Cybersecurity - Applicable Clauses

This document establishes the cybersecurity clauses that the Naturgy group applies in the contracting of services or products from third parties to ensure the cybersecurity of its supply chain.

In the event that the contracted service or product has specific cybersecurity clauses, which must in any case have been agreed upon with the Naturgy group's Cybersecurity, that set of cybersecurity clauses will prevail over this document.

For any inquiries regarding this document, the supplier may contact their designated point of contact of the Naturgy group, who, if necessary, will involve Naturgy's Cybersecurity Unit applicable in each case.

The clauses are structured into four sections based on the types of the services or products contracted. Depending on the specific service or product, the supplier must comply with the clauses outlined in one or more sections.

1) General Clauses

Mandatory compliance for any contracted service or product, including those that by their nature do not involve the use of Naturgy group´s technological assets or the handling of the Naturgy group´s non-public information.

These measures aim to ensure cybersecurity governance within the supply chain and the communication between the parties in the event of a potential cybersecurity incident.

2) Clauses applicable when handling the Naturgy group´s private information

Mandatory compliance when the service involves processing, accessing, or storing Naturgy´s non-public information, including personal data, even if there is no direct access to the Naturgy group's information networks or technological infrastructure. Examples, but not exclusive, of this category can be consulting services, advisory services or SaaS services.

These measures are intended to safeguard the availability, confidentiality and integrity of the Naturgy group's private information accessed or managed by the provider, minimizing the risk of data leaks.

In the event that the service corresponds to this group, compliance with the clauses outlined in the section 1 is also mandatory.

3) Clauses applicable when accessing Naturgy group´s networks, systems or technological infrastructure

Mandatory for all products and/or services that require the use of the Naturgy group´s email or user accounts, or access to systems, information or industrial process networks, data centers (CPDs) or cloud infrastructures of the Naturgy group. Examples, but not exclusive, of this category can be contact center services, emergency services, technologists with access to industrial networks, construction management or operation and maintenance of information and communications systems.

These measures are intended to minimize the risk of a cybersecurity incident within the supply chain being transmitted to the Naturgy group's infrastructures and systems.

In the event that the service corresponds to this group, compliance with the clauses outlined in the sections 1) and 2) must be required.

4) Clauses applicable to the delivery of a product or development

Generally applicable to all products and/or services in which the supplier generates, develops or supplies specific products, focusing on delivery terms, quality and compliance with specifications. Examples, but not exclusive, of this category may be suppliers that develops software or manufacture industrial equipment, either within or outside the Naturgy's facilities.

These measures aim to ensure basic cybersecurity in the delivery of products to the Naturgy group.

If the service meets the conditions of this group, it must comply with the conditions of group 1 in any case, and with the conditions of groups 2 and 3 if applicable .

1) General Clauses

ID	Clause
Governance and Regulation	
GR_01	The PROVIDER must at all times comply with all applicable legal, regulatory, and contractual cybersecurity requirements, with a particular emphasis on those related to critical infrastructures, essential services and data protection. This commitment shall apply to all locations and infrastructures where Naturgy group information is stored, processed, or transmitted. By way of example and without limiting the above, the PROVIDER must comply, when applicable, with the provisions established in the NIS 2 Directive (and its local transposition), the Cyber Resilience Act, as well as any other applicable cybersecurity legislation or regulation.
GR_02	The PROVIDER must guarantee that all the tools used to provide the service to the Naturgy group do not infringe upon third-party intellectual property or contractual rights.
GR_03	At the beginning of the contract, the PROVIDER must designate a technological risk manager, who will be the sole interlocutor with the Naturgy group on cybersecurity matters and will be responsible for ensuring the integrity, reliability and availability of the systems involved in the service.
GR_04	The PROVIDER must identify potential risks and impacts that may exist in the service and implement the compensatory measures adopted to eliminate or mitigate these risks. Any cybersecurity liability exceptions must be documented in the contract.
GR_05	If the PROVIDER has a cybersecurity standard certification, it must be renewed according to the stipulated certification timelines. In the event of certification loss, it must be notified to the Naturgy group in the shortest possible time.
Training and awareness	
FO_01	The PROVIDER must have a continuous and updated cybersecurity training and awareness program, to help mitigate risks that could impact the service provided to the Naturgy group.
FO_02	The PROVIDER must verify, prior to hiring, the cybersecurity skills of employees/external parties for the performance of their functions and provide evidence of such verification to the Naturgy group, if required.

ID	Clause
FO_03	At the discretion of the Naturgy group, the PROVIDER's participation in cybersecurity training may be requested, including, but not limited to, participation in internal cyber exercises involving the contracted service.
Segregation of duties	
SD_01	The Naturgy group's information must only be accessible by authorized personnel to carry out their functions. The PROVIDER must keep access permissions to the Naturgy´s information (in digital or physical format) updated and monitored. These personnel, including subcontractors, must be individually identified by name. Permissions must be assigned and granted following the principle of least privilege (PoLP), using groups or roles that define collective profiles, avoiding assigning privileges directly to specific users.
SD_02	The PROVIDER must have a periodic review procedure for access permissions and controls to the Naturgy group's information, and ensuring that they are updated as needed, with special attention to revocation once they are no longer required (for example, in cases of role changes or service termination).
SD_03	The PROVIDER must have segmented the networks of its organization and maintain the necessary security levels in each network segments. Users must have a minimum necessary connection allowed to carry out their own functions.
Integrity and confidentiality	
IC_01	The PROVIDER will only access the information of the Naturgy group when strictly necessary for the provision of the service and undertakes to maintain the security and absolute confidentiality of the information shared within the context of the provision of the service. Such access must be maintained within the limits of its authorized purpose.
IC_02	The PROVIDER will only store permitted information and will refrain from storing any information without the knowledge and express authorization of the Naturgy group. In addition, the PROVIDER must implement a procedure to manage the output of information assets from its facilities within the Naturgy group's service. Mechanisms must be implemented to prevent the output of information from the devices that process the Naturgy group's information. In the event that the operation requires the transfer of information from the systems, it must be encrypted.

ID	Clause
IC_03	Specifically, the PROVIDER will guarantee that the information of the Naturgy group will not be transmitted to third parties or unknown technological assets without the prior and explicit authorization of the Naturgy group.
IC_04	The PROVIDER must guarantee the secure storage and encrypted transmission of the passwords related to the service provided to the Naturgy group.
IC_05	PROVIDER shall implement and maintain appropriate security measures to ensure the integrity and immutability of logs and backups.
IC_06	The PROVIDER must establish mechanisms that allow the dissociation, anonymization, obfuscation or tokenization of data or information that is subject to rules and/or regulations belonging to the Naturgy group.
Physical Security	
SF_01	The PROVIDER must establish appropriate security measures for the storage of Naturgy group information in physical format, ensuring a level of protection equivalent to that of digital format.
SF_02	The PROVIDER must implement the necessary physical security measures to protect information assets, with particular attention to database and file servers, in order to prevent physical damage and unauthorized access to logical information related to the service provided to the Naturgy group.
SF_03	At the end of the service, or when appropriate in other circumstances, the PROVIDER must guarantee the use of appropriate mechanisms for media destruction or recycling, as well as the secure deletion of information related to the service provided to the Naturgy group, in both physical and logical format, to ensure that transactions and other data cannot be recovered by unauthorized persons.
SF_04	In the event that the PROVIDER requires physical access to the Naturgy group's facilities, it must comply with the Naturgy group's regulations regarding physical access to its facilities.
Asset Management & Operations	
GO_01	The PROVIDER must identify its information assets involved in the service provided to the Naturgy Group, the data to be managed and the individual responsible for its management, guaranteeing their proper protection and registration.

ID	Clause
GO_02	The PROVIDER shall be responsible for developing and/or implementing security mechanisms, based on the latest versions of best practices and international standards, to ensure the optimal functioning of all information assets, including mobile and portable devices, as well as any newly acquired or developed applications or systems that are used in the contracted service or in communications with the Naturgy Group. Singularly but not exclusively, the PROVIDER must have a vulnerability management process in its hardware or software components, so that these components are updated in terms of versions and, specifically, any weakness or critical vulnerability in them is addressed urgently. Security updates, or any other necessary updates must be tested in pre-production environments before deployment to assess effectiveness and any potential collateral effects on the service provided to the Naturgy group.
GO_03	The PROVIDER must have permanently updated antivirus or EDR (end point protection and response) protection on user systems and equipment involved in the service provided to the Naturgy group. Access to the administration of this tool should be restricted to key personnel.
GO_04	PROVIDER must implement authentication mechanisms that guarantee unequivocal communication with the Naturgy group.
GO_05	The PROVIDER must establish robust mechanisms that verify the sender´s identity communications with the Naturgy group.
GO_06	PROVIDER must guarantee the correct recording of the information by means of time synchronization (NTP) across all the service components, as well as between the different network elements and their associated systems.
GO_07	The PROVIDER must carry out maintenance tasks on the technological infrastructure used in the service provided to the Naturgy group to prevent potential damage or breakdowns.
Cybersecurity Incident Response	
RI_01	The PROVIDER must notify the Naturgy group of any cybersecurity incidents affecting its data and/or services as soon as they are detected. The notification will be made in such a way as to always allow the Naturgy group to comply with the response times established in the current legislation.

ID	Clause
	Specifically, and without limitation, the PROVIDER must immediately notify the Naturgy group upon detecting or having a well-founded suspicion that systems, media or data have been compromised or used without authorization within the scope of the service, as well as any exposure or leakage of information of the Naturgy group This notification shall be made via e-mail to the SOC of the Naturgy group (soc@naturgy.com). If the PROVIDERS's email is unavailable, the PROVIDER must contact the designated Naturgy group point of contact through alternative means. In the event of a data leak, the point of contact at the Naturgy group must be contacted in parallel. In the security incident notification, the PROVIDER must provide all the information and evidence required by the Naturgy regarding the incident.
RI_02	Likewise, in the event of a security incident at the Naturgy group related to the service provided by the PROVIDER, the latter must provide support and assistance as required.
RI_03	For all the above, the PROVIDER is typically expected to have a security incident management and reporting procedure, which must be periodically reviewed and tested by the PROVIDER.
Third Party Management and Outsourcing	
SC_01	In the event that the PROVIDER engages a subcontractor company for the provision of services related to this agreement, the PROVIDER commits to ensuring that such subcontractor complies, at a minimum, with the same cybersecurity requirements set forth herein. In the event of any breach by a subcontractor, the PROVIDER shall assume full responsibility and implement the necessary corrective measures to resolve any cybersecurity incident.
SC_02	The Naturgy group reserves the right to review and approve any subcontractor proposed by the PROVIDER in advance. The Naturgy group may, at its sole discretion, reject the use of any subcontractor if it determines that the subcontractor does not comply with the cybersecurity requirements specified in this document or if its participation poses an unacceptable risk to the information security of the Naturgy group.

ID	Clause
Cybersecurity Assessments	
EC_01	The PROVIDER may be subject to review to verify compliance with the clauses included in this contract and must provide the necessary evidence and information to ensure such compliance. In the event of non-compliance with any clause in this contract, the PROVIDER must implement the necessary corrective measures to eliminate or mitigate the identified risk.
EC_02	The PROVIDER must facilitate compliance with the inspection, supervision and review obligations of the Naturgy group, which may be carried out by: (a) any competent regulator authority in the matter, (b) the internal review unit of the Naturgy group or any of its local units, either directly or through a third party designated for this purpose, and (c) its auditors in the exercise of their responsibilities. This applies all aspects of the services provided to the Naturgy group and any related information. Those responsible for the inspection or review shall have unrestricted access to the PROVIDER's facilities, equipment, systems and documents, provided they are related to the services for the Naturgy group. Any information obtained will be treated as confidential by both parties.
EC_03	Reviews and inspections of the PROVIDER or its subcontractors, where information from the Naturgy group is handled, may be conducted during normal working hours with a minimum notice of fifteen (15) days, specifying the purpose and justification, to minimize disruptions to business processes. The PROVIDER must provide the necessary resources for the analysis and resolution of incidents, allowing the Naturgy group to investigate system logs and other security elements, ensuring their integrity for at least seven (7) days from the notification and safeguarding any relevant evidence for a potential forensic copy. If the Naturgy group appoints a third party for the cybersecurity review, the PROVIDER may object in the event of a conflict of interest, in which case the Naturgy group shall appoint another third party with proven expertise. Before verification, the PROVIDER may request a confidentiality agreement under customary terms.
EC_04	In the contracted service or product is SaaS and holds a SOC1, SOC2 type 2 or High level ENS certification, cybersecurity reviews may, by mutual agreement, be replaced by the annual submission of certification renewal reports.
Artificial Intelligence	

ID	Clause
IA_01	In the event that the PROVIDER wishes to use tools that contain solutions, models, systems, or components of artificial intelligence (hereinafter, "AI Systems"), they shall inform the Naturgy Group before initiating the use of such AI Systems, and such use shall be subject to the prior written authorization of the Naturgy Group.
IA_02	When the PROVIDER uses, develops, or deploys AI Systems within the scope of the Service provision, it shall ensure by default the application of the principle of personal data minimization, so that only data that is strictly necessary and essential is processed, and shall apply pseudonymization and anonymization techniques as necessary to ensure effective compliance with said principle.
IA_03	Under no circumstances shall the PROVIDER use personal data owned by the Naturgy Group for the purpose of training, configuring, improving, scaling, developing, or optimizing such AI Systems.

2) Clauses applicable when dealing with private information of the Naturgy group

ID	Clause
Governance and Regulation	
GR_06	The PROVIDER must be aware of and comply with the Naturgy group's regulatory framework, particularly the policies related to the management of logical access to the group's information, and it is the PROVIDER´s responsibility to stay updated on any changes or updates to these policies. The PROVIDER shall ensure that all subcontractors understand and adhere to the cybersecurity policies, procedures and controls specified by the Naturgy group. In general, the PROVIDER shall first adapt to the existing security measures implemented by the Naturgy group, if any limitation prevents their adoption, the PROVIDER must justify it to the Naturgy group and provide an alternative protection measure of equal or greater security, ensuring that it allows for monitoring and oversight with the same guarantees and scope as the Naturgy group´s internal cybersecurity.
GR_07	In the event that a SaaS service or product is contracted from the PROVIDER, it must be properly secured and encrypted, with a SOC 2 Type 2 or High Level ENS certification for the contracted service. Certification is not mandatory if the contracted SaaS service or product supports Naturgy business process(s) classified as “Low” in the BIA (Business Impact Analysis), although mid-level ENS certification is recommended. In any case, if Naturgy group customers access the contracted website, it must have an Extended Validation certificate.
GR_08	In the event that a SaaS service or product is contracted that is relevant for Naturgy group’s internal control over financial information, in addition, that service or product must also have a SOC 1 type 2 certification for the contracted service.
Access Control	
CA_01	The PROVIDER must implement and communicate the appropriate perimeter logical security measures to protect the information of the services contracted by the Naturgy group.
CA_02	The PROVIDER shall establish and maintain a comprehensive password management procedure for the systems involved in the service to Naturgy. This procedure must include, among other aspects:

ID	Clause
	1. The mandatory change of the initial password. 2. Minimum requirements for a minimum length and level of complexity of passwords. 3. Password expiration. 4. Restrictions on reusing previous passwords. Additionally, the PROVIDER must include a password distribution procedure in its password management policy, ensuring that the password is only known by the user for the provision of the service offered to Naturgy.
CA_03	The PROVIDER´s technological infrastructure, when storing or processing Naturgy group information, must implement the logical separation measures in shared infrastructures with other customers or multitenant services. In addition, it must ensure the isolation of each service/client to prevent the spread of attacks between clients.
CA_04	If the service or product contracted by the Naturgy group includes databases hosted on the PROVIDER´s infrastructure, these must be located on separate systems from those used for the execution of the associated applications. In addition, there must be no direct communication between the internet these databases, and an intermediate technological component must be used to manage such access.
CA_05	Critical functions, e.g. administration, of the PROVIDER must be identified and separated from non-critical functions, e.g. regular operation.
CA_06	The PROVIDER must establish the necessary measures to ensure that access to the system administration tools of the service provided to Naturgy is strictly limited to key personnel. Depending on the criticality of the activity, Naturgy will coordinate with PROVIDER to determine the need for robust authentication, both at the password management level and at the two-factor authentication level for personnel performing administrative functions. In addition, the PROVIDER must implement the necessary mechanisms to ensure that administrators access to the information systems that provide services to the Naturgy Group is conducted using encrypted channels and strong authentication.
CA_07	The PROVIDER must implement the mechanisms to continuously monitor and control remote access to the technological environment of the service provided to the Naturgy group, preventing unauthorized access and ensuring the security of information.
CA_08	The PROVIDER must monitor and record all the access activity related to Naturgy groups-owned information and securely store these records for a minimum period of

ID	Clause
	fifteen (15) months. These measures are especially critical when accessing identifiable and sensitive information belonging to Naturgy group customers.
CA_09	The PROVIDER must agree with the Naturgy group on a service termination procedure that includes information security considerations. This procedure must include at least: 1. The return of all Naturgy groups assets and information under conditions that allow their reintegration into the Naturgy's systems. 2. The secure retention of relevant service-related logs and records. 3. The secure deletion of all Naturgy group information stored on the PROVIDER's systems, ensuring that it cannot be recovered or used.
CA_10	The PROVIDER must ensure, within its internal access management process, that any access to Naturgy information is revoked once it is no longer necessary (e.g., role changes or service cancellations).
CA_11	The PROVIDER must guarantee that all the resources used in the provision of the service are protected with multi-factor authentication (MFA).
Integrity and Confidentiality	
IC_07	Sensitive information must never be transmitted via email but must instead be exchanged through dedicated communication gateways between the Naturgy group´s and the PROVIDER´s systems.
IC_08	The PROVIDER must implement the necessary controls to ensure the integrity of the Naturgy group's private information. That is, controls designed to prevent unauthorized modifications to the data. In addition, the PROVIDER must conduct verification processes to assess the effectiveness of these controls.
IC_09	In the specific case of confidential information, the PROVIDER must sign a confidentiality agreement with the Naturgy group and ensure its compliance. The PROVIDER must establish procedures and mechanisms for classification, considering applicable legal requirements, as well as the criticality and sensitivity of each type of information. Furthermore, the PROVIDER must assist in classifying Naturgy group-owned or operated assets based on the Naturgy group´s current classification framework.
IC_10	In communications with customers, the PROVIDER must use the necessary tools to ensure that such communications are conducted in a manner that guarantees the integrity of the information sent from Naturgy.

ID	Clause
Encryption and data protection	
CP_01	The PROVIDER shall not use real data or information from the Naturgy group in any environments other than authorized production or testing environments. In the event that real data is required, the PROVIDER must obtain the explicit consent of the owner and the person responsible for the data.
CP_02	The PROVIDER must have the capacity to encrypt Naturgy group information using robust and recognized encryption algorithms. This encryption must be applied to both the temporary and permanent storage of such information on the PROVIDER´s systems. In addition, the PROVIDER must ensure that the implemented encryption mechanisms comply with current security regulations and standards.
CP_03	The PROVIDER must enforce data and communications encryption for transmissions over public and/or private networks that handle information related to Naturgy group´s service, especially when dealing with confidential data or data subject to regulatory requirements, thereby protecting the information against unauthorized disclosure.
Bastioning and Threat Protection	
BP_01	The PROVIDER must implement the necessary security controls, mechanisms and tools to detect and manage threats across all the PROVIDER's information assets, including those that store or process Naturgy group information, with the objective of preventing, mitigating and appropriately alerting the Naturgy group. These measures must be periodically reviewed and updated to ensure their effectiveness.
BP_02	Specifically, the PROVIDER must install behavioral analysis capabilities in any information asset that processes, stores, or accesses Naturgy information, enabling detection and response to unknown threats (EDR).
Technological and business continuity	
PC_01	The PROVIDER undertakes to implement and maintain a business continuity plan that guarantees the uninterrupted provision of the service to Naturgy in the event of significant disruptions. This plan should be periodically reviewed to identify and mitigate new potential risks that may affect business continuity and must be regularly tested to ensure its effectiveness and make necessary adjustments.

ID	Clause
	The PROVIDER shall provide the Naturgy group with periodic reports on the status and effectiveness of the business continuity program, as well as any significant updates or changes thereto.
PC_02	The PROVIDER must regularly perform backup copies of the systems and/or information involved in the provision of services to the Naturgy group in order to allow it to recover in the event of a disaster. The PROVIDER must have the necessary procedures in place to generate backups of the Naturgy group´s service data. These copies must be stored in alternative locations to those that support the usual operations.
PC_03	The PROVIDER must implement the necessary measures, both physical and logical, to ensure the correct handling of the backup copies of the information related to the provision of the Naturgy group's service. These copies must be correctly managed and stored to enable recovery without compromising the security and integrity of the information throughout its chain of custody.
PC_04	The PROVIDER must maintain a detailed and up-to-date Disaster Recovery Plan (DRP) for all the systems involved in the Naturgy group´s service provision. This plan must include specific procedures for the rapid and effective restoration of critical systems in the event of disasters, ensuring service continuity. In addition, the DRP must include periodic testing and regular reviews to ensure its effectiveness and be in accordance with current best practices and regulations, personnel involved in the recovery processes, detailed activities and responsibilities for each participant, notification procedures to the Naturgy group and a decision-making escalation tree. Likewise, the PROVIDER must train its personnel in the execution of this plan to minimize the impact of any interruption in the service.
PC_06	The PROVIDER shall implement immutable and offline backups to protect the data.

3) Clauses applicable when accessing networks, systems or technological infrastructure of the Naturgy group

ID	Clause
	Network Security and Connectivity
RC_01	Access to the Naturgy group's infrastructures and systems must be conducted in accordance with the group's policies in force at all times, including, where access to industrial process networks is required, the Naturgy group's industrial safety policies, based on the IEC-62443 standard. Specifically, the general solution for accessing Naturgy group systems that are not published on the Internet shall be the Zero trust solution that the Naturgy group will make available to the third party and that the third party must use.
RC_02	The PROVIDER, within its area of responsibility, must implement the necessary mechanisms to ensure that communications between its infrastructure and that of the Naturgy group preserve the confidentiality, integrity and availability of information, limited to the requirements of the service.
RC_03	Depending on the access modality, the Naturgy group's network and system access policies may require the PROVIDER to implement additional cybersecurity controls for access terminals involved in the provision of the service. Including, but not limited to, installing specific up-to-date security components on workstations that meet a minimum set of security requirements. Specifically, the Naturgy group reserves the right to apply risk analysis techniques to any device and/or user who want to connect to assets of the Naturgy group, not allowing access if risk of the connection is considered inadmissible by the automated risk analysis algorithms. These risk analyses will be performed using "conditional access" and "posture" techniques. The foregoing includes, among other options, the possibility of requiring the use of MFA for accessing the assets, based on the cybersecurity and risk management context that it considers appropriate for access control. Due to this fact, the PROVIDER must guarantee that all the resources involved in the provision of the service can be authenticated using multifactor.
RC_04	The PROVIDER must notify the Naturgy group, immediately of any users under its responsibility who cease to provide services and have logical access to the Naturgy group systems, enabling the Naturgy group to promptly revoke access.
RC_05	As part of the Naturgy group's threat and incident response plans, the PROVIDER's access to the assets and networks of the Naturgy group may be suspended or restricted in the event

ID	Clause
	that it is detected that the PROVIDER's situation represents a threat to the security of the assets of the Naturgy group.
RC_06	In the event that the PROVIDER accesses the Naturgy group's systems, it must at least consider its collaboration in the periodic tests of the Naturgy group's DRP (Disaster Recovery Plan).

4) Clauses applicable when a product or development is delivered

ID	Clause
Secure Product or Development	
	In the event that the scope of the PROVIDER's work includes software development, such development shall be carried out in accordance with the best security practices established in internationally recognized frameworks and mutually agreed upon by both parties. The PROVIDER shall ensure the implementation of security measures from the early stages of the software development lifecycle, including data validation and sanitization, secure authentication and authorization, and the protection of sensitive data through encryption.
PD_01	The PROVIDER must provide technical information on the resources that it will serve the Naturgy group, enabling application compatibility tests can be carried out before implementation. In the event of substantial modifications (updates, improvements, patches, etc.) to the certifications or security measures that apply to the service provided to the Naturgy group, the PROVIDER must provide the necessary information to the Naturgy group in order to be able to resolve any possible incidents arising from these modifications. In particular, the PROVIDER must have means that guarantee the compatibility of updates, patches and configurations with the rest of the system, through manufacturer validations or by providing evidence of compatibility in non-production environments.
PD_02	The PROVIDER must immediately notify any change or loss in the cybersecurity and data protection certifications or brand approvals and shall be liable for any damages that may be caused to the Naturgy group. In addition, the PROVIDER must present the alignment of its product and service with any international and/or national certification that is recommended or required for the implementation or deployment of the product in an industrial or IT environment owned by the Naturgy group.
PD_03	The PROVIDER must establish security controls in relation to the acquisition or development of new applications or systems for the provision of the service to the Naturgy group. It must have a segmentation between the development, testing and production environments for the applications of the Naturgy group's service. They must carry out any type of security review, development, update or purchase any component of the system incorporated in the service provided to the Naturgy group in environments other than production.

ID	Clause
PD_04	In the event the PROVIDER carries out software developments, it must apply techniques and standards aligned with the best practices of secure development established in internationally recognized frameworks, guaranteeing the implementation of security measures from the initial phases of the software development life cycle, including data validation and sanitization, secure authentication and authorization, and protecting sensitive data through encryption
PD_05	In the event that the PROVIDER provides industrial products or projects to the Naturgy group, they must be aligned with the Naturgy group´s industrial cybersecurity architectures and industrial cybersecurity standards, specifically with the IEC 62443 Standard, specifically, and not exclusively, in: 1. Cross-network segmentation. 2. Remote access for operation and maintenance. 3. Antivirus management, robustness and/or patching. 4. Life cycle. These measures must be reviewed and updated as a priority and periodically to ensure their effectiveness. The PROVIDER must identify and communicate the risks and countermeasures related to the product and its integration with Naturgy infrastructures. From a cybersecurity perspective, you will need to explicitly answer the following questions: 1. What are the risks of the product and/or solution? 2. What risks may arise when integrating the product with Naturgy infrastructures? 3. What measures are in place to protect both the product and infrastructure from the risks identified above?
PD_06	All software developed or delivered by the PROVIDER must undergo vulnerability analysis with recognized tools such as SAST and DAST before being delivered to Naturgy for implementation in production environments.
PD_07	The PROVIDER will validate the security of integrations with Naturgy group infrastructures, ensuring that they do not compromise the operation or cybersecurity of existing systems.

Glossary of Terms and Abbreviations

- **AES-256:** Advanced Encryption Standard.
- **DAST:** Dynamic application Security testing.
- **DRP:** (Disaster Recovery Plan).
- **ENS:** National Security Scheme.
- **EDR:** Endpoint detection and response.
- **GDPR:** General Data Protection Regulation.
- **IEC-62443:** Global Standard for Cyber Security in Industrial Systems.
- **MFA:** Multi-factor authentication.
- **NTP:** Network time protocol.
- **PoLP:** Principle of least privilege.
- **Posture:** A device's compliance status against defined cybersecurity controls, assessed to determine if it meets the minimum requirements to access a network or system
- **SaaS:** Software as a Service.
- **SAST:** Static application security testing.
- **SOC:** Operations Center.
- **SOC 1:** Report that assesses an organization's internal controls related to financial reporting.
- **SOC 2 Type 2:** Report that assesses an organization's internal controls over security, availability, integrity, confidentiality, and privacy.
- **TLS 1.2:** Trasport Layer Security 1.2.
- **Zero trust:** A security model that eliminates implicit trust and requires continuous verification of the identity and permissions of all users and devices.