

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av: 
<h1>Nødprosedyrer</h1>	Støttedokument Faktaark nr 11 Versjon: 2.1 Dato: 15.12.2010

Målgruppe Dette faktaarket er spesielt relevant for:	<input type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	Virksomhetens leder har ansvar for å etablere nødprosedyrer.		
Gjennomføring	Nødprosedyrer skal etableres før behandling av helse- og personopplysninger.		
Formål	Sikre at virksomhetens behandling av helse- og personopplysninger ivaretas ved ikke-planlagt driftsstans i IKT-systemene.		
Omfang	Omfatter alle systemer inklusive registre/systemer i medisinsk teknisk utstyr, som virksomheten benytter eller er avhengig av for å yte sine tjenester.		
Hjemmel	Personopplysningsforskriften § 2-12.		
Referanser	Norm for informasjonssikkerhet pkt 5.5.3.		

Nr.	Handling/Utførelse
1	Planlegge nødprosedyrer a) Gjennomgå resultat av risikovurderinger slik at restrisiko som ikke er ivaretatt med etablerte tiltak danner grunnlag for nødprosedyrer (det er ikke mulig å gardere seg mot alle årsaker for stans i IKT-løsninger) b) Gjennomgå klassifisering av systemer iht kritikalitet c) Beslutte hvilke systemer som skal ivaretas med nødprosedyrer og hvilke type nødprosedyrer som er nødvendig (manuelle prosedyrer, reetablering av teknisk reserveløsning, parallelle løsninger, osv)
2	Utarbeide nødprosedyrer for håndtering av krisesituasjoner a) Varslings- og eskaleringsprosedyrer slik at det ikke er tvil om hvem som skal gjøre hva b) Organisering av katastrofeteam og plassere ansvar c) Forutsetninger for iverksettelse av planen d) Definere katastrofenivå: for eksempel grønn, gul og rød e) Manuelle prosedyrer (alternative driftsprosedyrer) som skal fungere i en overgangsperiode frem til ordinær løsning er reetablert. Manuelle prosedyrer er gjerne basert på skjemaer (NB! Notér hvor disse oppbevares) og krever arkivering for senere ajourføring i for eksempel journalsystemer f) Kontakter og nødvendige avtaler med leverandører g) Varslingsprosedyre for leverandører h) Handlingsplan for reetablering av teknisk løsning i) Fjernlagring av sikkerhetskopi: <ul style="list-style-type: none"> – Hvem henter den? – Hvor er den? – Hvilke ”nøkler” trengs for å få sikkerhetskopi utlevert (passord, fysisk nøkkel, identifikasjonsdokument)? – Vær oppmerksom på at ved sikkerhetskopi over nett må prosedyren tilpasses etter avtale med leverandør for bl.a. tilbakekopiering av data j) Aktivitetslister k) Informasjon til kunder, ansatte og omgivelser l) Relaterte dokumenter (for eksempel tekniske prosedyrer for nøddrift og gjenoppretting av ordinær drift)

Nr.	Handling/Utførelse
3	Opplæring, test og revisjon a) Etablere prosedyre for opplæring av relevant personell b) Etablere prosedyre for periodisk test (minimum årlig) med trening av personellet c) Etablere prosedyre for oppdatering og vedlikehold av nødprosedyrene (minimum årlig)

Eksempler

Store virksomheter

Informasjonssystemer som behandler helse- og personopplysninger skal sikres for tilgjengelighet. Det må forberedes og etableres alternativ behandling for de tilfeller informasjonssystemene ikke er tilgjengelige. Alternativ behandling gjennomføres ved duplisering av utstyr/program i en reserveløsning (sekundær driftsløsning) i henhold til foretakets "Kartlegging og klassifisering av systemer iht kritikalitet".

For forhold/områder som ikke dekkes av en reserveløsning må det etableres manuelle nødprosedyrer i virksomheten.

Nødprosedyrer vil være ulike for ulike foretak, organisasjoner og systemer avhengig av hvor omfattende nødløsning som etableres. Eksempler på nødprosedyrer i denne sammenheng kan være:

- a) hvordan informasjon skal gis til involvert personell i virksomheten, eventuelt andre virksomheter når nødprosedyrer skal iverksettes
- b) hvordan behandle helse- og personopplysninger som oppstår under et avbrudd i tilgjengelighet; oppbevaring av opplysninger
- c) registrering og oppdatering av helse- og personopplysninger og tidspunkt for dette når systemet igjen er tilgjengelig
- d) kvalitetssikring at registrerte helse- og personopplysninger er komplette og korrekte

Middels virksomheter

I mindre virksomheter skal det være etablert en reserveløsning for å ivareta kunder/pasienter.

I tillegg bør det etableres nødprosedyrer for kritiske funksjoner som ikke er ivaretatt av reserveløsning, f.eks.

- a) forvaltning, registrering og kvalitetssikring av helse- og personopplysninger som oppstår under et avbrudd
- b) endring i lagerbeholdninger

Nødprosedyrer skal være dokumentert på en slik måte at de vil være tilgjengelig for personell ved stans i systemene.

Små virksomheter

I små virksomheter (for eksempel legekantor og apotek) vil det i liten grad være etablert en reserveløsning. Ved hendelser som kan føre til lengre stans i systemet (feil på utstyr, serverhavari og lignende) bør det vurderes å utarbeide en nødprosedyrer for reetablering av utstyr og alternative driftsprosedyrer for å holde virksomheten i gang (manuelle prosedyrer). Nødprosedyrer for å reetablere systemer bør inneholde følgende aktiviteter:

- a) anskaffe server, arbeidsstasjoner og nettverk
- b) installasjon av utstyr og system
- c) tilbakelegging av sikkerhetskopier
- d) oppstart av server og system
- e) kontroll at system er komplett og korrekt
- f) sette system(er) i drift
- g) overgang fra manuelle prosedyrer til ordinær drift

På bakgrunn av "Akseptkriterier for tilgjengelighet" avgjør daglig leder hvorvidt aktiviteter skal være forberedt på forhånd. Ved mindre feil som ikke kan løses av daglig leder kontaktes systemleverandør.

Eksempler på tiltak som kan være forberedt på forhånd er

- a) periodisk utskrift (eller overføring til annet utstyr) av relevante data slik at disse er tilgjengelig ved behov
- b) eksportere data til et format som lett kan gjøres tilgjengelig ved behov