Normens fjernaksessveileder

13.02.2020

Vedlikehold, fjernaksess eller fysisk service i Normen 6.0

- Leverandørens utstyr:
  - Fjernaksess
  - On-site
  - Sikret mot ondsinnet programvare e.l.
  - Sikret mot adgang fra uvedkommende
- All tilgang og fysisk adgang skal være autorisert av virksomheten. Tilgangen skal logges og adgangen skal kontrolleres.
- Tilgjengelighet til helse- og personopplysninger så vidt mulig skal opprettholdes
- Se ellers Normens fjernaksessveileder

Innhold

- Bakgrunn for veilederen
- Tema for veilederen
- Krav til sikkerhet ved fjernaksess
- Eksempel på tekniske løsninger
- Avtaler og prosedyrer
- Sjekkliste for Normens krav

- **Veilederen ble sist oppdatert ca 2014**
  - **Dermed ikke oppdatert etter GDPR eller Normen 6.0**

NORMEN

Bakgrunn for veilederen

- Leverandører til helsesektoren forventer fjernaksess for vedlikehold og oppdateringer av leveranser
- Ingen gjeldende standard for sikker fjernaksess
- Usikkerhet rundt krav til sikkerhet i eksisterende løsninger for fjernaksess

Tema for veilederen

- Stiller krav til leverandøren
- Stiller krav til virksomheten
- Beskriver mulige tekniske løsninger
- Beskriver avtaler og prosedyrer

Krav til sikkerhet

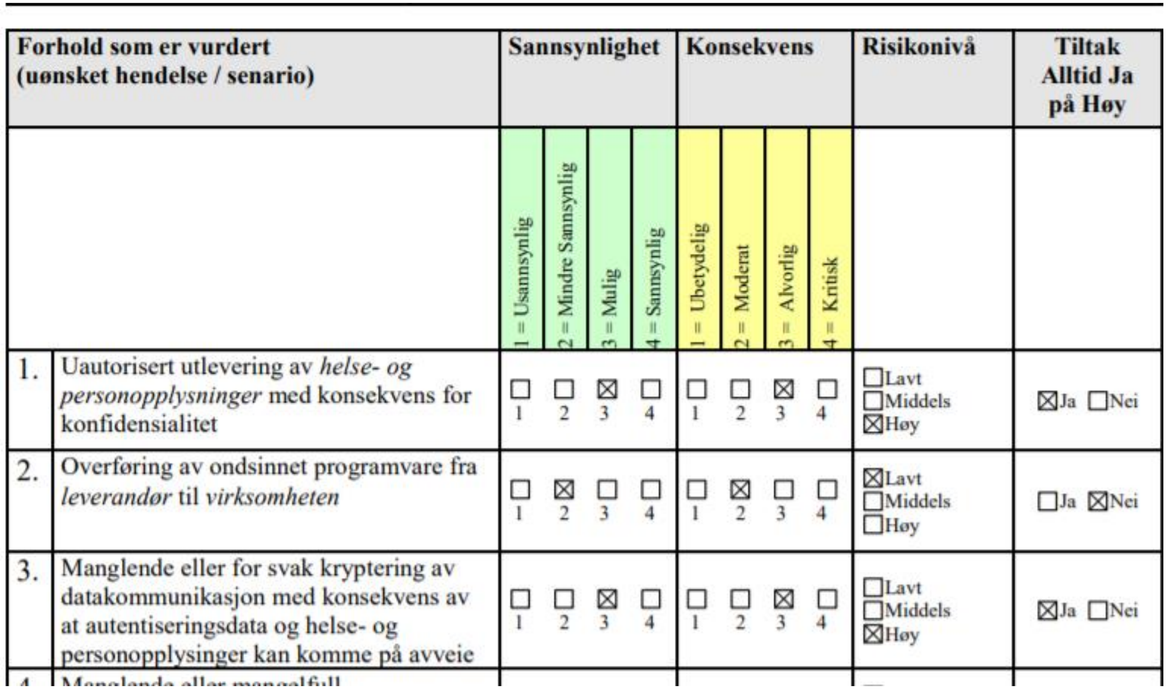
- Avtale
- Risikovurdering
- Opplæring
- Oppkobling og begrensning av trafikk
- Kryptering av ekstern kommunikasjon
- Forhindre ondsinnet kode
- Adgang til og sikring av utstyr
- Autorisering
- Autentisering og tilgang

2.11.1 Konfigurasjonskontroll (Normen kap. 5.5.1)
"Konfigurasjonskontroll skal reguleres gjennom avtale ved bruk av fjernaksess for vedlikehold og oppdateringer"

Innebærer for		Referanse til faktaark og veiledere
Virksomhet	Leverandør	
Bruk av *fjernadministrasjon* skal avtales med *leverandøren*. Avtalen skal beskrive hvordan konfigurasjonskontrollen blir ivaretatt. Verktøyet som benyttes skal ha aktiv konfigurasjonsstyring som ikke kan overstyres av servicemedarbeideren. Ved bruk av verktøy for *fjernadministrasjon* skal *virksomheten* konfigurere løsningen slik at *leverandøren* ikke kan benytte andre funksjoner enn de som er avtalt på forhånd. Oppkobling og bruk av verktøy for *fjernadministrasjon* bør som hovedprinsipp aksepteres fra *virksomheten* som en aktiv handling i det enkelte tilfelle.	*Leverandøren* skal forholde seg til den *konfigurasjonen* som er avtalt og prosedyre for endringshåndtering. *Leverandøren* skal kun benytte løsningen for *fjernaksess* slik det er avtalt på forhånd.	

Krav til sikkerhet

- Behandling av personopplysninger fra virksomheten
- Fjernadministrasjon
- Logging
- Kontroll av logger / Analyseverktøy
- Tilgang til logger hos leverandør



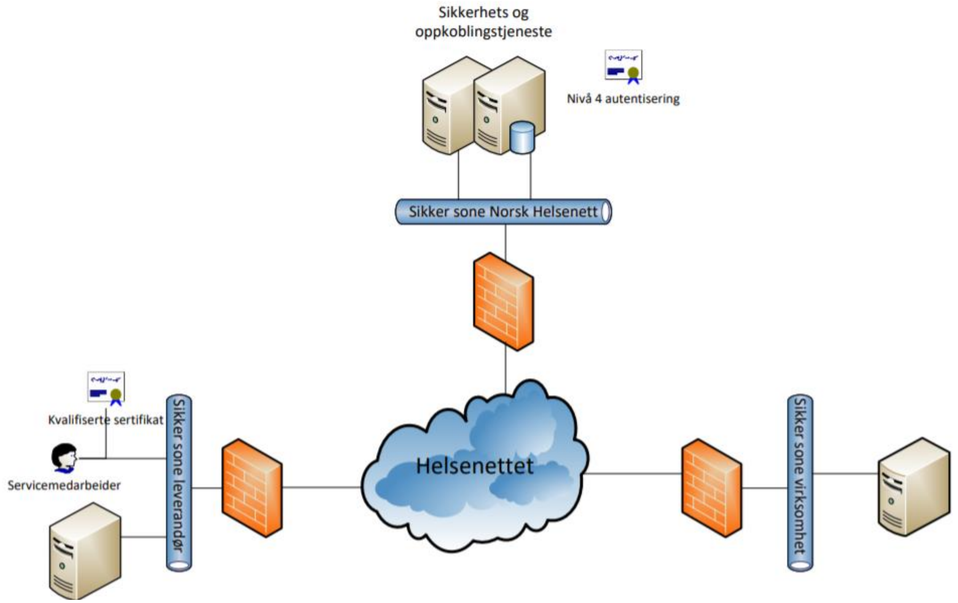
Forhold som er vurdert (uønsket hendelse / senario)		Sannsynlighet				Konsekvens				Risikonivå	Tiltak Alltid Ja på Høy
		1 = Usannsynlig	2 = Mindre Sannsynlig	3 = Mulig	4 = Sannsynlig	1 = Ubetydelig	2 = Moderat	3 = Alvorlig	4 = Kritisk		
1.	Uautorisert utlevering av *helse- og personopplysninger* med konsekvens for konfidensialitet	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei
2.	Overføring av ondsinnet programvare fra *leverandør* til *virksomheten*	☐ 1	☒ 2	☐ 3	☐ 4	☐ 1	☒ 2	☐ 3	☐ 4	☒Lavt ☐Middels ☐Høy	☐Ja ☒Nei
3.	Manglende eller for svak kryptering av datakommunikasjon med konsekvens av at autentiseringsdata og helse- og personopplysinger kan komme på avveie	☐ 1	☐ 2	☒ 3	☐ 4	☐ 1	☐ 2	☒ 3	☐ 4	☐Lavt ☐Middels ☒Høy	☒Ja ☐Nei

Leverandøren skal følge Normen:

- Avtale
- Styringssystem for informasjonssikkerhet
- Risikovurdering
  - Skal gjennomføres før leverandøren får tilgang til virksomhetens nett
- Avvik

Tekniske løsninger

- 4 eksempler
  - Løsning levert av Norsk Helsenett
  - Oppkobling over Internett der virksomheten har kontroll basert på VPN.
  - Oppkobling over Internett basert på å håndtere sikkerhet i en kontrollsone
  - Site-to-Site VPN løsning via helsenettet / internett
- Ansvar pr eksempel



Kap nr	Kapittel tittel	Ivaretatt av:		
		Virksomhet	Leverandør	Ikke relevant
2.1.1	Skriftlig avtale med leverandør (Normen kap. 5.8)	☒	☒	☐
2.1.2	Taushetserklæring (Normen kap. 5.8.3)	☒	☐	☐
2.1.3	Sikkerhetsrevisjon og avviksbehandling (Normen kap. 5.8.3, 6.1 og 6.3)	☒	☐	☐
2.1.4	Bevisstgjøring av taushetsplikten (Normen kap. 5.1)	☒	☐	☐

Avtaler og prosedyrer

- Sjekklister for begge områdene
- Avtaletekst

Anbefalte elementer i avtalen:

Nr	Element	Innarbeidet
1.	Hvem avtalepartene er	☐ Ja ☐ Nei
2.	Formålet med avtalen eller særavtalen	☐ Ja ☐ Nei
3.	Ansvarlige personer/roller	☐ Ja ☐ Nei
4.	*Virksomheten* skal ha tilgang til *leverandørens* dokumentasjon av sikkerhetsmål og strategi	☐ Ja ☐ Nei
5.	*Virksomheten* skal ha innsynsrett i *leverandørens* løsning for ivaretakelse av Normen	☐ Ja ☐ Nei

Nr	Element	Faktaark	Innarbeidet	Ansvar
1.	Signering av taushetserklæring og bekreftelse på at sikkerhetsinstruks er lest og akseptert		☐ Ja ☐ Nei	
2.	Opplæring av *servicemedarbeider*		☐ Ja ☐ Nei	
3.	Administrasjon av *autorisasjon* til utstyr som benyttes til *fjernaksess*	14	☐ Ja ☐ Nei	
4.	Bruk av løsning for sterk *autentisering*	24	☐ Ja ☐ Nei	
5.	Avviksbehandling ifm *fjernaksess*	8	☐ Ja ☐ Nei	

Sjekkliste for oppkobling

5.1 Sjekkliste for etablering av oppkobling

Kap nr	Kapittel tittel	Utført	Kommentar
2.1.1	Skriftlig avtale med leverandør (Normen kap. 5.8)	☐ Ja ☐ Nei	
2.1.2	Taushetserklæring (Normen kap. 5.8.3)	☐ Ja ☐ Nei	
2.1.3	Sikkerhetsrevisjon og avviksbehandling (Normen kap. 5.8.3, 6.1 og 6.3)	☐ Ja ☐ Nei	
2.1.4	Bevisstgjøring av taushetsplikten (Normen kap. 5.1)	☐ Ja ☐ Nei	
2.2.1	Risikovurdering før tilgang gis (Normen kap. 4.6)	☐ Ja ☐ Nei	
2.2.2	Risikovurdering i driften (Normen kap. 6.2)	☐ Ja ☐ Nei	
2.3.1	Opplæringstiltak (Normen kap. 5.6)	☐ Ja ☐ Nei	
2.4.1	Nettjenesteleverandør (Normen kap. 5.7)	☐ Ja ☐ Nei	