Octopus Deploy Data Processing Agreement

This Data Processing Agreement ("**Agreement**") is an addendum to our Octopus Deploy Customer Agreement ("**Customer Agreement**").

This Agreement applies to the extent that we act as a Processor and you act as a Controller of any Personal Data in connection with our Customer Agreement

We enter into this Agreement on our own behalf and on behalf of each of our Affiliates. If your Affiliates have the benefit of our Services, or provide Personal Data to us for the purposes of your Customer Agreement, you enter into this Agreement on your own behalf and on behalf of each of your Affiliates.

For the purposes of this Agreement only, save as indicated otherwise, a reference to "**we**", "**our**" or "**us**" is also a reference to each of our Affiliates, and a reference to "**you**" or "**your**" is also a reference to each of your Affiliates. For the avoidance of doubt, this does not impose any further rights or obligations on any of our respective Affiliates under the Customer Agreement.

In the event of any inconsistency between this Agreement and the Customer Agreement, the terms of this Agreement shall prevail in respect of our respective privacy and data security rights and obligations as described herein, and the terms of the Customer Agreement shall prevail in all other respects.

1. Definitions and Interpretation

1.1. Unless otherwise defined herein, capitalised terms and expressions used in this Agreement shall have the following meaning:

"**Agreement**" means this Data Processing Agreement and all schedules.

"**Affiliate**" means:

(a) the partners of any partnership;

(b) an incorporated entity that owns or controls, is owned or controlled by, or is under common ownership or control, with a party to this Agreement (the term "control" meaning the power to directly or indirectly direct the management or conduct of the entity by any means); or

(c) any unincorporated association, or the trustee of any trust, which, if incorporated, would be an Affiliate under (b).

"**Applicable Laws**" means:

(a) the CCPA;

(b) the GDPR;

(c) the UK Data Protection Laws

(d) the Australian *Privacy Act 1988* (Cth); and

(e) any other applicable law with respect to Your Data in respect of which we, our Affiliates, and / or a Subprocessor, are subject.

"**CA Personal Information**" means Personal Data that, under the CCPA, constitutes “personal information".

"**CCPA**" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

"**Controller**" means you, as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, whether defined as a controller or otherwise, or otherwise defined as a controller under Applicable Laws.

"**Data Subject**" means a person to whom Personal Data relates, whether defined as a data subject or otherwise, or otherwise defined as data subject under Applicable Laws.

"**GDPR**" means EU General Data Protection Regulation 2016/679.

"**ICO**" means the Information Commissioner's Office or such other data protection regulator responsible for monitoring or enforcing compliance with UK Data Protection Laws in the UK.

"**include**" includes without limitation.

"**Personal Data**" means data about an identified individual or a person whom is reasonably capable of being identified (whether by reference to the Personal Data or in combination with other data) or otherwise defined as personal data, personal information, or similar, under Applicable Laws.

"**Personal Data Breach**" means a breach of security resulting in the unauthorised or unlawful processing, damage, alteration, disclosure or access to, loss, destruction, or other dealing, of Personal Data.

"**Processing**" includes collecting, recording, storing, modifying, using, disclosing, distributing, publishing, deleting, or otherwise dealing with, Personal Data, whether defined as processing or otherwise, under Applicable Laws.

"**Processor**" means us, being a company which processes Personal Data on your behalf (as Controller), whether defined as a processor or otherwise, under Applicable Laws.

"**Services**" means:

(a) our commercially available downloadable software products;
(b) our cloud services; and
(c) any related support, maintenance, or professional services, provided by us,

as set out in our Customer Agreement.

"**Standard Contractual Clauses**" means the standard contractual clauses approved by the European Commission for transfers of Personal Data to countries not otherwise recognised as offering an adequate level of protection for Personal Data by the European Commission, being Module 2 controller to processor clauses as approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021 (as amended and updated from time to time).

"**Subprocessor**" means any person (whom we appoint or is appointed on our behalf, to process Personal Data on your behalf, in connection with the Customer Agreement (which may include our Affiliates, but which excludes our employees, agents, and sub-contractors, and those of our Affiliates).

"**UK Addendum**" means the UK International Data Transfer Addendum to the Standard Contractual Clauses version B1.0, as may be amended, replaced or superseded by the ICO from time to time (including as formally issued by the ICO under section 119A(1) of the DP Act).

"**UK Data Protection Laws**" means any applicable laws and regulations in the UK relating to the use or processing of personal data including:

(d) the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the *European Union (Withdrawal) Act 2018* ("**UK GDPR**");
(e) any laws or regulations ratifying, implementing, adopting, supplementing or replacing the GDPR;
(f) the *Data Protection Act 2018* ("**DP Act**");
(g) any laws and regulations implementing or made pursuant to EU Directive 2002/58/EC (as amended by 2009/136/EC); and
(h) the Privacy and Electronic Communications (EC Directive) Regulations 2003,

in each case, as updated, amended or replaced from time to time.

"**Your Data**" means any Personal Data which we, or a Subprocessor, Process on your behalf under or in connection with the Customer Agreement.

1.2. Plural or other derived terms of those terms defined in section 1.1 shall be construed accordingly.

2. Your use of Your Data

2.1. You acknowledge and agree, and represent and warrant, that:

(a) you appoint us as a Processor of Your Data for the purposes of the Applicable Laws;

(b) you are solely responsible for:

(i) the contents of Your Data including ensuring that it is accurate, complete, and up to date; and

(ii) your instructions to us and to our Sub-Processors in dealing with Your Data from time to time (including that those instructions comply with any Applicable Laws); and

(c) you have full legal right and authority (including any and all necessary consents) under Applicable Laws to provide us:

(i) the Your Data; and

(ii) instructions regarding the Your Data; and

(d) you will promptly inform us if any of the circumstances in sections 2.1(a) to 2.1(c) change.

2.2. Subject to section 5 below, you acknowledge and agree that your acceptance of our Customer Agreement (including this Agreement) constitutes your lawful, valid and final instructions to us, and authorisation for us to retain Subprocessors and direct our Subprocessors, to:

(a) process Your Data; and

(b) transfer Your Data to any country or territory,

(c) as reasonably necessary for the provision of the Services and consistent with the Customer Agreement and this Agreement.

2.3. You acknowledge and agree that:

(a) nothing in this Agreement (including, without limitation, sections 4, 6, and 7), is a substitute for you implementing your own independent policies and procedures for dealing with Your Data in accordance with your own obligations under contract, under Applicable Law, or otherwise (including technical and organisational policies, physical and electronic security measures, and legal measures); and

(b) we are not responsible, and you indemnify us from, any liability (including to a Data Subject), for any act, omission, or event (including a Personal Data Breach) which arises as a result of your breach of section 2.1 or your failure to implement and abide by appropriate policies and procedures as described in section 2.3(a) (including where we have done, or omitted to do, anything, in reliance on an instruction from you, where the instruction arises from your such failure).

3. Our obligations in respect of Your Data

3.1. We shall only Process Your Data for the purposes of the Customer Agreement and this Agreement and in compliance with Applicable Laws.

3.2. Where we process Your Data, we will in respect of Your Data, act only on written instructions and directions from the you (which includes, for the avoidance of doubt, all authorisations given by you under the Customer Agreement) and will comply promptly with all such instructions and directions received from you from time to time unless we are required to Process Your Data to comply with Applicable Law to which we are subject to in which case we will notify you of such legal requirement prior to such processing unless such law prohibits notice to you on public interest grounds.

4. Confidentiality and security

4.1. We shall take reasonable steps to ensure that access to Your Data is limited to those of our:

(a) employees, agents, and sub-contractors;

(b) Affiliates, and their respective employees, agents, and sub-contractors; and

(c) Sub-processors, and their respective employees, agents, and sub-contractors,

for the purposes of the Customer Agreement and of this Agreement, and subject to obligations of confidentiality (which may be under contract or under Applicable Law).

4.2. We shall implement all appropriate technical and organisational measures to ensure a level of security in relation to Your Data. The nature of these measures may change or vary from time to time but may include, as appropriate:
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and / or
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.3. The technical and organisational security measures that we may take from time to time may take into account matters including:
(a) the state of the art;
(b) the costs of implementation;
(c) the nature, scope, context and purposes of Processing;
(d) the risk of varying likelihood and severity for the rights and freedoms of natural persons; and
(e) the risk of Processing your Data, e.g. from a Personal Data Breach.

5. Subprocessors

5.1. We may engage Subprocessors from time to time, a current list of which is published on our website and kept up to date. Where we engage or intend to engage a Subprocessor, or change or intend to change a Subprocessor, we shall update such list in advance and such update shall constitute our notice to you of the engagement or change. We will ensure that any Subprocessors provide the level of protection of Your Data required under Applicable Laws, including as set out in the remainder of this section 5.

5.2. When appointing a Subprocessor in accordance with section 5.1, we shall enter into a written agreement with such Subprocessor, prior to any processing by such Subprocessor, requiring the Subprocessor to:
(a) process Your Data only in accordance with our written instructions;
(b) comply with data protection obligations equivalent in all material respects to those imposed on us under this Agreement.

5.3. Your authorisation pursuant to section 5.2(b) shall be conditional upon us ensuring there is adequate protection and appropriate safeguards for Your Data in accordance with Applicable Laws when it is transferred or accessed in that country or territory.

5.4. Notwithstanding the appointment of a Subprocessor, we are responsible and liable to you for any processing by the Subprocessor in breach of this Agreement.

6. Data Subject Rights

We shall as soon as reasonably practicable notify you if we receive a request, notice, communication or complaint from a Data Subject in respect of Your Data (where you are the Controller and we are the Processor). We shall give you our full co-operation and assistance in responding to the same, and to enable you to otherwise comply with Applicable Laws, including to provide you with ways in which you can reasonably manage Your Data.

7. Personal Data Breach

7.1. If we become aware of a Personal Data breach affecting Your Data, we will (subject to the requirements of any Applicable Laws) endeavour to:
(a) notify you as soon as practicable; and
(b) provide you with sufficient information as is available to us to allow you to meet any obligations to report or inform any affected Data Subjects of the Personal Data breach under Applicable Laws.

7.2. We shall co-operate with you and take such reasonable commercial steps as you direct to assist in the investigation, mitigation and remediation of each such Personal Data

Breach. We may require or request that you reimburse our reasonable costs of providing assistance where the assistance directed goes further than is necessary for the purpose of complying with Applicable Law.

8. Your Data post-termination or expiry of Customer Agreement

8.1. We will delete or return all Your Data Processed under this Agreement in accordance with Applicable Law and our Customer Agreement.

8.2. We may retain Your Data to the extent required or permitted by Applicable Law and our Customer Agreement. We shall ensure that any such retained Your Data is kept confidential and only used, disclosed, retained, or otherwise dealt with, as permitted under Applicable Law and our Customer Agreement.

9. Assistance

9.1. We shall, on request or where otherwise reasonable to do so, provide reasonable assistance to you with any data protection impact assessments, or any prior consultations with competent data privacy authorities, in relation to our, and any Subprocessors, Processing of Your Data.

9.2. We may, where permitted by Applicable Laws, require or request that you reimburse our reasonable costs of providing assistance under section 9.1.

10. Compliance

10.1. We will provide you with any information reasonably necessary to demonstrate our compliance with this Agreement (which may include inspection or audit of relevant records) in accordance with this section 10.

10.2. Any request by you or any of your Affiliates, is deemed to be a request by you and all of your Affiliates jointly.

10.3. You may make a request for information once in any calendar year unless you have genuine reasons for a request sooner or are required or entitled to do so under Applicable Laws, and have identified those reasons to us when making the request.

10.4. Your right to request information only applies to the extent relevant to our compliance with the requirements of Applicable Laws and does not constitute a general right to request any other information.

10.5. The persons to whom any information is provided in response to your request must keep the information provided to them confidential save to the extent necessary to confirm to you our compliance with this Agreement. Those persons must further (at our option) return or destroy that information upon delivery of their final report to you.

10.6. You must provide us a reasonable time to respond to your request.

10.7. If our response to your request includes your inspection or audit of any of our infrastructure or premises, the persons carrying out such inspection must avoid or minimise any disruption to us, and comply with any directions, policies, or procedures, which we may require (including physical or electronic security policies).

10.8. We may require your auditor or representative to provide reasonable evidence of identity or authority before responding to their request or permitting access to any information or to conduct any audit.

10.9. We may, only where expressly permitted by Applicable Laws or where the assistance that you request and we may provide exceeds the scope of the assistance which we are required to provide under Applicable Laws, require or request that you reimburse our reasonable costs of providing assistance under this section 10.

11. Restricted data transfers under the GDPR

11.1. This section 11 applies to the extent that you instruct us to Process Personal Data originating from within the European Union and/or European Economic Area and to the extent that the GDPR applies to our Processing when making that transfer, such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR. Such transfer shall constitute an "EU SCCs Transfer".

11.2. Subject to our compliance with this section 11 you consent to our transferring Your Data (including Personal Data) to countries outside of the European Union and/or European Economic Area.

11.3. Where there is an EU SCCs Transfer, such transfer shall be permitted provided that where we process Personal data as a Processor, and you are a Controller, we shall be bound by and comply with the Standard Contractual Clauses and the following shall apply:

(a) Clause 7 (docking) shall not apply;

(b) In respect of Clause 9 (sub-processors), Option 2 (general authorisation) applies, and we shall specifically inform you in writing of any intended changes to our Subprocessors in accordance with section 5;

(c) The "OPTION" in Clause 11(a) shall not apply and the wording in square brackets in that Clause shall be deleted;

(d) In respect of Clause 17 (governing law), the Parties agree that the governing law shall be Ireland;

(e) In respect of Clause 18 (choice of forum and jurisdiction), the relevant courts shall be the courts of Ireland;

(f) Annex I, Section A of the Standard Contractual Clauses shall be completed with the information set out in Schedule 1 of this Agreement and the signature and date shall be deemed to be as at the date of this Agreement;

(g) Annex I, Section B of the Standard Contractual Clauses shall be completed with the information set out in Schedule 1 of this Agreement;

(h) Annex I, Section C shall be completed as follows: [*the Data Exporter's competent supervisory authority as determined by the EU GDPR*]; and

(i) Annex II of the Standard Contractual Clauses shall be completed with the information set out in section 4 and Schedule 2 of this Agreement.

11.4. In the event of any inconsistency between this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail to the extent of the inconsistency.

11.5. If the Standard Contractual Clauses entered into in accordance with section 11.3 are deemed at any time not to provide an adequate level of protection in relation to Your Data or transfers of data within/to the under the Applicable Laws, on receipt of notice of such from either party, the parties will work to implement such alternative measures and execute all such documents as may be required to comply with the Applicable Laws to ensure that the relevant transfer and all resulting Processing are compliant with Applicable Laws.

12. Restricted data transfers under the UK GDPR

12.1. Where Your Data is transferred by you to us outside the UK, then to the extent that the UK GDPR applies to our Processing when making that transfer, and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the DP Act, such transfer shall constitute a "UK Addendum Transfer".

12.2. Subject to our compliance with this section 12 you consent to our transferring Your Data (including Personal Data) to countries outside of the UK.

12.3. For the UK Addendum, the following shall apply:

(a) Table 1 shall be deemed completed with the relevant information from Schedule 1 of this Agreement;

(b) In Table 2, the first option shall be selected with the date being the date of this Agreement and the reference being to the EU SCCs identified in section 11.3 of this Agreement;

(c) Table 3 shall be deemed completed with the relevant information as set out in Schedule 1 of this Agreement; and

(d) Table 4 shall be deemed completed such that we have the right to end the UK Addendum as set out in Section 19 of Part 2 of the UK Addendum.

12.4. In the event of any inconsistency between this Agreement and the UK Addendum, the UK Addendum shall prevail to the extent of the inconsistency.

12.5. If the UK Addendum entered into in accordance with section 12.3 is deemed at any time not to provide an adequate level of protection in relation to Your Data or transfers of data within/to the under the Applicable Laws, on receipt of notice of such from either party, the parties will work to implement such alternative measures and execute all such documents as may be required to comply with the Applicable Laws to ensure that the relevant transfer and all resulting Processing are compliant with Applicable Laws.

13. Application of the CCPA

13.1. For the purpose of the CCPA, you acknowledge and agree that you are a Business and we are a Service Provider (as those terms are defined in the CCPA).

13.2. To the extent that any of Your Data is subject to the CCPA, we shall Process Your Data in accordance with and as permitted by the CCPA, this Agreement, and the Customer Agreement.

13.3. More particularly:

(a) We shall not:

(i) sell any CA Personal Information;

(ii) retain, use or disclose any CA Personal Information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the CA Personal Information for a commercial purpose (as defined in the CCPA) other than provision of the Services; or

(iii) retain, use or disclose the CA Personal Information outside of the direct business relationship between us and You. We hereby certify that we understand our obligations under this section and will comply with them.

(b) Notwithstanding anything in the Agreement or any order form entered in connection therewith, the parties acknowledge and agree that our access to CA Personal Information or any other of Your Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

14. General

14.1. All notices and communications given under this Agreement must be in writing and in accordance with the Customer Agreement.

14.2. Each party's liability (excluding under any liability) under this Agreement including the Standard Contractual Clauses, is limited as set out in the Customer Agreement.

14.3. Save to the extent that this Agreement or Applicable Law provides otherwise, this Agreement is subject to the law and jurisdiction, and the venue for any dispute, shall be as provided in the Customer Agreement.

Schedule 1

Data Processing Particulars

<table>
<tr><td>(A)</td><td>Role of Parties</td><td colspan="2">Octopus Deploy Pty Ltd (we, our, or us) act as processor on behalf of the Customer (you, your) as Controller.</td></tr>
<tr><td>(B)</td><td>Subject matter, nature and purpose of the processing of Personal Data</td><td colspan="2">Subject matter
Our provision of software and services to you in accordance with our Customer Agreement.

Nature
We may undertake Processing activities such as collecting, recording, storing, modifying, using, disclosing, distributing, publishing, deleting, and other operations.

Purpose
Personal Data is processed in order to facilitate our supply of and your use of software and services in accordance with the Customer Agreement.</td></tr>
<tr><td>(C)</td><td>Duration of the processing of Personal Data</td><td colspan="2">For the term of the Customer Agreement and for up to seven (7) years following termination or expiry of the agreement, subject to our lawful and legal requirements and obligations, and any request for earlier deletion which may be received.</td></tr>
<tr><td>(D)</td><td>Type of Personal Data processed</td><td colspan="2">Personal Data
The personal data transferred contains a data subject's name, contact information including email address(es), payment information (where applicable), data related to third party single sign on (SSO) services, and behavioural data while carrying out operations in respect of the software and services supplied under the Customer Agreement, including the time actions are performed.

Special Categories of Personal Data
No transfer of special categories of data is anticipated.

Criminal Records Data
No transfer of criminal records data is anticipated.</td></tr>
<tr><td>(E)</td><td>Categories of data subjects of the Personal Data</td><td colspan="2">The Personal Data transferred concerns technical representatives, billing representatives, project managers, end users, and other persons whom may act on your behalf from time to time for the purposes of the Customer Agreement.</td></tr>
<tr><td rowspan="7">(F)</td><td rowspan="7">Cross-Border Data Transfers
Which party is the data exporter and data importer will depend on how data flows between the Parties.</td><td colspan="2">Data exporter(s)
Note: the data exporter is the party transferring personal data outside of the UK/EEA, as applicable.</td></tr>
<tr><td>Name</td><td>As recorded in Octopus Deploy's licensing portal from time to time.</td></tr>
<tr><td>Address</td><td>As recorded in Octopus Deploy's licensing portal from time to time.</td></tr>
<tr><td>Contact person's name, position, and contact details</td><td>As recorded in Octopus Deploy's licensing portal from time to time.</td></tr>
<tr><td>Activities relevant to the data transferred under these Clauses</td><td>As agreed between the Parties, in accordance with this Agreement and the Customer Agreement.</td></tr>
<tr><td>Signature and Date</td><td>Signature and date shall be deemed to be as at the date of the Customer Agreement.</td></tr>
<tr><td>Role</td><td>Controller</td></tr>
</table>

		Data importer(s) Note: the data importer is the party receiving personal data outside of the UK/EEA, as applicable.	
		Name	Octopus Deploy Pty Ltd (and, where applicable, its Affiliates as defined in the Agreement)
		Address	(c/o) Octopus Deploy Pty Ltd Level 4, 199 Grey Street South Brisbane QLD 4101 Australia
		Contact person's name, position, and contact details	The Data Protection Officer privacy@octopus.com
		Activities relevant to the data transferred under these Clauses	As agreed between the Parties, in accordance with this Agreement and the Customer Agreement.
		Signature and Date	Signature and date shall be deemed to be as at the date of the Customer Agreement.
		Role	Processor
		Description of the Transfer	
		As set out in Items (B) to (E) of this Schedule.	
		Frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	
		Continuous	
(G)	**Is personal data received from the Data Importer combined with personal data collected by the Data Exporter?**	Yes, in some circumstances according to the Data Exporter's use of the software and services under the Customer Agreement.	
(H)	**List of Approved Subprocessors**	As set out from time to time at https://octopus.com/legal/gdpr	

Schedule 2

Technical and Organisational Security Measures

We shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

1. the pseudonymisation and encryption of Personal Data;

2. measures designed to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services and deliverables under the Agreement;

3. the ability to restore the availability and access to your Personal Data in a timely manner in the event of a physical or technical incident;

4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing;

5. a process and procedures to monitor and log processing systems for unauthorised changes and other evidence the processing environment has been compromised. We shall document and monitor compliance with these measures. Technical and organisational measures are subject to technical progress and further development and we may implement alternative adequate measures provided we shall not decrease the overall security of the services and deliverables during the term of the Agreement. The minimum security measures to be implemented by us are as follows:

   (a) **Encryption.** We shall use strong encryption methodologies to protect your Personal Data transferred over public networks, and shall implement whole disk encryption for all Personal Data at rest and in transit. We will fully document and comply with industry best practice and our key management procedures for crypto keys used for the encryption of your Personal Data.

   (b) **Storage.** We shall retain all your Personal Data in a physically and logically secure environment to protect from unauthorised access, modification, theft, misuse and destruction. We shall utilise platforms to host your Personal Data that are configured to conform to industry standard security requirements and will only use hardened platforms that are continuously monitored for unauthorised changes.

   (c) **Endpoint Detection & Response; Firewall.** We shall utilise programs that are capable of detecting, removing, and protecting against known types of malicious or unauthorised software. We will implement firewalls designed to ensure that all traffic from and to the supplier's systems that host your data systems are restricted to only what is necessary to ensure the proper functioning of the services and deliverables under the Agreement. All other unnecessary ports and services will be blocked by firewall rules at our network.

   (d) **Vulnerability Management**

      (i) **Updates and Patches.** With regards to the handling of your Personal Data, we shall establish and maintain mechanisms for vulnerability and patch management that are designed to evaluate application, system, and network device vulnerabilities and apply our operating system and application like Web Servers, Database etc., and our security fixes and patches in a timely manner taking a risk-based approach for prioritizing critical patches. For critical, zero-day, patches will be applied within 30 days.

      (ii) **Data Loss Prevention.** We shall implement appropriate controls that prevent data loss to protect your Personal Data, and shall integrate the results of that activity with its program for

audit logging and intrusion detection as described below.

(iii) **Audit Logging; Intrusion Detection.** We shall collect and retain audit logs recording privileged user access activities, authorised and unauthorised access attempts, system exceptions, and information security events, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and automated detection tools shall be implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorised Parties only.

(iv) **Information Risk Assessment.** On an annual basis, we shall cooperate with you, at your discretion, to perform formal risk assessments to determine the likelihood and impact of potential privacy and security risks to your Personal Data. We shall conduct the audit annually in accordance with all applicable local laws, regulations and where applicable requirements for credit card and privacy (including without limitation PCI DSS) as well as industry common standards for information security. An audit report shall be provided to you within three (3) months upon the completion of every year's Services by us to you.

(v) **Physical Security.** Where we are Processing your Personal Data, such Personal Data shall be housed in secure areas, physically protected from unauthorised access, with appropriate environmental and perimeter controls. the facilities shall be physically protected from unauthorised access, damage, theft and interference.

(vi) **Disaster Recovery Management.** We shall provide documentation of its formal and secure disaster recovery plan, meeting a standard of industry best practice standards and redacted for proprietary and confidential information. We shall share evidence with you that we conduct regular testing of that plan on at least an annual basis, which impacts any of your Systems and your Personal Data governed by the Agreement.