentisering av personer som kommuniserer helseopplysninger over et åpent nett skal det benyttes sikkerhetsnivå 4 for autentisering.

Kryptering av informasjon

Opplysninger sendt over et åpent nett sendes i utgangspunktet over i klartekst slik at det er mulig å lese dette dersom nettet avlyttes. Helse- og personopplysninger sendt over et åpent nett må derfor krypteres slik at innholdet i opplysningene er uleselig for andre enn mottaker.

Krypteringsstyrken skal være iht. gjeldende krav.

Kryptering av kommunikasjonskanal

Alternativt til å kryptere selve informasjonen kan en kryptere kommunikasjonskanalen som brukes. Både SSL (Secure Sockets Layer) og TLS (Transport Layer Security) kan brukes for å etablere en kryptert kommunikasjonskanal. SSL er primært for å kryptere oversendt informasjon over nettet og benyttes mye for eksempel på nettsteder hvor internettbrukere skal oversende helse- og personopplysninger. TLS er primært for å sette opp en sikker kommunikasjonskanal mellom klient/serverapplikasjoner som kommuniserer helse- og personopplysninger over et åpent nett. Andre metoder for å sikre kommunikasjonskanaler er for eksempel VPN (Virtuelt Privat Nettverk) eller IPSec (Internet Protocol Security).

Sikkerhet i tilkoblingsløsningen til Norsk Helsenett

Norsk Helsenett utplasserer en teknisk sikkerhetsløsning som virksomheten må forholde seg til og inkorporere i sitt eget nettverk. Sikkerhetstiltakene fra Norsk Helsenett utgjør en del av sikkerheten i tilkoblingsløsningen. Eksempler på sikkerhetstiltak er at Norsk Helsenett:

- Utplasserer en sikkerhetsbarrierer (ruter/brannmur) som er ferdigkonfigurert inn mot virksomhetens sikre sone. Hovedhensikten med ruteren er å sikre helsenettet og aktører i helsenettet.

- Gjennomfører sentrale tiltak for å hindre at ondsinnet programvare sprer seg til/fra kunder i helsenettet.
- Gir garantier for blant annet oppetid og tjenestekvalitet i nettet etter avtale med kunden.
- Gjennomfører overvåkning av nettet fra og med utplasserte sikkerhetsbarrierer i virksomheten.

Følgende ivaretas ikke av Norsk Helsenett og virksomheten må selv:

- Sørge for å kryptere helse- og personopplysninger før de sendes over helsenettet.
- Sørge for sikker autentisering av brukere ved tilgang til helse- og personopplysninger.
- Etablere løsninger mot ondsinnet programvare i virksomhetenes interne nettverk.

Fjernaksess

- Virksomheten bør etablere en enhetlig løsning for fjernaksess.
- Det anbefales at leverandør inngår avtale med Norsk Helsenett for tilgang til virksomheten.
- Det skal i størst mulig grad benyttes tekniske tiltak som utstyr og programvare. Det er ikke tilstrekkelig med bare skriftlige prosedyrer som viser ansvar og arbeidsoppgaver.
- All tilgang til virksomhetens systemer gjennom fjernaksess, skal kun skje etter en særskilt tillatelse, og med individuell pålogging også for leverandørens personell.
- Alle aktiviteter skal registreres som hendelse. Leverandør skal dokumentere hva som er utført i virksomheten. Hendelsesregistre kan være både elektroniske og manuelle.

E-post

Alminnelige e-postløsninger skal aldri benyttes for utveksling av helse- og personopplysninger. Dette gjelder både internt i en virksomhet, til kommunikasjon med pasienter og lignende. For kommunikasjon til pasienter skal det benyttes løsninger som sørger for sikker kommunikasjon, for eksempel via et webgrensesnitt, og som sørger for at helse- og personopplysninger ikke overføres ukryptert eller blir liggende på brukerens lokale PC.

Telemedisin

Ved bruk av telemedisinske løsninger må disse være utformet slik at informasjonssikkerheten er tilstrekkelig ivaretatt. Dette vil kunne innebære blant annet transportsikkerhet, autentisering av klienter som brukes i telemedisin og mekanismer for tilgangskontroll av brukere.

Hendelsesregistrering

Dersom man har tjenester som er tilgjengelige i et åpent nett er det viktig å registrere hvem som har hatt tilgang til tjenesten. Eksempelvis i en tjeneste for pasient-lege kommunikasjon må alle tilganger til tjenesten registreres slik at det i ettertid er mulig å finne om det er gjort urettmessige tilganger.

3.1 Prosedyremal

Formål

Hensikten med denne planen er å planlegge hvordan Midt-Telemarkkommunene skal forebygge og håndtere uønskede hendelser, samt å beskytte kritiske tjenester og systemer mot negative konsekvenser ved feil eller uhell.

Målsettinger med beredskapsplanen omfatter:

- Utarbeide og iverksette forebyggende tiltak for å forhindre uønskede hendelser.
- Utarbeide tiltak som begrenser konsekvensene av en eventuell uønsket hendelse.
- Gjennomføre effektive tiltak basert på skadeomfang og prioritering av systemer, slik at drift kan gjenopptas uten unødig opphold.
- Forberede IT-personell som naturlig vil yte støtte ved en beredskapssituasjon gjennom øvelser og revisjon av planen.
- Iverksette læreprosess etter hendelse for å redusere sannsynligheten for at lignende hendelser skjer igjen.

Omfang

Prosedyren gjelder

Dette dokument beskriver overordnet struktur for beredskapsplaner og organisering av beredskap for informasjonssystemene ved Midt-Telemarkkommunene.

Dokumentet beskriver også rutiner for håndtering av uønskede hendelser og iverksettelse av forebyggende og konsekvensreduserende tiltak i henhold til sikkerhetsstrategi definert i "Sikkerhetsstrategi".

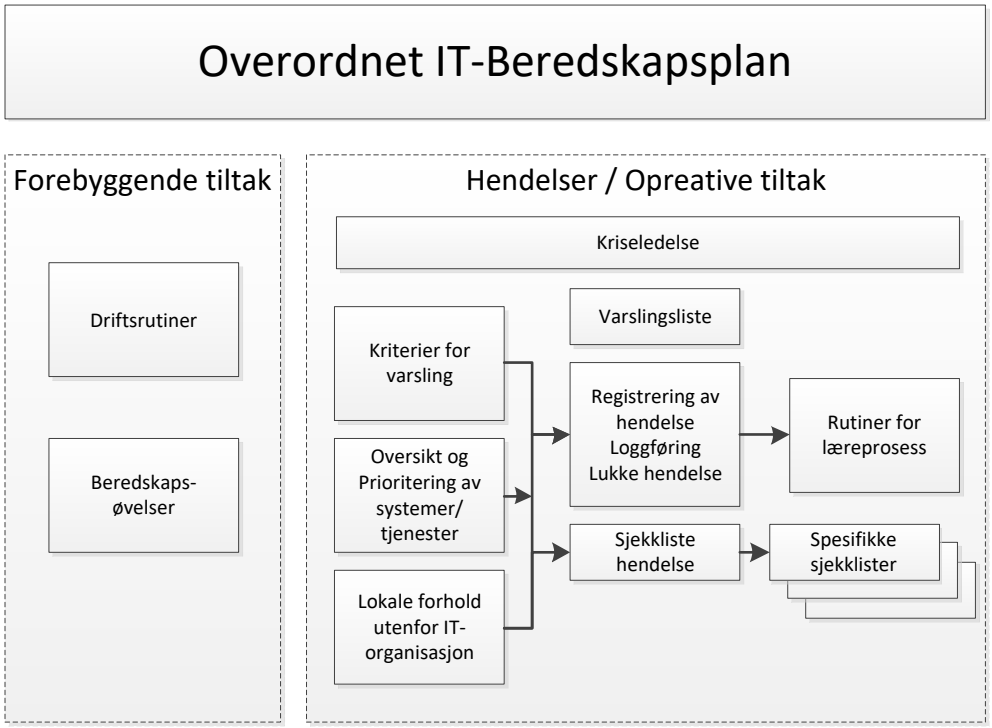
Beredskapsplanen gjelder for de systemer, tjenester og infrastruktur som behandler elektronisk informasjon som tilhører Kongsbergregionen og kommunene. Systemer som skal omfattes av beredskapsplanen må klassifiseres i henhold til beskyttelsesbehov (Konfidensialitet, Integritet og tilgjengelighet).

Beredskapsplanens detaljeringsgrad gjenspeiler de ulike systemenes beskyttelsesbehov (Meget høyt, Høyt, Middels og Lavt).

Beskrivelse

Struktur IT beredskapsplan

Midt-Telemarkkommunenes IT beredskapsplan er bygget opp rundt et rolleorientert rammeverk.



Figur 1 Struktur beredskapsplaner Midt-Telemarkkommunene

Overordnet IT beredskapsplan

Ansvarlig:	Personvern- og sikkerhetsansvarlig
Beskrivelse:	Overordnet beredskapsplan (dette dokument) er et styrings, opplærings- og oversiktsdokument) som bl.a. beskriver: • Struktur på beredskapsdokumentasjon • Ansvar / organisering • Forebyggende tiltak – Organisasjon (bl.a. prosess for kriseledelse) • Risiko- og trusselvurderinger • Beredskapsøvelser • Forebyggende tiltak for systemer og tjenester • Revisjon av beredskapsplaner, rutiner og tiltak
Revisjon:	Revideres i forbindelse med sikkerhetsrevisjoner, beredskapsøvelser og ved organisatoriske endringer. Normalt vil dokumentet være relativt statisk og

oppdateres sjelden.

Forebyggende tiltak

Forebyggende tiltak reduserer sannsynligheten for at en uønsket hendelse inntreffer. Etablerte driftsrutiner inneholder proaktive tiltak som benyttes under normal drift. Driftsrutinene inngår derfor som en del av Midt-Telemarkkommunenes IT beredskapsplan.

Ansvarlig for oppdatering, vedlikehold og gjennomføring av driftsrutinene er driftsansvarlig.

Konsekvensreduserende tiltak

Konsekvensreduserende tiltak tar sikte på å begrense konsekvensene av en uønsket hendelse. Etablerte driftsrutiner inneholder reaktive tiltak som benyttes under normal drift. Driftsrutinene inngår derfor som en del av Midt-Telemarkkommunenes IT beredskapsplan.

Ansvarlig for oppdatering, vedlikehold og gjennomføring av driftsrutinene er driftsansvarlig.

Korrigerende tiltak

Korrigerende tiltak innbefatter å iverksette læreprosesser etter uønskede hendelser for å redusere sannsynligheten for at lignende hendelser skjer igjen

Hjelpemidler ved hendelse

Beredskapsplanen omfatter et antall roller, rutiner og dokumenter som er vist i «Figur 1». Disse hjelpemidlene utgjør den operative delen av IT beredskapsplanen til Midt-Telemarkkommunene internt. Følgende roller og rutiner kan inngå:

- Kriseleder/driftsansvarlig
- Kriterier for hendelsens alvorlighet
- Kriterier for varsling
- Vaktliste/Varslingsliste
- Sjekklister hendelser
- Hendelseslogg
- Spesifikke sjekklister for konkrete hendelser
- Oversikt og prioritering/kategorisering av systemer, forbindelser og tjenester
- Systemrelaterte direktiver (manuelle brukerrutiner)

Ansvar og roller

Organisering av beredskap ved Midt-Telemarkkommunenes IT-avdeling omfatter et antall roller med ulikt ansvar relatert til håndtering av hendelser.

Rolle	Rollebeskrivelse av ansvar	Kommentar
Rådmann	Rådmannen har det overordnede ansvar for godkjenning og iverksettelse	Ansvarlig for kontakt med myndigheter / media

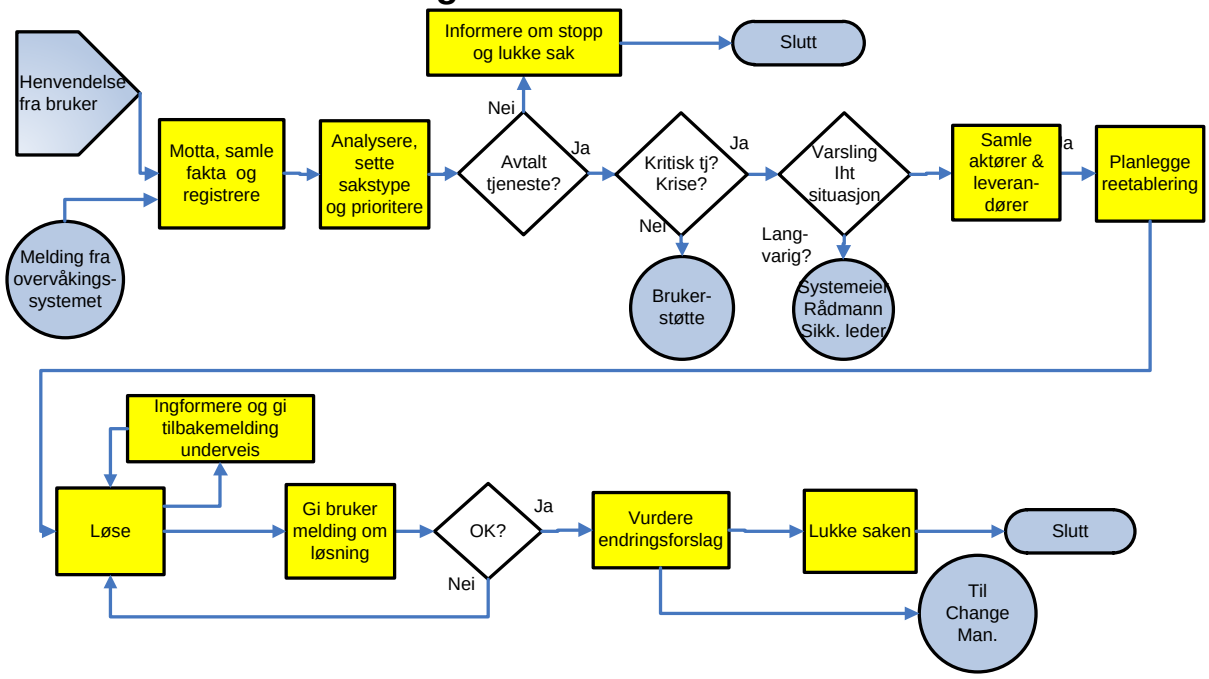
Rolle	Rollebeskrivelse av ansvar	Kommentar
	av beredskapsplaner i kommunen. Det daglige ansvar for IT-sikkerhet er delegert til IT sikkerhetsansvarlig. • Orienteres ved alvorlige eller virksomhetskritiske feil i IT-systemene	(dette ansvaret kan være delegert)
Systemeier (Leder nivå 1)	• Orienteres ved alvorlige eller virksomhetskritiske feil i IT-systemene vedkommende er ansvarlig for • Er ansvarlig for eventuelle reserveløsninger	
Kriseleder/Driftsansvarlig	Skal vurdere omfang og behov for å informere og involvere annet personell for å håndtere hendelse samt eskalering til ledelse. Skal lede og følge opp alvorlige hendelser. • Skal være tilgjengelig på telefon og ha tilgang til planlagte hjelpemidler • Skal være driftsorganisasjonens kontaktpunkt ved alvorlige hendelser. • Analysere hendelse og koordinere iverksettelse av tiltak for å begrense skade samt for å gjenopprette normal drift så raskt som mulig gjennom å involvere nødvendige enheter/personer hos Midt-Telemarkkommunene og leverandører.	
Personvern- og sikkerhetsansvarlige	Ansvarlig for rutiner relatert til lokale fysiske forhold.	
Brukermiljø	De ulike avdelingene ved Midt-Telemark kommunene er ansvarlig for å ha manuelle rutiner oppdaterte og	

Rolle	Rollebeskrivelse av ansvar	Kommentar
	tilgjengelige for brukere /roller i virksomheten.	
Kunde/bruker (internt/eksternt)	Brukere av Midt-Telemarkkommunenes informasjonssystemer skal henvende seg til servicetelefonen ved MT-IKT dersom informasjonssystemer ikke er tilgjengelige eller ved feil.	
Midt-Telemarkkommunenes brukerstøtte	Håndtering av hendelser er dekket opp av driftsrutiner for 1 og 2.. linje support (servicetelefonen, og bakvakter). Ved alvorlig hendelse skal driftsansvarlig kontaktes.	

Tabell 1 - Oversikt over IT beredskapsplanens roller og ansvar

Organisering

Hendelseshåndtering ved Midt-Telemarkkommunene



Figur 1: Skjematisk framstilling av involverte parter i krisehåndtering

Definisjon på alvorlige hendelser

Alvorlige hendelser skal formidles til vakthavende kriseleder. Alvorlige hendelser er definert som:

- Alle hendelser hvor liv og helse står på spill,
- Alle hendelser som medfører at Midt-Telemarkkommunenes informasjonssystemer eller tjenester er utilgjengelige lengre enn hva som er definert.
- Alle hendelser som medfører mistanke om at informasjon er blitt kjent av uvedkommende, inkludert alle hendelser hvor sensitive personopplysninger har kommet eller mistenkes å ha kommet uvedkommende i hende.

Forebyggende administrative tiltak

Alvorlige hendelser og kriser forebygges ved

- Oppfølging av sikkerhetshendelser, brudd og svakheter.
- Endringskontroll og konfigurasjonsstyring.
- Avtaler med leverandører.
- Risiko- og trusselvurderinger.
- Beredskapsøvelser / tester.

Forebyggende tekniske tiltak for systemer og tjenester

Tiltak og krav

		Systemer/tjenester med krav til tilgjengelighet				
	Krav til:	**Lavt**	**Middels**	**Høyt**	**Meget høyt**	**Merknad**
Organisatoriske tiltak	Beredskapsplan (iverksetting, ansvar, tiltak, varslingslister, rapportering)	-	x	x	x	
	Drift og vedlikeholdsrutiner (tilgangskontroll, passord, antivirus, backup, gjenoppretting, overvåking, oppdatering, logging, konfigurasjonskontroll, endringshåndtering, håndtering av avvik)	x	x	x	x	
	Fysisk sikkerhet (brann, vann, innbrudd, adgangs-kontroll, sikring av serverrom og bygninger, evakuering)	x	x	x	x	
	Gjennomføring av egen-kontroll/ øvelser og test av egne rutiner	-	x	x	x	
Generelle tiltak	Start feilsøking innen	24t	8t	2t	2t	I tidsrom hvor aktuelt system skal være tilgjengelig
	Gjenoppretting innen ***(Her må det vurderes krav mot kostnader)***	En uke	24 t	4t	2t	I tidsrom hvor aktuelt system skal være tilgjengelig
	Drift og brukerstøtte Service Desk	Man-fre 08-16	Man-fre 08-16	Man-fre 08-16	Man-fre 08-16	
	Driftsovervåking av systemer og tjenester	-	Alle dg 08-16	24/7	24/7	For systemer i kategori Lavt oppdages feil / hendelser gjennom varsling fra brukere
	Alternativt driftssenter/sted skal være tilgjengelig	-	-	x	x	
Systemer og tjenester	Redundans	-	-	x	x	
	Sikkerhetsmessig herding	x	x	x	x	Årlig gjennomgang
	Backup/sikkerhetskopiering	1 døgn	1 døgn	1 døgn	1 døgn	Ikke eldre enn

Tabell 1 – Generelle IT beredskapstiltak

Revisjon av beredskapsplaner, rutiner og tiltak

Beredskapsplaner, rutiner, sjekklister og tiltak for informasjonssystemene må vedlikeholdes for at beredskapsnivået skal være tilfredsstillende. Ansvar for revisjon, oppdatering og vedlikehold av overordnet beredskapsplan (dette dokumentet) er tillagt sikkerhetsansvarlig. Planene skal revideres/oppdateres årlig, eller ved behov mellom de årlige revisjonene.

3.2 Sikkerhetsrevisjoner

Formål

Formålet med å gjennomføre sikkerhetsrevisjon er:

- Kontrollere at det er gjennomført nødvendige sikkerhetstiltak.
- Verifisere at sikkerhetstiltakene fungerer.
- Kontrollere at lover og regler ift. informasjonssikkerhet følges.
- Sikre at etablerte prosedyrer for sikkerhet benyttes og fungerer etter hensikten.

Omfang

Sikkerhetsrevisjonen må tilpasses omfanget av virksomheten og det eller de tema som er bestemt for den aktuelle revisjonen.

Beskrivelse

Generelt

Gjennomføring av sikkerhetsrevisjon er et ansvar for virksomhetens ledelse. For mindre virksomheter bør daglig leder selv gjennomføre de interne revisjonene, i samarbeid med andre som har roller innen sikkerhet og drift av datasystemene.

Det anbefales ikke at IKT-ansvarlig eller tilsvarende er ansvarlig for gjennomføringen, da vedkommende normalt ikke vil være tilstrekkelig uavhengig av objektet som skal revideres, men vedkommende kan selvsagt bidra med å få frem informasjonen.

Samarbeid om eksterne revisjoner

I Midt-Telemark er det etablert et samarbeid om informasjonssikkerhet. Sikkerhetsansvarlig i kommunene har revisjonskompetanse og skal samarbeide om eksterne revisjoner i kommunene.

Sikkerhetsrevisjonene skal klarlegge om kommunenes dokumentasjon og praksis er i samsvar med de krav som er satt i lover, forskrifter, sentrale normer og lokale policydokumenter og prosedyrer. Revisjonene skal normalt ha klare og avgrensede tema som er tydelig kommunisert mot revidert kommune.

Metodikk

Midt-Telemarkkommunenes revisjoner innen informasjonssikkerhet inneholder fire trinn:

I Forberedelse
II Gjennomføring
III Rapport
IV Oppfølging
Ansvaret for trinn IV, Oppfølging, ligger til den enkelte kommune.

I Forberedelse

I forberedelsesfasen inngår følgende elementer

1) Revisjonsvarsel
2) Innhenting av dokumenter
3) Formøte
4) Dokumentgranskning
5) Sjekklister
6) Revisjonsprogram

Revisjonsvarsel

Sikkerhetsrevisjoner skal avtales god tid i forveien. Revisjonsvarsel skal sendes ut senest to uker før og inneholde:

- Revisjonens omfang og mål.
- Hvilke nøkkelpersoner i virksomheten som bør være tilstede under revisjonen.
- Anmodning om at virksomheten utpeker kontaktperson for den revidertes ledelse for revisjonen.
- Hvilke dokumenter som revisjonsgruppen har behov for å få tilsendt i forbindelse med forberedelsene til revisjonen.
- Angivelse av revisjonsgruppens medlemmer.
- Revisjonsaktivitetene som er planlagt.
- Distribusjon av revisjonsrapporten.

II Gjennomføring

Sikkerhetsrevisjoner gjennomføres med

7) Åpningsmøte
8) Intervju(er)
9) Evt. verifikasjon(er)
10) Befaring
11) Sluttmøte

III Rapport

Rapport etter sikkerhetsrevisjon skal utarbeides etter følgende prosedyre:

12) Utkast til rapport
13) Vurdere eventuelle kommentarer fra den reviderte
14) Endelig rapport

IV Ledelsens gjennomgang

Oppfølging av rapporten fra sikkerhetsrevisjonen skal dokumenteres og gjennomgås ifm ledelsens gjennomgang. Som del av dette skal det i etterkant av den enkelte revisjon vurderes gjennomføring av tiltak for å rette opp avvik som er avdekket.

3.3 Ledelsens gjennomgang

Gjennomføringsansvar: Det er rådmannen og ledere på nivå 1 og 2 som har ansvar for å gjennomføre ledelsens gjennomgang. Personvern og sikkerhetsansvarlig har ansvar for å tilrettelegge gjennomgangen for rådmannen. Ledelsens gjennomgang gjøres normalt en gang pr. år.

Formål

Hensikten med ledelsens gjennomgang er:

- Følge opp de mål som er satt.
- Gjøre korrigerende tiltak.
- Vurdere oppfølging av korrigerende tiltak.
- Endring av mål for prosess.
- Sørge for at internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessige, tilstrekkelig og effektive og at det tilfredsstiller relevante krav i personopplysningsloven og -forskriften.

Oppfølging av forbedringstiltak og korrigerende tiltak gjøres ved at resultatene fra egenkontroll og avviksbehandling gjennomgås og sammenlignes med de korrigerende tiltakene.

Utførelse

Revidering

Revidering av de elementer som er styrende for internkontroll og informasjonssikkerhet, som:

Internkontroll

Vurdere endringer i omfang av dagens internkontroll.

Sikkerhetsmål og -strategi

Vurdere eventuelle forslag til endringer i sikkerhetsmål og sikkerhetsstrategi, dersom endringene i vesentlig grad har økonomiske eller andre virksomhetsmessige konsekvenser.

Risiko- og sårbarhetsanalyse

Ønske om ny funksjonalitet som medfører vesentlige investeringer eller endringer i eksisterende sikkerhetskonsept.

Virksomhetskritisk informasjon og/eller system

Vurdering av endringer i hvilken informasjon eller hvilke systemer som er virksomhetskritisk for virksomheten.

Sikkerhetsmål

Sikkerhetsmål utarbeides for virksomheten. Bakgrunnsmateriale for utarbeidelse vil være:

- Resultater og hovedkonklusjoner fra risikoanalyser og egenkontroll.
- Endringer i offentlige sikkerhetskrav, som kan medføre vesentlig endringer for virksomheten.
- Vurdere om tilstrekkelige ressurser er tilgjengelige for å ivareta internkontroll og informasjonssikkerhet.

Gjennomgang av avvik og hendelser

Ledelsen går detaljert gjennom de alvorligste hendelsene og avvikene som har vært gjennom året, kun summarisk gjennom de mindre alvorlige. Diskusjon bør omfatte årsaker til hendelser og avvik i vid forstand og hvordan hendelser og avvik er håndtert.

Forbedringstiltak

Forbedringstiltak, gjennomføring av tiltak til fastsatte tidspunkter, utarbeides av personvern og sikkerhetsansvarlig på bakgrunn av oppsatte mål, innen områdene:

- Organisering av sikkerheten
- Partnere og leverandører
- Personell og sikkerhet
- Fysisk sikkerhet
- Systemteknisk sikkerhet
- Dokumentsikkerhet
- Beredskap

Forbedringstiltakene skal godkjennes av virksomhetsleder.

Oppfølging

Oppfølging av sikkerhetsmål for å se om de nås og om forbedringstiltak og korrigerende tiltak virker, gjøres blant annet gjennom egenkontroll. En plan for egenkontroll må derfor utarbeides.

Oppfølging av at forbedringstiltakene virker, gjøres i forbindelse med ledelsens gjennomgang, som gjennomføres normalt en gang pr. år.

Referat

Personvern- og sikkerhetsansvarlig skriver referat fra ledelsens gjennomgang og dette distribueres til ledelsen ved virksomheten.

I referatet skal det tydelig fremgå de avgjørelser og aksjoner som er bestemt og med hvilken begrunnelse.

3.4 Endringsstyring

Formål

Prosedyren skal sikre:

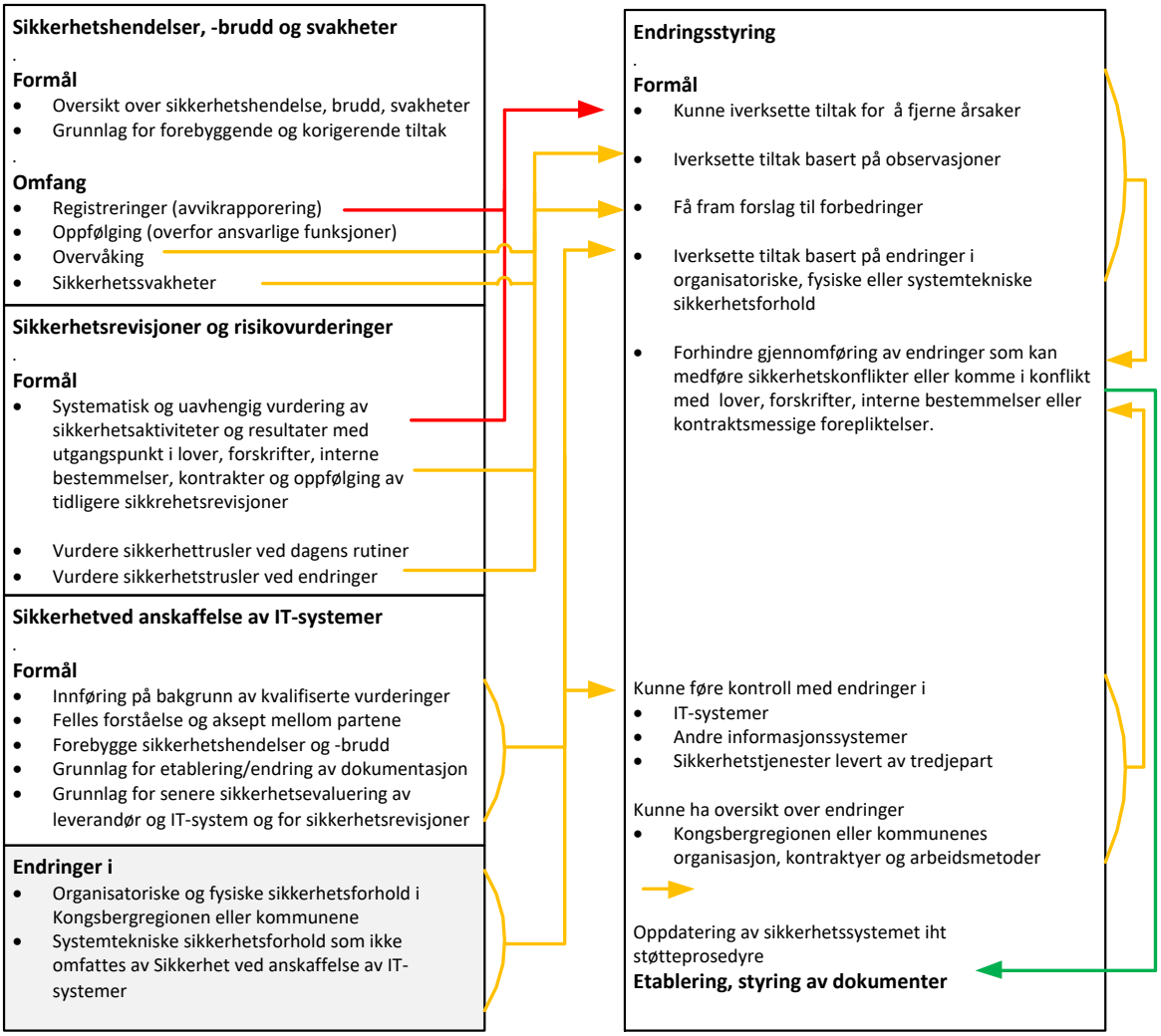
- At sikkerhetssystemet er hensiktsmessig og virker effektivt i forhold til lovverk, kontrakter, brukerkrav og interne mål.
- Kontroll med endringer som følge av registrerte sikkerhetshendelser, -brudd og -svakheter og resultater fra sikkerhetsrevisjoner og risikovurderinger.
- Kontroll med endringer i IT-systemer og sikkerhetstjenester.
- Oversikt over endringer i Midt-Telemarkkommunenes organisasjon, kontrakter, arbeidsmetoder eller lignende.

Omfang

Prosedyren gjelder evaluering og oppfølging av alle aktiviteter som angår informasjonssikkerhet i Midt-Telemarkkommunene.

Beskrivelse

Koordineringsansvarlig er ansvarlig for endringsstyring og skal sørge for at styringen er en del av fast dagsorden for møtene i Midt-Telemark IKT (MT-IKT) og fagstyret for MT-IKT etter følgende modell:



3.5 Etablering og styring av dokumenter

Formål og omfang

Prosedyren gjelder:

1. Veiledende standard ved etablering av systemdokumentasjon for informasjonssikkerhet.
2. Styring av dokumenter for informasjonssikkerhet og registreringer som følger av disse dokumentene.

1. Bruk av veiledende standard ved etablering av systemdokumentasjon skal:
   - Sikre tilstrekkelig og entydig informasjon.
   - Sikre enhetlig og effektiv utarbeidelse av sikkerhetsdokumentasjon.
   - Gjenfinne ønsket informasjon på en lettere måte.
   - Dele informasjon, erfaring, krav med samarbeidspartnere og brukere på en enkel måte.

2. Styring av dokumenter for informasjonssikkerhet og registreringer som følger dokumenter skal:
   - Sikre at kun korrekt dokumentasjon blir benyttet og er tilgjengelig for brukerne
   - Forhindre likelydende beskrivelser i flere uavhengige dokumenter
   - Forhindre konflikter mellom uavhengige dokumenter

Beskrivelse

Bruk av veiledende standard ved etablering av systemdokumentasjon

Ansvar

Dokumenteier er ansvarlig for at malen blir fulgt ved utarbeidelse av prosedyrer.

Formål

Kort beskrivelse av formålet med prosedyren.

Omfang

Omhandler: Hva prosedyren omhandler og eventuelt hvilke funksjoner som omfattes av prosedyren.

Beskrivelse

Avsnittet deles i underavsnitt avhengig av beskrivelsens omfang. Ansvaret skal henvise til funksjon og skal klart framgå av prosedyren. Ansvaret for og bruken av eventuelle hjelpemidler skal beskrives. Hjelpemidler kan være skjemaer, applikasjoner og eller detaljerte spesifikasjoner.

Dokumenteier skal vurdere om det er påkrevd med en bestemt kompetanse (faglige forutsetninger eller myndighet, for eksempel autorisasjoner eller lisenser) for å kunne utføre prosedyren.

Dokumenteier skal vurdere om det er behov for å beskrive hvordan eventuelle avvik fra prosedyren skal behandles og hvilken funksjon som har ansvaret for dette.

Under beskrivelsen skal dokumenteier angi hvordan registreringer skal gjennomføres og dokumenteres, herunder:

- Navn på hjelpemiddel.
- Arkivtid (for eksempel ved endring, vurderes, 3 måneder, 5 år, >= 10 år).
- Arkiveringsmetode (fysisk sikrede arkiv, Elektronisk).
- Arkiveringsansvar.

Styring av dokumenter for informasjonssikkerhet og registreringer som følger dokumenter

Dokumenteiere

Dokumenteiere utpekes av behandlingsansvarlig.

Dokumentstyring

Dokumenteier skal sørge for at dokumentet blir akseptert og forstått av de berørte funksjonene og skal:

- Påføre dokumentreferanser.
- Påse at det ikke er systemkonflikter med andre systemdokumenter (alle systemer) ved etablering.
- Sørge for at dokumentet blir redigert ved behov for endringer.

3.6 Vedlegg 1 – Skjema for informasjonssikkerhet ved virksomhet/avdeling X

Behandlinger i virksomheten

(Se 2.9 Meldeplikt - prosedyre)

Informasjon **Formål**	**Hjemmel**	**Klassifikasjon**	**Sikrings-** **tiltak**	**System** (Applikasjonsnavn) **Dataeier** (Stilling/Funksjon)

Risikovurdering

Viser til skjema for risikovurdering som Midt-Telemarkkommunene bruker i sitt HMS-system. Der er også informasjonssikkerhet inkludert. Eventuell handlingsplan eller tiltak for avdelingen kan limes inn i denne malen.

Autorisasjon og tilgangsstyring

Hvem i virksomheten skal ha tilgang til hvilke systemer og registre

Rolle	**System**	**Tilgangsnivå**

Hvordan gis det tilgang?

Prosedyre:

Skriv i klartekst, henvis til sentral prosedyre og lokale skjemaer.

Hvordan kontrolleres tilgangene?

Prosedyre:

Kontroll:

Dato	Kontroll utført av	Resultat

Hendelseslogg

Prosedyre for gjennomgang av hendelseslogg:

-

Hvor dokumenteres gjennomgang av hendelseslogg?

-

Fysisk sikring

Adgangssoner

Sone	Hvilke rom er i sonen	Tilgangskontroll
Åpen sone: Arealer hvor publikum har fri adgang, korridorer, venterom, fellesarealer, områder med alminnelig ferdsel		
Indre sone: Åpne arbeidsplasser, arealer beregnet kun for medarbeidere i virksomheten, evt. publikum i følge med medarbeidere.		
Sikker sone: Areal hvor kun spesielt godkjente medarbeidere har adgang, og hvor publikum ikke skal ha adgang		

Dokumenter og innsyn

Sone	Risikoforhold	Tiltak
Posthyller		
Dokumenter tilgjengelige på ulåst kontor		

Innsyn på skjerm		

Nøkkelsystem

Beskriv nøkkelsystem i klartekst

Kontroll av nøkkellister:

Dato	Kontroll utført av	Resultat

Daglig ansvarlig – momenter fra prosedyre Sikkerhetsorganisasjon

- *Gjennomføre risikovurdering.*
- *Bestemme tilgang til informasjon og* funksjonalitet for brukere.
- *Sørge for at all påkrevet dokumentasjon foreligger.*
- Sørge for at det finnes et opplæringstilbud med fokus på rutiner og informasjonssikkerhet.
- *Kontrollere jevnlig at gjeldende driftsrutiner blir fulgt og at nødvendig dokumentasjon foreligger.*
- Ta stilling til og følge opp meldte avvik i henhold til prosedyre for avviksbehandling.
- Minimum årlig å gjennomføre prosedyre for sikkerhetsrevisjon
- Årlig å gjennomføre risikovurdering, skjema ligger inkludert i den årlige rutine for risikovurdering i HMS-systemet

3.8 Personvernerklæring

Dokumentet et laget for publisering på kommunens nettsider

Bø kommune behandler store mengder personopplysninger.

Det rettslige grunnlaget for behandling av personopplysninger vil normalt være fastsatt i lov eller forskrift, og kommunen er pålagt meldeplikt til Datatilsynet om hvilke opplysninger som samles inn og til hvilket formål opplysningene skal benyttes til.

Selv om kommunen har lovhjemmel for å samle inn og bruke personopplysninger uten å spørre den registrerte om samtykke, har den registrerte likevel noen sentrale rettigheter.

Dine rettigheter etter personopplysningsloven:

Du har rett til innsyn

Du kan henvende deg til en hvilken som helst virksomhet og få vite hva slags behandlinger av personopplysninger som foretas der. På bakgrunn av dette kan du be om en utdyping på en del felter: Navn og adresse på den behandlingsansvarlige og hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter, formålet med behandlingen, hvilke typer personopplysninger som behandles og hvor de er hentet fra. Du kan også kreve å få vite hvem personopplysningene eventuelt vil bli utlevert til.

Dersom du er registrert hos den behandlingsansvarlige har du som hovedregel rett til å få vite hva som er registrert om deg (personopplysningsloven § 18). Det er imidlertid gjort unntak i loven for slikt innsyn dersom personopplysningene utelukkende behandles for statistiske formål og behandlingen ikke får noen direkte betydning for den registrerte.

Mangelfulle opplysninger skal rettes

Den behandlingsansvarlige har plikt til å rette og slette, på eget tiltak eller på anmodning, når opplysningene er feilaktige, mangelfulle eller unødvendige. Den behandlingsansvarlige skal sørge for at mangelfulle eller feilaktige opplysninger ikke får betydning for den registrerte.

Personopplysninger kan oppbevares til historiske, vitenskapelige og statistiske formål selv om de ikke er nødvendige lenger etter sitt opprinnelige formål. Forutsetningen er at samfunnets interesse i oppbevaring klart overstiger den registrertes interesse i personvern.

Generelt

Behandlingsansvarlig er rådmannen i Bø kommune. Det daglige ansvar for den behandlingsansvarliges plikter er tillagt den enkelte leder.

Personvern- og sikkerhetsansvarlig er Personal- og administrasjonssjefen. Personvern- og sikkerhetsansvarlig oppgaver er å koordinere kommunens sikkerhetsarbeid og holdningsskapende aktiviteter.

Alle virksomheter	**INTERNKONTROLL HMS**	**1. versjon: 02.11.2012** **Utarbeidet av: Midt-Telemarkrådet** **Godkjent av: AMU Bø, AMU Nome, AMU Sauherad**
	Sikkerhetsplan for Midt-Telemarkkommunene	**2. versjon: Desember 2015** **Godkjent av AMU Bø:** **Side 87 av 86**