

Annex Cyber Security

(Integral and Substantial Part of the General Contract Conditions for Software & Cloud Italy Ed. 7.4)

Version 1.0 – July 2026

This Annex sets forth the **contractual cyber security obligations** that the Supplier shall undertake towards ENEL in connection with the provisions of Cloud Services (SaaS/PaaS/IaaS); Generic Software (on-premise/commercial); Software Development Services (coding); application support services; system support services; Telecommunications Services; Telecommunications Products; HW Computing Products; HW Computing maintenance services; Application/Infrastructure Design Services; professional Cyber Security services; and Cyber Security Products.

1.1 Architecture

Part	Content	Applicability
A	Common Clauses (25 clauses)	Always applicable
B	Conditional clauses applicable according to the Role assumed by the Supplier (30 clauses)	Applicable according to the actual role assumed by the Supplier in relation to the specific clause and the scope of the supply/service
C	NIS2 Clauses (9 clauses)	Applicable where the supply/service falls within the NIS2 perimeter or is used by NIS2 entities
D	PSNC Clauses (12 clauses)	Applicable where the supply/service supports ICT assets within the PSNC perimeter
E	Clauses pursuant to Law No. 90/2024 and the Prime Ministerial Decree of 30 April 2025 (6 clauses)	Applicable where the supply/service is classified within such scope

1.2 Definitions

OWNER – the Supplier having primary responsibility for the subject matter of the Contract, and retaining full technical, organizational and decision-making thereover. The OWNER shall be accountable for the overall intended outcome and for any failure to comply with applicable requirements, to the extent that it defines the relevant processes, methodologies, architectures, or deliverables without ENEL exercising direct control over their execution.

OPERATOR – the Supplier that operationally performs the activities covered by the Contract within a framework established or approved by ENEL. The OPERATOR shall be responsible for the proper execution of such activities but shall not be responsible for defining the standard, processes or security baselines with which it is required to comply.

SUPPORT – the role assumed by the Supplier when providing assistance, support, or advisory services to ENEL in connection with activities that remain under the responsibility of ENEL or of third parties. The SUPPORT role shall be responsible for the quality, accuracy and timeliness of the support provided, but shall not be accountable for the final outcome of the supported activity. This role typically applies where the Supplier provides consulting, training, specialist assistance, or support in authorization processes without assuming ownership thereof.

PROVIDER – the Supplier of a standardized product or service, that is made available to and replicated across multiple customers, over which ENEL has no ability to exercise direct operational control or to materially influence underlying architecture. The PROVIDER shall be responsible for the inherent quality, security by design and proper provision of the product or service.

SHARED – the circumstance in which responsibility is allocated jointly between the Supplier and ENEL or, where applicable, among multiple parties within the contractual supply chain, pursuant to an expressly defined model requiring a clear contractual allocation of the respective areas of responsibility, typically document through a responsibility matrix.

ENEL internally provides, through its dedicated internal teams, the following security platforms: *Identity Provider (IDP)*, *Identity Management (IDM)*, *Multi-Factor Authentication (MFA)*, *Privileged Access Management (PAM)*, *remote access VPN / Zero Trust Network Access (ZTNA)*, and *WAF for internal protection*. Accordingly, the Supplier shall be required to:

- maintain internally, within its own systems and environments used for the provision of the Services to ENEL, equivalent capabilities as an integral component of its cybersecurity operating model and industrial security posture;
- use exclusively ENEL provided platforms whenever the Supplier's personnel require access to ENEL systems, applications, environments, or networks, without implementing, mandating, or relying upon alternative access solutions;
- ensure that the products and services provided to ENEL are fully capable of integration with ENEL's platforms through industry-standard federation and interoperability protocols, including SAML 2.0, OpenID Connect, SCIM and similar protocols, without requiring the adoption or use of the Supplier's own Identity Provider (IDP), Privileged Access Management (PAM), Multi-Factor Authentication (MFA), Identity Management (IDM), VPN, or other access control solutions as a substitute for those provided by ENEL.

2 Part A – Common Clauses

The clauses set forth in this Part shall apply to all Suppliers, regardless of the nature, scope, or subject matter of the products or services provided. Where the relevant products or services fall within the scope of NIS2, PSNC or Law No. 90/2024 and the Prime Ministerial

Decree of 30 April 2025, the specific provisions set forth in Parts C, D and E shall be read in addition with the requirements contained herein.

- A.1 **Supplier's cyber security framework.** The Supplier represents, warrants and undertakes that, throughout the term of this Contract, it shall maintain an adequate cyber security framework within its organization, implementing and continuously operating appropriate and proportionate technical and organizational measures designed to protect its systems, infrastructures, applications, processes and information assets against cyber threats that could affect the security, availability, integrity, confidentiality, or resilience of the Services or otherwise impact ENEL. The Supplier further undertakes to perform ongoing cyber risk assessments, monitoring and management activities, and to promptly review, update and enhance its security measures in response to evolving vulnerabilities, emerging threats, technological developments, and recognized industry standards and best practices. Such cybersecurity framework shall remain appropriate and proportionate to the nature, scope, criticality, and risk profile of the products and services provided under this Contract.
- A.2 **Legislative and regulatory compliance.** The Supplier represents and warrants that: (i) it possesses adequate and up-to-date knowledge, commensurate to the subject matter and scope of the Contract, of the applicable cybersecurity legislative and regulatory framework; and (ii) its standards, procedures, processes, controls and security measures are, in all material respects, compliant with the requirements set forth under all applicable laws, regulations, directives, regulatory provisions, and relevant guidelines in force. The Supplier further undertakes to promptly notify ENEL of any event or circumstance, regulatory action, identified non-compliance, or material change that may adversely affect, impair, or call into question the foregoing representations, warranties, or compliance status.
- A.3 **Compliance with the Client's security standards.** The Supplier undertakes to comply with ENEL's cyber security standards, to the extent applicable to the products or services provided and insofar as such requirements have been duly communicated or made available to the Supplier. The Supplier represents and warrants that its employees, personnel, consultants, subcontractors and any other individuals engaged in the performance of the Contract are appropriately informed of, trained on, and bound to comply with the with the foregoing requirements. The Supplier shall ensure that such compliance is maintained throughout the entire term of the Contract and, where applicable, during any subsequent period in which obligations relating to confidentiality, information protection, data retention, return, deletion, or secure disposal continue to apply.
- A.4 **Management of the Supplier's personnel.** The Supplier represents and warrants that all personnel engaged in the performance of the Contract are appropriately identified, vetted, authorized and traceable throughout their involvement in the provision of the Services. The Supplier shall promptly notify ENEL, through the channels and procedures defined from time to time, of any addition, removal, replacement or other change involving personnel to whom identities, credentials, access rights or privileged authorizations have been assigned in connection with ENEL's platforms, systems, applications or networks, as well as personnel holding credentials or administrative privileges on the Supplier's systems used in the provision of the Services. The Supplier further represents and warrants that adequate onboarding and offboarding processes for personnel are adopted and that the principle of least privilege is applied when assigning authorizations, as well as that, to the extent permitted by applicable law, reputational checks are carried out proportionate to the criticality of the role performed and to the access to ENEL's data and systems.
- A.5 **Processing of the Client's data. The Supplier undertakes to process ENEL's data, meaning any information, structured and unstructured data, logs, configurations, content and metadata owned by or made available to ENEL, solely for the purposes set forth in the Contract and in compliance with the instructions issued by ENEL.** The Supplier further represents and warrants that it maintains adequate onboarding, role-change, and offboarding processes to protect ENEL's data against unauthorized access, loss, disclosure, alteration or destruction, in accordance with the principles of least privilege, "need to know" and "need to use", using robust authentication and authorization mechanisms and adopting continuous monitoring and logging of access and operations executed.
- A.6 **Management of access to the Client's Systems. This clause shall apply exclusively where, for the performance of the Contract, the Supplier's personnel access or use ENEL Systems.** The Supplier may access ENEL's systems and applications only upon ENEL's prior authorization and shall be responsible for all activities carried out using accounts and credentials, including, by way of example, username, e-mail, PIN, codes, secrets and passwords, provided by ENEL for the performance of the Contract. The Supplier acknowledges that ENEL internally provides Identity Provider (IDP), Identity Management (IDM), Multi-Factor Authentication (MFA), Privileged Access Management (PAM), remote access platforms (VPN / Zero Trust Network Access) and WAF for the protection of internal applications, and undertakes to use them whenever the Supplier's personnel need to access ENEL's systems, applications or networks in the performance of the Contract.. In carrying out such activities, the Supplier and its employees shall comply with the following rules of conduct:
- never share accounts or authentication credentials with anyone;
 - never include credentials, secrets or security keys in e-mail messages or other electronic communications, nor disclose them to third parties, including through voice calls or text messages;
 - never store credentials using the "remember password" function available in web browsers or desktop applications;
 - ensure that no person is able to observe credentials being entered to access ENEL Systems;
 - never use ENEL credentials to authenticate to, or register with systems or applications other than those contemplated by the Contract;
 - use ENEL network services and connections exclusively for purposes related to the performance of the Contract;
 - not carry out any activity or develop any solution through ENEL Systems in violation of applicable laws or regulations;
 - equip the systems used to access ENEL services with continuously updated anti-malware solutions;
 - provide for and implement, on the systems and devices used to access ENEL services, all security measures necessary prevent the introduction of malicious software or vulnerabilities;
 - ensure that any temporary or permanent equipment assigned for access to ENEL Systems connects exclusively through ENEL-approved remote access solutions, including ENEL VPN or through such other access methods as may be defined by ENEL which enables multi-factor authentication and ensures the integrity and confidentiality of the data processed;

- k. use exclusively e-mail accounts, file storage tools and/or communication platforms expressly provided or authorized by ENEL;
 - l. not modify system configurations in order to circumvent, bypass or disable security controls and protections.
- A.7 **Cyber hygiene of the Supplier's personnel.** The Supplier warrants that the personnel engaged in the performance of the Contract adopt cyber hygiene practices appropriate to the nature of the supply/service, including, by way of example, the exclusive use of corporate managed and regularly updated corporate workstations, the use of strong credentials and multi-factor authentication mechanisms for access to corporate resources, the proper management of removable media, and the prohibition on the use of personal or unauthorized cloud services for the processing of information related to the Contract.
- A.8 **Multi-factor authentication for access to ENEL Systems.** This clause is applicable to the Supplier, at any time, during the term of the Contract, in the event that for the performance of the Contract it is required or necessary that the Supplier has access to and/or uses any application available in ENEL's systems and/or ENEL's IT infrastructure ("ENEL System"). At ENEL's request, at any time and for any reason, the Supplier shall accept and implement the ENEL's two-factor authentication system (the "Multifactor Authentication System"), as a mandatory requirement for access to and / or use of any ENEL System. The only accepted configuration of authentication methods is (i) a unique mobile phone number (previously registered in the user database) and (ii) a smartphone compatible with the MFA Passkey method through MS Authenticator; and (iii) single MS Authenticator application associated with the single device where the unique mobile phone number resides. It is not allowed to use more than one device for both authentication methods. The Supplier, in order to use and implement the "Multifactor Authentication System", undertakes that (i) a smartphone and a functioning SIM card (business or private if the business is not available) are available; therefore, in countries where legal constraints prohibit the use of smartphones within call center buildings, Suppliers may exceptionally use an alternative MFA method proposed by ENEL. (ii) Each smartphone (or alternative MFA method proposed by ENEL) used for the purposes of the "Multifactor Authentication System" shall be associated exclusively with the personal identity of the Supplier's employee, agent, representative or other personnel who have access to and / or will use the ENEL Systems on behalf of the Supplier; and (iii) the Supplier shall comply with all the foregoing requirements at its own risk, cost and expense. ENEL does not assume any charge (economic or otherwise) for the supply of the smartphone or the alternative MFA method proposed by ENEL and shall not be liable to the Supplier or any third party for any damages, claims or losses, direct or indirect, deriving from or connected or related to the failure and/or malfunction or illegal use of any smartphone or the alternative MFA method proposed by ENEL used for the "Multifactor Authentication System" by Supplier's employees, agents, representatives or other personnel.
- A.9 **Management of privileged access within the Supplier's systems.** The Supplier warrants that privileged, administrative or high-privilege accounts on its own systems used for the provision of the service to ENEL are managed through an internal Privileged Access Management (PAM) solution, assigned on a unique named-user basis, subject to multi-factor authentication, logged, periodically reviewed and revoked when the relevant operational need ceases to exist. The Supplier further warrants that privileged sessions carried out on its own systems are managed, recorded and monitored so as to enable reconstruction of the activities performed and attribution thereof to the individual operator, and undertakes to make available to ENEL, upon reasonable request, documentary evidence of the proper management of such accounts.
- A.10 **Traceability and logging of the Supplier's activities.** The Supplier warrants that the activities carried out by its personnel, collaborators and sub-suppliers on ENEL's systems, data and infrastructures, or on the Supplier's own systems where used for the provision of the service to ENEL, are logged in such a way as to ensure traceability, integrity, non-repudiation and availability of the relevant audit evidence. The Supplier shall protect logs against unauthorized access, alteration or improper deletion, ensuring their retention for the period required by applicable law and, in any case, for a period of not less than twelve (12) months, and shall make them available to ENEL upon request, in accordance with the agreed procedures.
- A.11 **Vulnerability management.** The Supplier warrants the existence, adequacy and effectiveness of formalized processes for the identification, assessment, prioritization and remediation of security vulnerabilities that may affect the products, services, systems or components covered by the supply/service. The Supplier shall perform security checks using industry recognized methodologies and best practices, document the results in dedicated reports and share them with ENEL, upon request, together with the relevant remediation action plan. The Supplier further warrants that any identified vulnerabilities, including those reported by ENEL or by third parties, shall be assessed and remediated within timeframes consistent with their severity level.
- A.12 **Security patches and updates.** The Supplier undertakes to keep the systems, components, products, firmware and applications covered by the supply/service up to date, by making available appropriate security patches aimed at preventing and remediating known vulnerabilities, based on their criticality and within the timeframes agreed with ENEL. The provision of patches and, where required by the scope of supply, all patching activities shall be guaranteed and included in the Contract, at no additional cost to ENEL. Where immediate application of a patch is not possible, the Supplier shall provide temporary mitigations and/or alternative solutions ("workarounds") reasonable designed to prevent the exploitation of such vulnerabilities, without any additional charge. The Supplier further warrants the authenticity and integrity of the updates and patches made available or applied (including hardware, software and firmware patches and updates, including those of third parties).
- A.13 **Hardening of the supplied components.** The Supplier warrants that the products, components, systems and applications covered by the supply/service are configured and maintained in accordance with recognized security principles, by disabling unnecessary functionalities, removing default credentials, and adopting security configurations consistent with recognized benchmarks, including, by way of example, CIS benchmarks and applicable vendor security baselines, as well as with ENEL's security standards, where made available. The Supplier shall keep the hardening documentation up to date and make it available to ENEL upon request.
- A.14 **Management of security incidents.** In the event of a security incident that may compromise ENEL, its data or the services provided, the Supplier undertakes to implement all measures necessary to identify, contain, eradicate, mitigate and resolve the incident within the timeframes agreed with ENEL. The Supplier warrants the existence of formalized incident management processes, the adoption of appropriate detection, analysis and response mechanisms, as well as the availability of qualified personnel dedicated to the performance of incident response activities for the entire contractual term.

- A.15 **Notification of incidents to the Client.** In the event of violations, incidents, cyber-attacks or any other cyber-security relevant event that may have a potential impact on ENEL's Information Technology (IT)/Operational Technology (OT)/Internet of Things (IoT) infrastructures and applications or on the scope of the supply/service (hereinafter "Cyber Incidents"), the Supplier, exercising the level of skill, care and promptness required under professional standards, shall report the Cyber Incident to ENEL at the e-mail address: cert@enel.com, and to the Contract Manager. In order to effectively convey all Cyber Incidents, including potential ones, as well as any communication regarding cyber security, the Supplier designates and keeps updated a Cyber Security Referent and at least a delegate, contactable by email and telephone by completing the "Company contacts" document (Cyber Security)", available on the WeBUY digital platform at the path of Enel Qualification Register: Personal Data \Company Profile \ Profile Data.
- A.16 **Cooperation in response and forensic activities.** The Supplier undertakes to cooperate with ENEL and with the parties authorized by ENEL in connection with analysis, containment, resolution, recovery and forensic analysis activities in relation to any Cyber Incidents involving the supply/service. Such cooperation shall include, by way of example and without limitation, making available qualified personnel, access to logs, technical evidence, indicators of compromise (IoCs), system configurations and any other information reasonably required for the proper management of the event and for compliance with applicable legal and regulatory obligations.
- A.17 **Business Continuity and Disaster Recovery.** The Supplier shall have in place, maintain active and periodically test business continuity and disaster recovery plans suitable to ensure the resilience of the services provided and the availability of ENEL's data and information. Such plans shall take into account the Recovery Time Objectives (RTO), Recovery Point Objectives (RPO) and any further business continuity objectives defined in the SLA, included in the technical documents of the Contract.
- A.18 **Backup and restore.** The Supplier, where applicable to the nature of the supply/service, warrants the creation, retention and protection of backups of ENEL's data and configurations within the contractually defined terms, ensuring the encryption of such backups, logical and/or physical separation from production environments, periodic restoration testing, the integrity and confidentiality of the backups themselves, and their storage and location in accordance with any applicable territoriality clauses.
- A.19 **Change management.** Any significant changes ("major changes") that may affect the overall security posture of the systems and services provided shall be properly identified, assessed and communicated to ENEL, and shall be subject to a prior security assessment before the new versions or configurations incorporating them are released into ENEL's production environment or deployed as part of the services provided to ENEL.
- A.20 **Right of audit.** With respect to services provided in multi-tenant or standardized mode, the Supplier may share compliance attestations issued by independent bodies widely recognized within the industry, including, by way of example, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II, C5, PCI-DSS, FedRAMP or IRAP, provided that such attestations are up to date and their scope is aligned with the service provided to ENEL. ENEL's right to request on-site audits in the event of significant Cyber Incidents, or material breaches of compliance obligations, or requests from competent authorities shall remain unaffected. The Supplier undertakes to ensure full cooperation, making available the necessary documentation, systems and personnel.
- A.21 **Security documentation update.** The Supplier undertakes to prepare, keep up to date and make available to ENEL, upon reasonable request, the security documentation relevant to the supply/service, including, by way of example and without limitation, security policies, operating procedures, architectural diagrams, role and responsibility matrices, security configurations, test results, compliance evidence, vulnerability registers and incident registers.
- A.22 **Asset management.** The Supplier warrants the existence of asset management processes for the assets within the scope of the supply/service, including hardware, software, network components, identities, certificates, cryptographic keys, secrets and data. The Supplier shall maintain an up-to-date inventory of such assets, ensure their protection and their secure disposal and decommissioning at the end of their lifecycle or of the supply, so as to prevent unauthorized access to the information contained therein.
- A.23 **Cryptography.** In order to protect ENEL's data, both at rest and in transit, the Supplier undertakes to adopt appropriate, standardized and non-deprecated cryptographic technologies, in compliance with the cryptographic standards and guidelines of the National Institute for Standards and Technology (NIST), the European Union Agency for Cybersecurity (ENISA), and any further applicable international standards. The Supplier undertakes to update such cryptographic methods and systems whenever required by ENEL or imposed by the competent authorities, ensuring that the transition to new technologies, including, by way of example, Post-Quantum Cryptography algorithms, occurs without any technical or economic impact for ENEL unless otherwise agreed. Where used, the Supplier further warrants the implementation of adequate lifecycle management of cryptographic keys and secrets, including their generation, storage, rotation, revocation and secure destruction.
- A.24 **Physical and logical security of the Supplier's premises.** The Supplier warrants that the premises, data centers, laboratories and any other physical facilities used for the provision of the service/supply or for the storage of ENEL's data are adequately protected through physical and logical security measures appropriate and proportionate to prevent unauthorized access, tampering, removal of assets and misappropriation of information, in accordance with the risk level of the supply/service and recognized industry best practices.
- A.25 **Secure communications between the Client and the Supplier.** Communications between ENEL and the Supplier, and between the Supplier and ENEL's systems, including for operational, administrative and support purposes, shall be carried out using secure, authenticated and appropriately encrypted communication channels. The Supplier undertakes to adopt tools, secure, authenticated and appropriately encrypted configurations and protocols information, or data, relating to the Contract.

3 Part B – Clauses applicable based on the Supplier's role in relation to the activities covered by the Contract.

The clauses set forth in this Part shall apply exclusively where the conditions of applicability specified in each clause are met, irrespective of the product or service category of the supply/service.

B.1 Security of the Software Development Life Cycle (SSDLC).

Scope of application: the supply/service includes activities for the design, development, evolution, modification, configuration, integration or maintenance of software, applications, microservices, APIs, scripts, components or source code.

Responsibility Model: OWNER / SHARED.

The Supplier represents that it develops, maintains and updates the software and code covered by the supply, including the software and code used for the provision of services to the Client, in accordance with formalized Secure Software Development Life Cycle (SSDLC) process, which shall be duly documented and available to ENEL upon request. Such process shall ensure the integration of security requirements, activities and controls throughout the entire software lifecycle, from requirements gathering and design, to coding, testing, release and ongoing vulnerability management, including, among others, threat modeling, secure code review, management of third-party and open source components, and controls designed to ensure the integrity of the build and release chain.

B.2 Segregation of environments and protection of non-production data.

Scope of application: the supply/service provides for the development, management, maintenance or operation of applications, systems, platforms or services for ENEL with multiple development, test, pre-production and production environments, or the provision of cloud services involving the coexistence of such environments within the Supplier's supply chain.

Responsibility Model: OWNER / OPERATOR / SHARED.

The Supplier warrants the logical and/or physical separation of its development, test, pre-production and production environments, ensuring segregation of networks, identities, credentials, secrets, datastores and CI/CD pipelines, with change and release controls commensurate with the criticality of each environment. The use of raw production data classified as confidential or strictly confidential in development and test environments is prohibited. Where specific supply needs make such use necessary, the Supplier may only use synthetic or properly anonymized/masked data, ensuring that re-identification is not possible through techniques recognized as effective under industry best practices. The use, in non-production environments, of the same credentials, cryptographic keys or certificates used in production environments is also prohibited. The Supplier warrants the independent generation, rotation and revocation of credentials for each environment. For multi-tenant cloud services and standardized products, the Supplier shall comply by making available independent third-party attestations that are widely recognized within the industry, including ISO/IEC 27001 or SOC 2 Type II, with a scope consistent with the service provided, covering environment segregation controls, including, by way of example, ISO/IEC 27002:2022 control A.8.31.

B.3 Availability and transferability of development artifacts.

Scope of application: the supply/service involves the production of source code, customized configurations, data schemas, models, parameterizations or any further development artifacts intended for ENEL.

Responsibility Model: OWNER.

The Supplier warrants the availability, completeness, integrity and transferability of the development artifacts, technical documentation, installation documentation (where applicable), configuration and operating manuals, security models and any documentation, material or asset necessary for the proper management, maintenance, evolution and recovery of the solution provided, both throughout the entire contractual term and upon its termination. The Supplier further undertakes to deliver such artifacts to ENEL or to any entity designated by ENEL in accordance with procedures and timelines agreed between the relevant technical functions of the Parties.

B.4 Security in the provision of application services.

Scope of application: the supply/service provides for the provision, operational management, application support, corrective, adaptive or evolutionary maintenance of applications used by ENEL.

Responsibility Model: OPERATOR / SHARED.

The Supplier warrants that application support and management activities are performed exclusively within the limits of the authorizations expressly granted by ENEL and in accordance with the operating, change management and incident management processes defined or approved by ENEL. The Supplier shall ensure compliance with the segregation of roles and privileges, the full traceability of the activities performed and the adoption of break-glass procedures for extraordinary access. Where application support activities require access to ENEL systems and applications, the Supplier's personnel shall use the IDP, IDM, MFA, PAM, VPN/ZTNA platforms made available by ENEL, in accordance with the procedures communicated by ENEL from time to time.

B.5 Security of system administration activities.

Scope of application: the supply/service provides for management, administration, configuration, maintenance or support activities concerning infrastructures, operating systems, databases, middleware, virtualization environments, containers, networks or automation platforms used by ENEL.

Responsibility Model: OPERATOR.

The Supplier warrants that system administration activities performed on ENEL systems are carried out by expressly authorized personnel, through named identities managed by ENEL's IDM/IDP, subject to multi-factor authentication through ENEL's MFA platform and, where applicable, governed through ENEL's PAM platform. All administrative sessions on ENEL systems shall therefore be logged, recorded and verifiable through the aforementioned platforms. The Supplier further warrants that any

configuration, patching or security modification of security settings to the systems is carried out exclusively within authorized change management processes and in compliance with the hardening baselines defined or approved by ENEL.

B.6 Security of on-site activities.

Scope of application: the Supplier's personnel perform activities at ENEL premises, data centers, plants, technical sites or offices.

Responsibility Model: OPERATOR.

The Supplier warrants that the personnel engaged at ENEL premises are identified, authorized and trained to comply with ENEL's physical and information security standard applicable to the site where the activities are performed, including rules on access, custody of tools, management of removable media, handling of paper-based information, occupational safety and prevention of the risk of compromise of ENEL's infrastructures. The Supplier undertakes to notify in advance the list of assigned personnel and any subsequent changes thereto, and to ensure the return of badges, devices, credentials and ENEL materials upon completion of the activities.

B.7 Continuity of telecommunications services.

Scope of application: the supply includes the provision of telecommunications services, connectivity, data transport, access, mobile, voice, contact center or managed network services for ENEL.

Responsibility Model: PROVIDER.

The Supplier warrants adequate levels of availability, resilience and continuity of the telecommunications services provided to ENEL, consistent with the service levels defined in the SLA of the Contract, through the adoption of resilient and redundant network architectures, alternative routes, failover and fault tolerance mechanisms, 24x7 monitoring and proactive event management aimed at preventing and mitigating events that may compromise the service.

B.8 Protection of telecommunications infrastructures.

Scope of application: the supply includes telecommunications services or products that transport, process or route the Client's traffic, data or signals.

Responsibility Model: PROVIDER.

The Supplier warrants the adoption of technical and organizational measures aimed at protecting the telecommunications infrastructures and services provided to ENEL against security threats, including, by way of example, Denial of Service attacks, traffic manipulation, interception, compromise of network components, abuse of routing and signaling protocols, and compromise of the network component supply chain. The Supplier warrants the segregation of the Client's traffic from that of other customers, the protection of interconnection points and, where applicable to the scope of the supply/service, the continuous monitoring of security events relating to the service provided.

B.9 Security by design of the product.

Scope of application: the supply provides for the design, production, customization or commercialization of hardware, software, firmware, equipment or appliances intended to be used by ENEL.

Responsibility Model: OWNER / PROVIDER.

The Supplier warrants that the products covered by the supply are designed, developed and manufactured in accordance with the principles of Security by Design and Security by Default, in line with industry best practices and applicable legislation, including, where relevant, the requirements of the Cyber Resilience Act. The Supplier warrants the existence of formalized product security management processes, the performance of risk assessments and security testing activities prior to placing the product on the market, the adoption of mechanisms ensuring the integrity, authenticity and non-repudiation of updates, and the availability of technical documentation relating to the product's components, dependencies, architecture and security configurations.

B.10 Product vulnerability management.

Scope of application: the supply includes hardware, software, firmware products or equipment used by the Client.

Responsibility Model: PROVIDER.

The Supplier shall maintain formalized processes for the identification, assessment, communication and management of security vulnerabilities that may affect the products supplied, including Coordinated Vulnerability Disclosure (CVD) programs, timely publication of security advisories and provision of patches or mitigations. The Supplier undertakes to notify ENEL of any vulnerabilities that may impact the supply within timeframes consistent with their severity, providing the operational guidance necessary for remediation.

B.11 Security support throughout the product lifecycle.

Scope of application: the Supplier provides support, product and software maintenance, assistance or update services for hardware, software or firmware products during the contractual term.

Responsibility Model: PROVIDER.

The Supplier warrants the availability of security support, including corrective updates, security patches and advisories, for the entire contractual term. In the event that the product/software reaches the End of Support, End of Life and End of Security



Support during the contractual term, the Supplier warrants the availability of a support roadmap and Long-Term Support (LTS) for the product versions, provided and/or maintained for ENEL, and shall communicate the backport policies of the security patches to LTS versions as well as recommended migration path to subsequent versions.

B.12 Integrity of the product supply chain.

Scope of application: the supply includes the delivery to ENEL of physical products or software products distributed through media, images or repositories of the Supplier.

Responsibility Model: PROVIDER.

The Supplier shall adopt suitable measures to ensure the integrity, traceability and security of its supply chain, including controls over its sub-suppliers, sealing and product integrity verification mechanisms, protection against the insertion of counterfeit, malicious or unauthorized components and the implementation of secure logistics management. The Supplier shall make available, upon Enel reasonable request, the evidence of implementation of measure to ensure integrity, including, by way of example, digital signatures, hashes, certificates of origin and certification of conformity.

B.13 Security in hardware maintenance activities.

Scope of application: the Supplier performs maintenance, repair, replacement or intervention activities on ENEL hardware components or hardware components supplied to ENEL.

Responsibility Model: OPERATOR.

The Supplier warrants that hardware maintenance activities are performed by duly authorized and trained personnel, in compliance with ENEL's physical and logical security standards, applicable to the site and to the scope of the intervention, adopting the measures necessary to prevent unauthorized access to data contained in the equipment, the introduction of unauthorized components, the manipulation of configurations and the misappropriation of information. Maintenance activities shall be logged, documented and communicated to ENEL in accordance with the procedures set out in the contractual documents.

B.14 Return and secure disposal of components.

Scope of application: the supply entails the replacement, removal, decommissioning or withdrawal by the Supplier of hardware components, storage media, equipment or devices owned by ENEL or intended for ENEL.

Responsibility Model: OPERATOR.

The Supplier warrants that the return, sanitization, physical destruction or disposal of hardware components and storage media are carried out in accordance with industry recognized methods, including, by way of example, NIST SP 800-88, and in a manner suitable to ensure that the information contained therein cannot be recovered. Upon ENEL's request, the Supplier shall provide documentary evidence of the sanitization or destruction performed.

B.15 Security by design in design activities.

Scope of application: the supply/service includes application, infrastructure, network, security, cloud architecture, data architecture or end-to-end solution design activities intended for ENEL.

Responsibility Model: OWNER.

The Supplier warrants that the design activities are performed in accordance with the principles of Security by Design and Privacy by Design, integrating security requirements into the design deliverables, taking into account the threats applicable to the context of the solution, ENEL's legal and regulatory obligations, ENEL's internal standards, where made available, and industry best practices. The Supplier shall document and maintain records of the security design decisions, the trade-offs made, the residual risks and the proposed mitigations.

Moreover, The Supplier shall assess and document the main security risks associated with the designed solution, identifying the applicable threats, the inherent vulnerabilities of the selected components, the relevant attack scenarios, the potential impacts and the design countermeasures adopted, so as to enable ENEL to assess the risk profile of the solution.

B.16 Qualification of cyber security personnel.

Scope of application: the supply includes the provision of professional cyber security services.

Responsibility Model: OWNER.

The Supplier warrants that the activities are performed by personnel having adequate experience, professional qualification and, where applicable, industry recognized certifications, including, by way of example, CISSP, CISM, CISA, OSCP, GIAC, CCSP, ISO 27001 LA/LI and ISA/IEC 62443. The Supplier shall make available to ENEL, upon reasonable request, documentary evidence of the qualifications of the personnel employed, and warrants the continuity and substitutability of resources without compromising the quality of the service.

B.17 Management of sensitive evidence.

Scope of application: the activities covered by the supply entail the acquisition, generation or custody of ENEL technical security information.

Responsibility Model: OWNER / OPERATOR.

The Supplier shall ensure adequate protection and confidentiality measures for sensitive evidence acquired or generated within the scope of the supply/service, ensuring encryption at rest and in transit, segregated storage, access limited to authorized personnel in accordance with the principles of least privilege and need to know, traceability of operations and secure destruction upon completion of the activities or termination of the Contract.

B.18 Independence in cyber assessment activities.

Scope of application: the supply provides for the provision of independent verification services, such as audits, assessments, compliance assessments, penetration tests, red teaming, vulnerability assessments, certifications or security attestations.

Responsibility Model: OWNER.

The Supplier warrants the professional independence, objectivity and absence of conflicts of interest of the personnel appointed to perform independent verification activities, and shall disclose in advance to ENEL any contractual, corporate or financial relationships with the entities, technologies or suppliers subject to verification.

B.19 Functional continuity of cyber security products.

Scope of application: the supply includes the delivery to ENEL of products intended for the protection, detection, response or governance of cyber security.

Responsibility Model: PROVIDER.

The Supplier warrants the ongoing effectiveness, maintenance, updating and security support of the products supplied, ensuring the continuous update of signatures, detection models, integrated threat intelligence, detection content and security components of the product.

B.20 Integrability of the Service or Supply with the Client's security ecosystem.

Scope of application: the supply includes products or services that must integrate, exchange information or interoperate with the Client's security ecosystem.

Responsibility Model: PROVIDER / OWNER.

Where the supply includes products, services or applications used by ENEL, the Supplier warrants, where technically applicable to the nature of the service or product, full interoperability with the security platforms adopted by ENEL from time to time, including: the Identity Provider through standard federation protocols (SAML 2.0, OpenID Connect, SCIM); Identity Management for provisioning, deprovisioning and identity lifecycle management; the Multi-Factor Authentication system for strong user authentication; Privileged Access Management for the mediation and tracing of privileged accounts; VPN or Zero Trust Network Access remote access platforms; and SIEM platforms for the centralized transmission of logs and security telemetry. The Supplier warrants that the product or service provided does not require the use of identity, authentication, remote access or privileged access management solutions, other than those adopted by ENEL, unless technical exceptions have been previously agreed and documented.

B.21 Responsibility for the technical supply chain.

Scope of application: the supply/service significantly depends on components, technologies, cloud services, libraries, Artificial Intelligence models or further elements provided by third parties.

Responsibility Model: OWNER / PROVIDER.

The Supplier shall maintain adequate processes for the assessment, qualification and continuous monitoring of security risks arising from its technical supply chain, including the prior assessment of critical suppliers, verification of their security posture, management of significant changes to its technological ecosystem, and identification of critical dependencies on third-party technologies, that may impact the supply/service.

B.22 Software Bill of Materials and component transparency.

Scope of application: the supply/service includes the development, commercialization, maintenance or provision of software, firmware, containers, embedded products or cyber security products.

Responsibility Model: OWNER / PROVIDER.

The Supplier undertakes to produce, keep up to date and make available to ENEL, upon request and in a manner consistent with the nature of the supply, a Software Bill of Materials ("SBOM") prepared in a recognized industry standard format, including, by way of example, CycloneDX, identifying the third-party and Open Source software components incorporated in the product or service provided. The SBOM shall be provided for the components falling within the Supplier's direct responsibility, it being understood that, for platform layers or multi-tenant managed service layers, the Supplier may comply by making available equivalent technical documentation, security advisories and recognized compliance attestations.

B.23 Compliance with security requirements for OT/industrial environments.

Scope of application: the supply/service includes products, services, design, development, integration, maintenance or support activities involving industrial automation systems, control systems (ICS/SCADA), energy plant management systems, IIoT/IoT devices, OT systems or functional safety systems.

Responsibility Model: OWNER / PROVIDER.

The Supplier warrants that the design, development, installation, configuration, maintenance and support of products and services intended for ENEL OT/industrial environments are performed in accordance with the principles and requirements of the IEC 62443 family of standards, with particular reference to IEC 62443-2-4 for service providers and IEC 62443-4-1/4-2 for products, taking into account the specific features of OT environments in terms of availability, functional safety, industrial process continuity constraints and long asset lifecycle.

B.24 Multi-tenant isolation in Cloud Services.

Scope of application: the supply/service includes cloud services provided in multi-tenant SaaS, PaaS or IaaS mode.

Responsibility Model: PROVIDER.

The Supplier warrants that the cloud services provided to ENEL are designed and configured so as to ensure the logical segregation of ENEL tenant resources, data, identities, cryptographic keys, logs and configurations from those of other customers of the Supplier or other tenants hosted on the same infrastructure. The Supplier further warrants the effectiveness of isolation mechanisms at application, network and storage layers, and undertakes to notify ENEL of any event or vulnerability that may have compromised, or reasonably be expected to compromise, tenant isolation, including on a potential basis.

B.25 Conformity certificates for Cloud Services.

Scope of application: the supply/service includes cloud services provided in multi-tenant SaaS, PaaS or IaaS mode.

Responsibility Model: PROVIDER.

The Supplier undertakes to make available to ENEL, for the entire term of the Contract, valid certifications and periodical independent attestation report related to the cloud services provided and, where applicable, to the processing of economic data. In particular:

- a. *SOC 2 Type II Report (mandatory)*– the Supplier shall transmit to ENEL, at least once a year and without interruption between one observation period and the next, a report SOC 2 Type II issued by an independent reviewer AICPA certified, written in compliance with the Trust Services Criteria (TSC). The Supplier shall transmit to ENEL, together with the report, the Management Assertion, the System Description and the remediation plan (Management Response) for any exceptions identified by the reviewer.
- b. *ISO/IEC 27001 (Mandatory)*. The Supplier warrants to have a valid ISO/IEC 27001 certification, released by a IAF accredited certification body, with scope statement extended to the processes, the sites, the infrastructures, the services and the personnel actually used in the supply/service to ENEL. The Supplier shall transmit to ENEL, together with the certificate: (i) the Statement of Applicability – "SoA" updated to the last version of the current standard, with evidence of the excluded controls and the reasons for the exclusion.
- c. *ISO/IEC 27017 e ISO/IEC 27018* – Extensions for Cloud Services. The Supplier shall transmit to Enel, if available, the ISO/IEC 27017 standard conformity certificates (Code of practice for information security controls based on ISO/IEC 27002 for cloud services) and, where data protection treatment applies, ISO/IEC 27018 (Code of practice for protection of personally identifiable information in public clouds acting as PII processors), with scope statement extended to the service to ENEL and updated with the same frequency of the reference ISO/IEC 27001 certification.
- d. *PCI DSS* – When the SaaS or PaaS supply/service involve the treatment, the transmission or the storage of cardholder data (CHD) or sensitive authentication data (SAD), the Supplier warrants the conformity with the current PCI DSS standard version published by PCI Security Standards Council and shall transmit to ENEL, at least yearly once: (i) the Attestation of Compliance (AoC) subscribed by a Qualified Security Assessor (QSA); (ii) the Report on Compliance (RoC).

B.26 Management of cryptographic keys in Cloud Services.

Scope of application: the supply/service includes cloud services providing for the encryption of ENEL data.

Responsibility Model: PROVIDER / SHARED.

Where the cloud service provides for the encryption of ENEL data, the Supplier warrants, where technically applicable to the nature of the service provided, the possibility for ENEL to use key management methods compliant with its security standards, including Customer Managed Keys (CMK), Bring Your Own Key (BYOK) or Hold Your Own Key (HYOK) models. The Supplier warrants the adoption of key lifecycle management practices consistent with industry best practices.

B.27 Management of sub-processors and sub-cloud providers.

Scope of application: the supply/service includes cloud services provided with the involvement of sub-processors or additional cloud providers.

Responsibility Model: PROVIDER.

The Supplier shall maintain an up-to-date list of the sub-processors, additional cloud providers or third parties used for the provision of the cloud service to ENEL, identifying for each of them the services or functions performed, processing locations and applicable security obligations. The Supplier shall notify ENEL in advance, with reasonable notice, of the introduction, replacement or termination of critical sub-processors used in the provision of the service.

B.28 Transparency of Cloud Service status.

Scope of application: the supply/service includes cloud services provided in SaaS, PaaS or IaaS mode.

Responsibility Model: PROVIDER.

The Supplier warrants to ENEL the availability of transparency and reporting tools relating to the status of the cloud service, including service status pages, security advisories, scheduled maintenance notices, service disruption communications and historical availability indicators. The Supplier undertakes to promptly notify ENEL of any events that may impact the availability, integrity or confidentiality of ENEL's data and services.

B.29 Security in the distribution of On-Premise Software.

Scope of application: the supply/service includes software intended to be installed and executed within ENEL environments.

Responsibility Model: OWNER / PROVIDER.

Where the supply includes the distribution of software intended to be installed and executed within ENEL environments, the Supplier warrants the integrity and authenticity of the distributed packages (security patches included) through digital signature, publication of the relevant hashes or trusted distribution channels, the existence of documented secure installation and configuration procedures, the absence of hard-coded credentials or secrets, the absence of backdoors and undocumented functionalities, and the availability of hardening guides aligned with industry best practices.

B.30 Management of Software licences and usage rights.

Scope of application: the supply/service includes software subject to licensing or usage rights management mechanisms.

Responsibility Model: PROVIDER.

The Supplier warrants that the licensing mechanisms of the software provided do not entail, directly or indirectly, undocumented network connectivity dependencies, unauthorized collection of telemetry data, or constraints that may compromise the confidentiality, integrity or availability of ENEL's environments.

4 Part C – Additional clauses applicable under NIS2 legislation

The clauses set out in this Part shall apply where the supply/service is designed by ENEL as falling within the scope of Legislative Decree No. 138 of 4 September 2024 ("NIS2 Decree") and the implementing determinations issued by the National Cybersecurity Agency (ACN).

- C.1 **Adequacy of the cyber security framework in the NIS2 context.** The Supplier represents and warrants that, for the entire duration of this Contract, it shall maintain an adequate cyber security framework within its organization, commensurate with the nature, scale and criticality of the supply/service in line with the outcome of the "Cyber Security Supplier Assessment Questionnaire", which also forms an integral and substantial part of the Contract, adopting appropriate and proportionate technical and organizational measures to ensure the protection of systems, infrastructures and information against cyber threats that may impact the supply or ENEL. The Supplier further undertakes to continuously assess and manage cyber security risks and to promptly update its security measures in relation to the evolution of vulnerabilities and industry best practices, consistently with any improvement actions identified in the Questionnaire, to be implemented in accordance with the plan agreed with ENEL.
- C.2 **NIS2 incident notification and management Support.** The Supplier undertakes to provide ENEL with all information and cooperation necessary to enable ENEL to comply with the notification obligations set forth under Articles 25 and 26 of Legislative Decree No. 138 of 4 September 2024 ("NIS2 Decree") and the implementing determinations of the National Cybersecurity Agency (ACN). Therefore, the Supplier shall promptly inform ENEL of all events falling within the taxonomy of significant incidents, regardless of their cause, including incidents arising from natural, accidental or human-induced events, including, by way of example, floods, failures, human errors, misconfigurations and unintentional actions by personnel. In addition:
- the Supplier shall designate a "Supplier Cyber Security Point of Contact" and at least one deputy, who may be contacted by e-mail and telephone, with the task of interacting with ENEL's representatives for the entire duration and throughout all phases of the Contract in relation to cyber security activities, including oversight of identified vulnerabilities and related remediation and patch management activities, within the scope of the Contract, the coordination of security controls and audits on the Supplier's cyber posture carried out by ENEL or by third parties selected by ENEL, and the coordination of cyber security analyses and verification of compliance with the cybersecurity requirements applicable to the supply/service;
 - the Supplier shall promptly notify the Client, using the e-mail address **cert@enel.com** and the e-mail address of the ENEL Contract Manager:
 - any incidents affecting the Client's network and information systems, where the Supplier provides managed security services or other managed services to the Client;
 - incidents affecting the Supplier's own network and information systems, where such incidents impact the Client's services or activities, in the event that the Supplier provides managed services to the Client;
 - the Supplier undertakes, within two (2) hours from recognition of the occurrence of the incident, to share the following information:
 - the nature of the incident;
 - all information reasonably necessary for ENEL to classify the event for the purposes of the applicable regulatory obligations;
 - description of the incident and its root cause, where known;
 - date and time of detection;
 - assets involved;

- viii. type of information involved, if belonging to the Client;
 - ix. actual or potential impacts;
 - x. mitigation measures adopted;
- d. the Supplier shall update the Client on the status of incident management every twelve (12) hours and until the incident has been fully resolved, and shall submit a final report within eight (8) hours following closure of the incident, containing digital evidence, logs, IoCs, the root cause analysis and corrective measures applied.
- C.3 **NIS2 supply chain risk management.** The Supplier, within the limits of its control and of its contractual rights vis-à-vis the relevant third parties, with respect to its direct suppliers and sub-suppliers involved in the performance of the Contract, shall maintain and provide to ENEL an up-to-date register of all subcontractors, cloud providers, affiliates and critical third parties that materially support the services/supply within the scope of the supply. For each such party, the Supplier shall identify the supported function, role, categories of data potentially impacted, processing location and applicable contractual cyber security obligations. The Supplier shall ensure that each such party is contractually bound to comply with security and resilience obligations commensurate with the service/supply in scope, and shall promptly notify ENEL of any deviation from, or impediment to, full compliance with such obligations and requirements.
- C.4 **Notification of material changes in the NIS2 context.** The Supplier undertakes to promptly notify ENEL of any material change to the supply chain, technological, organizational or operational ecosystem used for the design, development, maintenance, support, management or provision of the supply/service that may affect its cyber risk profile or the risk assessments carried out by ENEL for the purposes of NIS2 legislation. By way of example and without limitation, such changes shall include: the introduction, replacement or discontinuation of critical suppliers, sub-suppliers, sub-processors, affiliates or third parties relevant to the supply/service; the introduction, replacement or modification of cloud providers, hosting providers, data centers, development environments, support centers or maintenance centers used within the scope of the supply; changes to the geographic location of development, maintenance, support, data processing, storage or backup activities; significant changes to software development, build, release, update distribution, vulnerability management or privileged identity management processes; the introduction of new software components, libraries, open-source software or external dependencies that play a relevant role in the security or operation of the supply; mergers, acquisitions, changes of corporate control or other extraordinary transactions that may affect the security, resilience or governance of the supply. The Supplier shall provide a description of the change, the related cyber security impact assessment and the mitigation measures adopted, as well as any further information reasonably necessary to enable ENEL to update its cyber and supply chain risk assessments.
- C.5 **Update of ACN compliance information.** The Supplier undertakes to provide the ENEL Contract Manager, no later than twelve (12) days following the occurrence of the relevant event or any subsequent change thereto, with all information necessary to enable the Client update, on an ongoing basis and at least annually, the information maintained on the ACN platform, declare the relevant suppliers, and list and categorize its activities and services based on their potential impact. The Supplier warrants the accuracy, completeness and ongoing updating of the data relating to its services, assets and ICT supplies.
- C.6 **Training of the Supplier's personnel in the NIS2 context.** The Supplier shall ensure that its personnel as well as the personnel of its supply chain, involved in any capacity in the performance of the activities and in the provision of the services covered by the Contract, are adequately trained and subject to cyber security awareness programs and initiatives, in line with NIS2 legislation and industry best practices. Such training obligations shall also include personnel holding privileged and/or administrative accounts with rights on ENEL Systems or on the Supplier's systems used for the provision of the service. ENEL reserves the right, upon request, to obtain documentary evidence of the training delivered, including details of the training content.
- C.7 **Right of audit in the NIS2 context.** ENEL, or third parties appointed by ENEL and bound by confidentiality obligations, shall have the right, upon reasonable prior notice, to carry out audits aimed at verifying both the Supplier's cybersecurity maturity and the Supplier's compliance with the obligations to which it is bound as a supplier of a NIS2 entity. The Supplier undertakes to provide and ensure full cooperation, making available the necessary documentation, systems and personnel. If any non-compliance is identified, the Supplier shall submit a remediation plan setting out the corrective actions to be implemented, which shall be approved and implemented within the timelines agreed with ENEL.
- C.8 **KPIs and formalized review of the effectiveness of security measures.** The Supplier undertakes to define, monitor and periodically review a formalized set of metrics and key performance indicators ("KPIs") and key risk indicators ("KRIs") suitable to measure the effectiveness of the cyber risk management measures implemented within the scope of the supply/service. Upon ENEL's request, the Supplier shall make available the outcomes of the review, the documentary evidence of the measurements performed and the corrective actions undertaken, with a level of detail proportionate and commensurate to the nature of the supply/service.
- C.9 **Digital sign and integrity of the release artifacts.** Where the supply/service includes the development, the distribution, the update and the release of software, firmware, container image, package or artifacts intended to be installed or used within ENEL environment, the Supplier warrants the adoption of mechanisms that assure the integrity, the authenticity and the non-repudiation, such as for example: digital sign of the artifacts, publication of the related cryptographic hash or use of attested repository. The Supplier shall make available, upon Enel's reasonable request, the necessary information to verify the integrity of the released artifacts.

5 Part D – Additional clauses applicable pursuant to PSNC legislation

The clauses set out in this Part shall apply where the supply/service directly or indirectly supports ICT assets or adjacent assets designed by ENEL pursuant to Legislative Decree No. 105/2019 and the relevant Prime Ministerial Decrees ("PSNC").

- D.1 **Adequacy of the cyber security framework.** The Supplier represents and warrants that, for the entire duration of this Contract, it shall maintain an adequate cyber security framework within its organization, commensurate with the nature, criticality and risk profile of the supply/service consistent with the outcome of the “*Cyber Security Supplier Assessment Questionnaire*”, which forms an integral and substantial part of the Contract, and undertakes to ensure that any improvement actions identified in such Questionnaire are implemented in accordance with the plan agreed with ENEL. The Supplier shall also adopt appropriate and proportionate technical and organizational measures to ensure the protection of systems, infrastructures and information against cyber threats that may impact the supply/service or ENEL. The Supplier further undertakes to continuously assess and manage cyber security risks and to promptly update its security measures in line with the evolution of vulnerabilities, threat scenarios and industry best practices.
- D.2 **Data localization in the PSNC context.** Where the Supplier is required to process or handle data and/or information belonging to and/or made available by ENEL through systems and infrastructures belonging to the Supplier, the Supplier shall ensure compliance with the data localization requirements applicable to the processing, handling and storage of data and backups to which ENEL is subject under Legislative Decree No. 105/2019 and the relevant Prime Ministerial Decrees, including where such activities are performed through sub-suppliers. Unless otherwise justified by documented regulatory or operational requirements and expressly agreed with ENEL, the components of the supply/service relevant for PSNC purposes, the management infrastructures, the operational data and the related backups connected with the supply/service to ENEL shall be located within the territory of the European Union.
- D.3 **Supply chain management in the PSNC context.** The Supplier, within the limits of its control and of its contractual rights vis-à-vis the relevant third parties, with respect to its direct suppliers and sub-suppliers involved in the performance of the Contract, shall maintain and provide to ENEL an up-to-date register of all subcontractors, cloud providers, affiliates and critical third parties that materially support the services within the scope of the supply; shall identify, for each such party, the supported function, role, categories of data potentially impacted, processing location and applicable contractual cyber security obligations; shall ensure that each such party is contractually bound to comply with security and resilience obligations commensurate with the service provided and the associated risk profile, and shall promptly notify ENEL of any deviation from, or impediment to, full compliance with such obligations and requirements.
- D.4 **Notification of relevant changes in PSNC context.** Where the supply supports ICT assets or adjacent assets subject to the National Cybersecurity Perimeter regime (PSNC, Legislative Decree No. 105/2019 and relevant Prime Ministerial Decrees), the Supplier undertakes to notify ENEL in advance, where reasonably possible, and in any case without delay as soon as it becomes aware thereof, of any material change to the supply chain, technological ecosystem, architecture, organization or operating methods used for the implementation, maintenance, updating, support or provision of the supply, which may affect the security, resilience, availability, integrity or localization of the relevant ICT assets or adjacent assets. This obligation shall include, by way of example and without limitation: the introduction, replacement or termination of suppliers, sub-suppliers, cloud providers, software houses, development centers, support centers, SOCs, NOCs or other third parties involved in the supply chain; changes to the technological infrastructures, cloud platforms, management systems, administration environments or critical components used by the supply; changes to the geographical location of systems, infrastructures, data, backups, administration activities, operating centers or development and maintenance activities; substantial changes to software development, update distribution, vulnerability management, privileged identity management processes or security mechanisms adopted by the Supplier; the introduction of software, firmware, hardware components, libraries, open-source dependencies or technologies that may affect the risk profile of the supply; mergers, acquisitions, changes of corporate control, transfers of business or other extraordinary transactions that may affect supply chain security. The Supplier shall make available to ENEL all technical and organizational information necessary to enable the assessment of the impact of the change on the relevant ICT assets and adjacent assets and to support any obligations arising under PSNC legislation. No material change may result in a reduction of the security, resilience, traceability, verifiability, localization or regulatory compliance measures required for the supply/service without Enel's prior assessment, where required.
- D.5 **Notification and management of significant PSNC incidents.** The Supplier acknowledges that the Client is subject to the cyber incident reporting obligations provided for under PSNC legislation. The Supplier therefore undertakes to:
- a. notify the Client, without delay and in any case within thirty (30) minutes from detection, of any incident, anomaly, compromise, unavailability, failure, malfunction, critical vulnerability or security event that:
 - i. directly affects services, platforms, infrastructures or components provided to the Client;
 - ii. affects systems, infrastructures, cloud services, management platforms, shared components, administration environments, authentication, virtualization or monitoring systems, or other assets used for the provision of the service;
 - iii. may directly or indirectly cause an actual or potential impact on the Client's ICT assets subject to PSNC legislation or on the adjacent assets thereto;
 - b. ensure that the notification obligation referred to under letter a) applies irrespective of the cause of the event, the place where the event occurred, the actual interruption of the service and whether the event involved systems of the Supplier, sub-suppliers or third parties related to the provision of the service;
 - c. provide the Client with any information, technical evidence, log data, indicators of compromise, investigative elements, technical analysis or updates necessary for the Client to assess whether reporting obligations to CSIRT Italia and the other competent Authorities exist;
 - d. ensure the continuous availability, on a 24x7 basis, of qualified personnel appointed to cooperate with the Client during all phases of classification, management, containment, analysis and resolution of the incident and until the completion of any interactions with the competent Authorities;

- e. retain all evidence, logs and technical elements relating to the event and make them available to the Client without delay where necessary to comply with the obligations arising from PSNC legislation, ensuring their integrity, confidentiality and non-alterability for the applicable retention periods.
- D.6 **Training of personnel in the PSNC context.** The Supplier shall ensure that its personnel and the personnel of its supply chain involved in any capacity in the performance of the activities and in the provision of the services covered by the Contract are adequately trained and subject to cyber security awareness programs and initiatives, with specific reference to the obligations and requirements applicable in the PSNC context, in line with best practices and applicable legislation and in compliance with the security and confidentiality obligations and requirements set out in the clauses of the Contract. Such training obligations shall also include personnel holding privileged and/or administrative accounts with rights on ENEL Systems or on the Supplier's systems used for the provision of the service. ENEL reserves the right, upon request, to obtain documentary evidence of the training delivered, including details of the training content.
- D.7 **Right of audit in the PSNC context.** ENEL, or third parties appointed by ENEL and bound by confidentiality obligations, including any persons designated for such purpose by the competent authorities, shall have the right, upon reasonable prior notice, to carry out audits aimed at verifying both the Supplier's cybersecurity maturity and the Supplier's compliance with the obligations to which it is bound as supplier of a PSNC entity. The Supplier undertakes to provide and ensure full cooperation, making available the necessary documentation, systems and personnel. If any non-compliance is identified, the Supplier shall submit a remediation plan, setting out the corrective measures to be implemented, which shall be approved and implemented within the timelines agreed with ENEL.
- D.8 **Support for PSNC authorization and change processes.** Where applicable in relation to the scope of the supply/service, the Supplier shall support ENEL in release/change/decommissioning processes and internal approval workflows, including the drafting of documentation and the performance of preventive security activities and controls aligned with the requirements established by the PSNC regime (Legislative Decree No. 105/2019 and relevant Prime Ministerial Decrees). In particular, the Supplier undertakes to promptly provide the technical evidence, security assessments and information necessary to enable ENEL to complete the authorization processes required under PSNC legislation, including any obligations towards the CVCN, where applicable, and to cooperate with the parties involved in the preventive assessment processes.
- D.9 **Traceability of Supply Chain origin and compliance with geopolitical restrictions.** The Supplier represents and warrants that it is not subject to, and is not controlled by entities subject to, restrictive measures adopted by the European Union, the United Nations or the Italian State that may affect the performance of the Contract, and that it is not subject to non-EU regulatory obligations, that may materially impair its ability to ensure the confidentiality, integrity or availability of ENEL's data and systems. The Supplier shall promptly notify ENEL of the country of origin of the critical components used for the provision of the supply/service, its corporate control structure and the occurrence of any circumstances affecting the above representation. The Supplier further undertakes to notify ENEL of the presence, within its supply chain, of critical sub-suppliers established in non-EU countries that may affect the risk profile of the supply for PSNC purposes and under national Golden Power legislation.
- D.10 **Prior notification of patches and releases affecting PSNC ICT assets.** The Supplier undertakes to notify ENEL in advance, in accordance with the methods and prior notice agreed, of planned releases of security patches, firmware updates, new product versions and configuration changes affecting ICT assets within the PSNC perimeter, making available the information necessary for ENEL to activate any PSNC authorization processes that may be required. It is understood that, in the presence of critical vulnerabilities or where immediate intervention is required, the Supplier may proceed with urgent releases by notifying ENEL in accordance with previously agreed emergency procedures.
- D.11 **KPIs and formalized review of the effectiveness of security measures.** The Supplier undertakes to define, monitor and periodically review a formalized set of metrics and key performance indicators ("KPIs") and key risk indicators ("KRIs") suitable to measure the effectiveness of the cyber risk management measures implemented within the scope of the supply/service. Upon ENEL's request, the Supplier shall make available the outcomes of the review, the documentary evidence of the measurements performed and the corrective actions undertaken, with a level of detail commensurate with the nature of the supply.
- D.12 **Digital sign and integrity of the release artifacts.** Where the supply/service includes the development, the distribution, the update and the release of software, firmware, container image, package or artifacts intended to be installed or used within ENEL environment, the Supplier warrants the adoption of mechanisms that assure the integrity, the authenticity and the non-repudiation, such as for example: digital sign of the artifacts, publication of the related cryptographic hash or use of attested repository. The Supplier shall make available, upon Enel's reasonable request, the necessary information to verify the integrity of the released artifacts.

6 Part E – Additional clauses applicable pursuant to Law No. 90/2024 and the Prime Ministerial Decree of 30 April 2025

The clauses set out in this Part shall apply where the supply/service falls within the scope of Law No. 90 of 28 June 2024 ("Cyber Law") and/or of the Prime Ministerial Decree of 30 April 2025 implementing Article 14 of such Law.

- E.1 **Compliance with the essential cyber security elements.** The Supplier represents and warrants that the IT goods and services covered by the supply/service comply with the essential cyber security elements identified in Annex 1 to the Prime Ministerial Decree of 30 April 2025, both with respect to the intrinsic properties of the good or service and with respect to vulnerability management. The Supplier undertakes to provide ENEL, upon request, with the documentary evidence necessary to demonstrate compliance with such essential elements and to promptly update and provide such evidence whenever regulatory requirements or the characteristics of the supplied good or service change.
- E.2 **Intrinsic security properties of the IT good or service.** The Supplier warrants that the IT goods and services covered by the supply/service are designed, developed, configured and maintained in accordance with security by design and security by default principles, including, to the extent applicable to the nature of the supply, the adoption of authentication and access management

mechanisms compliant with industry best practices, the availability of logging functions, the adoption of hardening measures, encryption of data at rest and in transit by means of non-deprecated algorithms, minimization of the attack surface and disabling of services and interfaces that are not necessary for the intended use.

- E.3 **Vulnerability management.** The Supplier shall maintain a formalized vulnerability management process including the identification, assessment, prioritization, remediation and timely communication to ENEL of relevant vulnerabilities relating to the goods and services supplied, throughout the entire contractual support period. The Supplier undertakes to make available patches, mitigations and security advisories within timeframes consistent with the criticality of the identified vulnerabilities and with industry best practices, ensuring the authenticity and integrity of the released updates.
- E.4 **Support for preferential use of EU/NATO origin technologies.** The Supplier shall inform ENEL, within its technical offer, of the origin of the cyber security technologies used, indicating whether they are attributable to Italian entities, entities of the European Union, NATO countries or third countries identified in Annex 3 to the Prime Ministerial Decree of 30 April 2025 as parties to cooperation agreements with the EU or NATO in the fields of cyber security, protection of classified information, research and innovation. The Supplier undertakes to make available to ENEL the documentation necessary to substantiate the statements made.
- E.5 **Cooperation with Reporting and Notification Requirements Relating to Cybersecurity Incidents.** The Supplier acknowledges that the Client may be subject to incident reporting and notification obligations to be fulfilled within twenty-four (24) hours for the initial report and seventy-two (72) hours for the full notification, according to the taxonomy adopted by technical determination of the Director General of ACN. The Supplier undertakes to inform the Client, without delay and, in any case, within timeframes compatible with compliance with the aforementioned deadlines, of any incident that may fall within the ACN taxonomy and that impacts, directly or indirectly, the supply or the Client's systems and services, making available all information and technical evidence necessary to enable the Client to fulfil its reporting and notification obligations towards ACN.
- E.6 **Cooperation with the cyber security point of contact.** The Supplier undertakes to cooperate with the cyber security point of contact designated by the Client, acting as the main point of contact for coordination, assessment and management of cyber risk activities connected with the supply/service. Such cooperation shall include the timely provision of the information reasonably requested and participation in security coordination activities, in compliance with the timelines agreed between the Parties and to the extent that such activities are relevant to the supply/service. The Parties shall cooperate in good faith in order to strengthen cyber resilience, taking into account the applicable legislation and, where relevant, the guidelines issued by the competent national authority (ACN), within the limits of their applicability to the subject matter of the supply/service.