INTESA SANPAOLO

**Subject: Security regulations**

The provisions of this Annex supplement - insofar as applicable - the provisions of the General Conditions 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 the 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, in relation to the services that will actually be provided by it under the agreements in place with the COMPANY and/or the other Companies of the Intesa Sanpaolo Group.

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

**1.1** The SUPPLIER undertakes, for all the activities inherent and attributable to the performance of the contractual services, to adopt internal policies, appropriately formalized and disclosed internally, consistent with the contents of current legislation.

**1.2** In particular, the SUPPLIER undertakes to adopt, in line with the COMPANY's objectives and risk strategy, security policies related to the storage and protection of data as well as processes, methodologies and technologies that contribute to compliance with the policies themselves.

**1.3** The SUPPLIER must process the data in accordance with their level of classification, with particular reference to confidentiality, applying the agreed data retention policies.

**1.4** The SUPPLIER acknowledges that the data related to the COMPANY's architectures and configurations of the information systems, the results of the checks carried out, the security measures adopted by the latter, as well as - in any case - the data related to any vulnerabilities encountered during the execution of the service, is the COMPANY'S confidential information for the purposes of the contractual provisions on confidentiality and that their external disclosure can lead to serious damage to the COMPANY and/or to the other Companies of the Intesa Sanpaolo Group, also in terms of exposure to external attacks or effects on image and reputation.

**1.5** The SUPPLIER acknowledges the COMPANY'S exclusive ownership of data, of the software, of the technical and regulatory documentation and of ICT resources (and/or the other Companies of the Intesa Sanpaolo Group and/or their cause) whether they are used to supply the service or made available for the provision of the service.

**1.6** The SUPPLIER acknowledges that the violation of the security obligations indicated in this Annex constitutes a serious breach on behalf of the SUPPLIER, for the potential termination of the Agreement.

**1.7** The SUPPLIER recognizes the COMPANY the right to revoke the authorization to

INTESA SANPAOLO

access its premises at any time (and/or to revoke any users/access to its systems) and to carry out any activity on the assets, including data.

**1.8** The SUPPLIER undertakes, in any case of termination of the Agreement, to erase - by making use of appropriate tools and technical solutions, duly documented - the COMPANY's data that are present on its systems or supports due to previously provided services, without prejudice to the regulations concerning personal data.

**1.9** The SUPPLIER undertakes to return the COMPANY'S assets (including data, licenses and equipment) without undue delay and without hindering the COMPANY, whether the latter decides for another supplier, in order to guarantee the continuity of the service.

**1.10** The SUPPLIER guarantees, whether a specific case is not expressly declined by the provided requirements, to act in compliance with what is indicated by the best practices and recognized standards on the matter.

**1.10.1** The SUPPLIER guarantees to carry out and/or provide the services using the most recent Strong Customer Authentication technologies on the market and in any case, with regard to specific security issues, in compliance with any legislations/regulations/technical specifications related to the areas subject to development (e.g., RTS PSD2, PCI-DSS).

**1.11** The SUPPLIER undertakes to guarantee the security requirements that are present within this Annex, even when the service is provided by teleworking.

**1.11.1** In the event that the service is carried out by the SUPPLIER outside the European Union and/or its employees operate from outside the European Union, they must request prior authorization to the COMPANY.

**1.12** Whether the SUPPLIER provides an outsourced service that is identified as essential or important, the SUPPLIER must prove with adequate certifications (e.g., ISO27001, Report SOC1, Report SOC2) its compliance with the IT security standards appropriate to the provision of the service.

**1.13** The SUPPLIER, in case the service supplied provides for the use of cloud solutions that are directly delivered from the SUPPLIER or through the use of additional third parties, agrees to make available the certifications in the cyber domain (e.g., ISO 27001, PCI -DSS, SOC-1 etc.) also for the Cloud Datacenter (ISO27001, CSA CCM, SSAE-16/ISAE3402).

## 2. Contact persons for security issues

**2.1** The SUPPLIER and the COMPANY, in order to share the tasks and responsibilities related to the implementation of the Information Security policy, commit to communicate to each other the names of the contact person entrusted with the management of the contractual activities and in particular the management of the information security aspects.

**2.2** Unless otherwise expressly indicated by the SUPPLIER, the contact person appointed for the management of contractual activities is also considered responsible for the connection between the two Company structure, responsible for managing all aspects

of information security. The COMPANY and the SUPPLIER undertake to promptly notify each other of any changes in this regard.

**2.3** The COMPANY and the SUPPLIER must jointly define the communication, coordination and management procedures, in the event of an incident that could compromise data security and/or business continuity and/or contractually defined service levels.

**3. Staff and organization of the SUPPLIER**

**3.1** In relation to the personnel involved throughout the execution of contractual obligations (including collaborators in any capacity), the SUPPLIER undertakes, also for the purposes of information security and for the entire duration of the Contract, to:

a) to ensure that the personnel have adequate qualifications for the tasks performed and, where foreseen, to employ adequately certified personnel;
b) to ensure that such personnel receive the necessary training and the adequate information on the rules referred to in paragraph 1 - Security standards to protect the information assets, at least annually;
c) to provide evidence of the training, when requested by the COMPANY;
d) to respect, the principles of the segregation of duties during the assignment of duties and tasks;
e) to guarantee, in the event of termination of the employment relationship or in case of a change of assignment - through formalized and secure processes - the immediate revocation of the credentials granted to its staff and to return the tools assigned for the performance of the activities related to contractual services (e.g., badges, keys and other access tools, identification and authentication).

**3.2** The SUPPLIER undertakes to collaborate with the COMPANY in order to ensure the connection with roles and procedures defined within the COMPANY for the IT risk analysis process established to guarantee the effectiveness of the protection measures concerning the ICT resources and for the data management system that continuously ensures the integrity, accessibility, availability, confidentiality, completeness, correctness and security of the data stored and the information represented.

**3.3** The SUPPLIER undertakes to keep a list of the places where they host: (i) the data, (ii) the services and (iii) the data centers used by the SUPPLIER for the provision of the service.

**3.3.1** The SUPPLIER undertakes to keep a document, regularly updated, indicating the management of physical and logical accesses, to be made available to the COMPANY and/or the Companies of the Intesa Sanpaolo Group, upon written request by the COMPANY and/or each of the Companies of the Intesa Sanpaolo Group.

**3.4** The SUPPLIER undertakes to communicate to the COMPANY, with at least 30 days' notice, the need to transfer resources and data (including backups) from one site/data center (its own or a third party's one) to another and to implement in the new center the

Place and Date

Stamp and Signature of SUPPLIER

same security measures as the primary site. However, it is understood that the transfer of resources and data from one site/data center (yours or that of a third party) to another must be authorized in advance by the COMPANY.
This is without prejudice to any prohibitions/restrictions on the transfer of resources and data that may already be provided within the Contract.

**3.5** In case of the SUPPLIER'S organizational changes, also due to transfer events, changes of technologies or concerning architectures which may impact the levels of security provided within the Agreement and the levels of integrity, availability and confidentiality of the data, the SUPPLIER must notify the COMPANY in advance in order to allow for appropriate assessments and verifications, including by means of an audit.

**3.6** The SUPPLIER undertakes not to introduce changes (technological, service organization and related to the sub-contracting chain) that may diminish the security of the service.

**3.7** The SUPPLIER agrees to ensure that time-out sessions are implemented on all systems that process the COMPANY's data.

**4. Physical and logical security of the SUPPLIER**

**4.1** The SUPPLIER - without prejudice to the foregoing - undertakes to use, for all its corporate services, inherent or attributable to the performance of contractual services, security measures for the management of credentials and access privileges:

a) compliant with the law, providing for unique and personal user profiles;
b) that provide, with reference to the password, periodic expiration and mandatory modification at first access, guarantee of non-reusability and historicization over time and automatic robustness checks;
c) that provide policies for assigning credentials and access privileges that guarantee the adoption of the principles concerning segregation of duties, need to know and privileges denied unless explicitly granted to guarantee the principle of minimum privilege;
d) that provide policies and criteria concerning the levels of access privileges, that make a distinction between access to production data, access and maintenance of systems, software and network;
e) that provide tools and policies for the safekeeping of data received and storage media in order 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 etc.) at all critical sites used for or in connection with the supplied service (and in the connection from or towards such sites). Whether the service is provided on the COMPANY's premises 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 related deficiencies/malfunctions.

Place and Date

Stamp and Signature of SUPPLIER

INTESA SANPAOLO

**4.3** The destruction of data/media at the end of the contractually planned activities or upon specific request by the COMPANY, will be carried out through procedures and standards that comply with the security requirements indicated in the Agreement and/or agreed with the COMPANY.

**4.4** The SUPPLIER undertakes to implement appropriate data isolation mechanisms managed on behalf of the COMPANY regarding data managed on behalf of other customers to guarantee their confidentiality, availability and integrity.

**4.5** The SUPPLIER undertakes to provide a technical description of the ways in which, in execution of the Agreement, it intends to provide the service and to implement and manage the IT, physical and organizational security measures for the protection of the COMPANY's assets, aimed at guaranteeing a service compliant with the required classification level, with particular reference to procedures and tools for:

a) the management of the life cycle (provisioning/deprovisioning) of all user standards and the related profiling problems of the same regarding access to systems, applications, networks and data;
b) to ensure adequate levels of authentication, authorization and tracing in the case of remote access to the information assets of the COMPANY;
c) the physical and logical protection of the SUPPLIER's data center;
d) the protection against 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 management and tracing of events relevant to security purposes and on the basis of the provisions of the external regulations' reference;
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;
j) the internal management of changes within the production environment and the related roles/rights/responsibilities also for what concerns the cloud.

## 5. Secure use of the SUPPLIER's systems

**5.1** The SUPPLIER undertakes to guarantee the management of IT security events and/or business continuity through the identification, containment, reporting, notification, tracking, analysis and remediation activities of IT security events and/or business continuity, identifying an escalation list, formalizing it in an appropriate procedure periodically tested and updated.

**5.1.1** Having regard to the previous requirement, the SUPPLIER undertakes:

a) to inform, without undue delay and as soon as it becomes aware of it, the

Place and Date

Stamp and Signature of SUPPLIER

INTESA SANPAOLO

COMPANY in the person of the Operational Representative or structure to be define jointly, of any significant event occurring in relation to the integrity, availability, accessibility, confidentiality, and security of the information related to the service subject of the Contract, also by sending the appropriate document duly completed (Information Set) as the appendix to this Annex;

b) to ensure compliance with the response times to security incidents agreed within the Agreement or, in absence of this, the management of the same in ways that guarantee compliance with the contractual service levels;
c) to notify the COMPANY (in the person of the Operational Representative or structure to be jointly defined) of the occurrence of any significant IT security and/or business continuity event that directly/indirectly impacts the supply provided to the COMPANY;
d) to notify the COMPANY in the event of end of support of platforms and IT solutions that are subject matter of this Agreement (e.g., operating systems or database server versions no longer supported by the reference vendor), taking into consideration the obligation to keep them updated;
e) to guarantee the management of security patch management activities carried out with controlled update processes, without undue delay and with times adequate to the severity of the vulnerabilities, in any case not exceeding six months or, in the most serious cases, 15 days;
f) in the case of applications and systems within the PCI-DSS scope, the SUPPLIER undertakes to guarantee the implementation of the security patch management activities carried out with controlled updated processes, without undue delay and with times adequate to the severity of the vulnerabilities, in any case not exceeding three months or, in the most serious cases, 15 days;
g) to guarantee the implementation of antivirus management activities carried out with periodic updating in compliance with the requirements for a correct use of the adopted antivirus system;
h) to guarantee the deployment of change management activities through the implementation of authorization processes for the execution of changes;
i) to guarantee the controlled disposal of assets by adopting systems for the secure deletion of information from storage media;
j) not to issue press releases or comments (also through channels such as media, social media, regulators, etc.) which present events that have compromised the integrity, availability and confidentiality of the data;
k) to employ adequate antispam tools by implementing the most recent protocols (for example, SPF - Sender Policy Framework, DKIM - Domain Keys Identified Mail and, if supported, also DMARC - Domain-based Message Authentication, Reporting and Conformance);
l) to employ strong encryption systems and, in particular, the AES256 protocol for data at rest;

m) to use strong encryption systems and, in particular, the TLS1.2 protocol for data in transit;
n) to implement open encryption methods (3.4AES, AES, etc.) to protect the data in the event that these must cross public networks (e.g., Internet).

**6. Data backup**

**6.1** The SUPPLIER undertakes to periodically back up the data related to the activities and processes agreed in the Agreement. In particular, the SUPPLIER must ensure:

a) the storage of backup copies in a safe and fire-proof and intrusion-proof place;
b) the recovery from backup copies and the execution of dedicated recovery tests with an agreed frequency;
c) the storage of backup copies concerning the contractual relationship;
d) the retention of backup copies concerning configuration data originated from the systems and from the equipment that contribute to ensuring the provision of the service.

**6.2** The COMPANY reserves the right to view the contents of the backup copies made by the SUPPLIER related to the COMPANY's data, by making a prior written request to the SUPPLIER.

**6.3** The SUPPLIER undertakes to apply encryption techniques to the devices containing the backups, ensuring at least the same level of protection as the original dataset (see reference to requirement 5.1.1 l,m,n), and to protect them from unauthorized access, modification, and deletion when historicized, on-site and off-site. The measures implemented must ensure that the dataset is protected from deletion or malicious encryption (e.g., ransomware attack).

**6.4** 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 on the identification of the channel through which the migration of the data must be performed.

**7. Tracking**

**7.1** The SUPPLIER undertakes to carry out in a systematic and formalized manner:

a) application tracking for software inherent or attributable to the performance of contractual services;
b) tracking for systems and devices used for or in connection to the service covered by the Agreement.

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:

a) the code of the customer involved in the transaction;
b) the type of contractual relationship of the customer.

**7.2** Furthermore, the SUPPLIER undertakes to adopt security policies for the management of system logs as well as processes, methodologies and technologies that contribute to compliance with security policies with particular regard to the integrity and availability of the logs.

**7.3** The SUPPLIER ensures that 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.

**7.4** The SUPPLIER must ensure the traceability of all accesses and changes made to the COSTUMER's data.

**8. Software development and maintenance**

**8.1** In the case of software development or maintenance activities 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 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 duration of the Agreement, the SUPPLIER undertakes to comply with the secure coding guidelines of the software listed in the Open Web Application Security Project (OWASP) and by the CWE/SANS Top 25.

**8.1.1** The SUPPLIER also undertakes to respond, without undue delay and as soon as it receives notification from the COMPANY to any vulnerabilities that may emerge from the assessment carried out using the COMPANY tools for verifying the secure software development requirements.

**8.2** In case the development referred to applications within the PCI-DSS scope, the SUPPLIER is committed to keep the members of its team up to date on the secure code development techniques through specific training initiatives on a minimum annual basis.

**8.3** To the extent that the above activities take place on environments managed by the SUPPLIER, the latter must ensure:

a) the presence of a change management procedure for ICT applications and resources that formally define and guarantee control over changes, replacements or technological adjustments;
b) at least the logical separation between the production environment and the other environments;

c) 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;
d) the execution of test activities in order to ensure their objectivity, verifiability and repeatability;
e) that production data owned by the COMPANY is not being used (and/or the Intesa Sanpaolo Group) for test activities unless appropriately anonymized;
f) to produce complete documentation of the tests carried out in the security field;
g) that access to production data or in any case to personal data is limited to cases of actual and real need (e.g., "emergency corrective maintenance"), is limited to the time strictly necessary and is in any case specifically and previously agreed upon.

**9. Connection to the systems managed by the COMPANY**

**9.1** In the case of activities that require the connection of the SUPPLIER's equipment to the networks and/or systems managed by the COMPANY, the SUPPLIER (subject in particular to compliance, in relation to such equipment, with the provisions of the previous points 1, 4 and 5) undertakes to use (where set up by the COMPANY):

a) only dedicated access networks or in any case separate from the internal network managed by the COMPANY (and/or the other Companies of the Intesa Sanpaolo Group);
b) such connections, and the IDs, passwords and "user credentials" provided, only for the purposes strictly necessary to complete the contractual activities;
c) secure connections (also by means of VPN or encryption tools) for connections made via open networks (internet, wi-fi, ...).

**9.2** The SUPPLIER acknowledges and accepts that the COMPANY (and/or the parent COMPANY Intesa Sanpaolo S.p.A.) has the right to monitor the access and the use made of the connection, also for security reasons, for regularity and for the business continuity, and to request information on the technical characteristics of such equipment.

**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 the COMPANY's systems (and/or of the other Companies of the Intesa Sanpaolo Group), the SUPPLIER, in accordance with the applicable provisions of law, must:

a) provide assurance as to the ability and reliability of the person assigned to the task for which the credentials/tools are being provided;
b) ensure that such credentials/tools are kept with care and are not in any way made available to third parties and are used only for the performance of the contractually

INTESA SANPAOLO

provided services;

c) ensure that no copies are made, unless authorized by the COMPANY;
d) ensure that these 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 will be signed certifying this change;
e) promptly report to the COMPANY any loss of possession (even temporary) as well as any possible violation of the above rules;
f) report to the COMPANY any other event (e.g., termination of the employment relationship; change in duties, etc.) which make the credentials or tools 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 allow 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.

**11. Activities regarding hardware - system engineering services and TLC**

**11.1** In case of withdrawal or replacement of IT equipment made available by the SUPPLIER and used by the COMPANY and/or any type of memories that may contain programs to process data of the COMPANY or of the Intesa Sanpaolo Group Companies, all data contained in the replaced memories must be irreversibly erased by the SUPPLIER, after transferring the data on the new equipment or on suitable support, as requested by the COMPANY.

**11.2** In all maintenance activities, as well as in systems and network management, measures will have to be taken - in coordination with the COMPANY - in order to prevent accidental loss of data, also resident on equipment other than that where interventions are performed.

**12. Administrators**

**12.1** The SUPPLIER is required to maintain an updated list of the system administrators authorized to operate on the COMPANY's data or systems, to proceed with their formal assignment and to communicate their details upon request and/or according to the agreed intervals.

**12.2** The SUPPLIER is required to carry out the necessary preventive reliability checks, as well as the periodic checks required by the law, reporting them when necessary.

**12.3** The SUPPLIER undertakes to ensure that the system administrators authorized to operate on the COMPANY's data or systems receive adequate training on the roles and responsibilities deriving from this assignment.

Place and Date

Stamp and Signature of SUPPLIER

**12.4** Access to the information system of the COMPANY (and/or the Intesa Sanpaolo Group Companies) by personnel with administrative privileges requires access with 2-factor authentication based on a mobile device. Therefore, refer to the provisions of requirement 10.2. However, the COMPANY reserves the right to adopt alternative forms to the mobile device for the management of the second factor by giving prior and timely information to the SUPPLIER.

**13. Auditability and checks**

**13.1** The SUPPLIER shall perform regular auditing activities, relying on third parties recognized by the certifying bodies and identified by the COMPANY, to verify the effectiveness of its security safeguards. The SUPPLIER shall allow independent assessment and verification of compliance with this obligation and the agreed provisions by making available, for example, certification according to industry standards or audit reports.

**13.2** What stated above does not affect the right to carry out direct audits and/or investigations as provided by the law or by the Agreement in favor of the COMPANY, its auditors and the Authorities and/or Institutions, either in case of a security incident or within the framework of a periodical verification concerning the compliance with the legal and contractual provisions.

**13.3** The SUPPLIER must cooperate appropriately in carrying out audit activities and in any case allow the subjects indicated in the previous paragraph to:

a) interview their staff (in compliance with the laws and regulations in force);
b) have access to all the information and documents related to the services;
c) access to systems, tools, networks, databases, business continuity plans, and other service-related information;
d) have access to the facilities and premises where the service is delivered.

**13.4** Upon explicit written request submitted by the COMPANY, the SUPPLIER undertakes to collaborate with the same in the execution of assessments aimed at certifying the presence of adequate safeguards in the area of IT security, business continuity and data protection. As part of the assessments, the SUPPLIER undertakes to share timely evidence requested by the COMPANY.

**13.5** 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 related to one of the Intesa Sanpaolo Group legal entities.

**13.6** Where requested, the SUPPLIER undertakes, without undue delay and as soon as it becomes aware of it, to prepare the appropriate remediation plans in order to remove non-conformities arising from the audit activities.

**14. Vulnerability Assessment and Penetration Test**

**14.1** The SUPPLIER shall ensure the performance, by specialized personnel and according to industry best practices, (for the application verifications the reference is to the OWASP

Web Security Testing Guide, for the infrastructural verifications the reference is to the Open Source Security Testing Methodology Manual (OSSTMM), of internal vulnerability assessment activities at least every six months on the scope of the services provided to the COMPANY.

**14.2** The SUPPLIER shall guarantee the performance, by specialized personnel and according to industry best practices, (for the application verifications the reference is to the OWASP Web Security Testing Guide, for the infrastructural verifications the reference is to the Open Source Security Testing Methodology Manual (OSSTMM), of internal penetration tests on an annual basis, on the scope of the services provided to the COMPANY.

**14.3** 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, and associated remediation plans on identified vulnerabilities.

## 15. Technical Requirements

**15.1** The SUPPLIER undertakes to adopt Multi-factor Authentication tools for all users accessing the SUPPLIER's corporate network.

**15.2** The SUPPLIER undertakes to adopt End Point Detection and Response (EDR) tools.

**15.3** The SUPPLIER undertakes to adopt tools to detect the presence of malicious software in the perimeter related to the offered service and block its potential malicious actions (Antimalware).

**15.4** The SUPPLIER undertakes to adopt a threat detection system, based on the identification of anomalous user behavior and subsequent management of detected incidents (Security Information and Event Management - SIEM).

**15.5** The SUPPLIER undertakes to adopt monitoring solutions to identify possible DoS (Denial of Service) attacks and, at the same time, to monitor that there are sufficient resources to cope with the possibility of this type of attack.

**15.6** The SUPPLIER undertakes to adopt Identity Access Management (IAM) tools in order to identify and authorize users' access to IT resources or enterprise applications.

**15.7** The SUPPLIER undertakes to adopt Privileged Asset Management (PAM) tools to authorize and manage access to privileged users (e.g., system administrators).

**15.8** The SUPPLIER undertakes to adopt Data Loss Prevention (DLP) tools to identify, monitor and protect data to prevent unauthorized use or the data loss.

**15.9** The SUPPLIER is committed to a Mobile Device Management (MDM) solution that provides protection, monitoring and support for mobile device use.

**15.10** The SUPPLIER undertakes to adopt anti-spoofing tools to verify the IP addresses of the e-mails' senders.

**15.11** The SUPPLIER undertakes to adopt isolated virtual environments (Sandbox) where uncertified applications can be carried out, where files can be downloaded and where

websites can be viewed without exposing the entire system to risks.
**15.12** The SUPPLIER undertakes to adopt Network Access Control (NAC) tools to block access to the local network of unrecognized devices.
**15.13** The SUPPLIER undertakes to adopt Network Firewall Systems (NFS) tools aimed at blocking unauthorized traffic between multiple networks, based on its defined corporate security policies.
**15.14** The SUPPLIER undertakes to adopt Web Application Firewall (WAF) systems in order to protect web applications within the scope of the contracted service from cyber attacks.
**15.15** The SUPPLIER undertakes to adopt private network connections between devices (Virtual Private Network - VPN), aimed at the secure transmission of data.
**15.16** The SUPPLIER undertakes to carry out, under its total and exclusive responsibility, all the activities necessary to ensure the total restoration of the ICT assets exposed to a security event (e.g., Data Backup).

## 16. Technical verifications

### 16.1 Introduction and objectives

The following provisions (paragraphs 16.1 and 16.2) regulate the operational procedures between the COMPANY and the SUPPLIER, with respect only to technical audits such as Vulnerability Assessment (performed using automated tools) or Penetration Test (performed in White, Black and Gray/Box modes) - hereinafter referred to as "ICT Security Controls" and do not prejudice or limit the audit or access powers established by the Agreement or by the current legislation. Such "ICT Security Controls" must be appropriately agreed and formalized between the parties within a specific document.

### 16.2 ICT Security controls

The COMPANY will send appropriate communication to the SUPPLIER in order to agree on the timing of the execution of ICT security controls. This communication will include the type of detail of the technical audits that will be performed, the COMPANY's references for the specific activities, the suggested period for performing the ICT security controls, and the target's information request.
Except in cases of urgency (and in particular as a result of potential security incidents), where shorter deadlines will apply, the communication will be sent to the SUPPLIER 30 calendar days before the period suggested by the COMPANY, to perform the ICT Security Controls, while the SUPPLIER will send all the requested information at least 10 calendar days before the chosen date, in the range suggested by the COMPANY, to perform the audits themselves.
The SUPPLIER expressly acknowledges and agrees:

a) that the COMPANY will be authorized to perform security controls on all (or, if the COMPANY decides, part of) the ICT assets used by the SUPPLIER to provide the

service subject matter of the Agreement;

b) to provide, without delay and under its own responsibility, all information necessary for the proper technical control, requested by appropriate notice;

c) to treat the COMPANY's data/information as confidential (including, by way of example, scanning techniques, analysis results, vulnerabilities detected, template used for the presentation of results, etc.). "Treat as confidential" means that, except where there are more stringent provisions contained in the Agreement concerning the confidentiality of information, the communication should occur only to its collaborators (where, for "collaborators" it means all people related to the SUPPLIER, such as employees, consultants and third party suppliers), whose knowledge is necessary for the performance of the applicable activities; and take all necessary measures to prevent it from being made available and/or disclosed, in whole or in part, to third parties without the prior and explicit authorisation of the COMPANY.

Place and Date

Stamp and Signature of SUPPLIER

# INFORMATION SET
# FOR EVENT NOTIFICATION

**November 2021**

# 1. INFORMATION SET

To be filled in, by the Third Party Provider with all the information available and applicable related to the specific event occurred.

## GENERAL INFORMATION

| ***General description of the event*** |
|---|
| *Please, insert all the necessary information that allow to reconstruct the event occurred (in Italian or in English).* |

| ***Event Timeline*** |
|---|
| 1. *Date and Time of the detection[1] of the event:* _____ |
| 2. *Date and Time of the occurrence of the event, if known:* _____ |
| 3. *Date and Time of the event closure, if available:* _____ |

| ***Who, inside the Company, has detected the event?*** | | | |
|---|---|---|---|
| ***Internal organization*** | | ***External organization*** | |
| *IT security* | ☐ | *External auditor* | ☐ |
| *IMT functions / Internal Functions (Business or Support) – Staff Member* | ☐ | *Third party provider* | ☐ |
| | | *Customer/ Payment service user* | ☐ |
| *Internal Audit* | ☐ | *Attacker (warning)* | ☐ |
| ***Other*** | | | ☐ |
| *Please specify:* | | | |

[1] *In case of data breach detected by an external provider, the Date and Time of Detection, is considered the moment when the communication from the provider arrives to the Intesa Sanpaolo Group Legal Entity competent contact point, as indicated into the agreement.*

## 1.1 EVENT TAXONOMY

| ***Cyber Event*** | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Malware*** | | ***Social engineering*** | | ***Insider/Third Party Provider event*** | | ***Unauthorised access*** | |
| *Ransomware* | ☐ | *Phishing / *ishing* | ☐ | *Accidental misuse of access rights* | ☐ | *Brute force attack* | ☐ |
| *Trojan horse* | ☐ | *Spear phishing* | ☐ | *Intentional misuse of access rights by service provider* | ☐ | *Malicious script injection and/or OS commanding* | ☐ |
| *Virus* | ☐ | *Pretexting* | ☐ | *Intentional misuse of access rights by insider* | ☐ | *SQL injection* | ☐ |
| *Worm* | ☐ | *Cyber squatting* | ☐ | *Policy violation (Insider or TPP)* | ☐ | *Other exploited Vulnerability* | ☐ |
| *Spyware/Adware* | ☐ | *Other social engineering* | ☐ | *Other Insider/TPP Threat* | ☐ | *Information exposure* | ☐ |
| *Mobile malware* | ☐ | | | | | *Other unauthorised access event* | ☐ |
| *Other malware* | ☐ | | | | | | |

| ***Denial of Service Attack*** | | ***Other Cyber Events*** | | ***Additional Classification**: classified as APT?* | ☐ |
|---|---|---|---|---|---|
| *DoS* | ☐ | *Defacement* | ☐ | *Please specify:* | |
| *DDos* | ☐ | *Brand Abuse on Mass and Social Media* | ☐ | | |
| | | *Libel of apical persons on Mass and Social Media* | ☐ | | |
| | | *Vulnerability Scan* | ☐ | | |
| | | *Other* | ☐ | | |

| ***Operational Event*** | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Process failure*** | ☐ | ***Accidental events*** *(e.g., human error)* | ☐ | ***SW problem/system failure*** | ☐ | ***Sabotage (physical attack)*** | ☐ |
| ***HW problem*** | ☐ | ***Infrastructural issues*** *(Internal and external)* | ☐ | ***Key persons / skills unavailability*** | ☐ | ***External Provider Issue*** | ☐ |
| ***External events*** *(Natural, Socio political, Criminal, Transport issue, Environmental issue, Health/Sanitary, Wars/Conflict, Pandemic, Other external)* | | | | | ☐ | ***Other operational event*** | ☐ |

| |
|---|
| *Please specify:* |

## 1.2 IMPACT PERIMETER

| ***Geographical extension*** | | | |
|---|---|---|---|
| *Select the Geographical extension of the events* | | | |
| *International* | ☐ | *Region* | ☐ |
| *Country* | ☐ | *City* | ☐ |
| *Please specify:* | | | |

| ***Countermeasures activated / To be activated*** | | | |
|---|---|---|---|
| *Please specify if any countermeasures have been activated as a consequences of the event* | | | |
| *BCP activated* | ☐ | *DRP activated* | ☐ |
| *Cyber insurance* | ☐ | *Other emergency plan activated* | ☐ |
| *Other contingency measures activated* | ☐ | *Other countermeasures activated* | ☐ |
| *Other countermeasures to be activated* | ☐ | *Please specify:* | |

| ***Overall Impact*** | | | |
|---|---|---|---|
| *Which dimension have been affected by the event?* | | | |
| *Availability*[2] | ☐ | *Integrity*[3] | ☐ |
| *Confidentiality*[4] | ☐ | *Authenticity*[5] | ☐ |
| *Continuity*[6] | ☐ | *Please specify*[7]*:* | |

| ***Commercial Channel affected*** ***(If Applicable)*** | | | |
|---|---|---|---|
| *Commercial channel that have been affected by the event* | | | |
| *Branches* | ☐ | *Mobile Banking* | ☐ |

[2] *The property of process/service being accessible and usable users and customers*
[3] *The property of safeguarding the accuracy and completeness of assets (including data)*
[4] *The property that information is not made available or disclosed to unauthorised individuals, entities or processes*
[5] *The property of a source being what it claims to be*
[6] *The property of an organisation's processes, tasks and services being fully accessible and running at acceptable predefined levels*
[7] *In case of personal data, please compile the specific table for Personal Data Breach (GDPR scope).*

| | | | |
|---|---|---|---|
| *E-Banking* | ☐ | *ATMs* | ☐ |
| *Telephone Banking* | ☐ | *Point of sales* | ☐ |
| *Other* | ☐ | *If other, please specify:* | |
| *Additional information:* | | | |

| ***Business Lines affected* (If Applicable)** | | | |
|---|---|---|---|
| *Business line intended as described in 'Basel III: International regulatory framework for banks'* | | | |
| *Corporate Finance* | ☐ | *Retail Brokerage* | ☐ |
| *Commercial Banking* | ☐ | *Retail Banking* | ☐ |
| *Asset Management* | ☐ | *Agency Services* | ☐ |
| *Trading & Sales* | ☐ | *Payment & Settlement* | ☐ |
| *Other* | ☐ | *Please specify:* | |

| ***Cash Supply – Bank Account* (Applicable only to Intesa Sanpaolo S.p.A. perimeter)** | | | |
|---|---|---|---|
| *Servizi oggetto di malfunzionamento a causa dell'evento rilevato* | | | |
| *Erogazione del Contante* | | *Servizi di base connessi alla gestione dei conti correnti* | |
| *Gestione ATM* | ☐ | *Saldo ed elenco movimenti* | ☐ |
| *Prelievo Contanti* | ☐ | *Operazioni di pagamento mediante carta di debito* | ☐ |
| *Pagamento Pensioni* | ☐ | *Accredito di fondi sul conto (es. deposito di contante, ricezione di bonifici)* | ☐ |
| | | *Addebito di fondi sul conto (es. pagamento bonifico nazionale o bonifico SEPA; addebiti diretti e addebiti ricorrenti)* | ☐ |
| *Informazioni addizionali:* | | | |

| ***Payment Service affected (PSD2 scope)* (If Applicable)** | | | |
|---|---|---|---|
| *Payment services (as defined in annex 1 – PSD2) that are not working properly as a result of the event* | | | |
| *Cash placement on a payment account* | ☐ | *Card payments* | ☐ |
| *Cash withdrawal from a payment account* | ☐ | *Issuing of payment instruments* | ☐ |
| *Operations required for operating a payment account* | ☐ | *Money remittance* | ☐ |
| *Acquiring of payment instruments* | ☐ | *Payment initiation service* | ☐ |
| *Credit transfers* | ☐ | *Account information service* | ☐ |
| *Direct debits* | ☐ | *Other* | ☐ |

| |
|---|
| *If other, please specify:* |

| ***Functional Area affected (PSD2 scope) (If Applicable)*** | | | |
|---|---|---|---|
| *Steps of the payment process that have been affected by the event* | | | |
| *Authentication/ Authorisation* | ☐ | *Direct settlement* | ☐ |
| *Communication* | ☐ | *Indirect settlement* | ☐ |
| *Clearing* | ☐ | *Other* | ☐ |
| *If other, please specify:* | | | |

| ***Trust Service affected (eIDAS scope) (If applicable)*** | | | |
|---|---|---|---|
| *Steps of the payment process that have been affected by the event* | | | |
| *Electronic signature service* | ☐ | *Electronic seal service* | ☐ |
| *Electronic tile stamp service* | ☐ | *Registered delivery service* | ☐ |
| *Website authentication certificate service* | ☐ | *Preservation service* | ☐ |
| *If other, please specify:* | | | |

| ***System & components affected*** | | | |
|---|---|---|---|
| *Technological infrastructure that have been affected by the incident* | | | |
| *Hardware* | ☐ | *Internet platforms* | ☐ |
| *Endpoints/clients* | ☐ | *Networking and telecommunications* | ☐ |
| *Enterprise software applications* | ☐ | *Data management and storage* | ☐ |
| *Banking-related user applications/software* | ☐ | *Other impact* | ☐ |
| *If Other, please specify:* | | | |
| *In case of Data Breach, please provide the reference to the ISP Application Area impacted[8]:* | | | |
| *Additional information:* | | | |

| ***Type of process/service disruption*** |
|---|

[8] *To identify the application area, refer to excel file "MyAPM", column "Desc. Ambito".*

| *Type of disruption caused by the event on service and components* | | | |
|---|---|---|---|
| *Slowdown* | ☐ | *Malfunction (Partial Unavailability)* | ☐ |
| *Total Unavailability* | ☐ | *Other* | ☐ |
| *Please specify the number of internal user that are experimenting the consequences of the event:* | | | |
| *Additional information:* | | | |

| ***Type of Customers affected (If Applicable)*** | | | |
|---|---|---|---|
| *The event generates any consequences on customers? If Yes, please specify the type of customer that have experimented the consequences of the event.* | | | |
| *Retail customers* | ☐ | *Private customers* | ☐ |
| *Corporate* | ☐ | *Financial Institutions* | ☐ |
| *Please specify:* | | | |

| ***Personal Data Breach (GDPR scope)*** | | | |
|---|---|---|---|
| **The event causes a personal data breach?<br>If Yes, specify the Type, the Data subject and records concerned (following sections)** | | | |
| ***Type of personal data breach*** | | | |
| *Availability breach - accidental or unauthorized loss of access to, or destruction of, personal data.* | | | ☐ |
| *Integrity breach - unauthorized or accidental alteration of personal data.* | | | ☐ |
| *Confidentiality breach - unauthorized or accidental disclosure of, or access to, personal data.* | | | ☐ |
| ***Data subject concerned*** | | | |
| *Corporate customers* | ☐ | *Retail/Private customers* | ☐ |
| *Employees* | ☐ | *Management* | ☐ |
| *Special categories (VIP, minors, Public figures)* | ☐ | *Other categories*[9] | ☐ |
| *Please specify:* | | | |
| *Please specify the approximate number of data subject concerned:* | | | |
| *Are any third parties that process personal data involved? If yes, specify:* | | | |
| ***Category of personal data*** | | | |

[9] E.g. Prospect customers, suppliers, promoters, employees' family, candidates, legal representatives

| | | | |
|---|---|---|---|
| *Demographic personal data*[10] | ☐ | *Banking and operational data*[11] | ☐ |
| *Special categories of personal data*[12] | ☐ | *Geolocation data* | ☐ |
| *Access credentials (e.g. userID, password)* | ☐ | *Please specify:* | |
| ***Data history*** | | | |
| *Data of the last month* | ☐ | *Data of more than a year* | ☐ |
| *Data of the last year* | ☐ | | |
| ***Personal data records concerned (Ease of identification)*** | | | |
| *Data not identifiable* | ☐ | *Data indirectly but uniquely identifiable* | ☐ |
| *Data directly but not uniquely identifiable* | ☐ | *Data directly and uniquely identifiable* | ☐ |
| *Please specify:* | | | |
| *Please specify the security measures already taken to protect the data (e.g., encryption, pseudonymisation):* | | | |
| *Additional information:* | | | |
| ***Kind of risk to the right and freedom for the Data Subject (potential or effective)*** | | | |
| *Discrimination* | ☐ | *Fraud* | ☐ |
| *Damage to reputation* | ☐ | *Limitation of rights of the data subject* | ☐ |
| *Financial loss* | ☐ | *Identity theft* | ☐ |
| *Loss of confidentiality of data* | ☐ | *Additional information:* | |

| ***Event Correlation*** | | | |
|---|---|---|---|
| *Assess whether the event is connected to other events (Threat or Incident)* | | | |
| *Stand-alone event* | ☐ | *Replicated occurrence of the same event* | ☐ |
| *Event correlated to other event* | ☐ | *Other* | ☐ |
| *Please specify:* | | | |

## ***General Comments on Impact Perimeter (Optional Filed)***

[10] E.g. Identification data, contact details, data related to instruction, job, personal relationship, family

[11] E.g. Data related to economical activities, commercial activities, retribution, banking, property, investment, credit card

[12] Including: sensitive data, data relating to criminal convictions and offences or related security measures, behavioural data, biometric data