SPECIFIC CONTRACT CONDITIONS FOR THE SUPPLY OF SOFTWARE IN *ON-PREMISE* MODE
GRAPHOMETRIC ELECTRONIC SIGNATURE

Section I - General Provisions

1. Value of these Specific Conditions

These specific contract conditions ("Specific Conditions") govern the supply of the software identified in the subject matter hereof.
These Specific Conditions supplement the Additional Conditions and refer to the services identified in the Commercial Proposal.
In the event of a conflict between the Additional Conditions and these Specific Conditions, the latter shall prevail.
The Definitions set out in the General Conditions apply to these Specific Conditions.

Section II - Specific Conditions

A – Definitions
In addition to the definitions set out in the General Conditions, the following definitions shall apply in addition to and/or in replacement thereof:

- "User": the individual(s) who, following activation of the Service by the Client, is/are invited to participate in the collaboration activities offered by the Services.
- "Encryption Certificate": means the certificate for the protection of biometric data, consisting of a public key, i.e. a credential used to encrypt the biometric data of electronic signatures affixed to Electronic Documents, and a private key which, in the absence of different agreements between the parties, is presumed to be known exclusively by Namirial S.p.A., and which is necessary to decrypt such biometric data (the Encryption Certificate is also referred to in company practice as "Master Key");
- "Code": means the Italian Digital Administration Code pursuant to Legislative Decree No. 82 of 7 March 2005, as amended and supplemented by Legislative Decree No. 235 of 30 December 2010 and further subsequent amendments and supplements;
- "Electronic Document": any electronic document (file) containing the digital representation of legally relevant acts, facts or data. The law identifies which documents may be signed with an AES;
- "AES": means the Advanced Electronic Signature, i.e. a set of data in electronic form attached to or logically associated with an Electronic Document, which allow the identification of the signatory and guarantee a unique link to the signatory, created using means over which the signatory can maintain exclusive control, and linked to the data to which the signature relates in such a manner as to allow any subsequent modification of that data to be detected;
- "SES": means the Simple Electronic Signature, i.e. the set of data in electronic form attached to or logically associated with other electronic data and used by the signatory to sign;
- "Digital Signature": means Namirial S.p.A.'s qualified electronic signature, based on an asymmetric key-pair system consisting of a public key and a private key, which allows both the signatory (through the use of the private key) and the recipient (through the use of the public key) to verify and evidence the origin and integrity of an Electronic Document or a set of Electronic Documents. The legal validity of a Digital Signature is equivalent to that of a handwritten signature;
- "Operating Manual": means Namirial S.p.A.'s operating manual, published in its most up-to-date version on the website https://documentation.namirial.com/, setting out the purposes and the technical and operational specifications of the Signature Solution, including those of its individual hardware and software components, and defining the procedures and rules to be complied with by entities providing advanced electronic signature services;
- "Namirial Policy": means the Namirial S.p.A. document defining the process for the generation and custody of the Encryption Certificate;
- "Technical Rules": means the technical rules governing the generation, affixing and verification of advanced, qualified and digital electronic signatures, pursuant to Articles 20(3), 24(4), 28(3), 32(3)(b), 35(2), 36(2) and 71 of the Code, as set forth in the Prime Ministerial Decree of 22 February 2013 and subsequent amendments and supplements;
- "Software": means the complete set of software elements comprising the graphometric electronic signature process, conceived and developed by Namirial S.p.A., which has duly obtained ISO 27001 certification for the conformity of its related information security management system;
- "Signature Solution": means Namirial S.p.A.'s graphometric electronic signature solution, either simple or advanced, conceived in compliance with applicable legislation, in particular the Technical Rules. Such solution consists of specific hardware and software components distributed by Namirial S.p.A., as well as interoperability processes for the same and procedures to be followed by entities providing AES services, all as described in Namirial S.p.A.'s Operating Manual.

B – Contract Structure
The agreement for the supply of the Signature Solution consists of the following documents:

- General Conditions (Mod.Nam.Contracts01);
- Additional Conditions (Mod.Nam.Contracts02);
- Specific Conditions (Mod.Nam.Contracts02S);
- Commercial Proposal;
- Operating Manual.

C – Subject Matter of the Agreement
The Agreement concerns the supply to the Client of the Signature Solution, including the individual software and/or hardware components thereof, as specifically described in the Commercial Proposal, in exchange for the fees set out therein.
The Signature Solution is designed in accordance with specific characteristics and technical specifications, exclusively for the purposes set out in the related Operating Manual; any other or different use by the Client is not guaranteed by Namirial S.p.A..

D – Characteristics of the SES
The SES possesses the technical and legal requirements that allow it to be legally qualified as an electronic signature; Electronic

Documents signed therewith satisfy the written form requirement and, in terms of evidence, may be freely assessed by a court, taking into account the objective characteristics of quality, security, integrity and immutability of the document itself.
It enables document dematerialisation in numerous contexts, meeting the written form requirement.
On a technical level, Namirial S.p.A.'s SES solution is capable of ensuring:

- the association of signatory Users with Electronic Documents;
- the unique link of the signature to the User, as signatory of Electronic Documents;
- the ability to verify at any time that the signed Electronic Document has not been modified after the signature was affixed;
- the ability for the User, as signatory of Electronic Documents, to obtain evidence of what has been signed;
- the identification of the Client providing electronic signature services;
- the absence of any element in the subject matter of the signature capable of altering the acts, facts or data represented therein;
- the unique link of the signature to the signed document.

The SES enables the capture of only the graphic stroke of Users who are signatories of Electronic Documents, through the interoperability of hardware and software components, which is ultimately embedded in the Electronic Document and meets the security requirements defined by applicable legislation. Such graphic stroke is embedded in the PDF by means of a technical certificate issued by Namirial S.p.A. in order to guarantee the immutability and integrity of the document.
The hardware components covered by the Commercial Proposal are warranted by the manufacturer for the entire warranty period indicated therein.

E – Characteristics of the AES
The AES possesses the technical and legal requirements that allow it to be legally qualified as an advanced electronic signature; Electronic Documents signed therewith have, from a legal standpoint, the same value as paper documents signed with a handwritten signature and, on a technical level, meet the security requirements defined by applicable legislation. Electronic Documents signed with an AES are accordingly accorded the legal effect provided for under Article 2702 of the Italian Civil Code, i.e. the legal effect of private deeds.
The AES satisfies the requirements for the identifiability of the author of the signature generated, as well as the integrity and immutability of the Electronic Documents signed.
It enables document dematerialisation in numerous contexts, satisfying the written form requirement; in particular, subject to the provisions of Article 25 of the Code, private deeds referred to in Article 1350, first paragraph, numbers 1 to 12, of the Italian Civil Code, if made by means of an Electronic Document, must be signed, under penalty of nullity, with a qualified electronic signature or a Digital Signature.
On a technical level, the AES, in accordance with the Technical Rules, is capable of ensuring:

- the identification of Users, as signatories of Electronic Documents;
- the unique link of the signature to the User, as signatory of Electronic Documents;
- the exclusive control by the User, as signatory of Electronic Documents, over the signature generation system, including the biometric data used for the generation of the signature;
- the ability to verify at any time that the signed Electronic Document has not been modified after the signature was affixed;
- the ability for the User, as signatory of Electronic Documents, to obtain evidence of what has been signed;
- the identification of the Client providing advanced electronic signature services;
- the absence of any element in the subject matter of the signature capable of altering the acts, facts or data represented therein;
- the unique link of the signature to the signed document.

The AES enables the capture of the biometric data of Users who are signatories of Electronic Documents, through the interoperability of hardware and software components, and the encryption of such data by means of an Encryption Certificate; the resulting encrypted biometric data, subsequently signed by means of a Digital Signature device or alternatively an electronic signature software device and ultimately embedded in the Electronic Document, meets the security requirements defined by applicable legislation.
The encryption of biometric data is carried out in particular by means of the public key of the Encryption Certificate issued by Namirial S.p.A.; a copy of the public key is made available to the Client, whilst the private key, which is capable of decrypting the biometric data in clear form, is held by a third-party guarantor entity, which may be Namirial S.p.A. where expressly appointed in writing by the Client, in accordance with the custody procedures set out in the Namirial Policy.
The hardware components covered by the Commercial Proposal are warranted by the manufacturer for the entire warranty period indicated therein.

F – Service Delivery Conditions
It is further understood that Namirial S.p.A. may at any time modify the Service delivery conditions and the content of the Operating Manual, without any obligation to notify the Client, as such conditions may be consulted at any time on the website https://www.namirial.com/it/.

G – Client's Obligations and Liabilities
The Technical Rules set out the obligations incumbent upon entities providing AES services; in particular, the Client is legally required to comply with the provisions of Article 57 of the Technical Rules and any subsequent amendments and supplements thereto.
The Client, possibly also jointly and severally with its appointees responsible for carrying out the procedures set out in the Operating Manual, assumes full liability towards Users, third parties and Namirial S.p.A. for any damage arising from the breach of the obligations it has undertaken upon signing the Agreement.
Namirial S.p.A. shall be entitled to verify at any time the regularity of the signature acquisition process adopted by the Client, by sending its own appointees to the Client's premises with five (5) working days' written notice. Namirial S.p.A.'s appointees shall be entitled to inspect all documentation relating to the Signature Solution; upon completion of such activity, a related verification report shall be drawn up, which the Client hereby undertakes to sign in acknowledgement of acceptance of the findings obtained.
The Client further acknowledges and accepts that the Encryption Certificate, if entrusted to Namirial S.p.A. for custody, may only be used pursuant to an order of the judicial authority, in the event of any disputes regarding the correct use of the Signature

Solution.

H – Final Provisions
The AES has been designed by Namirial S.p.A. in order to ensure that Electronic Documents are accorded the legal effect provided for under Article 2702 of the Italian Civil Code, in accordance with the provisions of the Code and the Technical Rules; Namirial S.p.A. guarantees to the Client that the AES, in its current state, fully fulfils this purpose when used correctly, in accordance with Namirial S.p.A.'s own instructions. Any Software updates necessitated by future amendments to the applicable national legislation shall be made available to the Client through the provision of the Service, against the fees determined in accordance with the provisions of Article 6 of the General Conditions.
The Client acknowledges and accepts that the use of Digital Signature devices is in any event conditional upon the Client's prior execution of the specific documentation prepared by Namirial S.p.A. for this purpose (in its capacity as Certification Authority); it is acknowledged that this clause is of an essential nature.

Client Signature* _____

*please sign digitally

Client Name _____