

ADDITIONAL CONDITIONS FOR THE SUPPLY OF SOFTWARE IN SAAS MODE**Section I - General Provisions****1. Value of these Additional Conditions**

These Additional Contract Terms (hereinafter "Additional Conditions") govern the supply of Namirial Software provided in Software as a Service ("SaaS") mode. These Additional Conditions supplement the General Terms and refer to the services indicated in the Commercial Proposal. In the event of a conflict between the General Terms and the Additional Conditions, the latter shall prevail. The Definitions indicated in the General Terms apply to these Additional Conditions.

2. Service Object

The supply allows the Client to use the SaaS for the purposes indicated in the Contract, under the terms and conditions specified in these Additional Conditions, any specific Conditions, and as indicated in the technical documentation published on the website <https://www.namirial.com/en/> (hereinafter "Technical Documentation"). The supply of SaaS includes, for the entire duration of the Contract, the Connected Services according to the methods and terms defined in article 5 of these Additional Conditions, as well as any additional connected and/or accessory services indicated in the Contract.

Unless otherwise expressly agreed, the following services are not included in the supply:

- a. interventions for the restoration of archives and services caused by non-compliant use of the SaaS or otherwise due to culpable acts attributable to the Client (e.g., negligence, failure to comply with Usage Rules, tampering by personnel, etc.);
- b. intervention and/or maintenance activities on the Client's infrastructure (e.g., firewall, networking devices, switches, Wi-Fi, client workstation configuration, printers, and/or other local network peripherals).

3. Content

The content consists of all data or information that the Client provides, authorizes for access, or inputs into the Software. Namirial will not have the ability to access, view, or listen to any Client content unless reasonably necessary to execute the Software. The Client represents and warrants that they own all rights to the content they submit; that such content is truthful and accurate; and that the use of the content provided by the Client does not violate these Additional Conditions, any specific Conditions, the General Terms, or applicable law. The Client acknowledges and agrees that they are solely responsible for the content provided and that they have full responsibility for the legal validity and copyright of the content.

4. Data Portability

With SaaS, unless otherwise provided in the Contract, a connected document archiving service is not provided, nor does the Software constitute an archiving tool. Notwithstanding the above, and unless otherwise specifically agreed, Namirial guarantees the Client the availability and the ability to extract (via download) the data and documents processed by the Client through the Software for the entire duration of the Contract, as well as for the additional period following the termination of the Contract specified in the Technical Documentation. After this period, Namirial will proceed with the deletion of data and documents and any other Client content. The Client has the option to activate a paid archiving and/or substitute storage service for the period following the termination of the Contract, which will be governed by specific contract terms.

5. Connected Services

The Connected Services include:

- a) corrective maintenance service, which includes the diagnosis and removal of the causes and effects of Software malfunctions;
- b) adaptive maintenance service, which includes the release to the Client of Software updates following any legislative, regulatory, or administrative changes ("regulatory requirements"), which entail variations attributable to the concept of ordinary administration and which do not involve the creation of a new Software module or a different product. Adaptive maintenance does not include the implementation or removal of new functionalities, even if the intervention is necessary to meet a regulatory requirement, except for functionalities implemented at Namirial's initiative. In any case, adaptive maintenance interventions are considered included in the economic conditions agreed in the Contract if the total working effort for all interventions in the reference calendar year (effort) is equal to or less than 20 (twenty) working days;
- c) the release to the Client of any new versions of the Software that Namirial, or its licensors, may make available; therefore, the sending of additional Software modules and/or newly designed Software is excluded;
- d) the release to the Client of any corrections of errors or malfunctions present in the Software, as soon as they are available;
- e) SaaS software assistance is provided during the normal working hours observed by Namirial personnel or, if present, by the Partner. The service does not include the provision of assistance at the Client's premises. Assistance may be provided by Namirial, even remotely, through remote access to the Client's computer, previously and each time authorized by the latter, with the direct acceptance of each intervention request. Assistance requests are guaranteed through the channels indicated on the website <https://www.namirial.com/en/>.

The Service will be provided to the Client limited to the last two supported versions of the Software, without considering any modifications or integrations made by the Client or third parties appointed by the latter on the Software itself. Namirial, for the provision of assistance, may also use third parties outside its organization or directly from authorized resellers. If Namirial needs to proceed with the maintenance of the Software



Namirial S.p.A.

Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia
amm.namirial@sicurezzapostale.it | Tel. +39 071 63494
P.IVA, C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426
www.namirial.com



and/or infrastructures, where this involves an interruption of the Software functionalities, it will inform the Client at least 24 (twenty-four) hours in advance about the need to carry out these interventions, as well as their duration, through publication on the website <https://status.namirial.com/>. The Client acknowledges and accepts that, in all phases of assistance, Namirial or Partner operators, even external to the organization, may become aware of the Client's personal data found during the connection phases on the latter's IT devices.

6. Warranties

Namirial guarantees the conformity of the Software to the specifications contained in the Technical Documentation, without prejudice to the fact that Namirial does not guarantee that these specifications meet the Client's needs or that the quality of the Software will meet the Client's expectations. The warranty provided by Namirial is conditioned on the proper functioning and adequacy of the IT equipment and connectivity services available to the Client, as well as the proper use of the Software by the latter.

7. Intellectual Property

All intellectual and industrial property rights, including the related economic exploitation rights on the SaaS, documentation, updates and developments, preparatory works, and derivative works are and remain, in whole or in part and worldwide, the exclusive property of Namirial. The Client undertakes, also pursuant to art. 1381 c.c., for each User, to use the SaaS in compliance with Namirial's intellectual property rights. Therefore, by way of example and not exhaustive and in any case without prejudice to the mandatory legal limits, the Client may not:

- a) circumvent the technical limitations and technological protection measures present in the Software, including the authentication system;
- b) reproduce, modify, adapt, customize the Software or create derivative works from it.

Namirial retains all rights to user manuals, videos, presentations, or any accessory printed material, including trademarks, logos, names, domain names, and other distinctive signs associated with the SaaS, with the consequence that the Client may not use them in any way without Namirial's prior written authorization.

8. Security

The authentication credentials provided by Namirial are considered known exclusively by the Client, who is required to keep them confidential and with the utmost diligence, undertaking not to transfer them and not to allow third parties to use the Software in any way; otherwise, the Client will be considered responsible for any damage or prejudice caused directly or indirectly to Namirial and/or third parties due to the improper use of the Software by unauthorized persons. The security of the workstations and resources used for the services provided by Namirial is the responsibility of the Client. The Client therefore undertakes to ensure that account management is monitored according to current security procedures to limit the hypotheses of access attempts and/or violations through their systems. The Client also undertakes to ensure that log procedures are secure and verified and that access management is preordained to traceability and monitoring procedures. Namirial uses physical, electronic, and managerial procedures to safeguard and prevent unauthorized access to the Client's Content. Namirial chooses these guarantees based on the sensitivity of the information collected, processed, and stored and the current state of technology. Although Namirial takes measures to safeguard the disclosure of unauthorized information, the Internet and Software are not 100% secure, so Namirial will not guarantee the Client that the information collected or stored will be protected from all unauthorized access. Further specific security provisions are contained in Sections I and II of these Additional Conditions, applicable, respectively, in the case of service use through "Shared SaaS" or "Private SaaS".

9. Personal Data Processing

In the context of the supply of Namirial Software under these Additional Conditions, the Client, as Data Controller, undertakes to appoint Namirial as Data Processor pursuant to art. 28 of the GDPR through a Data Processing Agreement that will regulate in detail, also through specific processing sheets, depending on the type of Namirial Software used by the Client, the terms, methods, and responsibilities of the processing. However, if the Namirial Software provided to the Client is connected to the provision of Qualified Services by Namirial, the latter will act as Data Controller of the personal data. If the Client, for their exclusive purposes, needs to access the personal data of Users collected by Namirial in the context of the provision of Qualified Services, they will act as an independent Data Controller.

Section II - Shared SaaS security

10. Shared SaaS Security

These security clauses apply to the provision of software in "Shared SaaS" mode. Shared SaaS means a software distribution model in which multiple Clients share the same infrastructure, platform, and applications, hosted and managed by Namirial, as the Service provider.

11. Software and Server Operating System Update Periods

Patches and updates to new versions are managed by Namirial in accordance with its security policies and schedule. They cannot be delayed at the Client's request. The Client who needs a customized patch and update program must switch to private SaaS software.

12. Web Application Firewall

The Web Application Firewall (WAF) is enabled by default to ensure the protection of "Shared SaaS" software. The WAF cannot be disabled at the Client's request. The Client who needs full control over the WAF configuration must request the activation of the "Private SaaS" delivery mode.

13. Penetration Testing and Vulnerability Assessment

The Client cannot perform penetration testing or vulnerability assessments on Namirial's public shared multi-tenant infrastructure.



14. Audit and Test Execution

The Client is not authorized to participate in the execution of security tests. Namirial has implemented advanced Business Continuity (CO) and Disaster Recovery (DR) policies that include testing activities. Tests are carried out according to Namirial's schedule and in accordance with internal policies.

Section III - Private SaaS Security

15. Private SaaS Security

These security clauses apply to the provision of software in "Private SaaS" mode. "Private SaaS" means a software distribution model in which the application and infrastructure are dedicated exclusively to a single Client, while maintaining the typical advantages of the SaaS model, such as centralized management, maintenance, and updates managed by the provider.

16. Updates

Patches and updates to new versions can be managed individually by mutual agreement. Namirial informs the Client when patches or updates are available. The Client must refuse the patches within 9 (nine) days, after which they will be considered approved. If the Client refuses the patches, Namirial cannot be held responsible for incidents related to the obsolescence of the Operating System and software. To receive maintenance, the Client must use a Long Term Stability (LTS) version no older than 2 years or the current released version, which is also distributed in "Shared SaaS" Software.

17. Web Application Firewall

The Web Application Firewall (WAF) is not enabled by default in "Private SaaS" software. A support service is available on request to activate the WAF.

18. Penetration Testing and Vulnerability Assessment

Penetration testing and vulnerability assessments can only be performed if the "Private SaaS" software is accessible via a custom domain. A support service is available on request for the execution of penetration testing and vulnerability assessments.

19. Custom Domain Name

The Client must provide custom domain names (e.g., sign.Clientname.com or similar) for "Private SaaS" software; failure to do so will result in no access to the service. In any case, Namirial has the right to register a custom domain on behalf of the Client, on which the service will be provided directly or via URL redirection.

20. Audit and Test Execution

The Client is not authorized to participate in the execution of tests. Namirial has implemented advanced Business Continuity (CO) and Disaster Recovery (DR) policies that include testing activities. Tests are carried out according to Namirial's schedule and in accordance with internal policies.

Section IV - Specific Service Conditions

These Additional Conditions are accompanied by specific Conditions for the provision and use of certain SaaS Services that require specific regulations. They constitute an integral and essential part of the Contract.