

## **BIJLAGE D:**

### **OVEREENKOMST EXTERNE VERBINDINGEN in combinatie met artikel 2.15 remote service**

#### **Overwegende dat:**

- Leverancier ten einde (zo snel mogelijk) ondersteuning te bieden bij incidenten en calamiteiten danwel ten behoeve van reguliere onderhoudswerkzaamheden en ondersteuning, behoeft heeft aan toegang tot de ICT-infrastructuur van Opdrachtgever in het algemeen en de Apparatuur in het bijzonder;
- Ten behoeve van de ondersteunings- en onderhoudswerkzaamheden een zogenaamde Remote Service VPN-verbinding is gerealiseerd tussen het Service Center van Leverancier en de ICT-infrastructuur van Opdrachtgever.
- Leverancier middels deze VPN-verbinding toegang heeft of kan verkrijgen tot de ICT-infrastructuur van Opdrachtgever en de Apparatuur, zonder tussenkomst van Opdrachtgever;
- Onder toegang wordt verstaan, hetzij toegang vanaf de middels het Customer Center van Leverancier middels de VPN-verbinding, hetzij rechtstreekse toegang op de locatie;
- Leverancier erkent dat de bedrijfsvoering van Opdrachtgever leidt tot vertrouwelijke informatie welke valt onder de op Opdrachtgever rustende geheimhoudingsplicht;
- Leverancier erkent dat Opdrachtgever en/of derden (waaronder patiënten) aanzienlijke schade kunnen lijden wanneer die vertrouwelijke informatie ter kennis komt van derden danwel de vertrouwelijkheid, beschikbaarheid en integriteit van de informatie en/of de Apparatuur wordt geschaad;
- Leverancier zich realiseert dat de vertrouwelijkheid, beschikbaarheid en integriteit van de gegevens in de Apparatuur alsmede de juiste werking van de Apparatuur van Opdrachtgever gewaarborgd moeten blijven c.q. gegarandeerd moet worden.

#### **Verklaart als volgt:**

1. Leverancier zal strikte geheimhouding in acht nemen met betrekking tot het bestaan, de vorm, de inhoud en de strekking van alle (vertrouwelijke) informatie welke door de toegang aan haar blootgesteld zal worden;
2. Leverancier zal alle bestaande (wettelijke) richtlijnen in acht nemen (zoals onder meer de AVG, Algemene Verordening Gegevens en de van toepassing zijnde NEN7510 norm voor Informatiebeveiliging in de Zorg);
3. Leverancier zal de vertrouwelijkheid, beschikbaarheid en integriteit van de Apparatuur van Opdrachtgever waartoe zij toegang heeft of krijgt, alsmede de gegevens die daarin zijn opgeslagen, waarborgen en garanderen;
4. Leverancier draagt zorg dat haar medewerkers die gebruik maken van de faciliteiten voor toegang hebben kennisgenomen van, en zich houden aan de voorwaarden zoals beschreven in het Convenant "Veilige toepassingen van medische technologie in het ziekenhuis."
5. Leverancier draagt zorg voor vastlegging (logging) van alle activiteiten die door haar medewerkers middels de VPN-verbinding worden uitgevoerd op de Apparatuur van Opdrachtgever;
6. Leverancier verstrekt op aanvraag van Opdrachtgever een overzicht van voornoemde logging over de door Opdrachtgever gewenste periode;
7. Er wordt alleen verbinding gemaakt met de Apparatuur waar expliciet toegang voor is verleend;
8. Het niveau van Encrypting voor de VPN-verbinding is minimaal 3DES (168 bits) Mogelijke andere protocollen zijn: AES, AES-198, AES-256 etc.
9. Leverancier zal op verzoek van Opdrachtgever medewerking verlenen aan audits naar opzet, bestaan en werking van het Informatiebeveiligingssysteem ter zake van Leverancier;
10. Leverancier aanvaardt dat de Gedragscode van tijd tot tijd door Opdrachtgever kan worden aangepast;

11. Leverancier is verantwoordelijk voor de gevolgen en eventuele schade die voortvloeit uit het niet of onvoldoende naleven van de gedragscode door zijn medewerkers of door hem ingehuurd medewerkers.

#### **Gedragscode**

1. De medewerker van leverancier zal bij de uitoefening van zijn werkzaamheden voor Opdrachtgever, en bij toegang tot de ICT-infrastructuur van Opdrachtgever en de Apparatuur, de grootst mogelijke zorgvuldigheid in acht nemen;
2. Leverancier is verplicht om onbevoegd gebruik van de externe verbinding te voorkomen voor zover dat in zijn vermogen ligt. Dit kan onder andere inhouden dat deze verbinding en de toegang tot netwerk/applicaties/Apparatuur afgeschermd moeten worden tegen onbevoegd gebruik door derden, bijvoorbeeld door wachtwoorden en dergelijke geheim te houden.
3. De medewerker van Leverancier zal al hetgeen redelijkerwijs van hem/haar mag worden verlangd doen om de vertrouwelijkheid, integriteit en beschikbaarheid van de Apparatuur die voor hem/haar toegankelijk zijn en de gegevens die daarop aanwezig zijn te waarborgen;
4. De medewerker van Leverancier zal slechts op aanvraag van, danwel in overleg met Opdrachtgever gebruik maken van de mogelijkheid om toegang te verkrijgen tot de Apparatuur van Opdrachtgever;
5. De medewerker van leverancier zal slechts gebruik maken van de mogelijkheid om toegang te verkrijgen om activiteiten uit te voeren, welke direct te herleiden zijn naar het gebruik en goed functioneren van de Apparatuur van Opdrachtgever;
6. De medewerker van Leverancier zal geen wijzigingen doorvoeren in de Apparatuur die de goede werking kunnen beïnvloeden;
7. De medewerker van Leverancier zal enkel wijzigingen in de Apparatuur aanbrengen na overleg met en toestemming van Opdrachtgever;
8. In geval de medewerker van leverancier na overleg met en toestemming van Opdrachtgever wijzigingen aanbrengt in de Apparatuur, zal de medewerker schriftelijk of per e-mail verslag doen van de exacte aard van de wijzigingen en de reden waarom deze wijzigingen zijn aangebracht;
9. De medewerker van Leverancier zal alle (vermeende) beveiligingsincidenten, die hem/haar ter kennis komen direct melden aan zijn/haar leidinggevende binnen de Leveranciersorganisatie en aan de Servicedesk van Opdrachtgever;
10. De medewerker van leverancier zal alleen voor zover het noodzakelijk is voor de uitvoering van zijn/haar werkzaamheden gebruik maken van de verkregen bevoegdheden. Het gebruik van de bevoegdheden is werk gerelateerd en de bevoegdheden mogen niet voor andere doeleinden worden gebruikt;
11. De medewerker van Leverancier heeft specifieke bevoegdheden gekregen. Deze bevoegdheden mogen niet door anderen gebruikt worden of aan anderen worden overgedragen.