Krav ved innføring av ny leverandørtilgang/VPN.

Bakgrunn:

I de tilfeller hvor den etablerte løsningen for fjerntilgang for leverandører ikke tilfredsstiller de behovene som finnes, så er det ofte et ønske å etablere en produsentspesifikk løsning. Dette er ofte inkludert som en del av serviceavtalen som er inngått og man har derfor ikke noe særlig mulighet til å fange dette opp som en del av en anskaffelse.

Dette dokumentet søker å forenkle og standardisere innføringen av slike løsninger, noe som historisk sett har vært mye improvisert.

Kravene er beskrevet i Styringssystemene i DS7534 og RL6905 Leverandørhåndtering 4.1,4:
Andre tilganger som ikke kan løses gjennom punkt a) (f.eks. direktetilgang mellom leverandør og medisinskteknisk utstyr) må risikovurderes og godkjennes av berørte helseforetak og Helse Nord IKT. Dataansvarlige som har behov for en slik løsning er ansvarlig for at risikovurdering gjennomføres og for å ha oversikt over alle slike løsninger.

Ordliste:

Kunde: Helseforetak som ønsker fjerntilgang installert og som eier utstyret som skal vedlikeholdes.

Leverandør: Servicepartner/leverandør/produsent som skal benytte seg av tilgangen for å utføre vedlikehold. I tilfeller hvor en underleverandør benyttes så vil krav gjelde både kontraktspart og underleverandør, ansvar vil tilfalle kontraktspart.

HN IKT: Helse Nord IKT. Regionalt IKT foretak. Drifts og infrastrukturleverandør i Helse Nord.

H	**H**ovedansvarlig
U	**U**tfører
K	**K**onsulteres
I	**I**nformeres

Formalkrav:

Krav/Aktør	Kunde	Leverandør	HN IKT
1. Leverandør skal dokumentere sine internkontrollrutiner. Dokumentasjonen kan være i form av en ekstern revisjonsrapport eller sertifisering.	I	H/U	K
2. Leverandør skal fremlegge en rapport fra siste inntrengingstest samt hvor ofte disse utføres.	I	H/U	K
3. Leverandør skal framlegge en liste over de som skal bruke denne tilgangen. Det opprettes kontoer til disse brukerene	K	H	U/K

	opprettes etter gjeldende rutiner for leverandørkonto.			
4.	Gyldig databehandleravtale skal foreligge.	H/U	U	I
5.	For tilgang fra lokasjoner utenfor EU/EØS så skal gjeldende rettslige krav følges.	H	U	K
6.	Det skal foreligge en risikovurdering med fokus på nettverksåpninger fra terminering av forbindelsen.	H/U	I	U/K
7.	Det skal foreligge en risikovurdering rundt de opplysninger som vil bli eksponert for en ekstern leverandør.	H/U	I	K
8.	Det skal foreligge en anbefaling i fra Helse Nords Fagråd for informasjonssikkerhet (FRIS) om at tilgangen skal innføres	H/U	I	K
9.	Hvis det ikke er mulig å oppfylle disse kravene, eller at man i drift havner i avvik så skal det gjøres en ny risikovurdering og eventuelle tiltak skal implementeres før koblingen kan brukes.	H/U	I	K

Teknisk-funksjonelle krav:

1. Tilkobling skal initieres fra Helse nord sin side av tilgangen.
2. Tilkoblingen skal kobles ned når oppdraget er utført.
3. Tilgang skal logges. Minimum opp og nedkoblingstid, hvem som logger på, og formål for oppkobling.
4. Leverandør skal kunne dokumentere handlinger utført ved fjerntilganger eksempelvis ved sesjons opptak.
5. Programvare som benyttes skal være oppdatert, alle sikkerhetsoppdateringer skal installeres så snart som mulig.

Implementasjonskrav.

1. Tilkobling termineres i egen sikkerhetssone.
2. Det skal kun være nettverkstilgang til relevant utstyr fra sonen. Det skal være begrenset til relevante porter og protokoller.