Annexes to the Data Processing Terms and Conditions

These Annexes, once executed, form an integral part of the NEC XON Data Processing Terms and Conditions, located at https://www.nec.xon.co.za/wp-content/uploads/2021/11/Data-Processing-Terms-and-Conditions-for-NEC-XON-Website.pdf. These Annexes and the NEC XON Data Processing Terms and Conditions shall be read together as one complete document.

PARTIES

A. XON Systems Proprietary Limited or NEC XON Alternative Energy Proprietary Limited or NEC XON Retail Solutions ("Operator" and/ or the "Vendor")
B. [Insert Customer Name] ("Responsible Party" and/or the "Company")

These Annexes

(1) form part the NEC XON Data Processing Terms and Conditions
(2) The Parties have agreed to enter into the the NEC XON Data Processing Terms and Conditions to govern the processing of personal information received by the Operator in connection with the Services defined below.

The terms used in this Annexes shall have the meanings set forth in the NEC XON Data Processing Terms and Conditions.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Main Agreement with effect from the date first set out below.

Operator

Signature _____

Name _____

Title _____

Date Signed _____

Company

Signature _____

Name _____

Title _____

Date Signed _____

Annex 1. Processing of Personal Information

Subject Matter of the Processing	*[Delete this - Please include summary of the services that NEC XON provides to Customer]*
Purpose of the Processing	*[Delete this - Why is the information processed?]*
Type of Personal Information to which Operator may have access for the provision of the Services	*[Delete this - Type of info e.g. ID numbers, telephone numbers, email addresses etc.]*
Categories of Data Subjects	*[Delete this - Who are the data subjects? Are they the customer's end customers? Or employees?]*

Annex 2. Technical and organizational security measures implemented by the Operator:

People, awareness and training

- Regular awareness training on POPIA for all employees with access to the Personal Information.
- Personal accountability for technology security shall be incorporated in the organisational structures.
- The Operator's information assets shall be classified according to their criticality to classification requirements defined within the Operator's information classification policy so as to enable an appropriate level of protection.
- Access shall only be provided for the period during which it is required, and all access shall be formally authorised.

Organisation control

- Internal data privacy policies and procedures which comply with requirements of POPIA.
- The data privacy policy covers all Personal Information Processed by the Operator to access information resources.
- Data privacy is implemented and audited for compliance on an annual basis.
- All parties\users must only lawfully and in a reasonable manner Process Personal Information that is adequate, relevant and not excessive for the business purposes for which it is to be used.

- All parties\users must take reasonable steps, including physical, administrative and technical safeguards, to protect Personal Information from loss, misuse, unauthorised access, disclosure, alteration or destruction.
- All parties\users must take reasonable steps to ensure that Personal Information is retained only for as long as needed to meet the purposes for which it was collected and in accordance with the Operator's data management policy.
- In protecting its information assets, all parties shall comply with all applicable laws and regulations and requires its employees, contractors and agents to meet the highest ethical standards in dealing with all interested parties.

Physical security to Personal Information

- Access control and visitor management systems implemented for all visitors/guests.
- CCTV surveillance to protect restricted area.
- Locked cabinets for where paper files are stored.

Security to Personal Information

- The connection of unauthorised equipment to the Responsible Party's corporate LAN is prohibited. Authorisation must be obtained from the Responsible Party's Technology Security Officer with detailed motivations attached outlining the reason for the equipment to be connected.
- All servers, workstations, personal devices used to access the Operator's information resources, where technically possible, shall be loaded and protected with the latest approved anti-virus software.
- All servers, workstations, personal devices used to access the Operator's information resources, where technically possible, shall be password protected.
- Encryption technologies, where technically possible, shall be used to encrypt classified data stored on any device used to access the Operator's information resources.
- Recognising that some information is intended for specific individuals and shall not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages.
- Firewall policy management tools should be in place to protect against unauthorized electronic access to the Operator's network and to allow the Operator to track and monitor the flow of applications and important services over all areas of the network.
- All parties' firewalls must log all reports on daily, weekly, and monthly basis to allow the analysis of the network activity through the firewall.
- All incidents related to possible breach or compromise in information resources shall be escalated to the Operator's Information Officer\Privacy Officer and the Technology Security Officer.

Access control to Personal Information

- All service accounts shall be managed in accordance with the Operator's password policy.
- Users shall have a unique user name and password to identify them on the various systems. All user names and passwords shall conform to the approved naming and password conventions used by the Operator.
- Authorised users are responsible for the security of their passwords.
- Employees are given access on a need to know basis.
- All access logging and control to Personal Information should be logged.
- Access to the systems and data shall be immediately terminated as soon as evidence of non-compliance with the security requirements are observed.

Annex 3 Approved List of (Sub) Operators

Services provided	Not Applicable
Purpose of the Processing	Not Applicable
Type of Personal Information to which (Sub) Operator may have access for the provision of the Services	Not Applicable
Categories of Data Subjects	Not Applicable
Location	Not Applicable