Cybersecurity - Applicable Clauses

This document establishes the cybersecurity clauses applicable by the Naturgy group in the contracting of services or products from third parties, in order to ensure the cybersecurity of its supply chain.

These clauses are structured in four sections according to the typologies of the services or products contracted. Depending on the type of service or product, the supplier must comply with the clauses of one or more sections.

1) **General Clauses**
   Mandatory clauses for any contracted service or product, including those that by their nature do not involve the use of technological assets of the Naturgy group or the handling of non-public information of the Naturgy group.

   These measures are aimed at ensuring cybersecurity governance in the supply chain that guarantees the continuity of the service provided to the Naturgy group, and communication between both parties in the event of potential cybersecurity incidents.

2) **Clauses applicable when dealing with private information of the Naturgy group**
   Set of clauses that applies when the service processes, accesses or stores Naturgy information that is not publicly accessible, including personal information, even if the Naturgy group's information networks or technological infrastructure are not accessed. Examples, but not exclusive, of this category can be: consultancy or SaaS services

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

3) **Clauses applicable when accessing networks, systems or technological infrastructure of the Naturgy group**
   applicable for all products and/or services that require an email address or user of the Naturgy group or access to systems, information networks or industrial processes, data centers 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, operation and maintenance of information and communications systems, etc.

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

   If the service corresponds to this group, the clauses of group 2 must also be complied with.

4) **Clauses applicable to the delivery of a product or development**
   Of general application for all products and/or services in which the supplier generates, develops or supplies specific products, focusing on terms of delivery, quality and compliance with specifications. Examples, but not exclusive, of this category may be: suppliers that generate software developments or industrial equipment inside or outside Naturgy's facilities,

   These measures seek 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 groups 2 and 3 depending on its nature.

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

For any queries regarding this document, the supplier may contact its contact in the Naturgy group, which will involve the Cybersecurity function of the Naturgy group applicable in each case, if necessary.

1) General Clauses

ID	Clause
Legislation and Regulation	
CU_01	The PROVIDER must at all times maintain compliance with legal, regulatory or contractual requirements related to cybersecurity, with special focus on those referring to critical infrastructures or essential services, and data protection, including those of a personal nature, in all locations and infrastructures where your information is stored and processed.
CU_02	The PROVIDER must ensure that all tools used to provide the service to the Naturgy group do not violate the intellectual property or any regulation, contract, right or interest in the property of third parties.
Governance	
GO_01	At the beginning of the contract, the PROVIDER must appoint a technological risk manager, who will be the sole interlocutor with the Naturgy group in matters of cybersecurity and will be responsible for ensuring the integrity, reliability and availability of the systems involved in the service.
GO_02	The PROVIDER must identify the possible risks and impacts that may exist in the service, helping to validate the compensatory measures adopted to eliminate or mitigate the risk. Any exceptionality of responsibility in cybersecurity must be included and detailed in the contract.
Training and awareness	
FO_01	The PROVIDER must have a training/awareness program on information security on a regular basis, which allows its employees and/or subcontractors to know the correct action in any suspected breach of information security. It also ensures that the staff involved in the provision of customer service knows and follows the internal cybersecurity regulations applicable to the correct processing of the Naturgy group's information that they handle in the service.
FO_02	PROVIDER must verify, prior to contracting, the cybersecurity training of employees/external parties and provide evidence of this to the Naturgy group.
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.
Information Custody	
CI_01	The PROVIDER will only access the information of the Naturgy group for the provision of the service and undertakes to maintain the security of the information transferred in the context of the provision of the service.
CI_02	The PROVIDER will only store the 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 output of information from the systems, it must be encrypted.

ID	Clause
CI_03	The PROVIDER must treat the data and information of the Naturgy group with absolute confidentiality and comply at all times with the instructions received by the Naturgy group in relation to its purpose, content, use and processing.
CI_04	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 express authorization of the Naturgy group.
Physical Security	
SF_01	The PROVIDER must establish appropriate security measures for the storage of Naturgy group information in physical format, guaranteeing a level of protection equivalent to digital format.
SF_02	The PROVIDER must implement the necessary physical security measures to protect the information assets, in order to prevent physical damage and unauthorized access to logical information related to the service offered to the Naturgy group.
SF_03	The PROVIDER must guarantee the use of appropriate mechanisms for the destruction or recycling of media, as well as the secure disposal of information related to the service provided to the Naturgy group.
SF_04	PROVIDER has to properly and securely remove and destroy all instances of any Naturgy group information or data and related printed material to ensure that transactions and other data cannot be retrieved by unauthorized persons.
SF_05	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.
Technical Measures	
MT_01	The PROVIDER must identify its information assets involved in the service to the Naturgy Group, the data that will be managed and those responsible for its management.
MT_02	In general, the PROVIDER will adapt in the first instance to the existing protection measures in the Naturgy group, in the event of any impediment that does not allow them to be adopted, the PROVIDER must justify it to the Naturgy group and provide the same or greater protection and provide the means for their follow-up and monitoring with the same guarantees and scope as the internal cybersecurity measures of the Naturgy group.
MT_03	The PROVIDER shall be responsible for developing and/or implementing security mechanisms, based on the latest versions of best practices and international standards, that ensure the optimal functioning of all information assets, including mobile and portable devices, and also including any new acquisition or development of applications or systems that are used in the service contracted by, or for 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 Such security updates, or any other necessary updates, before being installed in production environments, must be tested in previous environments to assess their effectiveness and potential collateral effects on the service provided to the Naturgy group.
MT_04	The PROVIDER must have permanently updated antivirus or EDR (end point detection & response) protection on systems and user equipment involved in the service provided to

ID	Clause
	the Naturgy group. Access to the administration of this tool should be restricted to key personnel.
MT_05	PROVIDER must implement authentication mechanisms that guarantee unequivocal communication with the Naturgy group.
MT_06	The PROVIDER must establish mechanisms that ensure the identity of the sender in communications with the Naturgy group.
MT_07	The Naturgy group's information must only be accessible by authorised personnel to carry out their functions. The PROVIDER must keep updated and monitor the permissions for access to Naturgy information (in digital or physical format). These personnel, even if they were subcontracted, must be identified by name. Permissions must be assigned/granted in accordance with the principle of least privilege (PoLP, also known as the Principle of Least Privilege or the Principle of Least Authority). Privileges must be assigned/granted through the use of groups or roles (i.e., profiles that identify groups and non-privileges assigned to a specific user). The PROVIDER will ensure, within its internal access management process, that any access to Naturgy information is revoked once it is no longer necessary (for example, in cases of change of responsibilities or cancellations of service) Surveillance and assurance mechanisms must measure and monitor the process to ensure that legal, statutory, regulatory or contractual requirements related to cybersecurity and data protection are complied with, including those of a personal nature
MT_08	The PROVIDER must have a procedure for the periodic review of the permissions and access controls configured in the systems that serve the Naturgy group.
MT_09	The PROVIDER must guarantee the secure storage and encrypted transmission of the passwords for the service offered to the Naturgy group.
MT_10	PROVIDER must guarantee the correct recording of the information by means of time synchronization (NTP) between all the components of the service, as well as between the different network elements and the systems associated with it.
MT_11	The PROVIDER must have segmented the networks of its organization and maintain the necessary security levels in each of the network segments. Users must have a minimum necessary connection allowed to carry out their own functions.
MT_12	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.
MT_13	The PROVIDER must carry out maintenance tasks on the technological infrastructure used in the service offered to the Naturgy group, in order to avoid possible damage or breakdowns.
MT_14	PROVIDER shall implement and maintain appropriate security measures to ensure the integrity and immutability of logs and backups.
Cyber Incident Response	

ID	Clause
GI_01	The PROVIDER must notify the Naturgy group of 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 allow the Naturgy group to comply with the times established in the legislation in force at all times. Specifically, and without limitation, the PROVIDER must immediately notify the Naturgy group in the event that it detects or has a well-founded suspicion that the systems, media or data have been compromised or used without authorization within the provision of the service, as well as any exposure or leakage of information from the Naturgy group This notification will be made by e-mail to the SOC of the Naturgy group (soc@naturgy.com). In the event that the PROVIDER's email is not available, the PROVIDER's point of contact in the Naturgy group contact must be contacted by other means. In the event of a data leak, the point of contact in Naturgy group must be contacted in pararell. The PROVIDER must provide all the information and evidence required by the Naturgy group in relation to the incident. To this end, the PROVIDER will typically have a procedure for managing and reporting security incidents, which must be reviewed and tested by the PROVIDER periodically.
GI_02	Likewise, in the event of a security incident in the Naturgy group related to the service provided by the PROVIDER, the latter must provide support and help in everything required.
Third-Party Management and Outsourcing	
GT_01	In the event the PROVIDER engages a subcontracted company for the provision of services related to this agreement, the PROVIDER undertakes to ensure that such subcontractor complies, at a minimum, with the same cybersecurity requirements set forth herein. The PROVIDER shall ensure that all subcontractors understand and adhere to the cybersecurity policies, procedures and controls specified by the Naturgy group. In the event of any breach by a subcontractor, the PROVIDER shall assume full responsibility and take the necessary corrective measures to resolve any cybersecurity incident.
GT_02	The Naturgy group reserves the right to review and approve in advance any subcontractor proposed by the PROVIDER. The Naturgy group may, at its sole discretion, refuse the use of any subcontractor if it determines that such subcontractor does not comply with the cybersecurity requirements specified in this document, or if its participation represents an unacceptable risk to the information security of the Naturgy group.
Cybersecurity reviews and audits	
AU_01	The PROVIDER may be subject to audits in which the correct compliance with the clauses included in this contract is verified and will have to provide the necessary evidence and information to guarantee such compliance with these. In the event of non-compliance with any of the clauses included in this contract, the PROVIDER must apply the necessary corrective measures to eliminate or mitigate the risk detected.
AU_02	The PROVIDER shall facilitate compliance with the inspection, supervision and audit obligations of the Naturgy group, by the following: (a) any competent regulator in the matter, (b) the internal audit 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 obligation covers all aspects of the services provided to the Naturgy group, including any type of information asset. This includes all aspects of the

ID	Clause
	services provided to the Naturgy group and any related information. Those in charge of the inspection or audit will have free access to the facilities, equipment, systems and documents of the PROVIDER, provided that they are related to the services for the Naturgy group. The information obtained will be confidential and treated as such by both parties.
AU_03	Audits and inspections of the PROVIDER or its subcontractors, where information from the Naturgy group is handled, may be carried out during normal working hours and with a minimum notice of fifteen (15) days, specifying the purpose and justification, to minimise interruptions in business processes. The PROVIDER will provide the necessary resources for the analysis and correction of incidents, allowing the Naturgy group to investigate the logs of systems and other security elements, ensuring their integrity for at least seven (7) days from the notification of the incident, and will safeguard any useful evidence for a possible 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, and the Naturgy group will appoint another third party with accredited experience. Prior to verification, PROVIDER may require a confidentiality agreement on customary terms.
AU_04	In the event the PROVIDER is audited, the final report will be delivered by the Naturgy group to the PROVIDER. The PROVIDER must correct the control weaknesses identified in said report, following the action plans agreed between both parties.
AU_05	In the event the contracted service or product is a SaaS that has a SOC1 or SOC2 type 2 certification, by mutual agreement between the parties, the audits may be replaced by the annual delivery of certification renewal reports

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

ID	Clause
Logical segmentation and access to Naturgy information	
CA_01	The PROVIDER must be aware of and comply with the cybersecurity regulatory body established in the Naturgy group for the provision of the service, in particular, and not exclusively, with regard to logical access management. It is the responsibility of the PROVIDER to stay up to date regarding any changes or updates to such internal cybersecurity regulations. Specifically, but not exclusively, way, it will be required the installation of elements with the capacity to perform behavioural analysis for the detection and response to unknown threats (EDR) in any asset that manages or stores Naturgy information.
CA_02	In the event a SaaS service or product is contracted from the PROVIDER, it must be properly secured and encrypted, with a SOC 2 Type 2 certification on the contracted service. Whenever this website is accessed by customers of the Naturgy group, it must have an Extended Validation certificate.
CA_03	In the event a SaaS service or product is contracted from the PROVIDER, and such service or product is relevant for the internal control over the financial information of the Naturgy group, in addition, said service or product must have a SOC 1 type 2 certification on the contracted service.
CA_04	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_05	The PROVIDER must establish a password management procedure for the systems involved in the service to Naturgy. This procedure must require, among other aspects, the change of the initial password, a minimum length, level of complexity of the keys and that defines the expiration of the passwords or the number of records to avoid reuse. In addition, the PROVIDER must include in its password management policy a procedure for distributing passwords, which guarantees that they are only known by the user, for the provision of the service offered to Naturgy.
CA_06	The technological infrastructure of the PROVIDER that stores or processes information of the Naturgy group must have measures that allow the logical separation of information in the case of infrastructures shared with other customers or services with multiple customers. In addition, guaranteeing the isolation of each service/client to prevent the spread of attacks between clients.
CA_07	In the event the contracted service or product requires a database hosted on the PROVIDER's infrastructure, it must be taken into account that this database must be located in a system other than the one in which the application is executed. Additionally, there must be no direct communication from the internet to this database(s) and must make use of any intermediate technological component.
CA_08	The critical functions of the PROVIDER shall be identified and separated from the non-critical functions.

ID	Clause
CA_09	The PROVIDER must establish sufficient and necessary measures to ensure that access to the system administration tools of the service offered to Naturgy is strictly reserved for key personnel. Depending on the criticality of the activity, Naturgy will agree with PROVEEDOR on the need to use robust authentication, both at the password management level and at the two-factor level, in the access of personnel to perform their functions. In addition, the PROVIDER must implement the necessary mechanisms to ensure that the access of administrators to the information systems that provide services to the Naturgy Group is carried out using encrypted channels and strong authentication
CA_10	The PROVIDER must implement the necessary mechanisms to ensure that remote access to the technological environment of the service offered to the Naturgy group is controlled and monitored.
CA_11	The PROVIDER must monitor and record all the activity of access to information owned by the Naturgy group, and store the data of said activity in an appropriate manner for a minimum period of fifteen (15) months. These measures are especially relevant in the case of accessing identifying and sensitive information of Naturgy group customers.
CA_12	The PROVIDER must agree with the Naturgy group on a procedure for the termination of the service that includes aspects related to information security. It must include at least: the return of any information asset that belongs to the Naturgy group under conditions that allow the Naturgy group to incorporate information into its systems and infrastructures, ensuring its integrity, availability and confidentiality during the process, custody of logs, secure deletion of all information of the Naturgy group hosted in assets of the PROVIDER at the end of the process.
Physical Security	
SF_01	The PROVIDER must host all database servers, file servers and repositories owned by it that contain information from the Naturgy group in locations with reinforced physical security. The PROVIDER shall ensure the equivalent if its supply chain also stores Naturgy information.
Integrity and Confidentiality	
IC_01	The sending of sensitive information must never be done via email, but through communication gateways intended for this purpose between the systems of the Naturgy group and the PROVIDER.
IC_02	The PROVIDER must implement the necessary controls to ensure the integrity of the Naturgy group's private information. That is, controls aimed at preventing unauthorized modifications to the information. In addition, the PROVIDER must carry out verification processes of said controls
IC_03	In the specific case of information classified as confidential, the PROVIDER must sign a confidentiality agreement with the Naturgy group and guarantee its compliance. The PROVIDER must have procedures and mechanisms for classifying the information, considering the applicable legal requirements, as well as the criticality and sensitivity of each type of information. And it will help in the classification of its assets owned or operated by the Naturgy group based on the current classification of the Naturgy group.

ID	Clause
IC_04	In communications with customers, the PROVIDER must use the necessary tools to control that these occur in such a way as to ensure the integrity of the information sent from Naturgy.
Encryption and obfuscation of information	
CF_01	The PROVIDER will not use real data or information of the Naturgy group in environments other than authorised production or testing. In the event that real data is required, the PROVIDER must have the explicit consent of the owner and responsible for the data
CF_02	The PROVIDER must have the capacity to encrypt the information of the Naturgy group using robust and recognized encryption algorithms. This encryption should be applied to both the temporary and permanent storage of such information on your systems. In addition, the PROVIDER must ensure that the encryption mechanisms implemented comply with current security regulations and standards.
CF_03	The PROVIDER must establish the encryption of data and communications carried out through public and/or private networks and through which information related to the Naturgy group's service travels, especially when it is confidential data or data subject to any regulation. Protecting the information from unauthorized disclosure
Bastioning and Threat Protection	
BP_01	The PROVIDER must implement the security controls, mechanisms and tools necessary for the detection and management of the threat to all the PROVIDER's information assets, with the aim of preventing and solving them and, in the case of advanced and complex threats, alerting the Naturgy group when they are detected. They must periodically review the configurations of their information systems that store or process information of the Naturgy group.
Technological Continuity	
CT_01	The PROVIDER must periodically make backup copies of the systems involved in the provision of the service to the Naturgy group in order to allow it to recover in the event of a disaster. PROVIDER must have the necessary procedures in place to generate backup copies of the data of the service it provides to the Naturgy group. These copies must be stored in alternative locations to those that support the usual operations.
CT_02	The PROVIDER must implement the necessary measures, both physical and logical, to ensure the correct handling of the backup copies of the information relating to the provision of the Naturgy group's service. These copies must be treated and stored correctly in order to be recovered without the security and integrity of the information being compromised during the chain of custody of the same.
CT_03	The PROVIDER must have a detailed and updated Disaster Recovery Plan (DRP) for all the systems involved in the provision of the service to the Naturgy group. This plan should include specific procedures for the rapid and effective restoration of critical systems in the event of disasters, ensuring continuity of service. In addition, the DRP must include periodic tests 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 scaling

ID	Clause
	tree for decision-making. Likewise, the PROVIDER must train its personnel in the execution of this plan to minimize the impact of any interruption in the service.

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

ID	Clause
AN_01	Access to the Naturgy group's infrastructures and systems must be carried out in accordance with the group's policies in force at all times, including, in cases 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 access to Naturgy group systems not published on the Internet will be the Zerotrust solution that the Naturgy group will make available to the third party and that the third party must use.
AN_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 the information, limited to the needs of the service.
AN_03	Depending on the access modality, the Naturgy group's network and system access policies may require the PROVIDER to have additional cybersecurity controls for the access terminals that are involved in the provision of the service. Including, but not limited to, having certain updated security components installed in their workstations with a series of minimum characteristics. Specifically, the Naturgy group reserves the right to apply risk analysis techniques to the device and the user who want to connect to assets of the Naturgy group, not allowing access if the connection risk is considered inadmissible by the automated risk analysis algorithms. These risk analyses will be carried out using "conditional access" and "posture" techniques
AN_04	The PROVIDER must notify the Naturgy group of those users who cease to provide service and have logical access to the Naturgy group's systems, so that the Naturgy group can carry out the deregistration process in its area of responsibility.
AN_05	As part of the Naturgy group's threat response plans 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 that it is detected that the PROVIDER's situation represents a threat to the security of the assets of the Naturgy group.
AN_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
PD_01	The PROVIDER must provide technical information on the resources that it will serve the Naturgy group, so that application compatibility tests can be carried out before implementation. In the event of substantial modifications (updates, improvements, patches, etc.) in 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-productive environments.
PD_02	The PROVIDER must communicate any change or loss in the cybersecurity and data protection certifications or approvals of the brands immediately, and will be responsible 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 necessary 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 offered 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 of any component of the system incorporated in the service provided to the Naturgy group in environments other than production.
PD_04	In the event that the PROVIDER carries out software developments, it must apply techniques and standards aligned with good practices for secure development, for the applications offered to the Naturgy group.
PD_05	In the event the PROVIDER provides products or projects of an industrial nature to the Naturgy group, they must be aligned with the industrial cybersecurity architectures of the Naturgy group and with industrial cybersecurity standards and 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 indicate 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 the infrastructure from the risks identified above?