Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Sikring av trådløs teknologi

Støttedokument
Faktaark nr 26
Versjon: 3.1
Dato: 26.09.2018

Formål	Gi prinsipper for sikring av trådløse nett (WiFi)trådløs teknologi ifm. helse- og personopplysinger.		
Ansvar	IKT-ansvarlig skal etablere løsninger for trådløs teknologi som ivaretar krav til sikkerhet.		
Gjennomføring	Ved bruk av trådløs teknologi i LAN ifm. helse- og personopplysninger.		
Omfang	Alle virksomheter som bruker trådløs teknologi ifm. helse- og personopplysinger.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Leverandør ☒ IKT-ansvarlig ☐ Forsker ☐ Prosjektleder	☒ Sikkerhetsleder / sikkerhetskoordinator ☐ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☐ Medarbeider/ansatt ☒ Databehandler ☐ Personvernombud
Hjemmel	Personvernforordningen artikkel 32		
Referanser	• Norm for informasjonssikkerhet, kapittel 5.3.1 og 5.4.1 • Veiledning fra NorSIS Trådløse nettverk og sikkerhet: https://nettvett.no/tradlost-nettverk/		

Merknad 27.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Faktaarket inneholder ikke detaljerte beskrivelser av oppsett av forskjellige typer program- og maskinvare. Se brukerveiledningen for det enkelte produkt. Eksempler på utstyr med trådløs teknologi: PC, server, nettbrett, smarttelefoner, skriver og elektromedisinsk utstyr.

Virksomheten skal gjennomføre risikovurdering før etablering av trådløs teknologi. Det finnes også annen sikkerhetsteknologi for sikring av trådløse nett enn det som er beskrevet i dette faktaarket.

Nr.	Aktivitet/Beskrivelse

Nr.	Aktivitet/Beskrivelse
1.	**Generelt om WiFi** a) Når trådløs teknologi tas i bruk vil virksomheten utsettes for en ekstra sikkerhetsrisiko. Ut fra virksomhetens akseptkriterier skal det gjennomføres en risikovurdering for å fastsette at løsningen er innefor akseptabelt risikonivå b) Virksomheten bør utarbeide en sikkerhetsinstruks for bruk av trådløs teknologi. All bruk og konfigurasjon av trådløst utstyr forbys om det ikke er anskaffet og underlagt virksomhetens konfigurasjonskontroll. c) Trådløst LAN benytter radiosignaler. Disse brer seg uhindret utenfor virksomhetens areal og kan nås av andre utenfor lokalene. Det er svært lett å avlytte radiosignaler i et usikret trådløst nett og dermed gjøre datainnbrudd ved at f.eks. helse- og personopplysninger tappes d) I trådløst LAN kan det være et tilgjengelighetsproblem med bakgrunn i følgende: – Mikrobølgeovner og hustelefoner bruker samme frekvenser som trådløse LAN, og kan derfor forstyrre eller stoppe radiosignalene – Offentlig kjente frekvensbånd som er ulisensiert, som trådløst LAN, kan deles mellom flere. En tredjeperson kan enkelt sende ut radiosignaler som hindrer virksomhetens datatrafikk (jamming) – Om det brukes elektromedisinsk utstyr eller bærbart datautstyr som skal flyttes mellom flere rom (roaming) er det viktig at det trådløse nettet er testet for dette. Bruk av utstyr fra flere leverandører kan medføre at forbindelsen mistes når en beveger seg mellom flere basestasjoner (aksesspunkt) e) Virksomheten bør vurdere formålet med det trådløse nettverket og vurdere risiko ut fra dette. Hvis nettet skal brukes som pasient-/besøksnett er det viktig å sikre at nettet ikke er sammenknyttet med virksomhetens interne nett. Hvis nettet skal benyttes for å gi tilgang til interne ressurser må det iverksettes tiltak for å sikre tilgangen

Nr.	Aktivitet/Beskrivelse
2.	**Trådløst LAN i egen virksomhet** a) Med trådløst LAN i egen virksomhet menes nettverk virksomheten selv eier til bruk for virksomhetens eget personell. Det kan også være andre trådløse nett som f.eks. pasient- og besøksnett b) For tilgang til nett som behandler helse- og personopplysninger skal følgende – Sikkerhetsmekanismer i tillegg til bruker-ID og passord hensyntas: – Trådløst LAN skal krypteres iht. gjeldende krav beskrevet i " Kravspesifikasjon for PKI i offentlig sektor" (se www.difi.no). Virksomheten må være oppmerksom på at det kan være betydelige svakheter i enkelte krypteringsmetoder som levers standard med utstyret. WEP og WPA/WPA2 er et eksempel på en krypteringsmetode som ikke skal benyttes alene. – SSID, som er det enkelte trådløse nettverks signatur, blir kringkastet av en basestasjon og kan fanges opp annet trådløst datautstyr. Virksomheten må vurdere om det er nødvendig å kringkaste SSID ut fra et administrativt behov. Virksomheten bør vurdere om SSID navnene skal være intetsigende i forhold til å beskrive hvilket LAN det er snakk om – Det anbefales å slå på MAC-adressefiltrering slik at kun autoriserte maskiner/utstyr kan koble seg opp. MAC-adressen er nettkortets unike identitet i det trådløse nettet. Idet MAC-adresser kan etterlignes med egnet utstyr er det sikrere å benytte en access-controlboks og registrere basestasjonens MAC-adresse i denne, slik at kun kjente baser vil kunne benyttes i det trådløse nettet – Virksomheten skal ha konfigurasjonskontroll på utstyr som kobles opp ved hjelp av trådløs teknologi (for eksempel for å hindre ondsinnet programvare) – Det bør benyttes ekstern autentiseringsløsning for tilgang til nettet. Eksempler på dette er 802.1X og bruk av radiusserver. – Det anbefales bruk av VPN for trådløse nett der helse- og personopplysninger skal behandles. c) Det anbefales følgende tiltak på TCP/IP-protokollen: – Justere subnettmasken til det antallet IP-adresser som er nødvendig det aktuelle subnettet – For virksomheter som bruker "Private IP-adresser" anbefales det å endre IP-adressen på ruteren fra den mest vanlige 192.168.0.1 til for eksempel 10.11.12.13 selv om det bryter med konvensjoner om at den første adressen i et subnet bør være "default gateway"
3.	**Trådløst LAN i andre virksomheter (åpne nett)** a) Dette er nett som ligger utenfor virksomhetens kontroll, og som virksomhetens personell kan koble sitt bærbare datautstyr opp mot b) Eksempler på trådløse LAN i andre virksomheter er: – Trådløst LAN i samarbeidende virksomheter – Trådløst LAN i nabovirksomheter – Internettkafeer – Hoteller – Flyplasser – Andre offentlige rom c) Virksomheten skal ha konfigurasjonskontroll på utstyr som kobles opp ved hjelp av trådløs LAN i andre virksomheter (oppdatert antivirusprogramvare og brannmur) d) Om det lagres helse- og personopplysinger på bærbar PC, nettbrett, PDA eller mobiltelefon skal denne krypteres iht. gjeldende krav e) Det anbefales at man alltid benytter VPN ved bruk åpne nett.