

		Utgitt med støtte av: 
Norm for informasjonssikkerhet www.normen.no		
Kartlegging og klassifisering av systemer i henhold til kritikalitet i forhold til behov for tilgjengelighet		Støttedokument Faktaark nr 4 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	Virksomhetsleder har ansvar for å kartlegge og klassifisere alle systemer som behandler helse- og personopplysninger i virksomheten. I praksis er ansvaret delegert til avdelingsledere / systemeiere.		
Gjennomføring	Kartlegging og klassifisering av systemer i henhold til kritikalitet skal dokumenteres før behandling av helse- og personopplysninger starter.		
Formål	<ul style="list-style-type: none"> • Kartlegge hvilke systemer som er kritiske for at virksomheten kan yte sine tjenester • Prioritere systemene i henhold til kritikalitet - i hovedsak gjelder dette ikke-planlagte stopp 		
Omfang	Omfatter alle systemer som inneholder helse- og personopplysninger 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, kap 5.5.3 Tilgjengelighet		

Handling/Utførelse

Nr.	Aktivitet/Beskrivelse
1	<p>Store virksomheter (f.eks. sykehus, kommuner mv.)</p> <p>Med utgangspunkt i virksomhetens "Oversikt over behandlinger av helse- og personopplysninger" kan systemer prioriteres som følger:</p> <p>Prioritet 1: systemer hvor stopp av tjeneste er eller kan være livstruende for pasient inklusive feilbehandling av pasient, eller kritisk for virksomhetens drift</p> <p>Prioritet 2: systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre</p> <ul style="list-style-type: none"> - betydelig merarbeid for personell - tapt effektivitet i virksomheten <p>Prioritet 3: systemer hvor stopp av tjeneste kan føre til svekkelse av pasientens tillit</p> <p>Prioritet 4: systemer hvor stopp inntil 72 timer kan aksepteres</p> <p>Prioritet 5: systemer som ikke er prioritert</p> <p>Det skal også kartlegges hvilke andre systemer de prioriterte systemene er avhengig av. Disse skal ha samme prioritet som de prioriterte systemene.</p> <p>For hver av de 5 prioritertene skal ledelsen fastsette akseptkriterier for tilgjengelighet, som et minimum hva som er akseptabel avbruddstid, f.eks:</p> <p>Klasse 1: avbruddstid (stans i system) inntil 30 min – ingen tap av data</p> <p>Klasse 2: avbruddstid (stans i system) inntil 8 timer – ingen tap av data</p> <p>Klasse 3: avbruddstid (stans i system) inntil 24 timer – ingen tap av data</p> <p>Klasse 4: avbruddstid (stans i system) inntil 72 timer – ingen tap av data</p> <p>Klasse 5: ikke prioritert</p>
2	<p>Mindre virksomheter (f.eks rehabilitering- og opptreningsvirksomheter)</p> <p>Med utgangspunkt i virksomhetens "Oversikt over behandlinger av helse- og personopplysninger" kan systemer prioriteres som følger:</p>

Nr.	Aktivitet/Beskrivelse
	<p>Prioritet 1: systemer hvor stopp av tjeneste er eller kan være livstruende for kunde inklusive feilmedisinering av pasient, eller kritisk for virksomhetens drift</p> <p>Prioritet 2: systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre</p> <ul style="list-style-type: none"> - tapt tillit hos kunde - betydelig merarbeid for personell - tapt effektivitet <p>Prioritet 3: systemer hvor stopp inntil 72 timer kan aksepteres</p> <p>For hver av de 3 prioriteringene skal ledelsen fastsette akseptkriterier for tilgjengelighet, som et minimum hva som er akseptabel avbruddstid. F.eks. følgende grupper:</p> <p>Klasse 1: ingen avbrudd i åpningstiden på virkedager – ingen tap av data</p> <p>Klasse 2: avbruddstid (stans i system) inntil 2 timer – ingen tap av data</p> <p>Klasse 3: avbruddstid (stans i system) inntil 72 timer – ingen tap av data</p>
3	<p>Små virksomheter (f.eks. legekantor, tannlegeskantor, fysioterapinstitutt, psykologfelleskap, bedriftshelsetjeneste, mv.)</p> <p>Ved et legekantor kan systemer prioriteres som følger:</p> <p>Prioritet 1: systemer hvor helse- og personopplysninger skal være tilgjengelig når behandlende personell har tjenstlig behov for dem</p> <p>For prioriteringen fastsettes følgende akseptkriterier:</p> <p>Klasse 1: ingen data skal gå tapt</p>

Eksempel

System	Prioritet	Klasse (Akseptkriterier for tilgjengelighet)
Elektronisk pasientjournal (EPJ)	1	1. Ingen avbrudd i åpningstiden på virkedager – ingen tap av data
Pasientadministrativt system (PAS)	1	1. Ingen avbrudd i åpningstiden på virkedager – ingen tap av data
Laboratoriesystem	2	2. Avbruddstid (stans i system) inntil 2 timer – ingen tap av data
Elektronisk meldingsutveksling av svar på laboratorieprøver	2	2. Avbruddstid (stans i system) inntil 8 timer – ingen tap av data
Elektronisk meldingsutveksling av resepter	3	3. Avbruddstid (stans i system) inntil 72 timer – ingen tap av data