NORMEN

Sikring av bærbart utstyr (faktaark 18)

Versjon 3.1

26.09.2018

Utarbeidet med støtte fra direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler sikring av bærbart utstyr. Formålet er å 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. 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 nettbrett. All bruk av bærbart utstyr hvor det oppbevares helse- og personopplysninger og bærbart utstyr som kobles til virksomhetens interne nettverk omfattes. IKT-ansvarlig er ansvarlig for å legge til rette løsninger for å sikre bærbart utstyr.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er virksomheter som behandler helse- og personopplysninger og vil være særlig være relevant for: • IKT-ansvarlig • Sikkerhetsleder/sikkerhetskoordinator
Krav i Normen	Faktaarket gjelder for følgende kapitler i Normen • Kapittel 5.3.4 Mobilt utstyr og hjemmekontor
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser er spesielt relevante for faktaarket: • Personvernforordningen artikkel 32 Sikkerhet ved behandlingen • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008

Sikring av bærbart utstyr

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 dataansvarlig b) Fra andre lokasjoner (som krever flere tiltak enn ved kun bruk i lokalene til dataansvarlig) 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) Autentiseringsløsning i forbindelse med krav om autentisering på sikkerhetsnivå 4 e) Oppkobling fra fast plassering (hjemmekontor) eller mobil plassering (for eksempel via mobiltelefon eller nettbrett) f) Synkronisering (kopiering og utveksling) av data (inkl Outlook) på bærbart utstyr ift data på interne og eksterne nettverk. g) Sikkerhetskopiering av data på bærbart utstyr h) Tilgang til og bruk av eksterne lagringsenheter; minnepinne, CD, osv i) Tilgang til kommunikasjonsporter (tilkoblingsmuligheter som for eksempel trådløst nettverk) j) Utskrift fra bærbart utstyr k) Ondsinnet programvare l) Tyveri av bærbart utstyr m) Muligheten for overvåking av bærbart utstyr (spionprogramvare) n) Installasjon av privat programvare o) At PIN-kode til mobiltelefoner / nettbrett og sikkerhetskode for elektronisk ID kommer uvedkommende i hende p) Privat bruk av bærbart utstyr

Nr.	Aktivitet/Beskrivelse
	Se Veileder om risikostyring i informasjonssikkerhet og personvern
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 dataansvarlig (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)