

		Utgitt med støtte av:  Helsedirektoratet
Norm for informasjonssikkerhet www.normen.no		
<h1>Sikkerhetsrevisjon</h1>		Støttedokument Faktaark nr 6 Versjon: 2.1 Dato: 15.12.2010

Målgruppe Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input 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 ledelse har et ansvar for at det gjennomføres sikkerhetsrevisjoner. Databehandler har et selvstendig ansvar for egen sikkerhetsrevisjon		
Gjennomføring	Gjennomføres jevnlig, minimum årlig		
Formål	Formålet med å gjennomføre sikkerhetsrevisjon er å: <ul style="list-style-type: none"> • 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	Alle virksomheter som behandler helse- og personopplysninger er pålagt å gjennomføre sikkerhetsrevisjoner. Sikkerhetsrevisjonen må tilpasses omfanget av virksomheten.		
Hjemmel	Personopplysningsforskriften § 2-5		
Referanser	Norm for informasjonssikkerhet, kap 6. 1 Sikkerhetsrevisjon		

Gjennomføring av sikkerhetsrevisjon er et ansvar for virksomhetens ledelse. For mindre virksomheter bør daglig leder selv gjennomføre denne, i samarbeid med andre som har roller ift. sikkerhet og drift av datasystemene. I større virksomheter kan den praktiske gjennomføringen gjøres av for eksempel sikkerhetskoordinator eller eksterne konsulenter. 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.

Resultater fra sikkerhetsrevisjonen skal dokumenteres og gjennomgås ifm ledelsens gjennomgang. I tillegg skal det i etterkant av den enkelte revisjon vurderes gjennomføring av tiltak for å rette opp avvik som er avdekket. I den årlige sikkerhetsrevisjon skal det kontrolleres at alle avvik er håndtert.

Omfanget av sikkerhetsrevisjoner skal tilpasses virksomhetens størrelse og behov.

Tabellen nedenfor angir Normens minimumskarv til en sikkerhetsrevisjon.

Nr.	Sjekkpunkt	Faktaark
1.	Er ansvaret plassert og organiseringen av sikkerhetsarbeidet dokumentert og kjent?	1
2.	Er det etablert, dokumentert og tatt i bruk et styringssystem for informasjonssikkerhet?	2
3.	Dekker sikkerhetsmål og –strategi virksomhetens faktiske behandling av helse- og personopplysninger?	2
4.	Er det etablert nødvendige prosedyrer i styringssystemet?	3
5.	Overholdes prosedyrene i styringssystemet?	3
6.	Gjennomføres løpende nivåtilpasset opplæring i bruk av informasjonssystemene og relevante prosedyrer i styringssystemet?	9
7.	Er det etablert avtaler med kommunikasjonsleverandør, sikkerhetsleverandør og databehandler?	10 og 36
8.	Fungerer tilgangsstyringen og oppfølgingen av denne tilfredsstillende?	14

Tabellen nedenfor angir eksempler på områder som kan være aktuelle å sikkerhetsrevidere.

Nr	Sjekkpunkt	Faktaark
1.	Er det gjennomført nødvendig(e) risikovurdering(er) siste år?	7
2.	Er prosedyrene for avviksbehandling ift. informasjonssikkerhet kjent i virksomheten?	8
3.	Fungerer avviksbehandling ift. informasjonssikkerhet?	8
4.	Er det etablert nødprosedyrer ved stans i informasjonssystemene?	11
5.	Gjennomføres det jevnlig kontroll/gjennomgang av hendelsesregistre?	15
6.	Krypteres helse- og personopplysninger (f.eks. meldingsformidling) som overføres i åpne nett?	16 og 24
7.	Er det etablert tilfredsstillende fysisk sikring av områder og datautstyr?	17
8.	Er lagringsenhet på bærbart utstyr som benyttes til helse- og personopplysninger kryptert?	18
9.	Oppdateres antivirusprogramvaren kontinuerlig?	19
10.	Tas det daglig sikkerhetskopi?	21
11.	Oppbevares sikkerhetskopier utenfor huset?	21
12.	Er det kontroll med all ekstern tilgang til datasystemer?	22
13.	Følges ”Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet” ved eventuell ekstern tilgang?	36
14.	Er det etablert relevante avtaler for forskningsprosjekter?	23
15.	Slettes helse- og personopplysninger når formålet med behandlingen er avsluttet?	25
16.	Brukes trådløst utstyr og nett iht. etablerte prosedyrer?	26
17.	Etterleves prosedyrene for makulering?	27
18.	Etterleves prosedyrene for bruk av e-post og Internett?	27 og 33
19.	Etterleves prosedyrene for hjemmekontor og mobilt utstyr?	29 og 30
20.	Byttes passord iht. prosedyrene?	31
21.	Følges veileder ”Personvern og informasjonssikkerhet i forskningsprosjekter innefor helse- og omsorgssektoren” ifm utlevering av helse- og personopplysninger?	40
22.	Etterleves reglene for bruk av SMS i pasientkontakt?	42
23.	Etterleves reglene for bruk av testdata i systemer som inneholder helse- og personopplysninger?	43

Som et tillegg til dette faktaarket er det utarbeidet et skjema med en komplett revisjonsliste som dekker samtlige krav i Normen (Se Faktaark 6b – Sikkerhetsrevisjon - Sjekkliste). Skjemaet kan lastes ned fra www.normen.no.