

   	Utgitt med støtte av:  Helsedirektoratet
Norm for informasjonssikkerhet www.normen.no	
Tilbakerapportering av resultater fra IKT-driften	Støttedokument Faktaark nr 12 Versjon: 2.1 Dato: 15.12.2010

Målgruppe Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input 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	Ansvar for tilbakerapporteringen av resultater fra IKT-driften skal plasseres hos databehandler, leverandører, driftsansvarlige, etc. Virksomhetens ledelse må følge opp og behandle resultater fra tilbakerapporteringen.		
Gjennomføring	Tilbakerapportering av resultater fra IKT-driften må følges opp jevnlig (eksempelvis hver måned).		
Formål	Sikre at viktige/prioriterte resultater fra IKT-driften blir tilbakerapport og behandlet slik at nødvendige tiltak kan iverksettes.		
Omfang	Alle virksomheter skal ha tilbakerapportering av resultater fra IKT-driften. Omfanget av rapportering må tilpasses den enkelte virksomhet og tjeneste.		
Hjemmel	Personopplysningsforskriften § 2-5 og § 2-6		
Referanser	Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet.		

Nr.	Handling/Utførelse
1	Driftsstatus på kritiske system Generell driftsstatus på kritiske IKT-system, for eksempel EPJ (elektronisk pasientjournalssystem) eller PAS (pasientadministrativt system), bør jevnlig rapporteres til ledelse/beslutningspersoner. Eksempel på parametere som kan inngå i rapportering: <ul style="list-style-type: none"> – Oppetid på systemer – Planlagte avbrudd og tidslengde på avbrudd – Feilsituasjoner som ikke blir definert som avvik – Mislykkede pålogginger, glemte passord etc. – Feilsituasjoner som fremkommer i hendelsesregistre
2	Oppfølging av avviksrapportering Alvorlige feil og hendelser skal rapporteres som avvik. Spesielt bør dette gjøres når det er avdekket avvik fra vedtatte prosedyrer og nivå for akseptabel risiko. Oppfølging og status på avviksrapportering bør rapporteres jevnlig som en del av resultatene fra driften. Oppfølgingen bør omfatte både avvik og andre forhold som blir rapportert. For mer informasjon, se Faktaark 8 - Avviksbehandling.
3	Meldingskommunikasjon (EDI) Status på meldingskommunikasjonen sier noe om hvordan virksomheten ivaretar elektronisk samhandling med andre (for eksempel henvisning, epikrise, resepter, behandlerkrav, laboratoriesvar, SMS, applikasjonskvittering, osv). Gode prosedyrer rundt elektronisk samhandling er viktig for å ivareta tilfredsstillende informasjonssikkerhet. Parametere som kan inngå i rapportering er for eksempel <ul style="list-style-type: none"> – Meldinger uten kvittering – Ikke-planlagte stans i meldingskommunikasjon – Planlagte stans i meldingskommunikasjon – Feilsendte meldinger (for eksempel meldinger med feil mottaker og -adresse) – Meldinger med negativ applikasjonskvittering – antall og feiltype

Nr.	Handling/Utførelse
4	<p>Systemleverandør</p> <p>Rapportering fra systemleverandører (for eksempel for EPJ) er viktig med tanke på ha stabil og god drift av viktige systemer. Rapporteringer bør foregå jevnlig og inneholde viktig informasjon i forhold til informasjonssikkerhet. Eksempel på parametere som kan inngå i rapportering:</p> <ul style="list-style-type: none"> – Planlagte endringer, forventet effekt og tidspunkt de skal utføres – Sikkerhetsoppdateringer (med angivelse av resultat) – Feilrettinger – Systemoppdateringer (med angivelse av resultat)
5	<p>Databehandler</p> <p>Databehandler skal iht databehandleravtalen jevnlig gi statusrapporter om resultater fra sine ansvarsområder tilbake til databehandlingsansvarlig (som vanligvis er virksomhetens ledelse). Det presiseres at en databehandler er en ekstern person/virksomhet utenfor den databehandlingsansvarliges virksomhet. Eksempel på parametere som kan inngå i rapportering:</p> <ul style="list-style-type: none"> – Planlagte endringer, forventet effekt og tidspunkt de skal utføres – Feilsituasjoner – Konfigurasjonsendringer – Oppetid – Feilsituasjoner som fremkommer i hendelsesregistre – Manglende oppfyllelse av SLA (servicenivåavtale) og mulig årsaker
6	<p>Nettleverandører (for eksempel Norsk Helsenett)</p> <p>Nettleverandøren er som regel ansvarlig for at kommunikasjonskanalen er tilgjengelig og sørger for transport av kommunikasjon over nettet. At nettet fungerer som det skal er en viktig forutsetning for å kunne etablere sikker elektronisk kommunikasjon. Eksempel på parametere som kan inngå i rapportering:</p> <ul style="list-style-type: none"> – Feilsituasjoner, nedetid – Endringer i nettet som kan gi konsekvenser for virksomheten – Manglende oppfyllelse av SLA (servicenivåavtale) og mulig årsaker
7	<p>Ondsinnnet programvare</p> <p>Ondsinnnet programvare kan være en reell trussel mot informasjonssikkerheten og kan komme for eksempel gjennom e-post, CD, minnepinne eller ved nedlasting av data fra andre nett. Eksempel på parametere som kan inngå i rapportering:</p> <ul style="list-style-type: none"> – Hendelser som har medført konsekvenser for virksomheten – Hvilke tiltak som er iverksatt og resultater av disse – Forslag til eventuelle forebyggende tiltak
8	<p>Status for sikkerhetsbarriere (for eksempel brannmur)</p> <p>Trafikk som slipper gjennom sikkerhetsbarrierer kan være ondsinnede angrep som prøver å få tilgang til virksomhetens datanettverk. Sikkerhetsbarrierer krever jevnlig oppdateringer og konfigurasjonsendringer. Eksempel på parametere som kan inngå i rapportering:</p> <ul style="list-style-type: none"> – Hendelser som har medført konsekvenser for virksomheten – Hvilke tiltak som er iverksatt og resultater av disse – Forslag til eventuelle forebyggende tiltak