SECURITY RULES FOR INFORMATION ASSET PROTECTION OF THE COMPANIES OF THE ALMAVIVA GROUP AND CLIENT DATA MANAGEMENT

Contents

1.1 INTRODUCTION

1.1.1 The regulations provided in this document shall apply as a supplement to the General Conditions ("**Security Rules**"). Capitalised words not defined in the Security Rules shall be interpreted according to their meaning, as provided in the General Conditions. The Supplier acknowledges that these Security Rules are available on the Almaviva S.p.A. Website at the following link www.almaviva.it/it_IT/Area_fornitori and are subject to regular review.

1.1.2 The Security Rules define the security checks and standards that the Supplier undertakes to maintain active and efficient during the entire duration of a Purchase Order under which the Supplier can access the systems and/or process data and information of the Companies and/or their clients.

1.1.3 To perform any activity related or connected to the Service, the Supplier commits to comply with corporate policies - duly formalised, disseminated and available within the Company - in line with the current legislation and the security guidelines provided and explained in the following pages.

1.1.4 The Supplier shall process data and information according to their classification and service levels, as indicated by the Company.

1.1.5 The Supplier recognises that the data of the Company's IT configurations and architectures, the security measures adopted by the Company, and - in any case - that the data related to any vulnerability detected during the performance of the Service are confidential (including under Article 98 of the Italian Intellectual Property Code) and any dissemination of such data externally may result in severe damage for the Company, including, among others, in exposure to external threats or damage to the Company's image or reputation.

1.1.6 The Supplier shall ensure, where indicated, full compliance with the service levels as outlined in their contract with the Company, including in cases of emergency or contention of resources by their other clients.

1.1.7 The Supplier acknowledges the Company as the sole and exclusive owner of data, software, technical and legal documents and physical and logical ICT resources while using them or making them available while supplying the Service.

1.1.8 The Supplier acknowledges that the breach of the security obligations indicated in the Security Rules shall constitute cause termination at law of the Purchase Order under Article 1456 of the Italian Civil Code with the Company's right to compensation for damages (including image and/or reputation damages).

1.1.9 The Company shall be entitled to revoke the authorisation granted to a Supplier to carry out any activity on the Company's assets (including data).

1.1.10 Upon the Company's request, regardless of the termination of the contract, the Supplier undertakes, at any moment, to delete the data it has come into possession of and provide proof of the deletion.

1.1.11 The Supplier undertakes to return the Company asset (including data, licenses and equipment) within the time agreed and, in any case, within 60 days from the termination of the Purchase Order.

1.1.12 The Supplier undertakes to apply the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), and as for the processing of personal data carried out on behalf of the Company and/or third parties, they undertake to comply with the obligations, indications and technical and organisational security measures outlined

in the instrument of appointment as under Article 28 of the Regulation above-mentioned.

1.2. SECURITY REPRESENTATIVES

1.2.1 The Supplier and the Company, if required, shall communicate to each other the names of the representatives appointed to manage information and, if applicable, personal data security aspects ("Security Representative"), which are typically assigned to a Coordination Officer.

1.2.2 The Company and the Supplier shall undertake to communicate any change in this regard promptly.

1.2.3 The Company and the Supplier, through the Security Representatives, where appointed, or the Contact Managers, shall define together the communication, coordination and management procedures to adopt in case of cyber-security incidents, which may undermine the service levels defined in the contracts. In the case of personal data processing, the procedure and timing of the incident and breach reporting are provided in the legal instrument (named Data Processing Agreement) used by the Company to appoint the Supplier as defined under Article 28 of the Regulation (EU) 2016/679 (General Data Protection Regulation.

1.3. PERSONNEL AND ORGANISATION OF THE SUPPLIER

1.3.1 As for the personnel involved in the performance of the Purchase Order (including collaborators of any kind), in order to guarantee the protection of information, the Supplier undertakes to:

- ensure that such individual is qualified to perform the appointed and performed tasks;
- verify and ensure that each of the above personnel l has received the necessary training and information on the regulations outlined in section 1.1 above;
- adopt adequate policies for the separation of duties during the allocation of tasks;
- assign their employees adequate tasks and responsibilities to allow the latter to oversee and control the main internal and external threats;
- in cases of change in the task or termination of the employment contract, the Supplier undertakes to: promptly communicate the situation to the Company - through formalised and secure procedures -, and immediately revoke the access credentials to the employee and withdraw any other equipment provided to them for the performance of the contractual activities, including badges, keys and other access, identification and authentication means.

1.3.2 The Supplier undertakes to collaborate with the Company to ensure compliance with the duties and procedures defined by the Company to carry out risk analysis procedures and any other obligations related to the protection of personal data as under the Regulation (EU) 2016/679 (GDPR).

1.3.3 The Supplier commits to keeping:

- a list of the places where they are hosted:
  - data,
  - Services,
  - data centres used by the Supplier to provide the Service,
- a document providing indications on physical and logical access management

and detailed information on the number of operators entitled to access the Company data. The Supplier also commits to regularly updating such documentation and submitting them to the Company upon the latter's written request.

1.3.4 The Supplier commits to **(i)** promptly reporting to the Company in case of the need to transfer the data (including back-up) and resources from a specific location (of their own or third parties) to another before the transfer is carried out and (ii) implementing the same security measures on the new data location as those implemented in the previous one. Provided, however, that the transfer of data and resources from one location (of their own or third parties) to another shall be subject to the preliminary authorisation of the Company. Any prohibitions/restrictions on the movement of resources and data already provided for in the Purchase Order remain unaffected.

1.3.5 In case of sub-contracting - including partial - of the Service and/or related activities (which shall, in any case, be authorised in written by the Company and monitored according to the procedures outlined in the Purchase Order), the Supplier shall guarantee the application of the provisions on data management included in the Security Rules (specifically, those related to data confidentiality, retention and deletion), and the performance of audits and checks across all the supply chain. It remains understood that, in case of sub-contracting, the Supplier shall, in any case, ensure regular checks and monitoring on sub-contractors and shall defend and indemnify the Company against all damages caused by such sub-contractors (including reputation and image damages.

1.3.6 The Supplier shall commit to informing the Company in advance about any intention to implement changes in the Supplier's organisation which may impact the level of data integrity, availability, and confidentiality, to allow the performance of adequate assessment, checks and verifications on behalf of the Company, including employing an audit.

1.3.7 The Supplier commits to not implementing changes (technologies, service organisation, and sub-contracting supply chain) which may reduce the security of the Service.

1.4. SUPPLIER'S PHYSICAL AND LOGICAL SECURITY

1.4.1 The Supplier commits to using all their company services, related or connected to the activities established by the contract, the security measures for the management of access privileges and credentials in line with the best practices and the legal provisions defined under section 1.1.12 above, and which envisage at least:

- unequivocal and personal accounts;
- secure management of access credentials periodic expiry and mandatory modification at first access, guaranteed non-reusability and history policy setting, and automatic robustness checks;
- criteria and policies for assigning access credentials and privileges that are clearly based on the criterion of the separation of duties;
- criteria and policies for assigning access privileges that guarantee privileges denied unless explicitly granted and guarantee of the least privilege criterion granted;
- protection instruments and policies for safeguarding received media and data and preventing loss and access, even accidental, by third parties.

1.4.2 The Supplier guarantees the implementation of physical security measures (i.e., by

way of example, locked premises, "clean desk policy", custody of assigned hardware) within the areas related or connected to the Service provided (and during any transfer from and to these places).

1.4.3 Following the completion of the activities provided under the contract, the elimination of data/hardware shall be carried out according to the security requirements defined under section 1.1.12 above, and/or in the Purchase Order and/or communicated by the Company in due time.

1.4.4 The Supplier undertakes to implement adequate measures to isolate the data managed on behalf of the Company from other data managed on their behalf or on behalf of other clients to guarantee their confidentiality, integrity and availability.

1.4.5 Upon the request of the Company, the Supplier commits to sending a detailed description of the procedures adopted to supply the Service during the term of Purchase Order, implementing and managing IT security, physical security and organizational security measures to protect the Company asset, able to ensure compliance with the required classification level.

1.5. SECURE AND SAFE USE OF SUPPLIER'S SYSTEMS

1.5.1 The Supplier commits to ensuring, with regard to the scope of their responsibility, that the following activities are duly managed:

- security incident management, through the detection, containment, reporting, communication and analysis of information security events and incidents, identifying a suitable escalation list. More specifically, the Supplier commits to promptly inform the Company, including outside working hours, of any significant event that occurred in relation to the security of information and data for the Service envisaged by the Purchase Order by sending a report of the incident;
- compliance with the response times to the security incidents as agreed and specified under section 1.2.3 above;
- security patch management executed through controlled updating processes and at a time appropriate to the gravity of the vulnerability detected;
- anti-malware management with periodical updating;
- change management in the implementation of processes for the execution of changes;
- controlled disposal of assets with the adoption of systems for the secure deletion of information from storage media;
- prohibition of issuing press releases (including through channels such as the media, social media, regulators, etc.) concerning any IT security incidents that may have occurred, without first agreeing with the Company on the contents and timing of the communication.

1.5.2 The Supplier must guarantee the execution of internal Vulnerability Assessment and Penetration Tests on the infrastructures at least once every six months on the perimeter of the services supplied to the Company.

1.6. DATA BACK-UP

1.6.1 The Supplier undertakes to perform periodic back-ups of the data pertaining to the contractually agreed activities (including equipment and system configuration data) in such a way as to ensure:

- the storage of the backup copies in a safe, fireproof and intrusion-proof place;

- recovery from backup copies and the execution of dedicated recovery tests at fixed intervals.

1.6.2 The Company shall have the right to access the backup copies made by the Supplier.

1.7. FILE SHARING

1.7.1 Where the sharing of files, databases, and software code (file-sharing) is necessary for the performance of the activities assigned by the Company, the Supplier undertakes to use only file-sharing platforms authorised by the Company. It is, therefore, expressly forbidden to use other platforms for saving and sharing information. The Company reserves the right to carry out continuous monitoring activities of the file-sharing tools used by the Supplier.

1.8. LOG MANAGEMENT

1.8.1 The Supplier undertakes to perform in a systematic and formalised manner, in compliance with the law:

- the management of application logs for software related or connected to the performance of the contractual services;
- the log management for systems and equipment related or connected to the contractual Service. The "event records" generated by the authentication systems shall contain references to the "username" used, the date and time of the event ("timestamp"), a description of the event (such as, for example, the processing system or software used; whether it is a log-in event, a log-out event, or an error condition; which communication line or terminal device was used), the identification of the system on which the "username" has operated.

1.8.2 The results of the tracking shall be kept in a secure (with authenticated access and non-alterable content) and verifiable manner that guarantees readability, integrity and reliability and shall be shown to the Company upon request.

1.8.3 The Supplier shall ensure full reconstruction of the accesses and changes made to the data for inspection purposes.

1.9. SOFTWARE DEVELOPMENT AND MAINTENANCE

1.9.1 In the case of software development or maintenance activities or which in any case entail the writing/modification of software used by the Company, the Supplier undertakes to use secure software development techniques, which at least envisage the implementation of input data validation, internal processing validation checks, message and output validity checks, and the use of best practices referring to the specific programming language or environment used for development. Throughout the term of the Purchase Order, the Supplier undertakes to comply with the secure software coding guidelines listed in the Open Web Application Security Project (OWASP) and the current CWE/SANS Top 25. The Supplier also undertakes to comply with the document "*Linee guida per la realizzazione di applicazioni web sicure per i Fornitori*" (Secure Coding Practices for Suppliers) containing the guidelines for the secure development of the Company's software, which the Supplier acknowledges and accepts; these guidelines can be consulted in the reserved area in your page on the Suppliers Portal at the following address https://www.almaviva.it/it_IT/Area_fornitori; alternatively, they shall be delivered to

the Coordination Manager of the Company, as stated in the Purchase Order and shall be periodically reviewed.

1.9.2 To the extent that the above activities take place in environments managed by the Supplier, the latter is required to ensure:

- the logical separation between the production environment and other environments;
- that the development, test and production environments are dedicated to the Company and separated, at least logically, from the environments of other customers of the Supplier to guarantee their confidentiality and integrity;
- the performance of test activities in such a way as to guarantee their objectivity, verifiability and repeatability;
- that the production data owned by the Company are not used for testing activities unless suitably anonymised;
- the issue of complete documentation related to the security tests performed;
- that the access to production data is limited to cases of actual and proven need (e.g., "corrective emergency" maintenance) and the time strictly necessary and, in any case, expressly and previously agreed in advance.

1.9.3 The Supplier must guarantee the performance of static code analysis activities (Static Application Security Testing – SAST) on the applications on the perimeter pertaining to the services provided to the Company, also undertaking to provide the Company with the report certifying the absence of critical vulnerabilities within the timeframe agreed with the Company.

1.10. CONNECTION TO THE COMPANY-MANAGED SYSTEMS

1.10.1 In the event of activities that require the connection of the Supplier's equipment to networks, server systems, and applications managed by the Company, the Supplier (subject in particular to compliance, in relation to such equipment, with the provisions of paragraphs 1.1.4 and 1.1.5 above) undertakes to:

- use the methods and punctually follow the instructions given by the Company to make such connection;
- use (where established by the Company) only the dedicated access networks;
- use such connection, as well as the IDs, passwords and, in general, the "access credentials" provided, solely to carry out activities strictly related to contractual activities;
- use, where applicable, secure connections (including through VPN or encryption tools) for connections made through open networks (such as the Internet and Wi-Fi).

1.10.2 The Supplier acknowledges and accepts that the Company is entitled to monitor the accesses and the use made of the connection, also for reasons of security or regularity and operational continuity, and to request information on the technical characteristics of such equipment.

1.11. ACCESS CREDENTIALS OR COMPANY INSTRUMENTS

1.11.1 In all cases in which the Supplier has been provided with credentials or means of identification and access (such as, but not limited to, badges, keys, smart cards, digital certificates) required to access the Company's systems, the Supplier - in compliance with the regulations in force - must:

- guarantee the capacity and reliability of the assignee concerning the task for which the assignment of credentials/tools is requested;
- ensure that such credentials/tools are guarded with the utmost care and are not in any way made available to third parties, and are used only for the performance of the contractually envisaged services;
- ensure that no copies are made, except where authorised by the Company;
- ensure that credentials and tools are used exclusively by the assignees; in all cases in which - in compliance with the rules in force - a change of assignee is made, a document shall be signed to certify such change;
- promptly report to the Company any possible loss of possession (even momentary) as well as any possible violation of the above rules;
- notify the Company of any other event (such as termination of employment; or change of duties) that terminate the need to have such credentials or instruments.

1.11.2 In all cases where the Supplier operates on the Company's systems or procedures that require the use of multi-factor authentication (strong authentication) tools that require the use of mobile devices, the Supplier is required to provide its relevant staff with smartphones that are compatible with the Company's standards and have a cellular phone number that allows for the receipt of SMS and/or data traffic (e.g. Microsoft Authenticator), enabling the use of multi-factor authentication tools used by the Company to control and authorise access to its computer systems. The telephone number associated with the smartphone shall be assigned exclusively to the worker. It is the Supplier's responsibility to report any changes in assignment promptly.

1.12. HARDWARE-RELATED ACTIVITIES - SYSTEM SERVICES AND TLC

1.12.1 In the event of the withdrawal or replacement of computer equipment made available by the Supplier and used by the Company and/or memories of any kind that may contain programs to process or data of the Company, all data contained in the replaced memories shall be irreversibly erased by the Supplier, after the data has been inserted on the new equipment or another suitable support, following the Company's requests.

1.12.2 In all maintenance activities, as well as in system and network management services, measures must be taken - in coordination with the Company - to prevent the loss, even accidental, of data, even if located on equipment other than that on which the intervention is carried out.

1.13. SYSTEM ADMINISTRATORS EX PROVISION OF THE ITALIAN DATA PROTECTION AUTHORITY OF 27/11/2008 AS AMENDED AND SUPPLEMENTED

1.13.1 Should the processing of personal data by the Supplier also involve system administration activities in compliance with the conditions contained in the Provision of the Italian Data Protection Authority of 27/11/2008 as amended and supplemented, the Supplier is bound to apply the conditions set forth in the Provision, particularly those specified below.

1.13.2 The Supplier shall be bound to carry out the necessary preventive reliability checks on the system administrators and the periodic checks, at least once a year, on their work provided for by the Provision above, reporting to the Company upon request.

1.13.3 The Supplier is required to maintain an updated list of the "system administrators" authorised to operate on the Company's data and/or systems and to communicate their details upon request and/or at agreed intervals.

1.13.4 Access to the Company's information system by personnel with administrative privileges shall include access with two-factor authentication (multi-factor authentication) based on mobile devices, following the provisions outlined in section 1.10.2.

1.13.5 The Supplier must collect and keep for at least six months, on a non-alterable basis, the access logs of the administrators to the systems in accordance with the rules set forth in the Provision as mentioned earlier.

1.14. AUDITS AND CONTROLS

1.14.1 The Supplier must carry out regular auditing activities to verify its security systems' effectiveness. The Supplier must allow the Company to independently assess and verify compliance with the Security Rules and any additional agreed provisions by providing, for example, certification according to industry standards or audit reports.

1.14.2 The foregoing shall be without prejudice to the Company's right to conduct audits on the Supplier and/or to make enquiries, including from its auditors and supervisory authorities and/or bodies, either in the event of a security incident or as part of a periodic review of compliance with the regulatory and contractual provisions.

1.14.3 The Supplier shall provide appropriate cooperation in the performance of the audit and, in any event, allow the persons indicated in the preceding paragraph to interview its staff and to have access to:

- all information and documents related to the Services;
- systems, tools, networks, databases, business continuity plans, and other information relating to the Services;
- the facilities and premises where the Service is provided.

1.14.4 The Supplier undertakes, where required, to prepare appropriate remediation plans to eliminate any non-conformities found within the timeframe to be agreed with the Company.

1.14.5 The Supplier grants the Company the right to view - at the Company's request - the results of the Vulnerability Assessment and Penetration Tests carried out internally by the Supplier on the perimeter of the services provided to the Company.