Subject: Security Regulations

The provisions of this Annex supplement - insofar as applicable - the provisions of the Agreement /Framework Agreement to which they are attached, and the definitions contained therein apply to this document.
This Annex defines the control systems and the security standards that the SUPPLIER undertakes to maintain active and efficient for the entire term of any Agreement under which it is required to process confidential data and information of the COMPANY and/or of other companies of the Intesa Sanpaolo Group.

1. Security standards to protect the information assets of the Intesa Sanpaolo Group

1.1 In relation to all activities associated with the performance of an Agreement, the SUPPLIER undertakes to adopt formal internal policies consistent with the current legislation and with the Security Standards as communicated from time to time and to ensure that such policies are release throughout its own organization.

1.2 The SUPPLIER must process the data in accordance with the level of classification, with special reference to the confidentiality, and applying the agreed policies on data retention.

1.3 The SUPPLIER acknowledges and agrees that data relating to the architecture and the configuration of the COMPANY's IT systems, the security measures adopted by the latter and - in any event - data concerning any vulnerabilities found during the execution of the Service (the "Data") is confidential by nature (also pursuant to art. 98 CPI - Intellectual Property Code) and that any disclosure of said data to third parties may cause significant detriment to the COMPANY and/or to other companies of the Intesa Sanpaolo Group, also in terms of exposure to hacking or reputational damage.

1.4 The SUPPLIER undertakes to ensure compliance with the service levels contractually agreed with the COMPANY, also in case of emergency or dispute of resources by its other clients.

1.5 The SUPPLIER acknowledges that any data, software, technical or regulatory documentation and ICT resources of the COMPANY that are used to supply the service shall remain the exclusive property of the COMPANY (and/or the other companies of the Intesa Sanpaolo Group and/or their licensors).

1.6 The SUPPLIER acknowledges that violation of any of the security obligations reported in the present annex constitutes cause for the termination of the Agreement in according to the art. 1455 of the Civil Code.

1.7 The SUPPLIER acknowledges, at any time, that the COMPANY may withdraw permission to perform any activities on its own assets (including the data).

1.8 The SUPPLIER agrees to delete the data whenever requested by the COMPANY, regardless of the conclusion of the contractual relationship.

Milan, 1st December 2020

Place and Date

Stamp and Signature of Supplier

1.9 The SUPPLIER undertakes to return all assets to the COMPANY (including data, licenses and equipment) within the agreed period.
1.10 The SUPPLIER undertakes to apply best practices and generally accepted standards to any situation that is not covered by the required checks.

2. Contact persons for security issues
2.1 The SUPPLIER and the COMPANY shall communicate to each other the names of the persons appointed to manage the activities covered by the Agreement and in particular to manage the aspects of information security.
2.2 Save as provided otherwise by the party making the appointment, the contact person appointed to manage the contractual activities is also responsible for maintaining liaison with the company structures tasked with the management of all aspects of information security. The COMPANY and the SUPPLIER undertake to notify each other promptly of any changes in relation to the above.
2.3 The COMPANY and the SUPPLIER shall agree appropriate communication, coordination and management procedures on occurrence of IT security incidents that may compromise the contractually agreed service levels.

3. Staff and organization of the SUPPLIER
3.1 Having regard to the staff involved in the performance of the contractual obligations (including collaborators working in any capacity), the SUPPLIER undertakes, also in respect of information security, to:
(a) ensure that its staff members are appropriately qualified for the tasks they perform;
(b) ensure that its staff members receive the training necessary to perform their tasks, as well as adequate information concerning the provisions of the above section1;
(c) implement appropriate policies concerning the segregation of duties when assigning tasks;
(d) assign tasks and responsibilities to its staff members in a manner so as to ensure that key internal and external threats, also internet-related, are effectively monitored;
(e) Adopt formal and secure procedures to immediately revoke user credentials and ensure that all tools used to perform the contractual activities are returned, including badges, keys and other means of access, identification or authentication, when any of its staff members are transferred to other roles or their employment contract is terminated.
3.2 The SUPPLIER undertakes to cooperate with the COMPANY to ensure appropriate coordination with the roles and procedures defined internally by the COMPANY in connection with the risk analysis process and the data management system.

Milan, 1st December 2020

Place and Date

Stamp and Signature of Supplier

3.3 The SUPPLIER undertakes to maintain (a) a list of the sites in which are hosted (i) the data, (ii) the services and (iii) data centers used by the SUPPLIER to provide the Service and (b) a document indicating the number of staff members who have access to data of the COMPANY and/or of the Concerned Companies, and to update this document at regular intervals and provide a copy to the COMPANY and/or to the Concerned Companies, upon written request of the COMPANY and/or any of the companies involved.
3.4 The SUPPLIER promptly undertakes to notify the COMPANY of the need to transfer resources and data (including backups) from one site/data center (belonging to the SUPPLIER or to a third party) to another and to implement in the new data center the same security measures as in the primary site. It is however understood that the COMPANY must previously authorize the transfer of resources and data from one site/data center to another.
Furthermore, the SUPPLIER undertakes to implement in the new center the same security measures as the ones of the primary site. Any prohibitions / restrictions on the movement of resources and data that may already be foreseen in the Agreement remain unaffected.
3.5 The SUPPLIER guarantees that, in case of subcontracting of activities (which must be authorized and monitored in accordance with the procedures defined in the Agreement), all the provisions relating to the management of the data contained in these Security Regulations (with particular reference to confidentiality, retention and deletion of data), the audit and verifications are applied by the entire supply chain. It is understood that the sub-contracting does not decrease the responsibility of the SUPPLIER, who is in any case required to constantly check and monitor such subject.
3.6 In any case of change in the SUPPLIER organization (also due to transfer's events according to the article 3.4 above or changes of sub-contractors, or change of technologies or architectures of sub-contractors) that may affect the level of integrity, availability and confidentiality of data (anyway in case of change of sub-contractors), the SUPPLIER must notify the COMPANY in advance to allow the execution of appropriate assessments and verifications, also by means of audit.
3.7 The SUPPLIER undertakes not to introduce changes (technological, on the services organization and the supply chain) that can be decrease the security of the Service.

4. Physical and logical security of the SUPPLIER

4.1 As specified above - in respect to its own company services that are in any case related or linked to the performance of the services under the Agreement, the SUPPLIER undertakes to adopt legally compliant security measures to manage user credentials and access privileges, with provisions for:
(a) unique and personal user profiles;
(b) secure management of user credentials at regular intervals, mandatory modification at first time access, assurance that credentials cannot be re-used over time and automatic password strength tests;

Milan, 1st December 2020

Place and Date

Stamp and Signature of Supplier

(c) criteria and policies to ensure that access and user credentials are release in accordance to the segregation of duties criterion;
(d) criteria and policies to ensure that access is denied if access privileges have not explicitly been given and to ensure compliance with the principle of least privilege;
(e) criteria and policies concerning the levels of access privileges, which at least make a distinction between authority to access production data and authority to access and carry out maintenance on systems, software and the network.
(f) tools and policies concerning the safekeeping of data received and storage media so as to prevent loss and accidental access by third parties.

4.2 The SUPPLIER guarantees that physical security measures will be implemented (locked rooms, clean-desk policy, safe storage of media received...) at all critical sites used for or in connection with the service supplied (and in the routes from or to such sites). If the service is provided on the premises of the COMPANY and/or of the other companies of the Intesa Sanpaolo Group, the SUPPLIER undertakes to make correct use of the procedures present and to report any deficiencies/malfunctions.

4.3 The destruction of data/media on termination of contractually envisaged activities shall take place in accordance with procedures and standards that meet the security requirements of the related contractual service.

4.4 The SUPPLIER undertakes to adopt appropriate procedures to separate the data, which it manages on behalf of the COMPANY from data it manages on behalf of other customers to ensure the confidentiality, availability and integrity of such data.

4.5 The SUPPLIER undertakes to send a detailed technical description of the methodology it intends to use – in the execution of the Contract - to deliver the Service, and to implement and manage physical, organizational and IT security measures for the protection of the COMPANY's assets, and aimed at guaranteeing a service that is compliant with the level of classification required - with particular regard to procedures and tools for:
(a) The management of the life cycle (provisioning / deprovisioning), of user credentials (end users and administrators), and of the related problems of profiling in case of their access to systems, applications and networks;
(b) Guaranteeing adequate levels of authentication, authorization and tracking, in case of remote access to the COMPANY's IT assets;
(c) The physical and logical protection of the SUPPLIER's Data Center, in case of outsourced services;
(d) The protection from malicious software;
(e) The management of basic and application software patching, fixing and upgrading;
(f) The management and keeping of storage media;
(g)The controlled disposal of assets with the adoption of systems for the secure deletion of information from storage media;
(h) The tracking and management of events relevant to safety according to the external normative provisions on the subject;
(i) The implementation of adequate data isolation mechanisms between data managed by the SUPPLIER on behalf of the COMPANY and data managed on behalf of its other customers, to guarantee their confidentiality and integrity".

Milan, 1st December 2020
Place and Date

Stamp and Signature of Supplier

5. Secure use of the SUPPLIER's systems

5.1 The SUPPLIER undertakes to ensure the management of the following activities:

(a) Security incident management, including the identification, containment, reporting, timely notice and analysis of IT security incidents and events, using an appropriate escalation list. In detail, the SUPPLIER shall immediately inform the COMPANY, also in extra-working hours, of any significant event that involves information associated with the contractual services, also sending the appropriate document properly completed (Information Set) in the appendix to this Annex;

(b) ensuring compliance with the security incident response times agreed in the SLAs;

(c) security patch management, by means of controlled updating processes and timing appropriate to the seriousness of the vulnerability, not exceeding six months (in accordance with current legislation) and less than 5 days in the most serious cases;

(d) antivirus management, via regular updates in accordance with the specifications of the antivirus system used;

(e) change management: implementation of authorisation processes for permission to make changes;

(f) controlled data erasure, using secure systems to delete data from storage media;

(g) prohibition of issue press releases (also through channels such as media, social media, regulators, …) that concerning any IT security incidents occurred, without first agreeing with the COMPANY the contents and timing of the communication.

5.2 The SUPPLIER undertakes to implement SPF and DKIM protocols (and possibly DMARC as well) for all its corporate mail domains. Furthermore, in case the SUPPLIER shall provide services involving the sending of e-mails, on behalf of the COMPANY's corporate sub-domains (e.g. comunicazioni@intesasanpaolo.com), the SUPPLIER undertakes to implement the DMARC (Domain-based Message Authentication, Reporting and Conformance) protocol.

6. Data backup

6.1 The SUPPLIER undertakes to regularly backup the data associated with the contractual activities (including configuration data relating to devices and systems), ensuring that:

(a) backup copies are kept in a secure fireproof and intrusion-proof area;

(b) backup copies can be recovered and dedicated recovery tests are performed at regular intervals;

(c) User data are kept separate from the configuration data to be backed up.

6.2 The COMPANY reserves the right to access the backups made by the SUPPLIER by forwarding prior written request to the SUPPLIER.

6.3 The SUPPLIER undertakes to store and migrate the COMPANY's data in specific countries indicated by the COMPANY itself and, furthermore, undertakes to agree with the COMPANY to the channel through which the migration of the data must be performed.

Milan, 1st December 2020
Place and Date

Stamp and Signature of Supplier

7. Tracking

7.1 The SUPPLIER undertakes to perform the following activities in a systematic and formalized manner, in accordance with laws in force:

(a) Tracking of the software used for or in connection with the performance of the contractual services;

(b) Tracking of the systems and devices used for or in connection with the contractual services.

The event records generated by the authentication systems must indicate the "username" used, the date and time of the event ("timestamp"), a description of the event (e.g. the processing system or software used, whether it is a log-in or log-out event, error condition, the communication line or computer terminal used) and the system on which the "username" has operated.

In particular, if the recorded data refers to bank transactions that are processed and covered by the Decisions of the Italian Data Protection Authority regarding "*regulations* on *circulation of information in the banking sector and tracking of banking operations"* (Decision n. 192 of 2011 and following Decisions), the following data must also be tracked:

- The identifier of the customer referred to in the transaction;
- The type of contractual relationship in place with the customer.

7.2 The tracking results must be stored in a secure manner so as to ensure auditability, readability, integrity, reliability and the availability of the information on request (also directly by the Audit function of Intesa Sanpaolo S.p.A.).

7.3 The SUPPLIER shall ensure the traceability of all accesses and changes made to data, also for inspection purposes.

8. Software development and maintenance

8.1 In the case of software development or maintenance or activities that involve writing/modifying the software used by the COMPANY and/or the other companies of the Intesa Sanpaolo Group, the SUPPLIER undertakes to use secure software development techniques which include, at least, the validation of input data, internal processing validation checks, message and output validity checks, use of best practice in relation to the specific programming language or development environment used. For the whole duration of the Agreement, the SUPPLIER undertakes to comply with the software secure coding guidelines listed in the Open Web Application Security Project (OWASP) and the CWE/SANA Top 25 time by time in force. The SUPPLIER also undertakes to comply with the internal regulation document "Security measures for the safe development of the software" time by time in force.

8.2 If the development relates to application within the scope of PCI-DSS certification, the SUPPLIER undertakes to keep its team members up to date on secure code development techniques through appropriate training initiative on, at least, an annual basis.

Milan, 1st December 2020

Place and Date

Stamp and Signature of Supplier

8.3 Insofar as the aforementioned activities are carried out in environments which are managed by the SUPPLIER, the latter shall ensure:
(a) The logical separation between the development environment and all other environments relevant to the company;
(b) That the development, testing and production environments dedicated to the COMPANY and/or the other companies of the Intesa Sanpaolo Group are separated, at least in logical terms, from the environments used for the SUPPLIER's other customers so as to ensure confidentiality and integrity.
(c) Run the tests in an objective, verifiable and repeatable manner
(d) Do not use the proprietary production data of the COMPANY (and/or the Intesa Sanpaolo Group) for testing activities unless appropriately anonymized;
(e) Produce a complete documentation of the tests carried out in security areas;
(f) Access to "production" data or in any to case personal data should be limited to cases of actual and real need (e.g. "emergency corrective maintenance"), limited to the time strictly necessary and in any case specifically and previously agreed upon.

9. Connection to the systems managed by the COMPANY
9.1 In the case of activities which involve connecting the SUPPLIER's equipment to the COMPANY's networks and/or systems, the SUPPLIER (save as specifically provided in relation to said equipment under sections 1, 4 and 5 above) undertakes:
(a) Use only the dedicated access networks (where made available by the COMPANY) or those networks which are separated from the internal network managed by the COMPANY (and/or the other companies of the Intesa Sanpaolo Group);
(b) Use such connections, and the IDs, passwords and "user credentials" provided, only for the purposes strictly necessary to complete the contractual activities;
(c) Use secure connections (including VPN or encryption tools), where made available by the COMPANY, if the connection is via open networks (internet, Wi-Fi...).
9.2 The SUPPLIER acknowledges and agrees that the COMPANY (and/or the Parent Company INTESA SANPAOLO S.p.A.) may monitor accesses and uses of the connection, also for security reasons and to ensure that operations continue to run smoothly and may request information on the technical characteristics of the equipment used.

10. Credentials or tools owned by the COMPANY
10.1 In all cases in which the SUPPLIER is provided with credentials, IT tools or IDs and other means of access (e.g. badges, keys, smart cards, digital certificates, etc...) to access the systems of the COMPANY (and/or of the other companies of the Intesa Sanpaolo Group), the SUPPLIER - in accordance with the applicable provisions of law - shall:
(a) Provide assurance as to the ability and reliability of the person assigned to the task for which the credentials/tools are being provided;

Milan, 1st December 2020
Place and Date

Stamp and Signature of Supplier

(b) Ensure that such credentials/tools are kept safe, never made available to third parties and used only to perform the services under the Agreement;
(c) Ensure that no copies are made, unless authorized by the COMPANY;
(d) Ensure that the credentials and tools provided are used solely by the assignees; in all case in which - in accordance with current regulations - the assignee changes, a document shall be undersigned to confirm such change;
(e) Promptly notify the COMPANY of any loss of the credentials/tools (even temporary) and of any potential breaches of the provisions above;
(f) Notify the COMPANY of any other event (e.g. termination of employment Agreement; redeployment...) which results in such credentials or tools being no longer necessary

10.2 In all cases where the SUPPLIER operates on systems or procedures of the COMPANY (and/or the Companies of the Intesa Sanpaolo Group) that involve the use of multi-factor authentication tools (strong-authentication) requiring the use of mobile devices, the SUPPLIER is bound to provide to its involved staff smartphones with features compatible with the COMPANY's standards and that allows SMS and data traffic reception, elements enabling the use of multi-factor authentication tools used by the COMPANY to control and authorize access to its IT systems.
The phone number associated with the smartphone must be assigned exclusively to the worker and will be recorded by the COMPANY's Operating Representative in the COMPANY's Security Phone Book. It is the SUPPLIER's responsibility to report promptly any change of assignment.

11. Activities regarding hardware - system engineering services and TLC

11.1 In the case of withdrawal or replacement of IT equipment used by the COMPANY and/or of data storage devices of any kind containing computer programs or data of the COMPANY, of the companies of its Group and/or of its/their customers or assignees, all data contained in the storage devices to be replaced must be permanently erased by the SUPPLIER after transferring the data to the new equipment or to suitable media, as may be requested by the COMPANY.

11.2 In all maintenance activities and in all system engineering and network management activities, precautions must be taken – in coordination with the COMPANY – to avoid data loss, accidental or otherwise, including data stored on other equipment other than that subject to maintenance.

12. Administrators

12.1 The SUPPLIER shall maintain an updated list of the “system administrators” authorized to work with the COMPANY’s data or systems and shall provide these details upon request and/or in accordance with the agreed frequency.

12.2 The SUPPLIER shall conduct the required reliability checks in advance and any other regular checks required under the laws in force, providing an account of such checks whenever requested.

12.3 Access to the information system of the COMPANY (and/or of the Intesa Sanpaolo Group) by the personnel with administrative privileges requires access with 2-factor authentication on mobile devices. Therefore please refer to point 10.2.

Milan, 1st December 2020
Place and Date

Stamp and Signature of Supplier

13. Auditability and checks

13.1 The SUPPLIER shall conduct regular audits to verify the efficiency of the security systems. The SUPPLIER shall allow the independent assessment and verification of conformity with the agreed provisions, for example, by providing a certification that states the compliance with the industry-specific standards or an audit report.

13.2 The above sentence does not affect the right to conduct direct audits and/or to make requests for information required by law or by the Agreement in favor of the COMPANY, its auditors and by the Authorities and/or Institutions, and in the event of a security incidents and as part of a periodic verification of compliance with the regulatory and contractual provisions.

13.3 The SUPPLIER shall cooperate to perform the audit and any case allow the subjects indicated in the article above to interview its staff (in compliance with current legislation and regulations) and may access:

(a) All information and documents associated with the services;

(b) The systems, the instruments, the network, the databases, the business continuity plans and any other information relating to the services;

(c) The structures and areas in which the service is supplied.

13.4 The SUPPLIER agrees and accepts that the Internal Audit Function of the parent company Intesa Sanpaolo S.p.A. has the right to perform direct audits for all contractual relationship relating to one of the Intesa Sanpaolo Group legal entities.

13.5 The SUPPLIER undertakes, if required, to prepare the appropriate remediation plans to eliminate any unconformities within the agreed time frames.

14. Additional security requirements for cloud outsourcing

In case of cloud outsourcing of the service/solution, in addition to clauses reported in the previous chapters, at least, the following requirements must be guaranteed:

14.1 In the event of termination of the Agreement, the SUPPLIER undertakes to support the COMPANY in managing the exit strategy by transferring the devices, systems, data to a third party supplier or supporting the re-insourcing the activity.

14.2 In case in which the COMPANY does not use its own audit resources and in any case in which the service is not concerning an Important Operating Function (FOI) or a Critical Components of the Information System (CCSI), the COMPANY can use at least one of the following tools:

(a) Pooled audits organized jointly with other clients of the SUPPLIER;

(b) Third-party certifications and third party's or SUPPLIER's audit reports;

14.3 The SUPPLIER undertakes to implement the security checks specified in the cloud controls matrix provided by the COMPANY, defined by the CSA CCM (Cloud Security Alliance Cloud Controls Matrix) framework. Furthermore, the SUPPLIER undertakes to provide, on request of the COMPANY, the documentation and evidence necessary to confirm compliance.

14.4 The SUPPLIER undertakes to notify the COMPANY, via the appointed contact persons for security issues set out in section 2 above (Contact persons for security issues), about the impossibility to implement any of the checks envisaged in the cloud controls matrix.

Milan, 1st December 2020
Place and Date

Stamp and Signature of Supplier

This commitment must be maintained even after entering into the Agreement.

14.5 The SUPPLIER undertakes to prepare a specific documentation describing the internal management procedures of the changes in production and the related roles/rights/responsibilities within the Cloud.

14.6 The SUPPLIER undertakes to implement open encryption methods (3.4AES, AES, etc.) to protect data in case they need to pass through public networks (e.g. Internet);

15. Vulnerability Assessment and Penetration Test

15.1 The SUPPLIER shall ensure the performance of internal Vulnerability Assessment activities at least every six months on the scope of the services provided to the COMPANY;

15.2 The SUPPLIER shall guarantee the performance of internal Penetration Tests at least yearly, on the scope of the services provided to the COMPANY;

15.3 The SUPPLIER shall also grant to the COMPANY the right to examine upon request of the COMPANY the results of the Vulnerability Assessment and Penetration Tests carried out internally on the scope of the services provided to the COMPANY.

Milan, 1st December 2020

Place and Date

Stamp and Signature of Supplier