INFORMATION SECURITY AND QUALITY MEASURES

The information security and quality measures listed in this document are minimum measures applicable depending on the nature, context and scope of the Services (hereinafter, the **"Information Security and Quality Measure(s)"**). The validation of such measures by CLIENT (if any) does not relieve PROVIDER from its obligations under this document and the agreement entered into between CLIENT and PROVIDER (the **"Agreement"**) (as the case may be).

PROVIDER shall ensure, at its sole cost, compliance with all the Information Security and Quality Measures listed in this document.

In the event where PROVIDER considers that an Information Security and Quality Measure is not applicable to the nature, context and scope of the Services, PROVIDER shall have to justify such non-applicability with written evidence.

When the first letter is capitalized, the terms used in this document shall have the meaning set out in the Agreement, unless otherwise specified herein.

DEFINITIONS

Affiliated Company(ies): mean(s), as applicable, in relation to either CLIENT or PROVIDER, any company which is, either directly or indirectly, Controlled by, or under the common Control of, respectively, Sanofi (Paris Company and Trade Registration Number 395 030 844) or PROVIDER.

Applicable Laws: mean all laws, regulations (including Applicable Data Protection Law), applicable code of conducts, regulatory policies and licenses, including but not limited to regulations and/or code of conducts in connection with the pharmaceutical industry, privacy, labour law, data protection law, health, safety, and environment regulations, which are in force from time to time during the term of the Agreement on the relevant territory, including any amendments to any or all of them and which apply to the subject matter referenced in the Agreement. Applicable Laws include good laboratory practices, good clinical practices, good industry practices and/or good manufacturing practices ("**GxP**").

Applicable Data Protection Law: means the personal data protection laws, rules and regulations applicable in the country where Controller is established. In particular, the GDPR shall apply to all Processings falling within its scope, and all additional regulations and rules in force in the relevant Member State(s) of the European Union applicable to the Processing.

Audit Trail(s): means a chronological recording of events, such as creation, modification, deletion of – and access to (GxP or non-GxP) record or e-record, that allows reconstruction of the course of events and indicates who created, accessed, changed or deleted data and why.

Client Data: means all data, information, text, drawing, picture, video, sound, statistics, analysis and other materials embodied in any form relating to CLIENT or its Affiliated Companies and/or users (where relevant) and which may be supplied by CLIENT or its Affiliated Companies (and/or its users) (including Personal Data) and/or to which PROVIDER has access to, generates, collects, processes, stores or transmits and associated Audit Trail in the course of performing the Agreement.

Client Environment: means CLIENT's current computing and telecommunications environments (consisting of hardware and software) set out in the Agreement or on which CLIENT notifies PROVIDER that the Services are to be performed.

Control: means direct or indirect ownership of at least fifty per cent (50%) of the equity or more than fifty per cent (50%) of voting rights or the power to designate a majority of the members of its principal management body;
Controller shall have the meaning set forth in the GDPR.

Data Integrity: means a degree to which a collection of data is managed through effective organizational, operational, and technical mechanisms to ensure data reliability, confidentiality and availability.

Equipment: means all equipment, terminals, infrastructures, related hardware and software, including, as applicable, systems (i.e. any and all IT networks or resources that process, store, support, transmit or contain Client Data), applications, databases, central processing units, personal computers and other processors, controllers, storage devices, printers, phones, other peripherals and input as well as output devices, and other tangible mechanical and electronic equipment intended for the processing, input, output, storage, manipulation and retrieval of information and Client Data.

GDPR: means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and
repealing Directive 95/46/EC.

GxP and Other Health-related Regulations: means regulations such as good clinical practices, good laboratory practices, good pharmacovigilance practices, good manufacturing practices and good distribution practices, as well as any other regulation applicable to CLIENT and related to public health.

GxP Computerized System: means computerized system used in support of a GxP or other health-related regulated activity.

Incident: means any event that does not correspond to a normal process and that could lead to interruption or quality reduction of the Services provided to CLIENT.

IT Change(s): means any actual or proposed change to the nature, level and extent/scope of an IT System.

Personnel: means in relation to PROVIDER, any of: (i) its employees; (ii) individual consultants under its responsibility; or (iii) those of its providers, authorized agents or sub-contractors (including PROVIDER’s Affiliated Companies) assigned to the provision of the Services; and, in relation to CLIENT, any of CLIENT's or its Affiliated Companies’ (i) employees; (ii) agency workers; and/or (iii) individual consultants under CLIENT's or its Affiliated Companies’ responsibility.

Personal Data and Processing: has the meaning set forth in the GDPR.

Professional Standards: means, in relation to any particular undertaking or task included, contemplated or envisaged for the performance of the Agreement, those standards, practices, methods and procedures conforming to all Applicable Laws that must be complied with and followed with the highest degree of skill, diligence, prudence and foresight that may be reasonably expected of a provider completing similar activities or acting in similar circumstances, and all this in a manner that complies with recognized international standards.

Security Incident(s): includes, as further defined in this document, any virus and, without limitation, an actual, suspected, attempted or threatened unauthorized: (i) exposure, access, use, deletion, revision, encryption, reproduction, destruction, loss, theft, alteration, disclosure, copying, modification or transmission regarding any component of Client Data including users confidential information, which is or should be under control of PROVIDER or for which PROVIDER is responsible, or, as the case may be, (ii) access (physical or otherwise), theft or damage regarding any Client Equipment controlled by or for PROVIDER or on which Client Data is processed or stored.

Services: means the services provided by PROVIDER to CLIENT.

SOX: Sarbanes-Oxley Act of 2002 also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (in the House) and more commonly called Sarbanes–Oxley, Sarbox or SOX, is a United States federal law that set new or expanded requirements for all U.S. public company boards, management and public accounting firms.

Third Party(ies): means any person or entity that is not a Party to the Agreement (including government or related agencies or entities or courts).

1. Information security responsibilities and obligations

1.1 Information security and quality contacts

PROVIDER shall designate an individual responsible for information security. Such individual is considered as the single point of contact for information security topics and shall be in charge of implementation of all the Information Security and Quality Measures listed in this document.

The person responsible for information security shall designate a backup assistant in case of absence.

PROVIDER shall designate an individual responsible for quality (in the meaning of GxP and Other Health-related Regulations). Such individual is considered as the single point of contact for quality topics and shall be in charge of implementation of all the Information Security and Quality Measures listed in this document.

The person responsible for quality shall designate a backup assistant in case of absence.

1.2 Information security program

PROVIDER shall maintain, monitor, and as necessary improve and update a comprehensive, written "Information Security Program" applicable to the cloud and/or Services as well as to the protection of the security and Data Integrity.

Such Information Security Program shall be consistent with the Professional Standards, and shall contain documented policies and procedures, administrative, technical, and physical safeguards to protect and ensure the security, integrity and confidentiality of the cloud, the Services and Client Data.

1.3 Security Assurance Plan

PROVIDER shall maintain, monitor, and as necessary improve and update a comprehensive, written security assurance plan (the **“Security Assurance Plan”**). The Security Assurance Plan shall describe how PROVIDER will implement, when applicable, each security measure listed in this document. The Security Assurance Plan shall be validated by CLIENT prior to the performance of the Services.

1.4 Risk assessment program

PROVIDER shall provide and implement a regular assessment of the internal and external risks to the security, confidentiality, integrity and availability of Client Data, including without limitation identification and evaluation of vulnerabilities to PROVIDER’s Equipment.

1.5 Acceptable use policy

PROVIDER shall institute an acceptable use policy that its Personnel shall be aware of before gaining any access to PROVIDER's Equipment.

1.6 Security investigations

PROVIDER shall fully cooperate with CLIENT in case of any security investigation regarding potential breaches of its information security obligations.

1.7 Security issues notification

PROVIDER shall report and notify to CLIENT within twenty-four (24) hours any potential security issue regarding PROVIDER's and/or CLIENT's Equipment, solutions or data or any other event requiring notification under Applicable Laws. PROVIDER shall not exploit or disclose such security issues and shall resolve them as soon as possible and, in any case, prior to them resulting in a Security Incident.

1.8 Security Incident management

PROVIDER shall manage and proceed to the mitigation of Security Incidents regarding PROVIDER's Equipment and/or Services provided to CLIENT by following an Incident management process and adequate response plan.

1.9 Change management

PROVIDER shall follow a formal IT Change management process to control any IT Change which could potentially affect CLIENT Data Integrity, compliance, functionality or availability of Services provided to CLIENT. PROVIDER shall perform IT Changes to Client Data by using the normal functionality of the Services.

PROVIDER shall provide a dedicated pre-production environment to CLIENT to ensure proper testing of IT Changes before release into production.

PROVIDER agrees to provide a thirty (30) days’ notice to CLIENT before any IT Changes that impact directly or indirectly the Services. Regular operations such as maintenance or Incident response are not considered as IT Changes and should follow their dedicated processes.

In case of failures or issues resulting from an IT Change, PROVIDER shall be able to follow a rollback plan so that the Services which are used by or for CLIENT or Client Data get back to their state before the IT Change.

2. Infrastructure security

2.1 Network security

PROVIDER shall apply Professional Standards in terms of network partitioning to include but not limited to the following:

- Each network shall be isolated from other networks by the use of firewalls or equivalent measures;
- Only permitted incoming and/or outgoing communication flows shall be authorized.

2.2 Network protocols protection

PROVIDER shall ensure that all network protocols are secure, up-to-date and implemented with no known vulnerabilities.

2.3 Infrastructure hardening

PROVIDER shall ensure that its network key components, network flows and operating systems are hardened and the attack surface restricted as much as possible. This may include (but not limited to) the following:

- Network flows shall be filtered, unused or outdated network protocols shall be deactivated;
- Unused or outdated operating systems services or functions shall be deactivated;
- Unused or outdated network equipment’s services, functions or physical ports shall be deactivated;
- Default administration and/or connection passwords shall be changed;
- Software and/or add-on installations shall be strictly controlled;
- Configuration changes shall be strictly controlled.

2.4 Malware protection

PROVIDER shall ensure that network key components and the Equipment are protected against all types of known malware with adequate and updated anti-malware.

2.5 Network documentation

PROVIDER shall ensure that its network architecture is documented.

2.6 Administration platforms protection

PROVIDER shall restrict all remote administration platforms and infrastructure to PROVIDER IP sources addresses.

2.7 Wireless networks protection

PROVIDER shall ensure that its wireless networks are adequately protected. This may include (but is not limited to) the following:

- Wireless access shall be protected with a secure authentication protocol and with adequate key length;
- Wireless access points emission power shall be correctly dimensioned to PROVIDER area so that wireless cannot be reached from outside PROVIDER area (outside buildings);
- Wireless access points' default administration credentials and/or connection passwords shall be changed;
- Unused or outdated wireless access points' services, protocols, functions or physical ports shall be deactivated;
- Wireless networking devices shall have updated firmware;
- All wireless connections must be authenticated and authorized.

2.8 Dedicated Service and hosting environment

Client service Environment shall be logically separated from other PROVIDER's clients under a dedicated server instance. Client Data should physically reside in a dedicated database environment under a dedicated database instance.

2.9 Mobile devices protection

In case where PROVIDER's Personnel shall use their own and/or corporate mobile devices for the aim to deliver the Services to CLIENT:

- PROVIDER shall protect its mobile devices with a password. This password must be compliant with the following rules:
  - Password length: 8 characters minimum;
  - Password timeout: password must be re-entered after 5 minutes of inactivity;
  - Password change: password must be changed on a yearly basis;
  - Password history: the last two passwords must not be re-used.
- PROVIDER shall manage and administer its Personnel's mobile devices.
- PROVIDER shall ensure a clear segregation between professional and private applications and data.
- In the event any Client Data is stored on any mobile device, such devices shall be in an encrypted form.

2.10 Equipment management program

PROVIDER shall apply best practices in terms of Equipment management and IT infrastructure (network, endpoints, identity and access management) lifecycle (patching and regular updates, obsolescence anticipation) regarding its own and CLIENT managed Equipment.

2.11 Maintenance contracts

PROVIDER shall maintain maintenance contracts with all Equipment's providers in terms of information security.

2.12 Teleworking security

PROVIDER shall have a teleworking policy that effectively protects Client Data and Equipment. Such policy shall be communicated to CLIENT upon request.

3. Remote access

3.1 Access control

PROVIDER shall document its remote accesses procedures. Remote accesses shall rely on secure network protocols and shall use two-factor authentication.

3.2 Passwords protection

PROVIDER shall ensure that its password policy meets industry standard best practices ("Password Protection Policy" from SANS Institute or "DAT-NT-001/ANSSI/SDE/NP" from ANSSI) for strong password management, including at the minimum (but not limited to):

- Minimum password length: 8 characters minimum;
- Password complexity: 3 different types of characters including upper case, lower case, numbers, special characters;
- Password change: password must be changed every 3 months;
- Restriction of password reuse (minimum 10 rotations);
- Account lockout after 5 min of inactivity.

PROVIDER shall ensure that passwords are encrypted while transmitted and will be changed at the first connection.

PROVIDER shall ensure that its Personnel shall not store or write passwords in clear text.

3.3 Physical access to Client Environment

Should PROVIDER need to access the Internet network while on CLIENT's sites, PROVIDER shall refrain from using CLIENT's LAN network unless provided with appropriate equipment by CLIENT. If that is not the case, PROVIDER is strictly prohibited from using CLIENT's LAN network and may only use the Guest Wi-Fi network after requesting user codes from CLIENT.

3.4 Physical access control to Client Data

PROVIDER shall implement and maintain reasonable restrictions upon physical access to Client Data including procedure that sets forth the manner in which physical access is restricted.

PROVIDER shall maintain an Audit Trail of all physical access to the hosting premises of Client Data.

3.5 Logical access control to Client Data

In the event where PROVIDER may host, process, transmit or collect Client Data:

- PROVIDER shall document, implement, maintain and update adequate security controls to ensure that PROVIDER will never use or access Client Data without the explicit request of CLIENT or its approval or unless there is a legitimate identified business need validated by CLIENT;
- The logical access credentials to Client Data shall be strictly limited to authorized PROVIDER's Personnel;
- PROVIDER shall maintain an inventory of all authorized logical access to Client Data;

PROVIDER shall record the list of its Personnel that had/have access to Client Data via front and back-end access authorizations. PROVIDER shall provide documented evidence on request from CLIENT.

Both PROVIDER and CLIENT shall ensure that (i) only authorized Personnel are able to access or use the Services and/or the Client Data, (ii) creation, change and deactivation of user access authorizations are recorded, (iii) users are effectively trained before to authorize their access requests, (iv) access authorization levels are appropriate with the responsibilities and the role played in the system.

3.6 Logical access control to CLIENT network

In the event where PROVIDER's Personnel implement, maintain or administer any kind of Equipment remotely:

- PROVIDER shall document, implement, maintain and update adequate security controls to ensure that its Personnel will never access CLIENT's Equipment without the explicit request of CLIENT or its approval or unless there is a legitimate identified business need validated by CLIENT.
- The Access Codes to CLIENT network shall be strictly limited to authorized PROVIDER's Personnel.

For the purpose of performing the Services, PROVIDER may be granted remote access to Client Environment.

In order to allow PROVIDER to access Client Environment, CLIENT will provide PROVIDER one or more identifier(s) and one or more password(s) (collectively the "**Access Codes**"). PROVIDER shall treat the Access Codes as strictly confidential and shall not permit the disclosure or sharing of the Access Codes by its Personnel or with any Third Parties.

PROVIDER undertakes to use the Access Codes only for the purpose of and duration necessary for performing the Services and will take all reasonable steps to warn CLIENT of any disturbances to Client Environment or its contents.

Should PROVIDER distribute or use these Access Codes in a manner deemed contrary to the provisions of this Agreement, CLIENT may, in its sole discretion, revoke the Access Codes, suspend or terminate this Agreement for breach.

PROVIDER acknowledges that CLIENT may monitor PROVIDER's activity on Client Environment at CLIENT's discretion in accordance with Applicable Laws as set out in CLIENT's Information Technology (IT) and Solutions usage policy, as updated, replaced and/or supplemented from time to time by CLIENT.

PROVIDER acknowledges having received the said policy prior to any access on the site and consents to such monitoring.

PROVIDER shall be solely liable for the use of the Access Codes by Third Parties or for the actions thereof, whether these be fraudulent or not. PROVIDER shall hold CLIENT harmless against all claims or damages relating to the use of the Access Codes or the use of Client Environment or access thereto or arising out of or resulting from any actions performed on or through Client Environment via the use of the Access Codes. In addition, CLIENT does not have the obligation or the technical means to check the identity of the individual(s) using the Access Codes. If PROVIDER has reasons to believe that an unauthorized person is using its Access Codes, it shall inform CLIENT immediately. All actions performed through the Access Codes shall be deemed performed by PROVIDER.

3.7 Physical access control to CLIENT premises

In the event where the management of CLIENT premises is outsourced by PROVIDER:

- PROVIDER shall implement and maintain reasonable restrictions upon physical access to CLIENT premises, including procedure that sets forth the manner in which physical access is restricted;
- PROVIDER shall maintain an Audit Trail of all physical access to CLIENT premises.

3.8 Access logging and monitoring

PROVIDER shall log all activities related to the access to Client Data, including access requests. Retention period must be in compliance with local regulation and agreement with CLIENT.

3.9 Third Parties' access

PROVIDER shall not permit any Third Party to access Client Data, or Client Environment within PROVIDER or CLIENT infrastructure without prior written authorization by CLIENT.

3.10 Permanent access to Client Data

PROVIDER shall ensure CLIENT access to the Client Data throughout the duration of the performance of the Services within the format previously agreed with CLIENT.

4. Application security

4.1 Information security integration into application development

In case where PROVIDER is deemed to be an application's developer/provider/integrator, PROVIDER shall ensure (but not limited to) the following:

- PROVIDER shall integrate through all application development life cycle phases information security needs of the application with regards to confidentiality, integrity, availability and traceability aspects;
- PROVIDER shall rely on Open Web Application Security Project (OWASP)'s best practices in terms of secured application development;
- PROVIDER shall segregate the application development environment(s) from the application production environment(s);
- PROVIDER shall ensure access to the development and production environment follows best practices and enforces segregation of duties;
- PROVIDER shall ensure that (i) application source code has been reviewed and assessed regarding published well known information security source code vulnerabilities, and (ii) no code which is designed to corrupt data or adversely impact the performance of computer systems (including any virus, worm, logic bomb, disabling code, "backdoor" or routines or expiration dates) is introduced into the Services, deliverables or Client Environment. PROVIDER shall present to CLIENT upon request any evidence of this review;
- PROVIDER shall strictly control access to application source code;

- PROVIDER shall perform a vulnerability test on its provided application at least once a year and, in any case, prior to move to production. PROVIDER shall present to CLIENT upon request any evidence of this test;
- PROVIDER shall ensure that the test and development environments offer the same level of protection as the production environment;
- PROVIDER shall ensure that application has the ability to restrict access to Client Data to authorized users only;
- PROVIDER shall ensure that application logs all access to Client Data .

4.2 Application maintenance and support

PROVIDER agrees to provide, maintain and support its application and subsequent updates, upgrades, and bug fixes such that the application is, and remains secure from known vulnerabilities. In no case may such updates, upgrades and bug fixes reduce the security of the Services or Client Data.

PROVIDER agrees to provide at least thirty (30) days' notice to CLIENT if any update, upgrade or bug fix of its applications or IT environment may result or results in an impact for the user of the Services (user experience, service unavailability, etc..).

4.3 Application hardening

PROVIDER shall ensure that its provided application is hardened. This may include (but not limited to) the following:

- Unused or outdated application's services or functions shall be deactivated;
- Default administration passwords shall be changed;
- Whenever possible, application shall not integrate uncontrolled source code, adds-on or plugins;
- Configuration changes shall be strictly controlled.

4.4 Development data

In case where PROVIDER (or its Personnel) is deemed to be an application developer/provider/integrator:

- Developer shall never use or access Client Data without the explicit request of CLIENT or its approval or unless there is a legitimate identified business need validated by CLIENT; and
- Pseudonymized or anonymized data shall be used in the development and test environment.

5. Client Data security

5.1 Client Data protection

PROVIDER shall ensure that all Client Data is encrypted during transmission whether sent over the Internet or otherwise.

PROVIDER shall protect all Client Data stored on databases, servers, or other forms of non-mobile devices against all reasonably-anticipated forms of compromise, whether by use of encryption, logical access controls, or other robust safeguards.

Client Personal Data: Where possible, PROVIDER shall either encrypt all Personal Data stored at rest with separate key management or anonymize them entailing that re-identification is not possible.

In the event any Client Data is stored on any mobile device (including, but not limited to, laptop computers, compact discs, tablet computers, external hard drives, backup tapes and/or removable diskettes), such devices shall be in an encrypted form.

5.2 Client Data and system configuration backup

PROVIDER shall backup Client Data, associated Audit Trail and system configuration on a regular basis following Professional Standards for backup. Backups must be protected from crypto-locking attacks.

PROVIDER shall perform at least two backup copies onto different physical distant locations.

All backups shall be encrypted.

PROVIDER shall perform a three (3) years rotation restore test and provide documented written evidence to CLIENT.

- When a significant IT Change on the computerized system impacts the backup and restore functionality/Services/specifications, PROVIDER shall apply the IT Change management process (as described in section 1.9 IT Change management of the present document) must ensure that a new restore test is performed;
- PROVIDER shall provide documented evidence upon request from CLIENT that backups jobs have started and ended as planned.

5.3 Third Parties restriction

No Client Data shall be sold, assigned, leased to a third party or otherwise disposed of by PROVIDER or commercially exploited by or on behalf of PROVIDER.

6. <u>Personnel security</u>

6.1 IT segregation of duties

PROVIDER shall implement an information technology segregation of duties. PROVIDER shall segregate its Personnel'tasks based on a need to do basis as required by their job responsibilities.

6.2 Information security training and awareness program

During the term of the Agreement, PROVIDER will implement and maintain up to date a training and awareness program for its Personnel regarding its information security obligations.
In case where PROVIDER collects, provides, stores, transmits or process in any manner Client Data, this program shall include a section dedicated to Client Data protection. PROVIDER shall ensure that all its Personnel involved in the Services performance will regularly attend such program.

6.3 PROVIDER Personnel departure

Upon termination of a PROVIDER's Personnel agreement for whatever reason, PROVIDER's shall ensure that Personnel's departure is correctly managed in terms of information security.

This may include (but not limited to) the following:

- All Personnel logical and physical credentials have been correctly deactivated;

- All CLIENT's Equipment and Client Data have been returned;
- If Client Data have been locally stored for whatever reason on Personnel's workstation or mobile device, hard drives and/or storage memories shall be securely wiped.

7. Termination of the Agreement

7.1 Client Data return, destruction or sanitization

Unless otherwise required by law or regulation, upon termination of the Agreement for whatever reason, PROVIDER shall cease processing any Client Data on behalf of CLIENT and, at CLIENT's option, shall either return to CLIENT all of the Client Data and any copies thereof which it is processing, has processed or have had processed on behalf of CLIENT in a format agreed with CLIENT, or destroy the Client Data if requested by CLIENT or sanitize Client Data from PROVIDER's environment and provide evidence of such sanitization or destruction of Client Data within fifteen (15) days of termination of the Services (unless otherwise set out in the Agreement).

7.2 Equipment return

Upon termination of the Agreement for whatever reason, all CLIENT's Equipment shall be returned within thirty (30) days of termination of Agreement.

8. Information security and quality audits and controls

8.1 Right to audit

CLIENT or an appointed audit firm by CLIENT has the right to audit PROVIDER and carry out any controls it considers useful to ensure the compliance with its Information Security and Quality Measures obligations. To do so, PROVIDER shall allow representatives from CLIENT to have access for audit purposes to its related premises and facilities and agree to share documentation and evidence.

In addition, CLIENT shall be authorized to audit PROVIDER's subcontractors and their systems; this does not release PROVIDER from taking all reasonable steps to verify that its subcontractors comply with the provisions of this document.

CLIENT will ensure to cause the least amount of disruption to PROVIDER's activities.
Such controls shall be carried out as per the provisions of the Agreement (if any).

8.2 Information security

8.2.1 Annual information security assessment

In addition, each calendar year, PROVIDER shall engage at its cost and expense a nationally-recognized audit firm identified by CLIENT or proposed by PROVIDER to conduct an audit which shall cover, at a minimum, PROVIDER's security policies and procedures and controls, including cloud and data security. Upon CLIENT's request, PROVIDER shall provide CLIENT with a copy of such report.

8.2.2 Remediation plan

If an audit reveals any breaches or deficiencies pursuant to this Agreement or if CLIENT raises recommendations or reservations following an audit, PROVIDER shall promptly and at its sole cost and expense (i) execute a remediation plan to correct those breaches and/or deficiencies and (ii) implement the recommendations and reservations issued by CLIENT.

8.3 Quality audit

As part of pre-selection process and on a routine basis, no more than once a year, CLIENT may leverage the right to audit (on site or using a postal audit questionnaire).

Additionally, where significant issues are detected regarding the Services provided by PROVIDER, PROVIDER shall authorize CLIENT to carry out when needed an audit for cause designed to lead to resolution of these issues.

After provision of an audit report by CLIENT, PROVIDER shall respond with correction and/or corrective and preventive action plans to critical findings within fifteen (15) business days of receipt of any official request (audit report, close-up documentation, other). For audit reports not containing critical finding, PROVIDER shall provide a response within twenty (20) business days.

For SOX regulated systems, in addition, each calendar year, PROVIDER shall engage at its cost and expense a nationally-recognized audit firm acceptable by CLIENT to conduct an audit which shall cover, at a minimum, PROVIDER's quality policies and procedures and controls. Upon CLIENT's request, PROVIDER shall provide CLIENT with a copy of such report such as a SSAE-16 SOC 2 Type II.

8.4 PROVIDER oversight of subcontractors

PROVIDER shall ensure control over the delegated tasks to its authorized subcontractors on an ongoing basis.

9. Disaster recovery and business continuity

PROVIDER shall notify CLIENT in a timely manner when Services are scheduled to be unavailable due to non-emergency maintenance or enhancements.
PROVIDER shall be responsible for providing and testing contingency/continuity/Disaster recovery strategy to ensure Services to CLIENT if PROVIDER experiences or suffers a disaster. PROVIDER shall make associated testing report available to CLIENT on request.

PROVIDER shall maintain its capability to resume provisions of the Services in case of disaster and to bring an alternative arrangement into use for maintaining CLIENT access to the Services

In the case of unscheduled unavailability, PROVIDER shall inform and cooperate with CLIENT regarding the impacts on Services being unavailable (including causes, effect on Services, and estimated duration).

10. Quality responsibilities and obligations (applicable for GxP Computerized Systems and/or SOX regulated computerized systems)

10.1 Roles and responsibilities

PROVIDER shall communicate in writing to CLIENT the list of Personnel involved in communication interfaces for quality purpose and shall keep it current.

10.2 Obligations

PROVIDER shall provide Services to CLIENT in conformance with (i) GxP requirements (ii) the annex 11 volume 4 of the European Good Manufacturing Practice on GxP Computerized Systems (ii) the chapter 21 CFR Part 11 of the Food and Drug Administration on Electronic Records & Electronic Signatures.

PROVIDER shall take all reasonable steps to ensure that Services provided to CLIENT have been developed and validated for its intended use and in accordance with an appropriate quality management system.

PROVIDER shall provide when requested by CLIENT, objective evidence to demonstrate compliance with the clauses documented within this document.

PROVIDER shall ensure that all Personnel involved in the provision of computerized system and/or Services per the Agreement have been trained according to their job duties.

PROVIDER shall provide evidence of education and training on any relevant regulations, standards, and processes as applicable for those Personnel involved in Services provided.

PROVIDER shall ensure that Audit Trails are enabled properly for all applicable GxP records (i.e. user access records, master data, dynamic data etc.) and as per agreement with CLIENT.

PROVIDER shall maintain, monitor, and as necessary improve and update a comprehensive, written "Quality Assurance Plan". The Quality Assurance Plan shall describe how PROVIDER will implement, when applicable, each quality measure listed in this document. The Quality Assurance Plan shall be validated by CLIENT prior to the start of the performance of the Services.

10.3 Incident impacting Client Data Integrity or compliance (does not apply to security and Personal Data related incidents)

PROVIDER shall detect and record any Incident affecting CLIENT Data Integrity, or impacting compliance, functionality or availability of Services provided. PROVIDER must have an Incident process in place.

PROVIDER shall ensure an efficient and prompt handling of Incident affecting CLIENT Data Integrity, or impacting compliance, functionality or availability of Services and shall make the report to CLIENT upon discovery of critical Incident within reasonable timeframe.

PROVIDER shall implement correction and/or corrective and preventive action plans to remedy the Incident and prevent further similar event.

10.4 Regulatory inspections & inquiries and CLIENT internal audit

In the event either Party is notified of any regulatory inspection, inquiry or internal CLIENT audit that relates directly to Services provided by PROVIDER, the Party shall promptly inform the other Party of any such regulatory inspection, audit or inquiry.

In this case, PROVIDER shall permit a designee from CLIENT to be present at PROVIDER option.

PROVIDER agrees that, during any such regulatory inspection, it shall permit any inspection of its processes, documents and premises by or on behalf of regulatory authorities and shall have the resources available to address the requests of any inspectors. Documents maintained by PROVIDER must be "inspection-ready".

PROVIDER agrees that during CLIENT internal audit, PROVIDER shall provide the resources available to address the requests of internal CLIENT auditors.

PROVIDER shall not charge CLIENT for its time associated with assisting the inspectors/auditors during such event.