VI. Risicobeheersing, Gegevensbeheer, Informatiebeveiliging en assuranceverklaring

Deze bijlage bij de EETS-gebiedsverklaring Blankenburgverbinding bevat de eisen waaraan de dienstverlening van (E)ETS-aanbieders moet voldoen inzake Risicobeheersing, Gegevensbescherming, Informatiebeveiliging en assurance-verklaring, bedoeld in artikel 19.5 van de EETS-gebiedsverklaring.

1. Assurance-verklaring

1.1. De assurance-verklaring, bedoeld in artikel 19.5 van de EETS-gebiedsverklaring, heeft in ieder geval betrekking op de onderdelen genoemd in artikel 2 en artikel 3 van deze Bijlage VI van de EETS-gebiedsverklaring.

1.2. Behoudens de compensatie, bedoeld in artikel 19.8 van de EETS-gebiedsverklaring, zijn de kosten voor de assurance-verklaring, bedoeld in artikel 19.5 van de EETS-gebiedsverklaring, alsmede de kosten om bevindingen en aandachtspunten volgend uit (externe) audits en Inspecties zo snel als mogelijk en in afstemming met de Tolheffer door te voeren, voor rekening van de (E)ETS-aanbieder.

1.3. Ter toetsing van de assurance-verklaring, bedoeld in artikel 19.5 van de EETS-gebiedsverklaring, behoudt de Tolheffer zich het recht voor om Inspecties uit te (laten) voeren. Indien de (E)ETS-aanbieder niet de vereiste medewerking verleent aan de Inspecties, heeft de Tolheffer na voorafgaande schriftelijke kennisgeving met een termijn van ten minste 30 Kalenderdagen en maximaal eenmaal per Kalenderjaar, het recht een geautoriseerde partij namens de Tolheffer een Inspectie te laten uitvoeren bij de (E)ETS-aanbieder.

1.4. In het geval de Tolheffer het nodig acht dat er penetratietesten worden uitgevoerd op de dienstverlening van de (E)ETS-aanbieder ter toetsing van de Informatiebeveiliging, dan verstrekt de (E)ETS-aanbieder voorafgaand aan de penetratietesten een ondertekende vrijwaringsverklaring.

2. Gegevensbeheer

De (E)ETS-aanbieder dient met betrekking tot Gegevensbeheer, ten minste:

(i) een overzicht te creëren van de gegevens (of data-objecten en data-attributen) die hij in relatie tot zijn dienstverlening in het EETS-gebied Blankenburgverbinding vastlegt, door voor elk gegeven ten minste het volgende vast te leggen:

(a) definitie;

(b) bedrijfsproces(sen) waarvoor dit gegeven noodzakelijk is;

(c) dataformaat;

(d) of het gegeven optioneel of verplicht is;

(e) indien van toepassing, referentiedata of een controlemechanisme die voor dit gegeven worden toegepast;

(f) classificatie van de gevoeligheid van het gegeven ten aanzien van privacy, fraude en concurrentie;

(g) wie of welke rol toegang heeft tot dit gegeven, alsmede welke rechten deze persoon of rol krijgt;

(h) hoe lang dit gegeven bewaard mag worden op grond van geldende Wet- en Regelgeving;

(i) referentie naar standaarden die relevant zijn voor dit gegeven (bijv. ISO, NEN, etc.);

(ii) te borgen dat bij de invoer van gegevens in zijn systemen de daadwerkelijk verplichte gegevens conform het juiste dataformaat worden opgevoerd, inclusief het gebruik van referentiedata of controlemechanismen;

(iii) bij elke systeemwijziging een data-impactanalyse uit te voeren dat voorgaande punten revalueert en bijwerkt;

(iv) periodiek controle uit te voeren op de gegevens om de kwaliteit daarvan te bepalen middels het gebruik van dataformaten, verplichtingen, standaarden, referentiedata en controlemechanismen.

3. Risicobeheersing en Informatiebeveiliging

3.1. De (E)ETS-aanbieder voldoet aan de in dit artikel 3 genoemde eisen en implementeert de in dit artikel 3 genoemde maatregelen inzake risicobeheersing en Informatiebeveiliging, met inachtneming van de nadere specificering in artikel 3.8, tabel 1, van deze Bijlage VI.

3.2. Indien en voor zover de (E)ETS-aanbieder gebruik maakt van diensten van derden, dan gelden de eisen en verplichtingen tot implementatie van maatregelen ingevolge dit artikel 3 ook voor de desbetreffende derden. De (E)ETS-aanbieder stelt vast dat de desbetreffende derden voldoen aan de eisen en verplichtingen tot implementatie van maatregelen ingevolge dit artikel 3.

3.3. De (E)ETS-aanbieder implementeert maatregelen waarmee de beschikbaarheid van de dienstverlening conform de eisen, bedoeld in artikel 32 van de EETS-gebiedsverklaring is geborgd. Deze maatregelen worden periodiek maar minimaal eenmaal per Kalenderjaar en bij relevante wijzigingen aantoonbaar getest.

3.4. De (E)ETS-aanbieder test minimaal eenmaal per Kalenderjaar de koppelvlakken met de backoffice van de Tolheffer en onderliggende IT-componenten op het bestaan van kwetsbaarheden middels penetratietesten. De (E)ETS-aanbieder verhelpt bevindingen volgend uit de penetratietesten zo snel als mogelijk. De (E)ETS-aanbieder rapporteert aan de Tolheffer over de status en voortgang van de opvolging en respectievelijk

herstelwerkzaamheden.

3.5. De (E)ETS-aanbieder vereist dat de door hem in te zetten medewerkers een Verklaring Omtrent Gedrag ("VOG") verstrekken, of een verklaring met gelijkwaardige strekking en status in geval van medewerkers die niet in het bezit zijn van de Nederlandse nationaliteit. De VOG moet zijn verstrekt ten behoeve van de functie die de desbetreffende medewerker binnen de bedrijfsvoering van de (E)ETS-aanbieder zal vervullen en de daarbij behorende taakomschrijving. De VOG mag niet ouder zijn dan zes Kalendermaanden vanaf de datum van indiensttreding van de desbetreffende medewerker bij de (E)ETS-aanbieder.

3.6. De (E)ETS-aanbieder treft passende technische en organisatorische maatregelen voor Gegevensbescherming door ontwerp en standaardinstellingen, zoals bedoeld in artikel 25 van de algemene verordening Gegevensbescherming.

3.7. De (E)ETS-aanbieder treft maatregelen om te kunnen vaststellen dat rapportage over kritieke prestatie-indicatoren ingevolge artikel 19.4 van de EETS-gebiedsverklaring juist, volledig, tijdig en in overeenstemming met Bijlage VII van de EETS-gebiedsverklaring geschiedt.

3.8. De (E)ETS-aanbieder voldoet aan de hierna in *Tabel 1 eisen en maatregelen digitale veiligheid* gestelde eisen betreffende risicobeheersing en Informatiebeveiliging.

Tabel 1 Eisen en maatregelen digitale veiligheid

Referentie	Categorie	Eis
ID.AM.02	Asset Management	De (E)ETS-aanbieder houdt een register bij van alle gebruikte componenten en systemen, waarbij deze worden gekoppeld aan een systeemeigenaar. De (E)ETS-aanbieder biedt periodiek inzicht aan de Tolheffer met betrekking tot dit register.
PR.CM.3	Configuration Change control	De (E)ETS-aanbieder heeft een changemanagement proces dat zorg draagt voor een gecontroleerde wijze van doorvoeren van wijzigingen.
ID.RM	Risk Management Strategy	Risicomanagementprocessen worden opgezet en geïmplementeerd om risico's binnen de tolheffingsketen te identificeren, te beoordelen en te beheren.
ID.SC	Supply Chain Risk Management	Risicomanagementprocessen worden opgezet en geïmplementeerd om risico's met betrekking tot (onder)aannemers binnen de tolheffingsketen te identificeren, beoordelen en beheren.
ID.AM.02	Asset Management	De (E)ETS-aanbieder heeft maatregelen geïmplementeerd om periodiek (minimaal

		maandelijks) patches op IT-componenten te installeren om daarmee kwetsbaarheden te voorkomen.
PR.AC	Identity Management and Access Control	Gebruikersaccounts en (geheime) authenticatiegegevens worden uitgegeven, beheerd, geverifieerd, ingetrokken en gecontroleerd voor geautoriseerde apparaten, gebruikers en processen.
PR.AC.01	Identity Management and Access Control	De (E)ETS-aanbieder maakt gebruik van sterke sleutels volgens huidige geldende algoritmes en sleutellengtes die worden gebruikt in de communicatie tussen systemen in verschillende domeinen, en dient de toegang tot deze sleutels adequaat te beveiligen.
PR.AC.02	Identity Management and Access Control	De (E)ETS-aanbieder heeft een verzameling van minimale beveiligingseisen voor het creëren, uitwisselen en opslaan van sleutels, welke voldoen aan 'Webtrust for Certification Authorities' of aan 'ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates'.
PR.AC.03	Identity Management and Access Control	De (E)ETS-aanbieder volgt de specificaties in het beveiligingsraamwerk ISO/TS 19299:2015 voor het inrichten van sleutelmanagement.
PR.AC.07	Identity Management and Access Control	De (E)ETS-aanbieder zorgt er voor dat het autorisatiebeheer, zodanig is ingeregeld dat wordt voldaan aan NEN-ISO/IEC27001:2017.
PR.AC.08	Identity Management and Access Control	De (E)ETS-aanbieder stelt eisen op voor de wijze waarop het autorisatiebeheer vormgegeven wordt, bijvoorbeeld door specificaties van rollen, autorisatiematrix en wachtwoordbeleid.
PR.AC.09	Identity Management and Access Control	De (E)ETS-aanbieder specificeert voor elke component in het systeem van de (E)ETS-aanbieder: - hoe wordt bepaald wie er toegang krijgt? - wanneer wordt een toegang ingetrokken?
PR.AC.10	Identity Management and Access Control	Alle gebruikersaccounts en privileges voor alle componenten in de keten worden periodiek geanalyseerd. Hierbij geldt dat de toegang zodanig is ingeregeld dat wordt voldaan aan het principe van least privilege en scheiding in functie en/of rollen.
PR.AC.11	Identity Management and Access Control	De (E)ETS-aanbieder zorgt er voor dat elk systeem uitsluitend na autorisatie toegang verleent tot de opgeslagen data.

PR.AC.12	Identity Management and Access Control	De (E)ETS-aanbieder zorgt er voor dat de toegang tot de opgeslagen data uitsluitend wordt verleend via vastgelegde procedure en via goedgekeurde koppelvlakken.
PR.AT	Awareness and Training	Al het personeel en alle partners van de (E)ETS-aanbieder worden periodiek op cybersecurity getraind.
RC.RP	Recovery Planning	Herstelprocessen en -procedures worden uitgevoerd en onderhouden om succesvol herstel te kunnen waarborgen.
RC.CO	Recovery Communications	Herstelprocessen en -procedures worden gecoördineerd en gecommuniceerd met interne en externe belanghebbenden.
RC.IM	Recovery Improvements	Herstelprocessen en -procedures worden verbeterd uit huidige en voorgaande cybersecurityactiviteiten.
PR.MA	Maintenance	Apparatuur wordt correct onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
PR.MA.01	Maintenance	De (E)ETS-aanbieder organiseert het beheer en onderhoudsprocessen volgens de best practices zoals gedefinieerd in NIST Cyber Security Framework of NEN-ISO/IEC 27002:2013.
PR.DS	Data Security	Vertrouwelijkheid, integriteit en beschikbaarheid van data worden gewaarborgd.
PR.DS.01	Data Security	De (E)ETS-aanbieder dient ervoor te zorgen dat voor alle (tijdelijk) opgeslagen gegevens geldt dat: - de gegevens onveranderd blijven; - de vertrouwelijkheid van de gegevens gegarandeerd blijft bij het verlenen van toegang; - de herkomst van de gegevens te allen tijde te achterhalen is.
PR.DS.04	Data Security	De uitwisseling van data dient plaats te vinden over een kanaal waarvoor geldt dat: - de beschikbaarheid betrouwbaar is; - de vertrouwelijkheid van de gegevens gewaarborgd is; - de inhoud van de gegevens onveranderd blijft; - de identiteit van de afzender vaststaat; - het onbetwistbaar is dat de gegevens respectievelijk ontvangen of verzonden zijn; - beide partijen voor de uitwisseling elkaar geverifieerd hebben; - opnieuw verzonden berichten gedetecteerd worden;

		- grote hoeveelheden niet-aangekomen gegevens (zoals toldeclaraties of factureringsdetails) gedetecteerd worden (ter bescherming tegen koppelvlakfouten).
PR.DS.16	Data Security	De (E)ETS-aanbieder verifieert de herkomst van de ontvangen tolheffingsgegevens voordat de ontvangen gegevens worden geaccepteerd.
PR.DS.17	Data Security	De (E)ETS-aanbieder verstrekt aan de Tolheffer de cryptografisch getekende exception list.
PR.DS.18	Data Security	De (E)ETS-aanbieder verstrekt een cryptografisch getekende bevestiging van ontvangst van de tolheffingsgegevens aan de Tolheffer.
PR.DS.24	Data Security	De (E)ETS-aanbieder stelt gebruikers in staat om de juistheid van facturen te kunnen controleren.
PR.IP	Information Protection Processes and Procedures	Cybersecurityprocessen en -procedures worden opgezet, beheerd en uitgevoerd ter beveiliging van informatiesystemen en componenten van de (E)ETS-aanbieder.
PR.IP.01	Information Protection Processes and Procedures	De (E)ETS-aanbieder stelt richtlijnen vast voor veilige configuraties van alle IT-componenten in de keten en te implementeren voordat deze gebruikt mogen worden in Nederland.
PR.IP.14	Information Protection Processes and Procedures	De (E)ETS-aanbieder slaat alle gevoelige data (at rest) adequaat versleuteld op.
PR.IP.15	Information Protection Processes and Procedures	De (E)ETS-aanbieder verzendt elektronische klantenlijsten uitsluitend versleuteld. Hierbij wordt ten minste TLS1.3 op basis van Public-Key-Infrastructure (PKI) gebruikt.
PR.IP.22	Information Protection Processes and Procedures	Naast de versleuteling van communicatie op basis van TLS1.3 op basis van Public-Key-Infrastructure (PKI), versleutelt de (E)ETS-aanbieder facturen en registraties additioneel, alvorens deze verzonden worden.
PR.PT	Protective Technology	Technische beveiligingsmaatregelen worden geïmplementeerd en beheerd om de beveiliging van systemen en componenten te waarborgen, in overeenstemming met beleidsregels, procedures en afspraken.
PR.PT.02	Protective Technology	De (E)ETS-aanbieder stelt technische specificaties en additionele securitymaatregelen op voor het veilig tot

		stand brengen van communicatiestromen tussen twee actoren op te stellen.
PR.PT.05	Protective Technology	De (E)ETS-aanbieder zorgt er voor dat het niveau van beveiliging niet verlaagt bij de implementatie en integratie van externe producten of diensten.
DE.AE	Anomalies and Events	Datalekken en andere verdachte gebeurtenissen worden gedetecteerd en correct afgehandeld.
DE.CM	Security Continuous Monitoring	De informatiesystemen en componenten van de (E)ETS-aanbieder worden gemonitord om cybersecuritygebeurtenissen te kunnen identificeren.
DE.CM.01	Security Continuous Monitoring	De (E)ETS-aanbieder richt logging en monitoring in op de (administratieve) gebruikerstoegang.
DE.DP	Detection Processes	Detectieprocessen en -procedures worden onderhouden en getest om cybersecurity-gebeurtenissen en -incidenten inzichtelijk te kunnen maken. De (E)ETS-aanbieder treft maatregelen om meldingen van beveiligingsrisico's door externe instanties te ontvangen en te beoordelen.
DE.DP.01	Detection Processes	De (E)ETS-aanbieder en onderaannemers richten processen in om cybersecurityincidenten te voorkomen, te detecteren en binnen 24 uur af te handelen.
RS.RP	Response Planning	Cyberresponse activiteiten worden uitgevoerd en onderhouden om tijdige reactie op een incident te kunnen waarborgen.
RS.CO	Communications	Cyberresponse activiteiten worden gecoördineerd en gecommuniceerd met interne en externe belanghebbenden.
RS.CO.03	Communications	De (E)ETS-aanbieder meldt een gedetecteerd cybersecurityincident binnen 24 uur aan de Tolheffer. Beveiligingsincidenten, waarvan gevolgen voor de Tolheffer, in redelijkheid niet kunnen worden uitgesloten, worden terstond aan de Tolheffer gemeld.
RS.AN	Analysis	Analyses op de cybersecurity-gebeurtenissen en -incidenten worden uitgevoerd om de cyberresponse activiteiten te ondersteunen.
RS.MI	Mitigation	De afhandeling van cybersecuritygebeurtenissen gebeurt in samenwerking tussen interne en externe belanghebbenden.

RS.MI.02	Mitigation	De (E)ETS-aanbieder ondersteunt bij een incident omtrent cybersecurity ondersteuning n degenen die verantwoordelijk zijn voor de oplossing van deze gebeurtenissen.
RS.IM	Improvements	Cyberresponse activiteiten worden verbeterd uit huidige en voorgaande cybersecurityactiviteiten.
ID.GV.05	Governance	De (E)ETS-aanbieder en onderaannemers van de (E)ETS-aanbieder stellen een eigen cybersecuritybeleid op en overleggen dit aan de Tolheffer. Dit cybersecuritybeleid voldoet aan de standaard NIST Cybersecurity Framework of NEN-EN-ISO/IEC27001:2017.
ID.GV.07	Governance	De (E)ETS-aanbieder en zijn onderaannemers rapporteren periodiek aan de Tolheffer over de status van cybersecurity aan de Tolheffer.
ID.GV.08	Governance	De (E)ETS-aanbieder en zijn onderaannemers stellen richtlijnen op voor het veilig gebruik van componenten in tolheffingsketen. Deze richtlijnen dienen elke beheerder met geautoriseerde toegang tot componenten te worden gevolgd.