

 Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av: 
<h2>Sikring av bærbart utstyr</h2>	Støttedokument Faktaark nr 18 Versjon: 2.1 Dato: 15.12.2011

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 type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	IKT-ansvarlig er ansvarlig for å legge til rette løsninger for å sikre bærbart utstyr.		
Gjennomføring	Sikring av bærbart utstyr skal utføres før det settes i drift eller tas i bruk. Med bærbart utstyr menes bl.a. bærbar PC, mobiltelefon og PDA.		
Formål	Hindre uautorisert tilgang til helse- og personopplysninger lagret på bærbart utstyr og uautorisert tilgang via bærbart utstyr til virksomhetens interne nettverk. Sikre tilgjengelighet til korrekt og oppdatert informasjon for autorisert personell.		
Omfang	All bruk av bærbart utstyr hvor det oppbevares helse- og personopplysninger og bærbart utstyr som kobles til virksomhetens interne nettverk.		
Hjemmel	Personopplysningsforskriften §§ 2-11, 2-12, 2-13 og 2-14.		
Referanser	<ul style="list-style-type: none"> • Norm for informasjonssikkerhet pkt 5.4.4 • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008 		

Nr.	Aktivitet/Beskrivelse
1	Dokumentere hvilket bærbart utstyr virksomheten benytter Utarbeide en oversikt som viser hvilket bærbart utstyr som finnes (er planlagt anskaffet) og hva det (skal) benyttes til og hvor fra. Oversikten skal også vise hvem som er bruker eller ansvarlig for utstyret.
2	Risikovurdere løsningen slik at den er iht akseptkriterier Det er viktig å ta hensyn til hvor bærbart utstyr skal benyttes i vurderingen a) I lokalene til databehandlingsansvarlig b) Fra andre lokasjoner (som krever flere tiltak enn ved kun bruk i lokalene til databehandlingsansvarlig) Eksempler på områder som risikovurderes: a) Lagring av helse- og personopplysninger på bærbart utstyr b) Oppkobling av utstyr mot andre nettverk utenfor egen virksomhet (for eksempel Internett direkte fra det bærbare utstyret) c) Oppkobling av utstyr mot virksomhetens interne nettverk og hvilke type systemer og mapper brukeren skal ha tilgang til. Risiko er ulik om bruker skal ha tilgang til helse- og personopplysninger eller kun til annen informasjon d) Oppkobling fra fast plassering (hjemmekontor) eller mobil plassering (for eksempel via mobiltelefon) e) Synkronisering (kopiering og utveksling) av data (inkl Outlook) på bærbart utstyr ift data på interne og eksterne nettverk. f) Sikkerhetskopiering av data på bærbart utstyr g) Tilgang til og bruk av eksterne lagringsenheter; minnepinne, CD, osv h) Tilgang til kommunikasjonsporter (tilkoblingsmuligheter som for eksempel trådløst nettverk) i) Utskrift fra bærbart utstyr j) Ondsinnet programvare

Nr.	Aktivitet/Beskrivelse
	k) Tyveri av bærbart utstyr l) Muligheten for overvåking av bærbart utstyr (spionprogramvare) m) Installasjon av privat programvare n) Privat bruk av bærbart utstyr Se Faktaark 7 - Risikovurderinger.
3	Utarbeide prosedyrer for bruk av bærbart utstyr a) Tildeling og tilbaketrekking av utstyr som den enkelte kan benytte selvstendig (utstyret skal være virksomhetens eiendom) b) Avtale med den ansatte om bruk av bærbart utstyr. Avtalen skal regulere ansvar og plikter for både brukeren av utstyret og databehandlingsansvarlig (virksomheten). Avtalen skal fastsette hva bærbart utstyr skal benyttes til c) Kontroll med bærbart utstyr (bl.a. hendelsesregistrering og avviksbehandling) d) Utskifting og avhending av bærbart utstyr (rensing og sletting av lagringsenhet og lisenser for programvare)

Eksempel

Eksempler på tiltak (basert på risikovurdering og kontroll mot akseptkriterier)

- a) Kryptering av lagringsenheter om det lagres helse- og personopplysninger (kryptering anbefales som standard ettersom det alltid vil være data på lagringsenheten)
- b) Kryptering av kommunikasjon mellom bærbart utstyr og internt nettverk om det overføres helse- og personopplysninger
- c) Kryptering (eller annen sikring) av ekstern lagringsenhet (CD, minnepinne, osv)
- d) Antivirusløsning på bærbart utstyr
- e) Autentiseringsløsning (det stilles krav til sikkerhetsnivå 4 for autentisering) ved lokale lagring av helse- og personopplysninger og ved tilgang til nettverk i virksomheten hvor det behandles helse- og personopplysninger)
- f) Brannmur på bærbart utstyr slik at det kontrolleres at det kun kan kommuniseres med predefinert utstyr
- g) Kontinuerlig registrere tilkoblingspunkt (i brannmur) på virksomhetens nettverk
- h) Tyverimerking
- i) Sperring for utskrift
- j) Sperring av eksterne lagringsenheter (CD, minnepinne, osv)
- k) Sperring av kommunikasjonsporter (for eksempel trådløst nettverk)