Cybersecurity Requirements

These Cybersecurity Requirements (as defined below), are mandatory and non-waivable and will apply to you (the "Provider") in relation to services and/or goods that will lend or supply to Infraestructura Energética Nova, S.A.B. de C.V. or any of its subsidiaries (the "Company"), from the moment they sign this document, even if to date a contract or purchase order has not been signed (without distinction between one and the other, an "Instrument").

This document represents the main Cybersecurity Requirements and shall be understood as included with full force and validity in the Instrument when it is signed, based on the most recent templates, including cybersecurity after its completion.

The Provider that delivers the service and/or to the Company, agrees to maximize the security of its people, processes and technologies throughout the term of the Instrument, in accordance with the requirements set forth herein and all applicable laws (collectively, the "Cybersecurity Requirements"). The Company reserves the right to validate the effectiveness of the Cybersecurity Requirements and the Provider shall provide evidence of independent validation by third parties, at the request of the Company. The Company may modify the Cybersecurity Requirements by written notice to the Provider during the term of the Instrument, by common agreement reasonable deadlines will be defined to comply with the changes to the requirements. The term "Product", as used herein, means any service, hardware or software provided by the Provider to the Company in terms of the Instrument.

The operations of the products and services delivered to the Company refer to all assets, processes and systems (including information systems), data and metadata (including Customer data), personnel and sites, used or processed by the Provider from time to time in compliance with this agreement.

This document describes the generic cybersecurity requirements for the services or products delivered.

1.0 Cybersecurity framework. The Provider shall have a mature framework to address a secure by design, defense-in-depth approach to designing, building, maintaining, and retiring Products and/or Services (the "Cybersecurity Framework"). The Cybersecurity Framework will be established within the meaning of the ISO 2700x / IEC 62443 / Cloud Security Alliance / NIST 800 - xx series and will include, among others: information security policies, standards and processes, and the internal governance necessary to adequately protect the confidentiality, integrity and availability of the Content, Product and / or Service against the current landscape of general and specific threats of the Provider. The Provider will include Cybersecurity by design and by default in its Product and /or Service and in all related Information Systems, in accordance with the Good Security Practices established in the control frameworks set forth in this paragraph ("security by design" and "security by default"). This includes the complete life cycle of the Product and/or Service (see IEC 62443-4-1), as well as all related information systems (see ISO 2700x) necessary for its delivery.

2.0 Access Controls. The Provider will provide role-based access, authorization, and responsibility controls within its product, which comply with the guidelines and requirements set out in the Cybersecurity Requirements. Controls must be appropriate to the Company's policies. In addition, the product will provide separate roles for users, administrators, developers, and day-to-day support personnel, and that access will provide access only to authorized personnel who have received appropriate training on administrative responsibilities, security processes, and procedures. Access control shall provide the minimum access required for each role and shall deny access to unauthorized users in accordance with the term of the service and verified by the user requesting the service. The products hosted by the Provider, if any, will include controls to protect service accounts and generic accounts, to prevent their modification or unauthorized use. Service and generic account passwords must be changed at least every three months. The Provider will verify and disclose all known methods of accessing the products, and will not access or allow others to access the products without the prior consent of the Company (apart from the hosted products, and even in those cases, only the Provider will be able to access the hosted products). The Provider also ensures that administrators of the production environment of the hosted products will use two-factor authentication when providing remote administrative support for the environment. Before the Service is ready, the Provider shall provide the Company with the concept of the current general detailed authentication and authorization function (including the approximate number of persons authorized per function), which ensures restricted access to data and processes based on the principles of "least privilege", "need to know" and "segregation of duties". The Provider environment will offer two-factor authentication for privileged accounts for management interfaces. For users of the Company, the Provider shall support an authentication solution that enables strong authentication for users/accounts based on the Company's authentication options. For the exchange of Content between The Company's infrastructure and the Provider's infrastructure, the Provider shall provide certificate-based authentication to and from the Product and/or Service environment. Otherwise, both Parties shall agree to any other form of authentication.

3.0 Shared Architecture. The Provider agrees to identify the parties where the shared resources are used within its architecture by other customers and the security controls implemented to protect the Company's data from access by unauthorized users and third parties. If the Instrument contemplates a dedicated environment, then that environment will not contain shared resources, including, but not limited to, all components, systems, and infrastructure.

4.0 Incident Response and Notification of Non-Compliance. The Provider agrees that any breach, data breach or any other cybersecurity incident, internal or external, that may compromise multiple data sources or affect the services of the Company, you must promptly notify and inform [name of the contract administrator by the Company] and soc.noc@ienova.com.mx to the telephone number 800 626 6026 within 24 hours of knowledge of the infringement, shall cooperate fully to provide all related information, followed by a remediation plan, within 72 hours of remediation, and 2 business weeks from the initial notification to complete the full investigation by providing an executive and a detailed report of the incident, specifying the information that was compromised, exposed or with associated risks, as well as a summary of the forensic report. In case of not complying with these deadlines, the Company reserves the right to suspend the service and initiate the disconnection of the Provider's infrastructure with that of the Company if it exists to mitigate any cybersecurity commitment and/or risk that may be transferred to the Company.

5.0 Encryption. When the Instrument provides for encryption, or if the Company determines that encryption is acceptable to prevent unauthorized disclosure of Company information, to protect the Company's confidential information, Provider products will use cryptographic controls that meet the requirements of FIPS 197 in such a way that sensitive data and information become inaccessible by an unauthorized user, considering the use of Advanced Enrollment Algorithms (AES). Where the Provider's product uses encryption keys, the Provider's product will not store the encrypted encryption keys within the source code. Encryption keys will be stored and protected separately from the product while in transit and at rest and will be revocable for redeployment and maintenance. Content will be encrypted in transit, including, but not including, not later, content transmitted over public land and at rest. The Company's cryptographic certificates will be used for user interfaces, where applicable. All certificates, keys, and cryptographic tools will only be used for the intended purpose and will be protected against unauthorized access, modification, loss, and disclosure. The Provider will use a secure key management system (KMS) to store and archive the keys securely.

6.0 Password and Login Standards. The Provider's products will provide a unique (individually identifiable) identification for user accounts. Where individual responsibility for access to sensitive systems cannot be achieved, multifactor authentication should be used. The Provider's products will provide a password complexity that meets the following parameters: user accounts will require a minimum of 8 characters, a combination of uppercase and lowercase letters, numbers and special characters, passwords will be no more than 90 days old and the history of 10 previous passwords will be maintained. Administrator accounts will require a minimum of 10 characters, a combination of uppercase and lowercase letters, numbers, and special characters, will be no more than 90 days old, and the history of 10 previous passwords will be maintained. Login credentials and passwords will be protected by transport encryption that meets the minimum encryption requirements of Section 5.0.

7.0 Data Security. The Provider certifies that its product provides the necessary security to comply with all the laws of protection of personal data of the locality, hosting environment and infrastructure where the product or service is located, as well as the applicable regulatory requirements for the storage, processing and transmission of data. This specifically includes, but is not limited to, all laws and regulations that require specific protections for personally identifiable information, credit card and financial information, and audit logs. The Provider agrees that it will allow validation by the Company or by third parties contracted by it to verify compliance with all legal and regulatory requirements.

8.0 Error Logging and Details. The Provider agrees to record all use of products and applications, access, misuse and sufficient detailed error messages to monitor and analyze the use of the products, and will retain all information for a minimum of ninety (90) days from the date of registration. The Provider further agrees that the product includes an audit trail, time stamped registration entries and unique registration identification with attribution. The Company has the right to request registrations at any time and at no cost to the Company.

9.0 Operational Support. The Provider will conduct background checks including a 5-year criminal history, social security data verification, drug analysis, and credit history for staff supporting hosted products (if applicable) prior to commencing work with the Company and on an ongoing basis, at no cost to the Company. The Company reserves the right to request this documentation to confirm compliance with these verifications by the Provider.

10.0 Vulnerabilities and Defects. The Provider agrees to maintain a process of monitoring vulnerabilities and defects that identifies and remedies possible defects, in addition to classifying them by their impact on the security of the Provider's products and the components and software packages that support it, at no cost to the Company. The Company must be notified of critical vulnerabilities or defects by specifying remediation or mitigation times on a periodic basis agreed with the contract administrator on a semi-annual basisThe Provider also agrees that, at the provider's expense, it will test and remedy all software vulnerabilities, which may be identified by the Provider's vulnerability scanning exercises or publicly disclosed in the National Vulnerability Database (http://nvd.nist.gov/) and by the Open Web Application Security Project (www.owasp.org) within thirty (30) days of their publication. Overall, this will prevent the product from being easily susceptible to cross-site scripting, injection, SQL, buffer overflows, input validation, and other similar cyberattacks. The Provider further warrants that the product will not contain any code that may facilitate unexpected or unassuming access to or interruptions to the product, including, but not limited to: computer viruses, worms, time bombs, backdoors, Trojan horses, Easter eggs and any other forms of malicious code, and agrees to provide documentation detailing such processes at the request of the Company and at no cost to the Company. The Company reserves the right to request this documentation to confirm compliance with these verifications by the Provider.

11.0 Security Assessments and Tests. The Provider agrees that it will hire an independent third party, which will be agreed by the Provider and the Company, at the provider's expense, to test the product for cybersecurity vulnerabilities and risks through a detailed security test annually, or the Provider may choose to be certified under an accepted industry standard. Standard, which will be approved by the Company. If the Provider chooses an annual security test, that test will include all security controls that support the product, its production hosting environment, and the operational support infrastructure. The Provider shall require such third party to provide a report detailing the results of the test and the Provider shall provide the Company with a copy of such report within thirty (30) days of the test. If such report shows vulnerabilities in the product, the Provider shall immediately provide the Company with a proposed remediation plan and a timeline for its completion, all at no cost to the Company. All vulnerabilities, defects or errors of the product disclosed to the Provider will be corrected and remedied by the Provider, at the provider's expense, within thirty (30) days from the date of such report. The Company reserves the right to request this documentation to ratify the compliance of these verifications by the Provider, this documentation includes evidence of the tests, certifications of compliance in force, among others.

12.0 The Provider must always maintain adherence to the Cybersecurity policies of the Company and its subsidiaries and follow the established guidelines.

13.0 Industry standards and certifications. The Provider shall provide its Product and/or Service in accordance with Good Safety Practices and, in particular, shall comply with and/or be certified in the scope of the Product and/or Service provided in accordance with the following industry standards, policies and technical standards in its most recent version: ISO / IEC 27001 the equivalent. Upon request, the Provider must send its certificate and / or attestations, including declarations of applicability to IEnova, as well as all additional applicable and available Provider certifications or other evidence of capabilities requested in the context of Cybersecurity (e.g., ISO/IEC 27018, BSI C5, Cloud Security Alliance, IEC 62443-4-1, PCI-DSS, HIPAA). To prevent the Provider's relevant cybersecurity certifications from expiring during the term of the Agreement, the Provider agrees to continuously recertify for any relevant system used in the provision of the Product and/or Service prior to the expiration of any existing certification. The Provider must inform the Company immediately if any of the relevant certificates lose their validity. The Provider shall also comply with all applicable laws and regulations relating to the Product and/or Service.

14.0 Right to Inform. The Company and the Provider have the right to inform the organizations of public vulnerability reports in the National Territory about any defect or configuration condition that results in vulnerabilities to the information handled by the delivery, the delivery itself or other hardware, software or systems that would put the Company and /or the interests of the Company at risk.

15.0 Destruction of information and data. The Provider agrees that in accordance with the company's registration schedule or in agreement with the contract administrator the applicable data retention period will be established in the Instrument, on the data that is no longer necessary or, at the request of the Company, the Provider will destroy the data in a way that will make them completely unusable and irrecoverable , and provide the Company with a certificate of destruction, at the company's request. The Provider must return or destroy the data after the termination or expiration of the contract revokes all access to information and data owned by IEnova. The Provider must certify that the data owned by IEnova has been deleted or destroyed.

16.0 Formal Documentation. The Provider agrees to provide formal documentation to the user of the Company of the services contracted for the use, maintenance, and secure implementation of the Provider's product. The product documentation will be updated within thirty (30) days of the product update, patch, or similar change. The product documentation will include, among other things, an inventory of all components, a list of all system accounts (i.e., generic and/or default), configurations, cybersecurity controls, and dependencies. The Provider shall disclose in writing all known methods of administering the product, including, but not not known, undocumented user accounts and all commands, configurations and operations used to administer the product.

17.0 Network connection. If a connection is required between the Company and the Provider's network, the Provider shall provide a virtual private network solution or the Business Partner Access solution, i.e. other service providers) of the Company shall be used.

18.0 Assurance reports. At the request of the Company, but not more than once a year, the Provider shall provide the current SSAE-16 SOC2 Type II audit report, (and IEC 62443 if applicable) and other similar evidence/evidence (e.g., external audit reports) of a Cybersecurity Framework. The Provider shall manage the deficiencies identified in the evaluations /audits in accordance with the methods and measures for the audits defined in the Agreement. If the correctness of the audit findings has not been defined in the Agreement, the Provider shall remedy the deficiencies reported based on their severity stated in the audit reports (except where the Provider and the Company have agreed to a different correction prioritization), in a reasonable time and at no cost to the Company. After providing the audit findings, the Provider shall provide a timely work plan describing the remediation program and periodic status updates on the progress of the work plan and a statement of compliance after the completion of the work plan.

19.0 Registration and monitoring. The Provider shall record and monitor events relevant to security, including, but not related to, interfaces, changes in authorization, authentication of accounts of any kind and changes to the registration service itself, preferably backed by state-of-the-art security solutions. Tracking will be done regardless of the provision of the Service, i.e., without access to the Content. The Provider will intervene immediately in case of suspicious behavior and will carry out subsequent forensic investigations. The Provider will store such records for security-related events centrally, outside the environment of the Product and/or Service, with a retention time of at least 90 days. The Company's contractual audit rights will apply.

20.0 Prohibition of compromising functionalities. The Provider shall not include any functionality (e.g., "backdoor") in its hardware and software applicable to the Product and/or Service delivered to the Company that compromises the integrity, confidentiality and availability of hardware, software, content that are contrary to the company's interests with respect to confidentiality and security compliance. Such compromising functionality includes (i) unwanted downloading of Content, (ii) unwanted manipulation or changes to content or process logic, (iii) unwanted feeding of Content, or (iv) unwanted enhancement of functionality.

21.0 Notification obligation. The Provider shall only have the right to change or adapt the Product and/or Service provided that at least the same level of Good Safety Practices as requested and agreed between the Parties is provided. The Provider shall inform the Company prior to any relevant changes related to the Product and/or Service that may adversely affect the Provider's compliance with the Cybersecurity Requirements as set forth herein. In such a case, the rights of the Company set out in the Instrument shall apply. The Provider shall have in place an effective, documented and periodically reviewed process to inform the Company immediately in the event of any circumstances (e.g., Disaster) that materially affect the Product and/or Service, including modes of communication and interfaces.

22.0 Assessment of cybersecurity requirements. For the Service provided under the Instrument, upon the Company's request, the Provider will deliver a Cybersecurity Requirements Assessment describing the measures taken to comply with the cybersecurity requirements requested by the Company, which is based on the requirements of the Instrument and which will reflect the security levels of the corresponding offer or subsequent change requests. The Provider will deliver such evaluation preferably as part of any Product and/or Service offering, but no later than [30] days after the signing of the Instrument and before the Product and/or Service is ready and prior to any change of Product and/or Service if no otherwise agreed with the Company. Such evaluation must be implemented and fulfilled by the Provider before the Service is ready, if it is not mutually agreed otherwise, and will be subject to the prior approval of the Company. Based on the evaluation of the assessment, both Parties shall mutually define additional measures as indicated in the chapter "Additional Cybersecurity Measures", documented in a milestone plan and to be implemented by the Provider at no cost to the Company. The Company understands that the level of protection provided as described in the Cybersecurity Requirements Assessment by the Provider is subject to technical progress and development. In that sense, the Provider will have the right to implement adequate alternative protections that agree but will continue to provide at least the same level of security as requested in the respective evaluation. Other changes to the Cybersecurity Requirements Assessment will be subject to prior approval by the Company. The Provider shall inform the Company of updates to the Cybersecurity Requirements Assessment in due course and shall provide additional information and explanations (either in writing or at a workshop agreed between both Parties) with respect to such Cybersecurity Requirements if the Company so requests. Periodic changes within the Cybersecurity Requirements requested by the Company will be reviewed and implemented by the Provider in the Cybersecurity Requirements Assessment to the extent relevant to the Product and/or Service in due course after the publication of the updated Cybersecurity Requirements. Such changes to the Cybersecurity Requirements Assessment will be subject to company approval.

23.0 Data backup and recovery. The Provider shall use appropriate backup and recovery solutions and other measures to comply with the Recovery Time Objective (RTO) of [twenty-four (24) hours] and the Recovery Time Objective (RPO) of [eight (8) / hours] in the event of a disaster and (if applicable) with the emergency service levels as defined in the Instrument or related Annexes. Backups will be securely stored outside the Environment of the Product and/or Service. The Provider will create, implement and keep updated a (i) data backup and recovery and an (ii) Information Technology disaster recovery plan in accordance with the identified business requirements that will be periodically, at least once a year or after major changes, executed. Evidence of such proof will be provided to the Company upon request. For the avoidance of doubt and if necessary, a separate archived concept will be defined and agreed upon.

24.0 Availability of the service. The Provider shall continuously monitor the availability of the Service. If two outages occur in a two-hour period, the entire period from the beginning of the first outage to the end of the second outage will be considered downtime. The Provider guarantees a minimum availability of the service of [99.999] %.

25.0 Sanctions and penalties. The Company reserves the decision to decouple infrastructure, services, human resources involved from current and future activities and projects. The Company reserves the decision to penalize, through limiting the payment of one month of cost of the service or the proportional as appropriate during the first incident, in the event of a second recidivism, the Company may rescind the Instrument.

26.0 Conflicts. Nothing contained herein shall be construed as limiting in any way the obligations of the Provider contained elsewhere in the Instrument, including, but not limited to, the terms and conditions contained in the main body thereof. In the event of a conflict between the Instrument and this document, solely in relation to everything related to Cybersecurity, this document shall prevail.

Section 1 – Cybersecurity Requirements for Cloud Service Providers

In addition to and in addition to the cybersecurity requirements previously stated, the Provider must comply with the following guidelines if it offers services or products in the cloud.

1. The Provider shall provide at no additional cost to the Company a copy of a SOC 1 and SOC 2 - Type II report of the SSAE SSAE 1 and SOC 2 Statement on Standards for Attestation Engagements 16 (SASE 16) (and where applicable any successor category of audit reports, collectively "SOC Report") covering internal controls over financial reporting associated with services provided and hosting facilities. The SOC Report will include, without limitation, controls for data management based on five "trusted service principles": security, availability, integrity of processing, confidentiality and privacy. The SOC Report will cover a period of 12 months as defined by the Company and will be made annually by the service provider chosen by the Provider. The Provider will provide the latest available reports, or report covering a requested period, to the Company within 30 days of the request. If any SOC Report is subject to qualification or reveals material deficiencies in internal controls and procedures related to operations, services and products, the Provider shall develop and submit to the Company a plan to cure and correct such deficiencies ("Remediation Plan") within 10 business days of the completion of the SOC Report and commence implementation of the Remediation Plan promptly after approval of the Remediation Plan Remediation by the Company, or within another time frame agreed by the Parties.

2. If the products or services delivered by the Provider contain software, firmware, or chipsets:
   a. The Provider will implement the appropriate standards, processes and methods to prevent, identify, evaluate and repair any vulnerabilities, malicious code and security incidents in products and services that are consistent with the good practices and standards of the cybersecurity industry.
   b. The Provider will implement the appropriate standards, processes and methods to prevent, identify, evaluate and repair any vulnerabilities, malicious code and security incidents in products and services that are consistent with the good practices and standards of the cybersecurity industry.

c. The Provider will continue to support and provide services to repair, update and maintain products and services, including the provision of patches to the Company to remediate vulnerabilities during the reasonable life of the products and services.

d. The Provider shall provide the Company with a bill of materials identifying all third-party software components contained in the products. Third-party software will be up-to-date at the time of delivery to the Company.

e. The Provider will grant the Company the right, however, The Company will not be obliged, to test or have tested products for malicious code and vulnerabilities at any time, and will adequately support The Company in these exercises.

f. The Provider will provide the Company with a contact for all information security-related issues (available during business hours).

3. The Provider shall immediately inform the Company of all relevant information security incidents that have occurred or are suspected and vulnerabilities discovered in any operation, service and product provided by the Provider, to the extent that the Company is materially affected or is likely to be materially affected.

4. The Provider shall take appropriate measures to ensure that its suppliers are bound, within a reasonable time, to obligations similar to the provisions of this section.

5. If the Provider develops the product/software exclusively for the Company, the Provider will provide the Company with all related documentation and the source and readable code and software object code developed or converted for the Company.

6. The Company has the right to audit the Provider annually without cause and, in addition, if the Company has a justified suspicion that the Provider does not fully comply with these provisions, in each case upon reasonable notice. The audit covers the services contracted under the Instrument. In case of breaches it will be necessary for the Provider to present to the contract administrator a mitigation plan with established deadlines. The Company reserves the right to terminate the Instrument for breaches.

IN TESTIMONY OF THE FOREGOING, the Provider signs conformity on the day [•] of [•] of [•].

[•]

____

[•]

Legal Representative