

| | |
|--|--|
|  Norm for informasjonssikkerhet www.normen.no | Utgitt med støtte av:  |
| <h1>Hjemmekontor</h1> | Støttedokument Faktaark nr 29 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 checked="" type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud |
| Ansvar | IKT-ansvarlig har ansvaret for å ivareta kravene til oppsett av hjemmekontor. | | |
| Gjennomføring | Kontinuerlig ved opprettelse, bruk og avvikling av hjemmekontor | | |
| Formål | Hindre uautorisert adgang, bruk og tilgang til utstyr og data benyttet for behandling av helse- og personopplysninger på et hjemmekontor. | | |
| Omfang | Sikring (fysisk og elektronisk) av data og utstyr lokalisert på et hjemmekontor, inkludert kommunikasjonslinjer ut av hjemmekontoret. | | |
| Hjemmel | Personopplysningsforskriften §§ 2-10, 2-11, 2-12 og 2-13 | | |
| Referanser | <ul style="list-style-type: none"> • Norm for informasjonssikkerhet, kapittel 5.4.4 og 5.5.1 • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008 | | |

Med **utstyr** menes i det følgende kommunikasjonsutstyr og bærbar PC og/eller stasjonær PC. Utstyret skal kun benyttes for å gi tilgang til å behandle helse- og personopplysninger.

| Nr. | Aktivitet/Beskrivelse |
|-----|---|
| 1. | <p>Forutsetninger for etablering av hjemmekontor</p> <p>Virksomheten anbefales å etablere en enhetlig hjemmekontorløsning basert på følgende forutsetninger:</p> <p><u>Lagring av data</u> PC på hjemmekontor skal ikke ha helse- og personopplysninger lagret lokalt. Disse opplysningene skal kun nåes ved oppkobling til sentralt lagrede data (i virksomheten og/eller hos databehandler).</p> <p><u>Konfigurasjon</u> Virksomheten skal ha oversikt over og ha kontroll med konfigurasjon av alt utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger. Konfigurasjonen skal sikre at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt.</p> <p><u>Bruk av og eierskap til utstyr</u> Virksomheten skal eie PC på hjemmekontor, og: <ul style="list-style-type: none"> – PC skal ikke benyttes til annen bruk enn det virksomheten har bestemt – Virksomheten er konfigurasjonsansvarlig for PC slik at utstyret settes opp på sikker måte – Det bør inngås avtale om hjemmekontor mellom virksomhet og den enkelte bruker </p> <p><u>Kommunikasjon</u> <ul style="list-style-type: none"> – Terminalserverløsning er anbefalt og skal fortrinnsvis benyttes (bl.a. fordi kravet til at data ikke skal lagres lokalt på PC kan ivaretas, løsningen kan forhindre klipp og lim, løsningen kan forhindre utskrift lokalt, osv) – Kommunikasjonen skal være kryptert. VPN er en lukket og reservert kommunikasjonskanal som kan krypteres. Med kryptering er dette en anbefalt løsning som fortrinnsvis skal benyttes – Ved bruk av VPN må eget utstyr og kommunikasjonspartens utstyr konfigureres slik at det sikres at begge parter er de de gir seg ut for å være – VPN-løsning uten bruk av terminalserver kan benyttes, men er ikke anbefalt. Hvis </p> |

| Nr. | Aktivitet/Beskrivelse |
|-----|---|
| | dette likevel benyttes skal utstyret konfigureres og nødvendige mekanismer iverksettes for å sikre at lokal lagring av helse- og personopplysninger ikke er mulig |
| 2. | <p>Vurderinger før etablering av hjemmekontor</p> <p>a) Gjennomføre risikovurdering for å avgjøre hvilke tekniske sikkerhetstiltak som skal etableres for å redusere risikoen for at eksterne får tilgang til helse- og personopplysninger</p> <p>b) Basert på punkt a) bør følgende tiltak vurderes:</p> <ul style="list-style-type: none"> – Etablere antivirus- og brannmursikring på PC – Etablere teknisk løsning hvor brukeren autentiseres med sikkerhetsnivå 4 – Teknisk løsning konfigureres slik at hjemme-PC kun kan kommunisere med predefinert utstyr – Tidsstyring for låsing av PC tilpasset brukerens arbeidsøkt – All kommunikasjon, enten dette skjer vha. trådløst nett eller vha. datalinjer, skal sikres med kryptering iht. gjeldende krav – Helse- og personopplysninger skal ikke lagres lokalt på hjemme-PC. Det skal likefullt vurderes sikring av: <ul style="list-style-type: none"> - vinduer og dører (åpning og innsyn) - utstyret og hvordan det oppbevares - det aktuelle rommet hvor utstyret er plassert |
| 3. | <p>Krav til bruk av hjemmekontor</p> <p>På bakgrunn av tiltakene identifisert i risikovurderingen må det etableres administrative prosedyrer, gjerne i form av en brukeravtale, for bruk av hjemmekontor. Følgende bør vurderes:</p> <ul style="list-style-type: none"> – Virksomhetens prosedyrer for bruk av Internett og e-post skal følges i forbindelse med hjemmekontor – Helse- og personopplysninger skal ikke lagres lokalt på PC – Ingen andre enn den som er autorisert til å bruke virksomhetens PC skal benytte denne – Utskrifter som inneholder helse- og personopplysninger skal oppbevares sikkert og/eller umiddelbart makuleres etter bruk. Under bruk skal innsyn fra uautoriserte ikke forekomme – PC skal låses av bruker ved fravær – Privat bruk av hjemmekontor-PC følger de samme reglene som for privat bruk av PC på arbeidsplassen – Ved arbeid med helse- og personopplysninger skal det iverksettes tiltak for å hindre innsyn fra eksterne (f.eks. familiemedlemmer og andre) – Programvaren skal til enhver tid være oppdatert iht. gjeldende standarder og krav i virksomheten |
| 4. | <p>Avvikling av hjemmekontor</p> <p>Når utstyr som brukes i en hjemmekontorløsning skal avvikles (f.eks. ved avslutning av arbeidsforhold, skifte av utstyr, mv.) gjelder følgende:</p> <ul style="list-style-type: none"> – Alt utstyr skal leveres tilbake til virksomheten – Dersom utstyret skulle bli overtatt til privat bruk skal alle muligheter for pålogging til virksomhetens systemer fjernes – Alle helse- og personopplysninger som måtte finnes på hjemmekontor skal leveres tilbake til arbeidsgiver, slettes eller makuleres |