### VI. Risk management, Data Management, Information security and assurance statement

This Annex to the EETS Domain Statement Blankenburgverbinding contains the requirements that the services of (E)ETS Providers must meet in terms of Risk management, Data Management and Information security and sets out the requirements for the assurance statements referred to in Article 19.5 and Article 44.2 of the EETS Domain Statement.

### 1. Assurance statement

1.1. The assurance statements referred to in Article 19.5 and Article 44.2 of the EETS Domain Statement, shall in any case cover the elements mentioned in Article 2 and Article 3 of this Annex VI.

1.2. Except for the compensation fee referred to in Article 19.8 of the EETS Domain Statement, the costs for the assurance statements referred to in Article 19.5 and Article 44.2 of the EETS Domain Statement, as well as the costs of reporting findings and points of interest resulting from (external) audits and Inspections to be carried out as quickly as possible and in coordination with the Toll Charger, at the expense of the (E)ETS Provider.

1.3. If the (E)ETS Provider does not have an assurance statement referred to in Article 19.5 of the EETS Domain Statement, the (E)ETS Provider shall have an assurance statement as referred to in Article 19.5 of the EETS Domain Statement no later than six Calendar Months after the start of its services.

1.4. To verify the assurance statements, referred to in Article 19.5 and Article 44.2 of the EETS Domain Statement, the Toll Charger reserves the right to carry out for Inspections. If the (E)ETS Provider does not cooperate with the Inspections as required, the Toll Charger shall have the right, after prior written notice with a deadline of at least 30 Calendar Days and no more than once per Calendar Year, to have an authorised party perform an Inspection on behalf of the Toll Charger at the (E)ETS Provider.

1.5. In case the Toll Charger deems it necessary to perform penetration tests on the (E)ETS Provider's services to verify Information security, the (E)ETS Provider shall provide a signed indemnification declaration prior to the penetration tests.

### 2. Data management

With respect to Data Management, the (E)ETS Provider shall, as a minimum:

(i)     create an overview of the data (or data objects and data attributes) it records in relation to its services in the EETS Domain Blankenburgverbinding, by recording at least the following for each piece of data:

(a) definition;

(b) business process(es) for which this data is necessary;

(c) data format;

(d) whether the data is optional or mandatory;

(e) if applicable, reference dates or a control mechanism applied for this data;

(f) classification of the sensitivity of the data with respect to privacy, fraud and competition;

(g) Who or what roles have access to this data, as well as what rights this person or role is given;

(h) How long this data may be kept under applicable Laws and Regulations;

(i) reference to standards relevant to this data (e.g., ISO, NEN, etc.);

(ii) ensure that when entering data into its systems, the actual mandatory data is entered in accordance with the correct data format, including the use of reference data or control mechanisms;

(iii) Conduct a data impact analysis for each system change that re-evaluates and updates previous points;

(iv) Periodically check data to determine its quality through the use of data formats, obligations, standards, reference data and control mechanisms.

## 3. Risk management and Information security

3.1. The (E)ETS Provider shall comply with the requirements in this Article 2 and implements the requirements set out in this Article 2 regarding Risk management and Information security, taking into account the further specification in Article 3.8, Table 1, of this Annex VI.

3.2. If and to the extent that the (E)ETS Provider uses third party services, then the requirements and obligations to implement measures pursuant to this Article 2 shall also apply to the relevant third parties. The (E)ETS Provider shall ensure that the relevant third parties comply with the requirements and obligations to implement measures pursuant to this Article 3.

ETS ProviderETS ProviderETS Provider

3.3. The (E)ETS Provider shall implement measures that ensure the availability of the service in accordance with the requirements referred to in Article 32 of the EETS Domain Statement is ensured. These measures shall be tested periodically but at least once per Calendar Year and in case of relevant changes.

3.4. The (E)ETS Provider shall ETS ProviderToll ChargerToll ChargerETS ProviderETS ProviderToll Chargertest, at least once per Calendar Year, the interfaces with the Toll Charger's back office and underlying IT components

for the existence of vulnerabilities by means of penetration tests. The (E)ETS Provider shall remedy findings following the penetration tests as soon as possible. The (E)ETS Provider shall report to the Toll Charger on the status and progress of the follow-up and remedial actions.

3.5. The (E)ETS Provider shall require that the employees to be deployed by it provide a Certificate of Good Conduct (in Dutch: Verklaring omtrent Gedrag, "VOG"), or a certificate with an equivalent status in the case of employees who are not Dutch nationals. The VOG must have been issued for the purpose of the position to be held by the relevant employee within the operations of the (E)ETS Provider and the associated job description. The VOG must not be older than six months from the date of commencement of employment of the employee concerned with the (E)ETS Provider.

3.6. The (E)ETS Provider takes appropriate technical and organisational measures for Data Protection through design and default settings, as referred to in Article 25 of the General Data Protection Regulation.

3.7. The (E)ETS Provider shall take measures to ensure that reporting on key performance indicators pursuant to Article 19.4 of the EETS Domain Statement is accurate, complete, timely and in accordance with Annex VII of the EETS Domain Statement.

3.8. The (E)ETS Provider shall comply with the requirements in Table 1 below (Digital security requirements and measures).

*Table 1 Digital security requirements and measures*

| Reference | Category | Claim |
|---|---|---|
| ID.AM.02 | Asset Management | The (E)ETS Provider shall keep a register of all components and systems used, linking them to a system owner. The (E)ETS Provider shall provide periodic insight to the Toll Charger regarding this register. |
| PR.CM.3 | Configuration Change control | The (E)ETS Provider shall have a change management process that ensures a controlled way of implementing changes. |
| ID.RM | Risk management Strategy | Risk management processes shall be established and implemented to identify, assess and manage risks within the toll chain. |
| ID.SC | Supply chain Risk management | Risk management processes shall be established and implemented to identify, assess and manage risks related to (sub)contractors within the toll chain. |
| ID.AM.02 | Asset Management | The (E)ETS Provider shall implement measures to periodically (at least monthly) install patches on IT components to prevent vulnerabilities. |
| PR.AC | Identity Management | User accounts and (secret) authentication credentials shall be issued, managed, |

| | | and Access Control | verified, revoked and monitored for authorised devices, users and processes. |
|---|---|---|---|
| PR.AC.01 | Identity Management and Access Control | The (E)ETS Provider shall use strong keys according to current valid algorithms and key lengths used in communication between systems in different domains, and shall adequately secure access to these keys. |
| PR.AC.02 | Identity Management and Access Control | The (E)ETS Provider shall have a set of minimum security requirements for creating, exchanging and storing keys, which comply with 'Webtrust for Certification Authorities' or with 'ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates'. |
| PR.AC.03 | Identity Management and Access Control | The (E)ETS Provider shall follow the specifications in the security framework ISO/TS 19299:2015 for setting up key management. |
| PR.AC.07 | Identity Management and Access Control | The (E)ETS Provider shall ensure that the authorisation management, is configured to comply with NEN-ISO/IEC27001:2017. |
| PR.AC.08 | Identity Management and Access Control | The (E)ETS Provider shall set requirements for how authorisation management is designed, e.g. through specifications of roles, authorisation matrix and password policy. |
| PR.AC.09 | Identity Management and Access Control | The (E)ETS Provider shall specify for each component in the (E)ETS Provider's system: <br>- how access is determined - <br>- when access is revoked |
| PR.AC.10 | Identity Management and Access Control | All user accounts and privileges for all components in the chain shall be analysed periodically. Here, access shall be arranged in such a way that the principle of least privilege and separation into function and/or roles is met. |
| PR.AC.11 | Identity Management and Access Control | The (E)ETS Provider shall ensure that each system grants access to the stored data only after authorisation. |
| PR.AC.12 | Identity Management and Access Control | The (E)ETS Provider shall ensure that access to the stored data is only granted via established procedure and via approved interfaces. |
| PR.AT | Awareness and Training | All staff and all partners of the (E)ETS Provider shall be periodically trained on cybersecurity. |
| RC.RP | Recovery Planning | Recovery processes and procedures shall be implemented and maintained to ensure successful recovery. |

| RC.CO | Recovery Communications | Recovery processes and procedures shall be coordinated and communicated to internal and external stakeholders. |
|---|---|---|
| RC.IM | Recovery Improvements | Recovery processes and procedures shall be improved from current and previous cybersecurity activities. |
| PR.MA | Maintenance | Equipment shall be properly maintained to ensure its continuous availability and integrity. |
| PR.MA.01 | Maintenance | The (E)ETS Provider shall organise the management and maintenance processes according to the best practices defined in [NIST Cyber Security Framework] or NEN-ISO/IEC 27002:2013. |
| PR.DS | Data Security | Confidentiality, integrity and availability of data shall be ensured. |
| PR.DS.01 | Data Security | The (E)ETS Provider shall ensure that for all (temporarily) stored data: <br> - the data remain unchanged; <br> - the confidentiality of the data is guaranteed when access is granted; <br> - the origin of the data is traceable at all times. |
| PR.DS.04 | Data Security | The exchange of data shall take place over a channel for which: <br> - the availability is reliable; <br> - the confidentiality of the data is guaranteed; <br> - the content of the data remains unchanged; <br> - the identity of the sender is established; <br> - it is indisputable that the data has been received or sent respectively; <br> - both parties have verified each other prior to the exchange; <br> - resent messages are detected; <br> - large amounts of non-arrived data (such as toll declarations or billing details) are detected (to protect against interface errors). |
| PR.DS.16 | Data Security | The (E)ETS Provider shall verify the origin of the toll data received before accepting the received data. |
| PR.DS.17 | Data Security | The (E)ETS Provider shall provide the Toll Charger with the cryptographically signed exception list. |
| PR.DS.18 | Data Security | The (E)ETS Provider shall provide a cryptographically signed acknowledgement of receipt of the toll data to the Toll Charger. |
| PR.DS.24 | Data Security | The (E)ETS Provider enables users to check the accuracy of invoices. |

| PR.IP | Information Protection Processes and Procedures | Cybersecurity processes and procedures are established, managed and implemented to secure information systems and components of the (E)ETS Provider. |
|---|---|---|
| PR.IP.01 | Information Protection Processes and Procedures | The (E)ETS Provider establishes guidelines for secure configurations of all IT components in the chain and to be implemented before they may be used in the Netherlands. |
| PR.IP.14 | Information Protection Processes and Procedures | The (E)ETS Provider stores all sensitive data (at rest) adequately encrypted. |
| PR.IP.15 | Information Protection Processes and Procedures | The (E)ETS Provider shall transmit customer lists exclusively in encrypted form. Here, at least TLS1.3 based on Public-Key-Infrastructure (PKI) shall be used. |
| PR.IP.22 | Information Protection Processes and Procedures | Besides encrypting communications based on TLS1.3 based on Public-Key-Infrastructure (PKI), the (E)ETS Provider additionally encrypts invoices and registrations before sending them. |
| PR.PT | Protective Technology | Technical security measures are implemented and managed to ensure the security of systems and components, in accordance with policies, procedures and Agreements. |
| PR.PT.02 | Protective Technology | The (E)ETS Provider shall establish technical specifications and additional security measures for the secure establishment of communication flows between two actors. |
| PR.PT.05 | Protective Technology | The (E)ETS Provider shall ensure that the level of security does not decrease when implementing and integrating external products or services. |
| DE.AE | Anomalies and Events | Data breaches and other suspicious events are detected and handled properly. |
| DE.CM | Security Continuous Monitoring | The (E)ETS Provider's information systems and components are monitored to identify cybersecurity events. |
| DE.CM.01 | Security Continuous Monitoring | The (E)ETS Provider shall set up logging and monitoring on (administrative) user access. |
| DE.DP | Detection Processes | Detection processes and procedures are maintained and tested to provide insight into cybersecurity events and incidents. The (E)ETS Provider takes measures to receive and assess notifications of security risks by external bodies. |
| DE.DP.01 | Detection Processes | The (E)ETS Provider and subcontractors set up processes to prevent, detect and handle cybersecurity incidents within 24 hours. |

| RS.RP | Response Planning | Cyber-response activities are implemented and maintained to ensure timely response to an incident. |
|-------|-------------------|---------------------------------------------------------------------------------------------------|
| RS.CO | Communications | Cyber-response activities are coordinated and communicated to internal and external stakeholders. |
| RS.CO.03 | Communications | The (E)ETS Provider shall report a detected cybersecurity incident to the Toll Charger within 24 hours. Security incidents in which consequences for the Toll Charger cannot reasonably be excluded, will be reported to the Toll Charger immediately. |
| RS.AN | Analysis | Analyses on cybersecurity events and incidents are conducted to support cyber-response activities. |
| RS.MI | Mitigation | The handling of cybersecurity events is done in collaboration between internal and external stakeholders. |
| RS.MI.02 | Mitigation | The (E)ETS Provider supports in the event of an incident concerning cybersecurity support n those responsible for resolving these events. |
| RS.IM | Improvements | Cyber-response activities are enhanced from current and previous cybersecurity activities. |
| ID.GV.05 | Governance | The (E)ETS Provider and subcontractors of the (E)ETS Provider shall prepare and submit its own cybersecurity policy to the Toll Charger. This cybersecurity policy shall comply with the standard NIST Cybersecurity Framework or NEN-EN-ISO/IEC27001:2017. |
| ID.GV.07 | Governance | The (E)ETS Provider and its subcontractors shall periodically report the status of cybersecurity to the Toll Charger. |
| ID.GV.08 | Governance | The (E)ETS Provider and its subcontractors shall establish guidelines for the safe use of components in toll chain. These guidelines should be followed by any administrator with authorised access to components. |