

 <p>Norm for informasjonssikkerhet www.normen.no</p>		Utgitt med støtte av:  HelseDirektoratet
<h2>Sikkerhetskopi (backup)</h2>		Støttedokument Faktaark nr 21 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	Databehandlingsansvarlig (v/ foretakets ledelse). Det bør imidlertid utnevnes en operativt ansvarlig og/eller delansvarlig f.eks. pr. fagsystem/systemeier		
Gjennomføring	Kontinuerlig etter en gitt frekvens		
Formål	Å sikre at helse- og personopplysninger kan gjenopprettes om de skulle gå tapt som følge av bl.a.: <ul style="list-style-type: none"> • Feil i utstyr eller programvare • Utilsiktet sletting av bruker • Tilsiktet ødeleggelse/hærverk • Tap/tyveri av utstyr 		
Omfang	Alle virksomheter i helsesektoren skal ta sikkerhetskopi av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk.		
Hjemmel	<ul style="list-style-type: none"> • Personopplysningsforskriften § 2-12 • Helseregisterloven § 16 		
Referanser	Norm for informasjonssikkerhet, kapittel 5.5.3		

Handling/Utførelse

Nr.	Aktivitet/Beskrivelse
1.	Utnevne ansvarlig for sikkerhetskopiering Det utnevnes en som er ansvarlig for at prosedyre for sikkerhetskopiering blir etablert og gjennomført.
2.	Utarbeide prosedyrer for sikkerhetskopiering Aktivitet 3-6 er aktiviteter som bør vurderes ifm. å utarbeide en prosedyre for sikkerhetskopiering.
3.	Vurder hvilke data som skal sikkerhetskopieres Generelt gjelder følgende: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – Hvilke data det skal tas sikkerhetskopi av og hvor ofte det skal sikkerhetskopieres, bør være basert på resultatene av en risikovurdering (se Faktaark 7 - 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)

Nr.	Aktivitet/Beskrivelse
4.	Vurdere type sikkerhetskopi <ul style="list-style-type: none"> – 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
5.	Vurdere frekvens på sikkerhetskopi <p>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:</p> <ul style="list-style-type: none"> – 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
6.	Merking av sikkerhetskopi <ul style="list-style-type: none"> – Lagringsenheter 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
7.	Planlegge gjennomføring av sikkerhetskopiering <p>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.</p>
8.	Kvalitetssikre sikkerhetskopieringen <p>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.</p> <p>Ved etablering av ny prosedyre for sikkerhetskopiering anbefales det å kontrollere at sikkerhetskopien faktisk inneholder data som kan tilbakekopieres.</p>
9.	Oppbevaring av sikkerhetskopi <ul style="list-style-type: none"> – Sikkerhetskopier skal oppbevares i tyveri- og brannsikker 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 (anbefalt avstand, med bakgrunn i krav fra forsikringsbransjen, til eksternt lokasjon er minimum 1 km)
10.	Gjenoppretting av sikkerhetskopi <p>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.</p>
11.	Utrangering av lagringsmedier <p>Sikkerhetskopien skal destrueres på en slik måte at innholdet ikke kan fremhentes. Det må benyttes godkjent sletteutstyr (f.eks. degausser eller godkjent sletteprogramvare). Alternativt må lagringsmediet destrueres fysisk.</p>

Eksempel på frekvens og type sikkerhetskopi (må tilpasses den enkelte virksomhet)

Daglig Tape navn:	Ukentlig Tape navn:	Månedlig Tape navn:	Repeteres hver:	Sikkerhetskopi type:	Lagringssted:	Kommentar:
Mandag			7. dag	Full kopi	Lokal safe	Samme tape brukes om igjen
Tirsdag			7. dag	Full kopi	Lokal safe	Samme tape brukes om igjen
Onsdag			7. dag	Full kopi	Lokal safe	Samme tape brukes om igjen
Torsdag			7. dag	Full kopi	Lokal safe	Samme tape brukes om igjen
	Uke 1		28. dag	Full kopi	Lokal safe	Samme tape brukes om igjen
	Uke 2		28. dag	Full kopi	Lokal safe	Samme tape brukes om igjen
	Uke 3		28. dag	Full kopi	Lokal safe	Samme tape brukes om igjen
		Måned	28. dag	Full kopi	Lokal safe/ Bankboks	Ny tape hver måned