JM INFORMATION SECURITY REQUIREMENTS

1.INFORMATION SECURITY MANAGEMENT – GENERAL

Any defined terms in this document, unless defined here, shall be as defined in the relevant Johnson Matthey Plc Standard Terms and Conditions of Purchase or such other agreement entered into between JM and the Supplier (the "**Agreement**"). In the event of any conflict between the requirements in this document and those of the Agreement, the requirements in this document shall take precedence.

For the purposes of this document:

(i) "**Good Industry Practice**": the exercise of that level of degree of skill, diligence, judgement, integrity, timeliness, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced service provider (i) complying with applicable laws, industry standards and security industry leading practices, and (ii) engaged in the provision of services the same as or similar to the Services.
(ii) "**JM**" means Johnson Matthey PLC incorporated and registered under the laws of England and Wales with its registered address at 5th Floor, 2 Gresham Street, London, EC2V 7A, and any of its affiliates.
(iii) "**JM Information**" means all and any Personal Data (where applicable), Confidential Information (which shall include without limitation all user credentials and passwords), PCI DSS Data (where applicable) or other data processed by Supplier (or any of its sub-contractors) on behalf of JM in connection with the Agreement.
(iv) "**NIS2 Directive**" means Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.
(v) "**PCI DSS Data**" means data that includes, but is not limited to, any of the following payment card data elements: primary account number, cardholder name, service code, card expiration data, full magnetic stripe data; CAV2/CVC2/CVV2/CID data and PIN/PIN block data and which is stored, processed or transmitted on behalf of JM group of companies or its customers and platform subscribers.
(vi) "**Services**" means the services (including technology and goods, if any) which are provided by the Supplier to JM pursuant to the Agreement.
(vii) "**Supplier**" means any third-party providing the Services.
(viii) "**Supplier Personnel**" means all employees, staff and consultants of the Supplier and its affiliates who are engaged in the provision of the Services.

1.1 The Supplier shall provide all Services utilising security technologies, techniques and measures in accordance with Good Industry Practice and, where applicable, the principles of the standards selected by the Supplier as applicable when responding to the JM information security questionnaire(s), for example:

ISO27001

SOC1 (SSAE18)

SOC2

ISAE 3000 /3402

PCI Data Security Standards (where applicable to the Services)

(or such other equivalent standards as are applicable from time to time together, the "**Standards**")

1.2 The Supplier shall supply copies of the relevant security certifications in compliance with the Standards upon written request from JM. Additionally, to the extent JM requests additional security certifications from Supplier that Supplier does not currently maintain in respect of the Services, then the parties will review such request under the change control procedure set out in the Agreement.

1.3 The Supplier shall, at all times during the term of the Agreement, have appointed a person (together with a suitable deputy) responsible for ensuring the Supplier's compliance with the requirements set out in the Agreement.

1.4 The Supplier shall throughout the term of the Agreement operate and maintain an information security management system which meets the requirements of the Standards.

1.5 All systems used to process, store or transmit JM Information must be securely configured in line with security Good Industry Practice.

1.6 The Supplier must not use any JM Information in non-production environments or for non-production purposes including testing or training.

1.7 The Supplier will promptly respond to any requests from JM to confirm the security controls it has in place to protect JM Information, including but not limited to completing an annual security questionnaire issued by JM.

2.ACCESS CONTROLS (TO JM'S SYSTEMS ENVIRONMENT)

2.1 Where the Supplier is granted access to the JM systems environment, it shall do so only from a range of designated and pre-agreed Supplier network addresses. Access other than as strictly necessary for the purpose of fulfilling its obligations under the Agreement is strictly forbidden. Access controls and limitations used to access JM's systems environment will be determined at the discretion of JM. Authentication credentials (including passwords, certificates, tokens and biometric data) that enable access to JM's systems environment must be kept strictly confidential and appropriately protected by the Supplier and must not be passed on to any third party or to any Supplier Personnel who are not authorised in writing by JM for the purposes of the Agreement.

2.2 All Supplier Personnel who access the Supplier's systems environment must be granted authorised access using formally defined and approved processes in accordance with Good Industry Practice. Such Supplier Personnel must be allocated a unique identifier for their personal and sole use and the Supplier shall ensure such personnel activities can be traced back to the responsible individual. The Supplier must not reallocate user identifiers issued to specific Supplier Personnel to any other person. Shared user identifiers are prohibited.

2.3 The Supplier must maintain a formal record of all Supplier Personnel authorised to have access to JM's systems environments, which must be subject to regular review (at least quarterly) and must provide JM with a copy of the record upon request. The Supplier will immediately remove, or request JM to remove, the access rights of any person who no longer need access to JM's systems environment and / or the Supplier's systems environment for the purposes of the Agreement. This will include (but not be limited to) disabling/deletion of the relevant user account, automatic expiry of the account on the termination of employment or engagement of any Supplier Personnel and the disablement of any user account which has been inactive for a period of 90 days unless prior written approval has been provided by JM for such account to remain active. The Supplier must keep a formal record of the checks carried out and these checks must be performed at least annually.

2.4 Passwords used to connect to the JM systems environment must follow Good Industry Practice, including but not limited to, the use of multi-factor authentication for privileged accounts (as a minimum) and appropriate complexity requirements.

2.5 The Supplier shall ensure that in respect of all matters arising from the Agreement, its Supplier Personnel and personnel of its sub-contractors or agents:

a) do not attempt to access, or allow access to, any JM Information to which they do not require access in connection with the Agreement or to which they are prohibited from accessing under any contract with JM or by applicable laws; and

b) use any email account allocated to them by JM only for the transfer or receipt of any data or information related to JM's business or activities.

c) are familiar with security industry practice and will comply with all JM security policies and standards communicated to them unless a suitable alternative is pre-agreed in writing with JM.

2.6 Supplier shall not load any software on to any JM owned computer or sent or supplied to Supplier Personnel unless pre-approved in writing by an JM IT Change Manager. NOTE: This only applies to equipment supplied by JM directly (laptops, routers, etc.).

3.PHYSICAL ACCESS TO FACILITIES

3.1 The Supplier shall:

a) maintain appropriate and adequate physical access control mechanisms to prevent unauthorised access to Supplier facilities in accordance with Good Industry Practice;

b) ensure that physical access control mechanisms within the Supplier's facilities for communications rooms, server rooms or any rooms providing connectivity or transport for JM's materials shall prevent unauthorised persons or other individuals from entering these locations, including ensuring that entry points shall be accessed via use of authentication which is unique to the individual accessing the location. (i.e. shared PIN codes or keys are not permitted);

c) ensure that entry and exit points to Supplier facilities, data centres and server rooms are monitored by CCTV (24x7). CCTV images shall be retained for a minimum of 30 days;

d) ensure that any third-party requiring access to provide support or maintenance for any equipment that is directly or indirectly involved in providing the Services shall be logged into and out of the Supplier's facilities including the reason for their visit and the responsible member of Supplier Personnel and shall be escorted by the responsible member of Supplier Personnel at all times;

e) ensure that logs will be maintained of access to the Supplier's data centres and that these logs are retained for at least 6 months;

f) ensure that data centre and server room locations must be constructed of floor to ceiling walls and either not contain windows or where windows are present these must be opaque and secured by suitable grills/bars to prevent physical ingress into the location; and

g) ensure that fire doors on security perimeters to the Supplier's data centre and server room facilities should be alarmed, close shut and fail secure.

4.SUPPLIER EQUIPMENT

4.1 All infrastructure, whether owned by the Supplier or provided by a third party, used by the Supplier in connection with the Agreement must be subject to system hardening in alignment with the Center for Internet Security ("**CIS**") standards and shall include the removal of unnecessary services, changes to default user accounts & passwords, tightly controlled restrictions to privileged, supervisor and hypervisor roles, implementation of anti-malware and/or virus protection, implementation of security event logging and monitoring and other security service as agreed with JM. Anti-malware software updates must be applied upon being released by the vendor and the software must be configured for at least daily scheduled and on-access scanning. Firewall and network-based intrusion detection software must be implemented to control and monitor connections to the Supplier's systems environment from the Internet or other networks.

4.2 All information security controls relating to the development, build, configuration, deployment, operation, change management, maintenance and support for all technologies relating to the Supplier's systems environment shall be in line with Good Industry Practice.

4.3 The Supplier shall implement a formal change management process to ensure changes made to the Supplier's systems environment are approved before being implemented.

5.SUPPLIER PERSONNEL

5.1 Unless there are equivalent obligations under the Agreement, the Supplier shall ensure that all Supplier Personnel used in the provision of the Services shall be appropriately vetted for security compliance relevant to the Services.

5.2 The Supplier shall maintain complete records of the checks performed for each person vetted.

6. DATA SECURITY

6.1 The Supplier shall ensure that:

a) technical (automatic data encryption controls for laptops and USB removable media) and procedural (policies and user awareness) controls are in place for all portable devices (e.g. laptops, tablets) and removable media (e.g. CDs, DVDs, USB storage devices, backup tapes) that contain JM Information, in accordance with current Good Industry Practice encryption standards, or such other standards as may be agreed in writing between the Supplier and JM; and

b) JM Information transferred electronically outside of the Supplier's systems environment, or over any public network, are encrypted using strong encryption when initiated by the Supplier. Decryption credentials (including passwords and keys) must not be shared via the same channel as that used for the transfer of the materials themselves.

6.2 The encryption mechanisms shall be in accordance with Good Industry Practice encryption standards.

6.3 Where paper copies of JM Information are kept these must be secured in accordance with Good Industry Practice.

6.4 Any JM Information must only be used for the purpose of the Agreement and be retained, returned and destroyed at JM's option and in accordance with JM instructions which shall be communicated in writing and in advance by JM. When JM Information is deleted, this must be done on a secure basis which renders such data irrecoverable by any means. Supplier will ensure that any JM Information it holds on back up, either directly or through a third party, will on JM's instructions be securely deleted in accordance with security industry leading

practice. Notwithstanding the foregoing, the Supplier may, in accordance with applicable laws, store copies of JM Information in an archival format provided that such copies shall remain subject to the confidentiality provisions under the Agreement for as long as they are so retained.

7.SECURITY INCIDENTS

7.1 Unless otherwise agreed under the Agreement, subject to 7.2, where applicable, any known or anticipated information risk, or other incident impacting the JM Information or the Services or that can be seen to directly or indirectly affect JM, its personnel, systems environment, materials, facilities, processes, operations or reputation shall be promptly notified to JM in writing, and in any event no later than 72 hours of such an incident being suspected by the Supplier, provided that in respect of any Personal Data breaches, the Supplier shall promptly notify JM in writing without undue delay, and in any event no later than 24 hours of becoming aware of such breach.

7.2 In accordance with the NIS2 Directive, enhanced incident notification is required for incidents defined within the NIS2 Directive as 'significant incidents' to include phased notification with an early warning. Accordingly, the Supplier shall notify JM in writing of the occurrence of such incident without undue delay, and in any event no later than 24 hours of becoming aware of such incident.

7.3 Formal investigation of any security incident involving Supplier Personnel, information or systems environment shall be carried out in accordance with Good Industry Practice.

7.4 The Supplier must maintain a register of security-related incidents (type, date, people involved) in relation to the JM Information and must immediately inform JM of critical incidents (i.e. incidents which might, even potentially, have exposed JM Information to unauthorised processing or which might, even potentially, have an adverse impact on JM Information). This register must be reviewed with JM at least annually and made available to JM on written request.

8.PENETRATION TESTING, AUDIT AND COMPLIANCE

8.1 Where the Supplier's systems environment is connected to the internet or to other organisations/networks (including JM's system environment), the Supplier shall perform an independent security penetration test to ensure the system's security at least annually and upon any major changes to the Supplier's systems environment that could have a security impact to the Supplier's systems environment.

8.2 The Supplier shall perform risk-based security audits of its system environment at least once every 12 months and upon many major changes to its systems environment.

8.3 If the Supplier provides a code development service to JM, the Supplier shall be required to follow Good Industry Practice for code development.

8.4 The Supplier shall ensure that it maintains compliance with this document and all necessary regulatory security requirements relating to the service that it provides to JM, including but not limited to NIS2 Directive, and shall provide written evidence of such compliance at JM's written request.

8.5 Where applicable to the Services, if PCI DSS Data can be accessed, stored, processed or transmitted as part of the Agreement, Supplier acknowledges responsibility for the security of such PCI DSS Data. Supplier will ensure compliance with the most recent version of the PCI Data Security Standards, as updated from time to time.

For any queries in relation to this document, please contact the JM Chief Information Security Officer at cyber@matthey.com.