Nødprosedyrer ved bortfall av IKT (faktaark 11)

Versjon 3.0

Publisert: 04.02.2021

Utarbeidet med støtte fra direktoratet for e-helse

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler nødprosedyrer ved bortfall av IKT. Formålet med faktaarket er å sikre at virksomhetens behandling av helse- og personopplysninger ivaretas ved ikke-planlagt driftsstans i IKT-systemene. Faktaarket omfatter nødprosedyrer for alle systemer, inklusive registre/systemer i medisinsk teknisk utstyr, som virksomheten benytter eller er avhengig av for å yte sine tjenester. Faktaarket har en prosessorientert tilnærming og inneholder veiledning og eksemplel fremgangsmåte for utarbeidelse av nødrutiner.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er • IKT-ansvarlig • Sikkerhetsleder / sikkerhetskoordinator • Virksomhetens leder/ledelse • Databehandler
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen • Kapittel 5.9 Nødrutiner
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: - NSMs grunnprinsipper for IKT-sikkerhet 2.0 Beskytte og opprettholde - NSMs grunnprinsipper for IKT-sikkerhet kapittel 4.3 Kontroller og håndter hendelser - NSMs grunnprinsipper for IKT-sikkerhet kapittel 4.4 Evaluer og lær av hendelser - Veileder om risikostyring for informasjonssikkerhet og personvern

Nødprosedyrer ved bortfall av IKT

Manglende tilgjengelighet til informasjonssystemer kan medføre skader både for virksomheten, virksomhetens autoriserte brukere, pasienten/brukeren ved ytelse av helsehjelpen og andre registrerte. Det er ikke mulig å forebygge mot alle mulige årsaker til stans i IKT-løsninger. Det må derfor forberedes og etableres alternative prosedyrer for de tilfeller informasjonssystemene ikke er tilgjengelige.

Nødprosedyrer bør tilpasses og inngå i eventuelle eksisterende planverk virksomheten har på området, f.eks kontinutetsplaner og IKT-beredskapsplaner. Begreper og roller i dette faktaarket er generiske, og kan tilpasses ut fra planer og organisering i hver enkelt virksomhet.

Nr.	Handling/Utførelse
1	**Planlegge nødprosedyrer** a) Kartlegg konsekvenser ved bortfall b) Gjennomgå klassifisering av systemer iht. kritikalitet og Normen kap. 5.9 c) Kartlegg avhengigheter til andre systemer og infrastruktur d) Gjennomgå risikovurderinger som er gjort av informasjonssystemene e) Beslutte nivå for akseptabel risiko for tilgjengelighet for hver aktuell klassifisering, med minimum maksimal avbruddstid f) Beslutte hvilke systemer som skal ivaretas med nødprosedyrer og hvilke typer nødprosedyrer som er nødvendig (manuelle prosedyrer, reetablering av teknisk reserveløsning, parallelle løsninger, osv) g) Dialog med driftsleverandør(er) om roller, ansvar, leveranser og deres nødprosedyrer
2	**Utarbeide nødprosedyrer eller -planer for håndtering av hendelser som kan forårsake ikke-planlagt driftsstans** a) Innledende vurdering av hendelsens alvorlighetsgrad b) Opprettelse av hendelseslogg c) Varsling *internt* og eskalering ut ifra ulike alvorlighetsgrader og type hendelse • Forutsetninger for iverksettelse av planen • Definere hendelseskategorier med tilhørende tiltak • Definere beredskapsnivå, f.eks. grønn, gul og rød, og hva disse innebærer • Hvem skal gjøre hva innen når • Kontaktinformasjon må oppdateres jevnlig d) Varsling *eksternt* (driftsleverandører og eventuelt overordnet organ) • Kontaktinformasjon over eksterne må oppdateres jevnlig e) Organisering av krisestab og plassere ansvar der hendelsen utgjør en hendelse

Nr.	Handling/Utførelse
	f) Alternative driftsrutiner som skal fungere i en overgangsperiode frem til ordinær løsning er re-etablert • Løpende registrering av nye og endrede opplysninger om f.eks. helseforhold, pasienter og lagerbeholdning (f.eks. på papir eller et alternativt informasjonssystem) • Arkivering for senere ajourføring når det primære informasjonssystemet er gjenopprettet g) Skadebegrensende tiltak • Basert på hendelseskategori • F.eks. isolering for å hindre spredning av skadevare eller vannlekkasje h) Gjenoppretting av teknisk løsning når virksomheten har kontroll og situasjonsforståelse i) Kommunikasjon til pasienter, ansatte, relevante myndigheter og andre som kan bli berørt j) Relaterte dokumenter (for eksempel tekniske prosedyrer for nøddrift og gjenoppretting av ordinær drift) k) Nødprosedyrer og -planer skal være dokumentert på en slik måte at de vil være tilgjengelig for personell ved stans i systemene.
3	**Opplæring, test og evaluering** a) Prosedyre for opplæring av relevant personell b) Plan for periodisk test (minimum årlig) • Håndtering av hendelser • Skadebegrensning • Gjenoppretting - av både systemer og data c) Foreta test, trening og øving på planen nevnt i foregående punkt d) Prosedyre for evaluering og revidering av nødprosedyrene (minimum årlig) • Måling av prosedyrenes effekt og evnen til å følge prosedyrene • Revisjon – internt og av leverandører • Forbedring NSMs grunnprinsipper for IKT-sikkerhet kapittel 4.3 og 4.4 beskriver gode tiltak for å håndtere og å lære av hendelser.