

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av: 
<h2>Kontroll og sikring av ekstern tilgang</h2>	Støttedokument Faktaark nr 22 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 checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	IKT-ansvarlig er ansvarlig for kontroll og sikring av ekstern tilgang.		
Gjennomføring	Ved innføring av nye løsninger for ekstern tilgang, og ved kontinuerlig oppfølging		
Formål	Påse at ekstern tilgang til datanettverk og IKT-systemer som behandler helse- og personopplysninger er sikret innenfor nivå for akseptabel risiko.		
Omfang	Alle typer ekstern tilgang.		
Hjemmel	Personopplysningsforskriften § 2-7		
Referanser	<ul style="list-style-type: none"> • Veileder i informasjonssikkerhet ved tilknytning mellom kommuner, fylkeskommuner og helsenettet • Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet • Faktaark 36 - Fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008 		

Kontroll og sikring av ekstern tilgang skal beskytte mot to hovedtrusler:

- At løsningen for ekstern tilgang kan gi uautoriserte tilgang til virksomhetens datanettverk
- At mobilt utstyr på avveie kan benyttes til å koble seg mot virksomhetens datanettverk

Nr.	Handling/Utførelse
1.	<p>Tilgang fra hjemmekontor og mobile løsninger</p> <p>Tilgang fra hjemmekontor og mobile løsninger bør kun gis basert på tjenestelig behov. Før det etableres slike løsninger bør det vurderes:</p> <ul style="list-style-type: none"> – hvilke systemer det er behov for tilgang til fra hjemmekontor og mobile løsninger – hvilke grupper ansatte som har behov for slik tilgang <p>Det skal benyttes sikkerhetsnivå 4 for autentisering for tilgang til helseopplysninger fra hjemmekontor og mobile løsninger.</p> <p>Ved bruk fra hjemmekontor og mobile løsninger må den tekniske løsningen konfigureres slik at den ikke kan utnyttes til uautorisert tilgang til virksomhetens datanettverk. Dette kan gjøres ved for eksempel å:</p> <ul style="list-style-type: none"> – Benytte løsninger for nettverkssikkerhet som sikrer at kun systemer med oppdaterte virusdefinisjoner, sikkerhetspatcher osv. kan koble seg til virksomhetens datanettverk – Tillate tilgang kun via terminalserverløsning – Benytte brannmur på PC som kontrolleres fra virksomheten for å hindre at trafikk går utenom oppkoblingen og ut på Internett

Nr.	Handling/Utførelse
2.	<p>Sammenkobling av virksomhetens geografisk adskilte enheter</p> <p>Ved sammenkobling av geografisk adskilte enheter forutsettes det at enhetene er underlagt et felles informasjonssikkerhetsregime og samordnet drift. Når enhetene er sammenkoblet vil de fungere som et felles datanettverk. Sammenkoblingen stiller således ikke ytterligere krav til sikkerhet på klientsystemene. Det bør stilles krav om:</p> <ul style="list-style-type: none"> – Kryptert datakommunikasjon (ref. Datatilsynets til enhver tid gjeldende krav) – Bruk av PKI-sertifikat skal være i samsvar med ”Kravspesifikasjon for PKI i offentlig sektor” (se www.difi.no)
3.	<p>Tilkobling fra leverandører (fjernaksess)</p> <p>Tilkobling fra leverandører skal kun skje etter forhåndsavtalt prosedyre. Tilgang bør godkjennes før hver tilkobling, og virksomheten bør ha mekanismer på plass for å kunne overvåke tilgangen. Kun autorisert personell fra leverandør skal gis tilgang. Disse skal ha underskrevet taushetserklæring og være forhåndsgodkjent. Brannmur eller nettverksfilter bør sikre at kun nødvendige porter er åpne for tilgang fra leverandøren. Fjernaksess skal benytte sikkerhetsnivå 4 for autentisering. All bruk av fjernaksess skal registreres som hendelse og hendelsesregistre skal gjennomgås. Den tekniske løsningen skal etableres på bakgrunn av en risikovurdering.</p> <p>Mulige tekniske løsninger:</p> <ul style="list-style-type: none"> – Virksomheten åpner for tilgang vha VPN (for eksempel IPSec eller SSL) basert på forhåndsutvekslet krypteringsnøkkel eller sertifikat – Leverandøren gis tilgang til en terminalserverløsning som overvåkes av virksomheten – Virksomheten åpner porter i egen brannmur for nødvendig administrasjonsverktøy iht. avtale med leverandøren <p>Virksomheten må sikre at tilgangen fjernes når den ikke lenger er nødvendig.</p>

Eksempel på hjemmekontor og mobile løsninger

Figuren under gir en oversikt over mulig konfigurasjon for ekstern tilgang. Her gis mobile brukere og hjemmekontor tilgang via et VPN-mottak i egen DMZ-soner. I tillegg kontrolleres konfigurasjon av enhetene, bla. sikkerhetspatcher, oppdaterte virusdefinisjoner osv. før enhetene får tilgang til nettverket.

