Fysisk sikring av områder og utstyr (faktaark 17)

Versjon 3.1
20.09.2018

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 fysisk sikring av områder og utstyr. Formålet med faktaarket er hindre uautorisert adgang til utstyr benyttet for behandling av helse- og personopplysninger. Faktaarket omhandler kun fysisk sikring av utstyr lokalisert i en virksomhet, og avgrenser seg fra Elektronisk sikring, sikring av mobilt utstyr og hjemmekontor. For veileding om sikring av bærbart utstyr og hjemmekontor, se Sikring av bærbart utstyr (faktaark 18) og Hjemmekontor og annet fjernarbeid (faktaark 29) Faktaarket har en praktisk tilnærming og inneholder eksempler på tiltak som kan gjennomføres for å hindre uautorisert adgang til utstyr.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er • IKT-ansvarlig • Prosjektleder • Sikkerhetsleder / sikkerhetskoordinator • Virksomhetens leder/ledelse • Medarbeider/ansatt
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen • Kapittel 5.3 Fysisk sikkerhet og håndtering av utstyr
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Personvernforordningen artikkel 32 Sikkerhet ved behandlingen • Veileder om risikostyring i informasjonssikkerhet og personvern

Fysisk sikring av områder og utstyr

Beskrivelsene nedenfor er eksempler på tiltak som kan gjennomføres for å hindre uautorisert adgang til utstyr. For å sikre at tiltakene er tilpasset den enkelte virksomhets behov og trusselbilde, bør alle de ulike områdene som er beskrevet i dette faktaarket vurderes og tiltak identifiseres gjennom en risikovurdering..

I likhet med at en PC med helse- og personopplysninger sikres med f.eks. autentiseringsløsning, brannmur, tilgang etter behov, er det av like stor betydning at fysisk sikring ivaretas. Brudd på den fysiske sikkerheten til områder og utstyr vil øke faren for at uvedkommende får tilgang til elektronisk lagrede helse- og personopplysninger. Det er et samspill mellom tiltak for den fysiske sikringen og tiltak som er iverksatt for elektronisk sikring. Tiltakene er gjensidig avhengig av hverandre for at en skal kunne oppnå tilfredsstillende sikring av helse- og personopplysninger.

Nr.	Aktivitet/Beskrivelse
1.	**Risikovurdering** a) Risikovurderingen må ta utgangspunkt i de konkrete fysiske arealene som skal sikres mot uautorisert adgang. b) Risikovurderingen bør belyse behov for å definere arealene i ulike soner, ut fra virksomhetens størrelse. En sonemodell for fysisk adgang til helse- og personopplysninger for interne og eksterne kan defineres slik: – Åpen sone: arealer hvor publikum har fri adgang, korridorer, venterom, fellesarealer, områder med alminnelig ferdsel – Indre sone: åpne arbeidsplasser (områder med begrenset ferdsel), arealer beregnet kun for medarbeidere i virksomheten, evt. publikum i følge med medarbeidere - resepsjonsarbeidsplassen, kontorer, vaktrom, behandlingsrom – Sikker sone: areal hvor kun spesielt godkjente medarbeidere har adgang, og hvor publikum ikke skal ha adgang (områder med sterk adgangsbegrensning), datarom, rom med nettverk, servere og kommunikasjonsutstyr c) For mindre virksomheter der soneinndeling ikke er mulig må risikovurderingen belyse risiko for adgang til helse- og personopplysninger innen det aktuelle arealet
2.	**Nøkler/adgangskort** a) Identifiser områder og rom hvor utstyr med helse- og personopplysninger er plassert b) Lag en oversikt over hvem som har tjenstlige behov for adgang til aktuelle områder og rom. Adgang til dedikerte rom med driftsutstyr (servere og utstyr) skal kun gis til personell med absolutt behov for adgang. Generelt skal adgang i størst mulig grad begrenses. c) Lag en kvitteringsliste for tildeling av nøkler/adgangskort. Alle som får utlevert og leverer inn nøkler/adgangskort skal kvittere med navn, sted og dato for utleveringen/innleveringen. Listen bør revideres f.eks. 1 gang i året, evt. hyppigere når adgangene ofte endres. d) I større virksomheter anbefales det en egen resepsjonstjeneste. Uautorisert personell og besøkende skal ledsages

Nr.	Aktivitet/Beskrivelse
3.	**Besøk av eksterne til eller via områder og rom hvor utstyr med helse- og personopplysninger er plassert** a) Etabler resepsjonstjeneste og/eller ledsagelse av uautorisert eksterne personer (besøkende) b) Skrivere og arbeidsstasjoner som er plassert i tilknytning til fellesområder (resepsjoner, venterom, vaktrom, korridorer mv.) fysisk sikres slik at uvedkommende ikke får adgang til helse- og personopplysninger
4.	**Adgang til driftsutstyr (data- og kommunikasjonsrom)** Sikkerhetstiltak skal hindre at annet enn autorisert personell får adgang til slikt utstyr. a) Mindre virksomhet: Servere og annet nettverksutstyr skal oppbevares i låst skap eller rom med sylinderlås. Dersom det benyttes et skap, skal dette skrus fast til veggen eller gulvet. Skapet skal ikke plasseres i resepsjonen/publikumsområde. Resepsjon/publikumsområde skal heller ikke benyttes som rom for oppbevaring av utstyret. b) Større virksomhet: Alle servere og annet nettverksutstyr skal oppbevares i et eget datarom, fortrinnsvis med kodelås. Det skal også være installert et system for varsling av innbrudd, som skal være tilkoplet kodelåsen. Systemet skal varsle en ansvarlig for datarommet, alternativt vaktsentral. Det kan vurderes å etablere en egen vaktordning. c) Adgang til data- og serverrom bør registreres. F.eks. kan det føres en oversikt, hvor alle besøk registreres med navn, leverandør, oppdragsbeskrivelse, dato, tid for inn og ut, og servicemedarbeiderens signatur.
5.	**Medisinsk teknisk utstyr** a) Lagringsenhet for medisinsk teknisk utstyr som behandler helse- og personopplysninger skal plasseres i avlåst rom eller i bemannet område. b) Medisinsk teknisk utstyr som behandler helse- og personopplysninger skal inkluderes i virksomhetens arbeid med informasjonssikkerhet, herunder risikovurderinger, adgangsregulering, fysisk sikring og prosedyrer for bruk, på linje med andre informasjonssystemer.