Information Security Schedule

Term	Definition
Affiliate:	means an entity that, either directly or indirectly, controls, is controlled by, or is under common control with, the relevant entity, where "control" means the ability to direct the affairs of another by ownership, contract or otherwise.
Agreement:	means the agreement between the Client and the Supplier which incorporates this information security schedule.
AI Systems	"AI System" is a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.
Asset:	means: (i) any item or element of hardware, software or equipment that is or may be used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying or transmitting data of any type); and (ii) any documentation (in whatever medium) that relates to the use or operation of such items and elements; and (iii) any data stored or transferred on the assets listed at (i).
Client:	means the person purchasing the Services under the Agreement.
Client Data:	means data that either: (a) the Client, or a person acting on its behalf, provides to the Supplier, or permits the Supplier to access, in connection with the Agreement; or (b) the Supplier creates or collects in connection with the Agreement; or (c) is derived from the data listed in (a) and (b) (including, where applicable all business and/or technical information: (i) relating to the Client; (ii) concerning the Client and its products, operations, research and development efforts, inventions, trade secrets, computer software, plans, intentions, know-how, product specifications, market opportunities, processes, methods, policies, recipes, formulae, vendor and customer relationships, finances and other business operations and affairs; (iii) of third parties that the Client maintains in confidence, that has been or may be disclosed to the Supplier in written and/or other materials, through the Supplier's access to premises, equipment or facilities of the Client, or by oral communication with employees, consultants, or agents of the Client, and all tangible embodiments of such information, and (iv) any information, findings, data or analysis derived from such information mentioned under (i), (ii) and (iii) above).
Client Group:	means the Client and all its Affiliates (and "member of the Client Group" shall be construed accordingly).
Client System:	means a System or Asset which is owned by or reserved (in whole or in part) for operation by or on behalf of any member of the Client Group.
Cloud Service	means a Service that is a cloud service.
Data Subject:	means an identified or identifiable natural or legal person; an "identifiable" person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Evidence:	means certification documentation that is no more than 12 months old, covers the scope of the Services, and provided by a reputable independent assessor. Such documentation could include: • SOC 2 Type II reports; • ISO 27001 Certification reports; • ISO/IEC 42001 Certification reports; • PCI-DSS AOC certification reports; • Vulnerability Assessment and Penetration Testing (VAPT) reports; and • Regulatory Compliance reports (e.g. FDA certifications). • Assessments conducted by an independent provider as designated by Client
Good Security Practice:	means measures and practices consistent with: (a) the technical and organizational measures and practices that are required by, or recommended in, internationally accepted management standards and codes of practice relating to Information Security such as ISO/IEC 27001 (Information Security Management

	Systems – Requirements) and ISO/IEC 27002 (Code of Practice for Information Security Management) ISO/IEC 42001 (Artificial Intelligence Management Systems – Requirements); and (b) accepted management standards and codes of practice relating to technical security (such as NIST SP 800-161 and NIST AI 100-1 (Artificial Intelligence Risk Management Framework)) and (c) security standards and guidelines (including generally accepted principles regarding the segregation of the duties of governance, implementation, administration and control) and techniques such as strong authentication, access control and auditing, "least privilege" assignment, all as reasonably made available to the general public or information security practitioners and stakeholders by generally recognized authorities and organizations regarding Information Security, as the same are expanded, varied and replaced from time to time.
to "**implement**" (and variants of it, such as "Implementation"):	means, in respect of a process, policy, procedure, a plan, a measure or a control (for the purposes of this definition, each a "process"), to plan that process; document the process; issue the process; require staff to follow the process; train staff on the process; embed the process in operations; enforce it; regularly review, and measure, the extent to which the process is followed and effective; and update it as appropriate.
Information Security:	means: (a) the protection and assurance of: (i) the confidentiality, integrity, reliability and availability of information and Systems; and (ii) related properties of information such as authenticity, accountability, and non-repudiation; and (b) compliance with all regulations applicable to the Processing of information.
Personal Data:	means any information relating to a Data Subject.
references to "**personnel**":	in addition to the relevant party's staff (permanent or otherwise), such references include also references to that party's Service Providers.
to "**Process**" (and variants of it, such as "Processing"):	means to perform any operation or set of operations upon data, whether or not by automatic means, such as collecting, recording, organizing, storing, adapting or altering, retrieving, consulting, using, disclosing (by transmission, dissemination or otherwise making available), aligning or combining, blocking, erasing or destroying.
"**Security Event**"	means any occurrence related to Supplier Systems, including any Assets provided to the Client in connection with the Services that (i) indicates a potential breach of information security (including a compromise to the confidentiality, integrity, or availability of Client Data); or (ii) indicates any identified vulnerability affecting any Assets provided to the Client in connection with the Services; or (iii) indicates a compromise of business operations; or (iv) may require a review of security arrangements.
"**Security Incident**"	means one or more Security Events that has or might compromise the confidentiality, integrity or availability of Client Data (including a Security Event that compromises business operations or threatens information security (including confidentiality, integrity, and availability of Client Data)).
Services:	means the services being provided by the Supplier under the Agreement.
Service Provider	means a subcontractor or subprocessor of the Supplier.
Supplier:	means the person providing the Services to the Client under the Agreement.
Supplier Personnel	means individuals who are employees, agents and officers of either: (a) the Supplier; or (b) the Supplier's Service Providers.
Supplier System:	means a System or Asset which is owned or reserved (in whole or in part) for operation by or on behalf of the Supplier or any of its Affiliates.
System:	means an information technology or communication system, network, service or solution (including all Assets that either (a) form part of it, or (b) are used to provide it).
System Data:	means the data used to operate a System, including metadata and system code.

Topic	Details of the Security Measures
General Security Measures	(a) The Supplier shall provide the Services and perform its obligations under the Agreement in accordance with: (i) this information security schedule; and (ii) Good Security Practice. (b) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals to whom the data may relate, the Supplier shall implement the technical and organizational measures described in the table below (the "**Security Measures**") to protect the Services and the Client Data in such a way as to ensure a level of security appropriate to the risk, taking into account evolving threat scenarios, such as those enabled by artificial intelligence techniques. (c) In assessing the appropriate level of security mentioned above: (i) where the Security Measures address a topic without indicating specific measures, the Supplier shall address the topic, taking account in particular of the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored or otherwise processed ("**Data Risks**"); and (ii) where the Security Measures indicate specific measures (for example, MFA requirements or password requirements), the Supplier may implement more stringent standards to ensure that the Data Risks are appropriately addressed, but may not implement a lesser standard. This information security schedule may be updated from time to time to reflect changes in applicable security requirements, standards, or regulatory expectations relevant to the Services. Following Client notice to the Supplier, The Supplier shall use commercially reasonable efforts to implement any such updates.
Compliance with internal policies:	1. The Supplier shall issue and comply with written policies and procedures that address each of the control areas for securing Client Data set out in this document. The Supplier shall support this with: (a) a documented approach; (b) a risk managed approach; (c) a mechanism for measuring compliance against the rules; (d) a plan for training and promoting awareness, including: (i) roles and responsibilities for protecting Client Data; (ii) legal and contractual obligations; and (iii) mitigating the risk of non-compliance. 2. The Supplier shall document how it: (a) organizes the security of Client Data; (b) assigns responsibilities; and (c) addresses security in mobile devices and remote working. 3. The Supplier shall implement internal policies and procedures that ensure: (a) that the confidentiality, integrity and availability of Client Data are maintained; and (b) compliance with legal and regulatory requirements to which the Client and the Client Data may be subject. 4. The Supplier shall review its policies and procedures at least annually, and in response to any significant change in circumstances. 5. The Supplier, with respect to these policies and procedures, shall: (a) train its employees and relevant third parties (such as contractors); (b) monitor compliance with its own policies and procedures; (c) to the extent the Supplier has access to any Client System: (i) ensure that Supplier Personnel who are engaged from time to time in the provision of the Services are trained on Client policies and procedures; and (ii) monitor compliance with the Supplier's obligations arising under this Agreement, except to the extent that only the Client can perform such monitoring;

Topic	Details of the Security Measures
	(d) implement processes to identify, assess, respond to, and monitor risks towards Client Data and the Services; and (e) inform, promptly as they are confirmed, the Client of such risks and measures to respond to them that are being taken or necessary. 6. Where Client Data is stored or processed on endpoints, including mobile devices (for example, smartphones, tablets), the Supplier shall employ software that allows IT administrators to control, secure and enforce policies on those endpoints.
Internal security management procedures:	1. The Supplier shall implement measures to secure Client Data by: (a) controlling Processing rights and access rights to Client Data (b) controlling use of systems that either protect Client Data, or that hold Client Data (both at rest and in transit) (or both); (c) monitoring access to the systems described in paragraph (b) above; (d) retaining, deleting and returning Client Data in accordance with periods agreed with the Client; (e) imposing, where the Supplier works with Service Providers on such Service Providers substantially the same security requirements as described in this document to protect Client Data. In addition the Supplier shall meet all of their responsibilities under any applicable shared responsibility model as provided by their cloud-Service Provider(s); and (f) implementing a process to provide annual assurance (where required by Client) of the security of Client Data (irrespective of whether it is processed by the Supplier or by any of its Service Providers) in accordance with the principles of this document, including Evidence to demonstrate that security. To the extent any areas are identified as requiring improvement, the Supplier agrees to improve them promptly. Associated costs of this assurance shall be borne by the Supplier. 2. To the extent that the Supplier Processes Client Data otherwise than directly on Client Systems, the Supplier has established, and implements, internal security management procedures that cover the following elements: (a) requesting and approving data processing rights in the Supplier's Systems; (b) granting such rights in the Systems; (c) reviewing such rights in the Systems; (d) attributing to different individuals the roles for requesting, approving, granting and reviewing such rights; and (e) documenting the roles and responsibilities in relation to the above, and to whom such responsibilities and rights are attributed. 3. In the event that the Supplier personnel provide any or all of these Services using Client Systems (for example staff augmentation services) then the Supplier shall classify Client Data and adhere to relevant Client IT standards in accordance with the Client's instructions and Supplier personnel shall undertake all training mandated by Client.
Building access controls:	1. The Supplier shall implement physical and environmental controls to prevent: (a) unauthorized physical access to Client Data; (b) damage to Client Data; (c) interference with Client Data; (d) loss of Client Data; and (e) theft of Client Data. 2. The Supplier maintains a list of the locations (e.g., data centers, computer rooms, offices) where Client Data under its control is processed or stored. 3. The Supplier controls access to such locations where Client data may be processed or stored through implementation of appropriate logical, physical or technical controls (or any combination of them). 4. The Supplier shall apply appropriate logical and/or technical controls for the protection of data in the Supplier's environment. These shall include physical controls such as fences, locked doors and windows, environmental controls to detect, alert and prevent inappropriate conditions for operating computer systems due to (amongst others) fire, temperature, electrical power, or humidity.

Topic	Details of the Security Measures
	5. The Supplier shall ensure that its representatives comply with those control arrangements agreed with the Client. 6. In addition, to the extent that the Supplier may process or store Client Data on fourth party system, the Supplier shall ensure measures are in place which deliver a similar level of protection to systems under their direct control.
Access and System infrastructure controls for Client Data:	1. The Supplier shall implement measures to control access to Client Data (including at rest and in transit) including: (a) the business aspects of access control; (b) user access management; (c) user responsibilities; and (d) system and access controls. 2. The Supplier shall document and enforce: (a) operational procedures and responsibilities ensuring the Supplier has adequate protections against malware and viruses; (b) System and data backup (including how to perform a back-up, when to do a back-up, who should perform a back-up, and logs of the back-ups made); (c) logging use of Supplier Systems (including details of who logged on, when did they log on and log off, what they did in the System (including changes made to the data)); (d) monitoring the above logs; (e) retaining the above logs for no less than 18 months or, where the Supplier gives the Client the opportunity to download the logs, for no less than 3 months; (f) protecting the integrity of operational software; and (g) technical vulnerability management. 3. The Supplier shall implement measures to protect the security of Client Data by: (a) controlling the purposes for which Client data may be used and ensuring such purposes are permitted by the Agreement; (b) controlling the extent to which copies of Client Data are made and limiting those copies to what is necessary (for example, the Supplier shall not use Client Data outside the production environment unless such use is necessary and has a business justification); (c) controlling the location of copies of Client Data; (d) controlling the disposal of Client Data; and (e) maintaining records of the above. 4. The Supplier shall process and store Client Data only through Assets and Systems effectively controlled by the Supplier. 5. The Supplier shall ensure that any access over the internet to Supplier Systems that store or process Client Data will be subject to Multi-Factor Authentication (MFA). 6. The Supplier shall ensure that all Supplier Personnel who require access to Client Systems and Data are equipped with devices that comply with the Client's Multi-Factor Authentication (MFA) requirements for such access. 7. To the extent that Client Data are Processed in a Supplier System, and to the extent that the Supplier Processes Client Data in a Client System and can exercise such control over the System, the Supplier shall restrict access to that System including by: (a) ensuring access is granted to a named individual only; (b) maintaining lists of individual access to production Systems and the permissions granted to user accounts; and (c) implementing access control which records and restricts the number of persons with privileged access to those with an approved business need. 8. The Supplier shall restrict individual access by users to only those parts of the System to which they need it to perform an approved role. 9. The Supplier shall restrict using the principles of: (a) authentication; (b) identity management; and (c) user access management. 10. The Supplier shall implement a process to:

Topic	Details of the Security Measures
	(a) manage access to Client Data systems to defined time periods, ensuring those periods have an approved business justification; and (b) record the following information against each instance where access permission is granted: (i) the date and time when the access starts; and (ii) the date and time when the access ends. 11. When any changes are made to an existing access, the Supplier shall record the change and its justification. 12. The Supplier shall implement a process for removing access permissions when the permission expires, whether: (a) on completion of the task for which access was granted; (b) on expiry of the initially approved time period; or (c) termination of the privileged users' role (including through termination of employment). 13. The Supplier shall: (a) review user access privileges used by or on behalf of the Supplier to access the Client Data and Systems holding Client Data with the frequency required by the Supplier's security policies; (b) in any event no less frequently than once per calendar year; (c) ensure that personnel who have access to the System act responsibly and with due care; (d) maintain access control lists to production systems and the permissions granted to user accounts; (e) disable or revoke a user's access rights when the user no longer needs such access rights; (f) have a process to ensure that access rights to Supplier Systems, and to other Systems (e.g. Client Systems) to which the Supplier (either itself or through a third party) has granted access, are revoked from the time the employment ends; and (g) Provide restricted remote access for infrastructure management supporting the Service. 14. The Supplier shall link all of the procedures in this section (on Access and System infrastructure controls for Client Data) to the Supplier's policy on Joiners, Movers and Leavers. 15. Where the Supplier requires access to, or copies of, any Client Data for the purposes of software development or testing, the Supplier shall protect the Client Data with equivalent system access restrictions to those used in production environments. 16. Where appropriate, the Supplier shall use separate secure environments for development (including updating data), testing and production. 17. The Supplier shall implement a process for periodic and timely maintenance of Systems where Client Data is Processed which will include procedures for patching and upgrades. 18. The Supplier shall maintain specifications of technical and organizational resources (covering System authentication, authorization and accounting) required to ensure the confidentiality, integrity and availability of Client Data that are Processed by the Supplier. 19. To the extent that the Supplier permits the Client to itself manage users' access rights, the Supplier shall: (a) ensure the Client's access to such Systems is secure; and (b) provide the Client with tools that enable it to perform the functions required to ensure the security of Client Data in the Supplier environment. 20. The Supplier shall periodically (and no less frequently than annually) review the identity and access management process. 21. The Supplier shall ensure that any systems where Client Data are Processed use a Secure Architecture approach that applies Security by Design principles. 22. Where changes are made to systems where Client Data are Processed the Change follows a documented process that embodies the principle of segregation of duties. 23. The Supplier shall apply suitable technical protections to Client Data to include: (a) firewalls (including a process to review firewall rules on a periodic basis) and other measures to identify and prevent unauthorized attempts to access applications sites or services; (b) configuring remote access methods to identify and prevent unauthorized connections;

Topic	Details of the Security Measures
	(c) restricting access to system features and settings to privileged users; (d) applying industry standard cryptographic protection measures to data used for authentication; (e) encryption to protect client data in transit; (f) encryption to protect client data at rest, where appropriate; (g) ensuring the effectiveness of technical protections is regularly reviewed and updated to address emerging threats; (h) enforcing a password policy that complies with one set out in a best practice framework (e.g., a combination of at least nine upper & lower case letters, numerals and special characters); (i) automatically disabling user accounts after invalid login attempts; and (j) automatically locking idle login sessions. 24. Where the Supplier is developing software on behalf of the Client, and whether that software is implemented on Client or Supplier Systems, the Supplier shall apply frameworks that are objectively considered to be best practice, e.g. Open Web Application Security Project (OWASP) as appropriate. The Supplier shall be prohibited from utilizing copyleft open source software, in any Services. 25. The Supplier shall store Source Code in an industry standard secure repository. 26. In software deployment, the Supplier shall, (a) ensure PINs and passwords are entered only in non-display fields; (b) remove all elements cached on the server upon termination of the session; (c) define standardized roles for the application which determine what kind of access is provided for each role; and (d) actively monitor applications to ensure availability 27. In software development, the Supplier shall: (a) have in place development standards, containing detailed descriptions and explanations of technology applications, systems, and procedures, and align those standards with the global SDLC best practices (such as OWASP, ASVS etc.) (b) design applications with a 3-tier architecture, separating the web presentation, business logic and database layers into separate servers and network zones; 28. Prior to go live of software (and prior to making any updates of it) and (to the extent such software is run on Supplier Systems) thereafter no less frequently than annually, conduct appropriate vulnerability testing. This should include: (a) a combination of Static Application Security Testing (SAST); and Software Composition Analysis (SCA); and (b) Dynamic Application Security Testing (DAST); and (c) vulnerability scanning of the underlying infrastructure. 29. Where dealing with Client Data the Supplier Systems, the Supplier shall document and implement standard operating procedures (SOPs) for: (a) resources and procedures for authenticating System users; (b) security hardening for the end user devices used to provide the Services; (c) management and use of System Data; (d) creation and use of copies of System Data; (e) programs and program tools used for backing-up and restoring Systems; (f) creation and maintenance of system data required for system testing and migration; (g) protection of any copies required for System backup, archiving and other purposes; (h) how to secure Systems against unauthorized access; (i) how Systems record who has accessed such Systems, stating the date and scope of such access; (j) how to conduct reviews and maintenance of media and Systems used for data processing; and (k) how to dispose securely of information that no longer needs to be retained including: (i) customization of data retention periods; and (ii) arrangements for deletion (including emergency deletion) of Client Data. 30. The Supplier shall implement a process to obtain assurance about the security of Client Data where Client Data is Processed by any Service Provider, to be available to the Client upon request, including:

Topic	Details of the Security Measures
	(a) maintaining guidelines for retention and disposal of business correspondence and other records; (b) maintaining policies and procedures regulating the downloading, use and retention of third-party software and data; (c) ensuring the information security of Client Data that is electronically transmitted (directly or via staging facilities) between Systems (whether at the Supplier's or other parties' facilities); and (d) managing removable and portable media in accordance with Good Security Practice, including where appropriate storing them in a safe, secure environment in accordance with manufacturers' specifications. 31. The Supplier shall, where appropriate, implement a Data Loss Prevention solution, including measures addressing insider threat risk, such as enhanced monitoring for anomalous or suspicious behavior. 32. The Supplier shall, at its own cost, use all commercially reasonable efforts to ensure that the security measures implemented under Supplier's information security program (including all cryptographic controls) and used in any Supplier system in connection with the Services, as well as in processing or storing Client Data, are resistant to cryptographic vulnerabilities that could be exploited by post-quantum computing ("PQC") threats. In particular, Supplier shall implement and maintain cryptographic controls comprising "quantum-safe" or "post-quantum" cryptography (i.e., quantum-resistant algorithms and protocols) applicable to the Services or Client Data in accordance with: a) all applicable PQC guidance and implementation guidelines and milestones issued by the US Department of Homeland Security (USDHS) from time to time; and b) recognized international standards (e.g., NIST PQC standards). 33. The Supplier shall maintain "cryptographic agility", meaning the capability to promptly update or replace algorithms, using commercially reasonable effort, as new applicable quantum-safe standards emerge. The Supplier shall ensure the security measures taken, as outlined in clause 1.1 above are periodically reviewed, updated, and maintained as necessary to remain effective against evolving threats throughout the Agreement. 34. For the avoidance of doubt, and in addition to the measures outlined in clause 32 and 33 above, the Supplier shall enforce secure lifecycle management of cryptographic keys and certificates, including rotation, prompt revocation of compromised or expired keys/certificates, and secure storage using industry standard key management solutions, including secure cryptographic devices such as hardware security modules for any Supplier systems used in relation to the Services. The Supplier shall not use wildcard certificates in relation to any Supplier system used to provide the Services or to handle Client Data.
Transmission	1. The Supplier shall document and enforce measures to protect Client Data during transmission by: (a) applying network security management (e.g., network segregation and segmentation); (b) applying measures to secure data in transit; (c) maintaining a network flow diagram depicting the environment of the Services; and (d) separate the network environment used for providing the Services to Client from environment used for providing services to other customers. 2. The Supplier shall not transmit, or request any user to transmit, passwords used to access Client Data in clear text over Systems or between Systems. 3. The Supplier shall not host, nor transmit to/from any member of the Client Group, or permit such transmission by any Supplier Personnel, of any Client Data, or any unstructured data, using any means other than through Supplier Systems or Client Systems. For example, the Supplier shall not use, and shall not permit the use, for those purposes, of: (a) non-corporate e-mail accounts (e.g. Yahoo!, Gmail, etc.); (b) unsecured FTP; or (c) consumer file sharing services.

Topic	Details of the Security Measures
	4. The Supplier shall not send any physical media device(s) containing Client Data to any recipient (including the Client or any of its Affiliates) via any postal or courier service except with the prior written (including e-mail) agreement of the Client's designated security contact. Any such approval shall be valid for only one individual transmission.
Artificial Intelligence controls for Client Data	To the extent the Supplier provides AI Systems in the Services: 1. Prohibiting Model Training with Client Data: The Supplier shall not use any Client Data to train, improve, or modify its AI models or to benefit third parties without the Clients explicit written consent. Explicit written consent constitutes a signed agreement or documented approval from the Client. 2. AI System Impact Assessment: The Supplier shall conduct regular relevant impact assessments of the AI systems to evaluate their effects on individuals, groups, and society. These assessments must align with ISO/IEC 42001 requirements, particularly focusing on the responsible design, development, and deployment of AI systems. Impact assessments should be conducted at least annually. 3. AI Disclosure and Transparency: The Supplier must disclose any use of AI in the performance of the Services or in any deliverables provided to the Client. This disclosure must include details on the AI technologies used, the data processed, and any potential biases or risks associated with the AI systems. 4. Continuous Monitoring and Improvement: The Supplier shall establish processes for continuous monitoring and improvement of AI systems. This includes regular audits, updates, and enhancements to ensure ongoing compliance with ISO/IEC 42001 and other applicable standards.
Managing Assets	1. The Supplier shall document and enforce measures to protect the security of the Client's Assets by: (a) identifying Client Assets on Supplier Systems; (b) understanding the risk classification of information Assets on Supplier Systems; and (c) ensuring that Client Data is not subject to unauthorized disclosure, modification, removal or destruction. 2. The Supplier shall develop and maintain inventories of: (a) physical devices and Systems where Client Data are Processed within the organization; and (b) software platforms and applications where Client Data are Processed within the organization, including in each case details of relevant resources (e.g., hardware, devices, data, and software) where Client Data are Processed prioritized based on their classification, criticality, and business value. 3. If the Supplier is to decommission, or dispose of, any Asset containing Client Data, the Supplier shall ensure either: (a) that the Asset is irretrievably destroyed or returned to the Client; or (b) that the Client Data or relevant information held on the Asset is deleted and rendered irrecoverable prior to decommissioning, or disposing of, the Asset.
Review reports and notification	1. The Supplier shall document and enforce measures to protect its data, and maintain Evidence of the effectiveness of these measures, taking into account the evolving threat landscape, including emerging threat scenarios, such as those enabled by artificial intelligence techniques, for example by: (a) external and internal audit; (b) logs and reports; (c) testing and scanning; and (d) evaluating performance against documented agreements. Where any Evidence, including audits, logs, reports, testing, scanning, or evaluations shared with or made available to the Client, identifies deficiencies, findings, or risks relevant to Client Data or the Services, the Supplier shall promptly implement corrective actions as part of the measures implemented under this Schedule to address them and, upon request, provide the Client with reasonable evidence of remediation and closure, within timeframes commensurate with their severity and agreed with the Client.

Topic	Details of the Security Measures
	2. The Supplier shall conduct regular risk-based audits, whether external or internal covering systems where Client Data is Processed. 3. The Supplier shall measure the effectiveness of the measures put in place to protect Client Data against: (a) formal agreement between the Client and Supplier; or (b) a recognized best practice framework such as ISO/IEC 27000, NIST or System and Organization Controls (SOC). 4. Where the Supplier is subject to external audit, the Supplier shall share with the Client such reports (or such elements of reports as are relevant to Client Data) with the Client. These reports are likely to include: (a) ISO/IEC certification and monitoring audit reports; and (b) System and Organization Controls (SOC) reports. 5. Where IT systems are in scope of Payment Card Industry Data Security Standard (PCI DSS), the Supplier shall maintain compliance with the current applicable version of PCI DSS as published by the PCI Security Standards Council. The Supplier will provide Evidence of such compliance to the Client to fulfil contractual requirements on request. 6. The Supplier shall conduct regular penetration testing. 7. The Supplier shall conduct regular vulnerability scanning. 8. The Supplier shall perform security assessments (including performing tests) of Systems that Process Client Data no less frequently than annually. 9. The Supplier shall: (a) share the reports created, and results of testing performed, in such audits with the Client in a timely manner, the format and timescale to be agreed with the Client; and (b) permit the Client to perform its own security assessments of such Systems in coordination with the Supplier. 10. The Supplier shall provide the Client, no less frequently than each quarter (or such other period as the Client may agree), with comprehensive and readily understandable overviews regarding: (a) the access permissions of all persons with access to the Client Data; (b) audit trails of all persons with access to the Client Data; (c) records of detection of unauthorized mobile code; (d) records of external Service Provider activity; (e) records of monitoring for unauthorized personnel, connections, devices, and software; and (f) records of vulnerability scans.
Incident management	1. In the event of any unauthorized access, loss or physical and/or technical incident impacting the Services, Client Confidential Information and/or Client Personal Data, or any identified vulnerability affecting any Assets provided to the Client in connection with the Services, the Supplier shall promptly notify the Client at soc@pmi.com and provide the Client with all reasonable assistance. 2. The Supplier shall document and implement technical and organizational measures for the secure management of Security Events and Security Incidents. These measures should include: (a) appointing employees to be responsible for particular roles so that the Supplier has a consistent approach to incidents; (b) an incident management process which shall include measures to: (i) detect, track, escalate and resolve any Security Events or Security Incidents, failures, or other operational risks; and (ii) understand the impact of the above in a timely manner; and (c) appointing an incident management team with a defined role and invocation point; (d) defined and prompt detection and response procedures and timelines, and sharing these with the Client; (e) procedures to minimize and control the potential impact of Security Incidents, including: (i) Asset management; (ii) impact assessment;

Topic	Details of the Security Measures
	(iii) creation of a response plan to promptly handle and remediate the impact of the Security Incident; and (iv) implementation of that response plan, including escalation to all appropriate parties.
Service continuity	1. The Supplier shall document and enforce measures to minimize disruption to service availability following a Security Incident or other disruptive event (e.g. earthquake, flood, power outage, pandemic). This shall include ensuring that: (a) security arrangements remain in place throughout; and (b) redundancy measures are in place for continued delivery of the Services. 2. The Supplier shall: (a) test, approve and deploy changes to the Supplier Systems in a controlled manner with only minimal disruption to the Client; (b) implement the appropriate organizational and technical measures necessary to sustain or rapidly recover the services being provided to the Client in the case of any reasonably foreseeable disruptive event; and (c) ensure that any stand-by or alternative location used for the purposes of the Supplier's service continuity is subject to information security controls at least equivalent to those in force at the facility from which the Supplier usually operates the relocated processes.
Third party access requests	Supplier certifies that: 1. Supplier has not purposefully created back doors or similar programming that could be used to access the Supplier system and/or Client Data; 2. Supplier has not purposefully created or changed its business processes in a manner that facilitates access to the Supplier system or Client Data; 3. Applicable law or government policy does not require Supplier to create or maintain back doors or to facilitate access to Client Data or Supplier's systems, or for Supplier to be in possession or to hand over the encryption key; and 4. Supplier has implemented organizational measures to challenge requests from applicable government authorities if such requests are disproportionate or unlawful.
Technical Addendum	**Details of the Additional Security Measures**
Applicability	Applicability of the Technical Addendum: This Technical Addendum sets out below additional technical requirements that apply where, and to the extent that, they are relevant to the Services, having regard to the nature of the Services, the related technical architecture, and any Processing of Client Data performed in connection therewith. For the avoidance of doubt, the requirements set out in this Technical Addendum apply in addition to, and not in substitution for, the requirements set out elsewhere in this Information Security Schedule.
Cloud Security	The Supplier shall: 1) perform assessments, at least annually, to validate compliance with relevant Good Security Practice standards (such as ISO27001, ISO27017, ISO27018) requirements applicable for all systems that are used to provide the Services; 2) have a process to destroy or purge any physical or logical (or both) storage media that are removed from production use, in a timely manner, using industry standard practices; 3) have plans and processes in place to address portability and third-party lock-in risks associated with the use of cloud service providers; 4) have plans and processes in place to manage risks of Cloud Provider regional outages and ensure Client Data is backed up in at least one additional region. 5) have plans and processes in place to identify, preserve, collect, and produce Client Data upon the Client's request; 6) ensure that all Client Systems are logically segregated and isolated from the Supplier's other customers;

Topic	Details of the Security Measures
	7) ensure that all relevant communications are filtered through Data Loss Prevention (DLP) solutions that detect Client's private, Personally Identifiable Information (PII) or confidential Data; 8) have a plan to address interoperability issues while contracting with a cloud service provider; 9) in respect of full administrative privileges to manage Client Systems that are used to provide any Cloud Services, have a process to grant such privileges only to approved individuals; 10) ensure that the contract with the cloud service provider includes defined roles and responsibilities; 11) ensure that security vulnerability testing of API's, Queues, MCP's or any other type of interface or entry point which are used to provide Cloud Services is performed prior to initiation of the Services and at regular intervals, no less frequently than annually, thereafter; 12) ensure that penetration testing is performed prior to all major releases and no less frequently than annually for all systems (including servers, operating systems, applications, databases, networking, storage, virtualization and security) that are used to provide Cloud Services; 13) ensure Client Data is encrypted whenever in transit, including internal communications between network tiers (i.e., web/presentation, application/logic and database/data); 14) ensure cloud service customer data is encrypted whenever at rest using application level encryption, field level database encryption, full database encryption, file/object encryption or volume encryption; 15) ensure that any Cloud Services utilized to deliver the service to the Client are configured appropriately to prevent public or anonymous access to the Client's Data, and are accessible solely by the Client or in accordance with 9).
Custom Application development	The Supplier shall: 1) perform data transfer from production systems in a planned and controlled manner that includes appropriate backup and testing procedures; 2) maintain archived data in accordance with applicable record retention requirements; 1) ensure all files and programs are backed up prior to the implementation of patches; 2) complete testing plans during the development phase and define testing frequency and standards; 3) Supplier should comply with the agreed specifications: Functional Specification and Hardware/Software Design specification; 4) put in place procedures for requesting, evaluating, approving, testing, installing, and documenting software modifications as part of emergency change control; 5) put in place activities for evaluating, approving, testing, installing, and documenting software modifications as per its change management process; 6) regulate use of open source tools and other components; 7) ensure hardcoded access credentials are not available on the application; and 8) ensure production code and software does not have back-end access. 9) Source code shall be subject to source Code Review prior to verification testing and during application lifecycle. This means that software shall be based on a documented, reviewed, well-structured design, and developed following established programming and secure coding practices, such as but not limited to: a) meeting functional and design specifications delivered b) programming standards documented and correctly / consistently applied c) reliable and robust operation d) easily maintainable e) capable of handling error conditions f) well laid out and commented in English g) modular in structure: Individual modules should perform a single, easily identifiable function. Modules should be distinct and as logically separate as possible. The use of subroutine or function side effects should be avoided.
Original Equipment Manufacturers (OEM)	The Supplier shall: 1) maintain documented software and firmware development standards, for all supplied components such as Operating Systems (OS) where applicable, applications, control

Topic	Details of the Security Measures
	logic and third-party software, and align those standards with global SDLC best practices (such as OWASP, IEC 62443-4-1 principles, etc.); 2) provide a documented secure configuration and hardening guide for all supplied components, defining the recommended secure settings and controls for user accounts, services, network ports and protocols, logging and monitoring, backup and recovery, time synchronization, and certificate lifecycle management. 3) maintain and provide to Client a complete and up-to-date inventory of software and firmware versions for the control system and its subsystems. All changes shall be described, including their security impact and rollback considerations, and associated test protocols and results shall be provided; 4) where PLC programming is used, control software shall be developed using IEC 61131-3 languages and PLCopen implementations shall be used where supported by the selected technology platform; 5) use the latest available programming tools for the selected controller series for the control software development; 6) have in place software upgrade management process standards covering security update management, end-of-support tracking, and communication to Client, for all in scope supplied Operating Systems (OS), firmware, applications and third-party software; 7) ensure that the hardware components of the system selected by the Supplier shall be commercially available for at least 5 years as spare parts after the first delivery; when a component becomes obsolete (no longer commercially available), the Supplier shall propose a like-for-like or functionally equivalent replacement, subject to Client validation, ensuring no regression in functionality, safety, or cybersecurity posture; 8) notify Client, post-contract award, of any software or firmware upgrade required to support the Supplier's technology roadmap or lifecycle evolution of supplied components, within a pre-negotiated period, as defined in the software upgrade management process, including a description of functional and security impacts. 9) test, apply and validate the upgrade on a baseline reference system before distribution. Application of software upgrade must occur before a software component reaches End of Support; 10) verify system functionality and relevant security controls, based on pre-negotiated procedures, at the conclusion of software upgrade, and provide documented evidence of the results; 11) detail its patch management process, for all supplied Operating Systems (OS), applications and third-party software. The process must include elements such as software package antivirus scanning and integrity checking, e.g. via state of the art cryptographic hash. Responsibility for distinct patching process steps (such as test, installation and validation) must be identified in agreement with Client; 12) implement its patch management process, post-contract award, in order to a. provide notification of known vulnerabilities affecting supplier-supplied OS, application, and third-party software within a pre-negotiated period after public disclosure; b. provide notification of security-relevant patches or mitigations within a pre-negotiated period as identified in the patch management process; c. test, apply and validate the appropriate updates and/or workarounds on a baseline reference system before distribution. Mitigation of these vulnerabilities must occur within a pre-negotiated period; d. verify system functionality and security-relevant configurations, based on pre-negotiated procedures, at the conclusion of patch updates, and provide documented evidence of the results. 13) Ensure that all communication between OEM Industrial Automation components (including each subsystem) and Client systems shall be based on OPC UA communication protocol, comply with OPC UA Foundation specification and TMC (Tobacco Machine Communication) companion specification.

Topic	Details of the Security Measures
	14) deploy a OPC UA security architecture (OPC 10000-2: OPC Unified Architecture) implementing security mechanisms appropriate to the use case, addressing at minimum the following security objectives: authentication, authorization, confidentiality, integrity, auditability and availability. Where technically supported, OPC UA connections shall use secure modes and policies (e.g. Sign And Encrypt, strong cryptographic profiles) and certificate-based trust management. 15) ensure that security-relevant events (logons, privilege changes, program downloads, config changes) shall be logged and retained for an agreed period and be exportable to Client SIEM where applicable. 16) deploy secure Programmable Logic Controller (PLC) coding Practices during software development: a) Track operating modes b) Leave operational logic in the PLC wherever feasible c) Use PLC flags as integrity checks d) Use cryptographic and / or checksum integrity checks for PLC code e) Validate timers and counters f) Validate and alert for paired inputs / outputs g) Validate HMI input variables at the PLC level, not only at HMI h) Assign designated register blocks by function (read/write/validate) i) Instrument for plausibility checks j) Validate inputs based on physical plausibility k) Disable unneeded / unused communication ports and protocols l) Restrict third-party data interfaces m) Define a safe process state in case of a PLC restart n) Summarize PLC cycle times and trend them on the HMI o) Log PLC uptime and trend it on the HMI p) Log PLC hard stops and trend them on the HMI q) Monitor PLC memory usage and trend it on the HMI r) Trap false negatives and false positives for critical alerts