

PowerHouse Workforce Platform



PowerHouse
Workforce

PowerHouse Workforce License Agreement and Service Level Agreement

June 2023

Version Information

Version	Date	Update / Details
2023-03	March, 2023	Annual Review and update
2023-06	June, 2023	Quarterly Review and update

Terms and Conditions for the Supply of the PowerHouse Workforce Platform

Introduction

- Mediasphere Holdings Pty Ltd (trading as PowerHouse Hub) ABN: 93 120 008 924, of 74 Smith Street Motorway, Southport, Queensland 4215, has developed the PowerHouse Workforce software platform which is a software application to source, recruit, pre-screen, onboard and upskill talent on a cloud-based platform. (hereafter “**Mediasphere**”)
- The Customer wishes to subscribe, from Mediasphere, to a non-exclusive license for the PowerHouse Workforce platform to host, manage and maintain their sourcing, recruitment, onboarding and upskilling portal in accordance with the Works Agreement (hereafter “**Customer**”).

It is agreed:

Definitions and interpretation

Definitions: In this Agreement:

1. Agreement means this document, the Works Agreement and any other schedule or annexure to this document.
2. Australian Privacy Principles has the meaning set out in the *Privacy Act 1988* (Cth)
3. Business Day means a day that is not a Saturday, Sunday or any other day which is a public holiday Brisbane, Australia and the United Kingdom.
4. Commencement Date means the date specified in the Works agreement.
5. Confidential Information means information relating to:
 - a. the design, specification and content of the Website that is not publicly available.
 - b. information contained on the Customer’s computer network systems.
 - c. personnel details, policies, business strategies or any other information or material provided to Mediasphere by the Customer.
 - d. the Development Tools and Templates.
 - e. the terms of this Agreement.
 - f. any proprietary information of either party that is not publicly available; and
 - g. any other information which is stated to be confidential or which, by its nature, should reasonably be considered to be confidential information.
6. Customer Content means all text, pictures, sound, graphics, video, embed codes, documents, files, end-user data generated on the Website and other data loaded and stored in the Website database as well all data and information (including Confidential Information) relating to the Customer and any third parties to whom the Customer provides products or services, and to their respective operations, facilities, assets, products, sales and transactions in whatever form whether entered, stored, generated or processed as part of the Services and includes any:
 - a. database in which such data or information is stored.
 - b. documentation or records related to such data or information; and
 - c. products resulting from the use or processing of such data or information.
7. Customer Deliverables expressly excludes Mediasphere Tools and Templates and means whether created before or after the date of this Agreement all textual, graphical, audio and other material displayed on the Website which are custom developed by Mediasphere for the Customer.
8. Data Protection Law means Privacy Laws (as that term is defined) and other relevant Australian laws and regulations including Privacy Amendment (Notifiable Data Breaches) Act 2017 (cth).
9. Developer Tools and Templates means the software developed prior to the date of this Agreement, or otherwise developed outside of the scope of this Agreement, that is proprietary to Mediasphere or licensed to Mediasphere by third parties.
10. GST Law means the A New Tax System (Goods and Services Tax) Act 1999 (Cth) and any other law dealing with the imposition or administration of a goods and services tax in Australia.

11. Hosting Fee means the monthly/annual fee that is payable by the Customer to Mediasphere for the annual hosting of the Website.
12. Installation Date means the date or period for installation of Software as set out in the Works.
13. Intellectual Property Rights means any and all now known or subsequently known tangible and intangible:
 - a. rights associated with works of authorship, including but not limited to copyrights and moral rights.
 - b. trademark and trade name rights and similar rights.
 - c. trade secret rights.
 - d. patents, designs, algorithms and other industrial property rights.
 - e. all other intellectual and industrial property rights of every kind and nature throughout the universe and however designated (including logos, rental rights and rights to remuneration), whether arising by operation of law, contract, license, or otherwise.
 - f. all registrations, initial applications, renewals, extensions, continuations, divisions or reissues hereof now or hereafter in force; and
 - g. all rights and causes of action for infringement or misappropriation of any of the foregoing.
14. Internet means the world-wide connection of computer networks providing for the transmission of electronic mail, on-line information, information retrieval and file transfer protocol.
15. Maintenance Services means the supply to the Licensee of Updates and Upgrades.
16. Off-peak Times means any time between 5:00pm and 11:59pm or 12:00am and 8:30am Australia time or at any time on a Saturday or Sunday.
17. Personal Information means personal information as defined under the *Privacy Act 1988* (Cth).
18. Privacy Laws means all applicable laws and regulations relating to privacy and the protection of Personal Information, including the *Privacy Act 1988* (Cth), the Health Records (Privacy and Access) Act 1997 (ACT), the *Health Records Act 2001* (Vic), the *Health Records and Information Privacy Act 2002* (NSW), the *Spam Act 2003* (Cth), and any other requirement under law or industry code relating to the handling of Personal Information.
19. Product means the PowerHouse Workforce Platform (which includes the following Products: Talent Network; Select; Onboard; Upskill; and Mobility).
20. Release means, in respect of an Update or Upgrade, the release of that Update or Upgrade (as the case may be) to the customers of the Licensor generally] (and "Released" shall be construed accordingly).
21. Sensitive Personal Data means sensitive information as defined in the *Privacy Act 1988* (Cth) and special category data – Article 9 GDPR.
22. Services means services under this contract for the provision of the works or additional services relating to web hosting, the maintenance of the Website and all other services reasonably required to run the website by Mediasphere to the Customer.
23. Server System means the hardware and software system owned or licensed by Customer on which the Website resides and that maintains the Website on the World Wide Web and which may change from time to time.
24. Site means the hardware system for the hosting of the Server Systems.
25. Software means Mediasphere Tools and Templates and any other computer program or programs consisting of a set of instructions or statements in machine readable form, and each and every component thereof to the extent that they are used in relation to the Website or produced under additional services requested by this Agreement.
26. Software License means the permission to use the Products on a non-exclusive basis and subject to the terms and conditions in this agreement. Access to the License is granted on the payment, in advance, of the annual recurring (or monthly) license fee.
27. Specifications means the requirements for the Customer Deliverables.
28. Term means a period of one (1) year which can be renewed on an annual license basis if granted by Mediasphere.

29. Third Party Materials means any software or other material owned by a company or individual other than Mediasphere or Customer which is employed on the Website and is supplied by Mediasphere.
30. Update means a hotfix, patch or minor version update to the Software.
31. Upgrade means a major version upgrade of the Software.
32. User means one of the following:
 - a) Active User – a user that can login and access the Products. A User can be reported on and their data is stored and backed-up. The user counts towards the commercial license counter and forms part of the Annual License Fee; or
 - b) Disabled User – a user that cannot login, however their data is still stored, backed-up and can be reported on. This user counts towards the commercial license counter; or
 - c) Deleted User – a user that has been removed from the Products by the Customer. No data is stored, no reporting can be done. This user does not count towards the commercial license counter.
33. User Account means an access credit that is used by the Customer to allow their users to access the Products. A User Account is activated by the Customer using a single credit to create a new user on the platform. The User Accounts are valid for 12 months and cannot be reissued to another user once activated.
34. User Account (eCommerce) means an access account that is added to the Products via an eCommerce transaction to provide the user with access to a course (content), event or webinar through the Products. The User Account (eCommerce) does not use an access credit, but it added automatically based on an agreed revenue share model. Mediasphere provides the Customer with eCommerce marketing portals, shopping cart, secure access to agreed third party eCommerce providers to manage the transactions, creation and delivery of payment invoices to the Customer and the creation of a user account with access to the purchased content or activity.
35. Website means the Products which are accessible on the Internet through the World Wide Web supplied by Mediasphere pursuant to the terms and conditions of this Agreement.
36. Website Graphics means the custom graphics and user interfaces developed for the Website by Mediasphere and included in the Customer Deliverables.
37. Works Agreement means the agreement for the deployment of Products and provision of integration and set-up services and the listed fees.
38. World Wide Web means a method of representing and obtaining graphical data and linking data items used by Internet users.

Interpretation Reference to:

- a. one gender includes the others.
- b. the singular includes the plural, and the plural includes the singular.
- c. a person includes a body corporate.
- d. a party includes the party's executors, administrators, successors and permitted assigns.
- e. a statute, regulation or provision of a statute or regulation (Statutory Provision) includes:
 - a. that Statutory Provision as amended or re-enacted from time to time; and
 - b. a statute, regulation or provision enacted in replacement of that Statutory Provision; and
- f. Money is the Australian dollar (\$), unless otherwise stated.
- g. "Including" and similar expressions are not words of limitation.
- h. Where a word or expression is given a particular meaning, other parts of speech and grammatical forms of that word or expression have a corresponding meaning.
- i. Headings are for convenience only and do not form part of this Agreement or affect its interpretation.
- j. A provision of this Agreement must not be construed to the disadvantage of a party merely because that party was responsible for the preparation of this Agreement or the inclusion of the provision in this Agreement.
- k. If an act must be done on a specified day which is not a Business Day, it must be done on the next Business Day.

1. Term

- i. This Agreement commences and is deemed to have effect on the date that the Works Agreement is executed by the Customer and continues for the Term unless terminated in accordance with the Termination clauses. Unless stated otherwise, the term of the license is 12 months with the option to renew for an additional subsequent 12-month term based on the payment of the annual license fee or the recurring monthly fee.

2. Supply and Installation of the Website

- i. Mediasphere must deploy the Products and provide the Services upon the terms of this Agreement.
- ii. Mediasphere agrees to provide the Products and the Services in accordance with the Works Agreement.
- iii. Mediasphere must deploy the Products in a competent, proper, efficient and timely manner in accordance with the Works agreement.
- iv. Mediasphere must deploy and provide access to the Products in accordance with the Works agreement and any agreed implementation plan and must do so in such a way as to avoid any reduction of or adverse effect on the then current business of the Customer.

3. Works Agreement and Payment Terms

- i. Works Agreement
 - o Mediasphere will work in good faith with the Customer to implement a Works Agreement.
 - o The Works Agreement will include all project deliverables and document all fees associated with the project.
 - o The Customer signs the Works Agreement to commence the project and accept the project fees. The Customer signs the Works Agreement to agree with the terms and conditions in this Terms of this license agreement.
 - o The Customer agrees to pay Mediasphere on or before the payment date in the Works Agreement and Customer invoice. In the event of a non-payment or overdue payment, 30 days after the payment date, Mediasphere may deactivate your site. A site-reinstatement fee may apply. A service fee may be charged to all overdue accounts.
- ii. GST
 - o Terms used in this clause which are defined in the GST Law have the meanings given in that law.
 - o Amounts payable under this Agreement do not include GST unless otherwise stated.
 - o If any payment made or other consideration given by a party (Payer) in connection with this Agreement does not include GST and is the consideration for a taxable supply for which the party who makes the supply (Supplier) is liable for GST, the Payer must, at the same time as the consideration is given, pay to the Supplier an additional amount equal to the amount of the consideration multiplied by the rate of GST under the GST Law.
 - o Any reference in this Agreement to a cost or expense to be reimbursed by one party to another (Payee) includes any GST payable in connection with a taxable supply to which that cost, or expense relates, less the amount of any input tax credit that the Payee or, if the Payee is a member of a GST group, the representative member of the GST group, is entitled to claim.

4. Assignment, licensing and allocation of rights on Products

- i. Mediasphere and Customer agree that the licensing will consist of:
 - a. Customer Deliverables.
 - b. Developer Tools and Templates; and
 - c. The Terms and Conditions.

5. Ownership of Developer Tools and Templates

- i. Mediasphere and Customer confirm that Mediasphere retains ownership of all rights, title and interest in and to Mediasphere Tools and Templates, including, without limitation, all applicable Intellectual Property Rights to Mediasphere Tools and Templates. Mediasphere retains all right, title and interest in and to all tools and other information and materials used in the creation or development of Mediasphere's Tools and Templates.

6. Developer Tools and Templates License

- i. Mediasphere grants to the Customer (and its Related Bodies Corporate) a fully paid, non-exclusive licence for the Term, to use, publicly perform, publicly display and digitally perform Mediasphere Tools and Templates solely for the purpose and to the extent necessary to operate the Products.
- ii. The licence granted in this agreement is revocable and is only for the term of this agreement.
- iii. Mediasphere retains the right not to renew the license for an additional Term after the expiry of the original Term if Mediasphere intends to enact its rights under this clause 6 (iii) then Mediasphere shall provide not less than 90 days' notice to the Customer.
- iv. Mediasphere may also terminate the licence granted with 180 days written notice prior to the expiry of the Term where there are reasonable grounds for alleging the Customer is in breach of a provision of this Agreement when the breach relates solely to:
 - a. the failure of the Customer to make a payment under this Agreement; or
 - b. A material breach of Mediasphere's Intellectual Property Rights in Mediasphere Tools and Templates by the Customer or its employees.

7. Customer Content and Customer Deliverables license

- i. The Customer confirms its grant to Mediasphere of a non-exclusive, royalty-free licence for the Term to deploy, distribute and digitally perform any Customer Content or Customer Deliverables only on or in conjunction with the Products, solely for the purpose and to the extent necessary to perform Mediasphere's obligations under this Agreement.

8. Ownership of Customer Content

- i. As between Mediasphere and Customer, any Customer Content stored or delivered on the Products under this Agreement or otherwise, and all Intellectual Property Rights therein, at all times remains the property of the Customer or its licensor or Website subscribers. Mediasphere has no rights to such Customer Content, other than the limited right to use such content for the purpose expressly set out in this Agreement.

9. Access to Server Systems

- i. The Customer agrees to provide Mediasphere with reasonable information and access to its relevant Server Systems (including without limitation, read, write and execute privileges where such privileges relate to the Products) to the extent necessary for Mediasphere to perform its obligations under this Agreement.
- ii. When accessing the Server Systems, Mediasphere must comply with any reasonable policies or directions given by the Customer.

10. Hosting of Customer Content

- i. Mediasphere will store all Customer Content on servers located on Amazon Web Services (AWS) servers in London for the United Kingdom and northern hemisphere clients and AWS servers in Sydney for Australian and southern hemisphere clients, unless otherwise specified.

- ii. Mediasphere will comply with all relevant data protection legislation.
- iii. Mediasphere will comply with all relevant privacy and data protection legislation.
- iv. Mediasphere will not store, disclose or otherwise permit access to Customer Content to anyone located outside of the countries of operation.

11. Developer's warranties

- i. Mediasphere warrants that all Software, supplied under this agreement, will upon installation conform in all material respect to the Product specifications and representations for the period of this agreement.
- ii. Mediasphere will take all the reasonable steps to ensure that the software operates in accordance with the Works agreement.

12. Warranties and covenants

- i. Mediasphere warrants as at the Commencement Date that:
 - a. The Customer Deliverables and Developer's Tools and Templates used in relation to the Website do not infringe the Intellectual Property Rights of any third party.
 - b. No proceedings have been instituted by any third party against Mediasphere for the infringement of that party's Intellectual Property Rights by Mediasphere's Intellectual Property.
 - c. No proceedings have been instituted by any third party against Mediasphere seeking to challenge the validity of Mediasphere's Intellectual Property Rights in the Development Tools and Templates.
 - d. The Deliverables will be provided in accordance with this Agreement, including the Works Agreement.
 - e. Any documentation provided as a part of the Deliverables will be adequate to enable a reasonably competent person to operate the Products; and
 - f. Mediasphere will only access the Customer Website, or Customer Content, in accordance with this Agreement, support issues, core pushes, security patches and or if required to provide Upgrades.

13. Services

- i. From the Commencement Date, Mediasphere agrees to perform the Services for the customer in return for the License Fee and any agreed additional fees as set out in the Works Agreement.
- ii. After the project commences, the Customer has the right to request project variations to cover out-of-project-scope changes to the project. Project variations requested by the Customer and not described in the Works Agreement will be managed with a written scope of work, delivery dates and aligned fees that the client can approve or reject. Mediasphere has the right to accept or reject project variations.
- iii. On and from the Commencement Date and until terminated in accordance with its terms, Mediasphere warrants that:
 - a. it will perform all Services in a professional manner, using appropriately qualified and trained personnel and in accordance with prevailing industry standards.
 - b. Performance of the Services by Mediasphere does not violate the terms of any other agreement between Mediasphere and a third party.

14. Upgrades

- i. Mediasphere shall keep the Customer reasonably informed during the Term of its plans for the release of Upgrades; however, except to the extent that the parties agree otherwise in writing, the Licensor shall have no obligation to release Upgrades with features requested by the Customer or to take into account the opinions of the Customer in relation to plans for the release of Upgrades.

- ii. Mediasphere may produce Upgrades during the Term and shall make such Upgrades available to the Customer.
- iii. Mediasphere shall give to the Customer at least 30 Business Days' prior written notice of [the Release of an Upgrade.
- iv. Mediasphere may apply each Upgrade to the Software within the period of 90 Business Days following Release.
- v. Upgrade fees do not apply to Products that have been deployed as a Version 7 core (out-of-the-box) platform as updates are seamlessly pushed to the core and updated to all deployments. Upgrade fees will apply if a Customer has requested and added custom programming to the core platform. The fees will include the integration of the programming overrides to a new version. Mediasphere will provide the Customer with the scheduled Upgrade fee in writing at least 30 Business Days before the Upgrade.
- vi. Mediasphere reserves to right to charge a cost recovery fee for the migration of the Customer's content and database to the updated version of the Product. Mediasphere will provide the Customer with the scheduled Upgrade fee in writing at least 30 Business Days before the Upgrade.

15. Customer warranties

Customer warrants that:

- i. It has full power, right and authority to enter into this Agreement and the Customer is not subject to any obligations that would prevent or otherwise restrict the Customer from performing its obligations under this Agreement.
- ii. The Customer Content does not infringe the Intellectual Property Rights of any person.
- iii. The Customer Content is not obscene, offensive, upsetting, or defamatory; and
- iv. The use of the Customer Content by Mediasphere in connection the performance of its obligations under this Agreement is not illegal, fraudulent or of a defamatory nature.

16. Indemnities

- i. Each party fully indemnifies the other against any loss, costs, expenses, demands or liability, in respect of third-party claims arising out of a breach of any warranty expressly given under this Agreement.
- ii. Mediasphere agrees to indemnify and keep indemnified the Customer to the extent required by relevant legislation against and in respect of all actions, proceedings, claims, demands and liabilities arising in any way that may be brought or incurred or suffered by the Customer as a result of:
 - a. a breach of this Agreement by Mediasphere; or
 - b. a breach of intellectual property rights, privacy, confidentiality or data breach obligations by Mediasphere.
- iii. Without limiting the obligations of Mediasphere under this clause, if a determination is made by any independent tribunal of fact or law or if it is agreed between the parties to the dispute that an infringement of Intellectual Property Rights has occurred, Mediasphere shall in a timely manner:
 - a. replace or modify the infringing product ensuring that the quality, performance or usefulness of the Website is not degraded and so that the infringement ceases; or
 - b. apply its best endeavours to procure for the Customer the right to possess and continue to use the whole or the relevant part of the Website or what was required under the Works Agreement.
- iv. The indemnities contained in this Agreement continue throughout the term of this Agreement.

17. Privacy

a. Privacy obligations

Mediasphere must:

- i. comply with the Privacy Laws in respect of any Personal Information;
- ii. only use Personal Information:
 1. where it is necessary for providing or receiving the Services or providing the Products; and
 2. for the purpose of providing or receiving the Services and providing the Products;
- iii. take all necessary technical and organisational measures to prevent:
 1. unauthorised or unlawful use or disclosure of; and
 2. accidental loss or destruction of, or damage to,
the Personal Information;
- iv. subject to the Privacy Laws and consents obtained from the relevant individuals:
 1. treat the Personal Information as Confidential Information; and
 2. destroy or permanently de-identify the Personal Information if that information is no longer needed to perform the obligations under this Agreement.
- v. take reasonable steps, when requested by another party from time to time, to assist that party to comply with its obligations under the Privacy Laws and any privacy statements or policies issued by it; and
- vi. notify the other party immediately if it becomes aware of a breach, or a suspected or possible breach, by the party of any of its obligations under this clause **Error!**
Reference source not found..

18. Independent Contractors

- i. Mediasphere and Customer are each independent contractors, and no agency, partnership, joint venture or employee-employer relationship is intended or created by this Agreement. Neither party has the power to obligate or bind the other party. Personnel supplied by Mediasphere must work exclusively for Mediasphere and must not, for any purpose, be considered employees or agents of the Customer and vice versa.

19. Confidentiality

- i. A party must not, without the prior written approval of the other party, disclose the other party's Confidential Information.
- ii. A party is not in breach of this clause in circumstances where:
 - a. it is legally compelled to disclose the other party's Confidential Information.
 - b. the information disclosed is generally available to the public (other than as a result of the wrongful disclosure by such party).
 - c. such party obtained the Confidential Information from a third party without breach by that third party of any obligation of confidence concerning the Confidential Information; or
 - d. The Confidential Information was already in such party's possession (as evidenced by written records) when provided by or on behalf of the other party.
- iii. Each party must take all reasonable steps to ensure that its employees and agents, and any sub-contractors engaged for the purposes of this Agreement, do not make public or disclose the other party's Confidential Information.
- iv. The Customer may at any time require Mediasphere to arrange for its employees, agents or sub-contractors engaged in the performance of this Agreement to execute a suitable confidentiality

deed and if requested Mediasphere must arrange for the deed to be executed within the time frame reasonably required by the Customer.

- v. Each party must on demand or on the expiration or termination of this Agreement, destroy or return to the other party (as directed by that party) any documents supplied to that party in connection with this Agreement.
- vi. Despite any other provision of this clause, each party may disclose the terms of this Agreement (other than Confidential Information of a technical nature) to its related companies, solicitors, auditors, insurers or accountants, but must ensure that every person to whom that disclosure is made uses that information solely for the purposes of advising or reporting to that party.

20. Termination

- i. Without prejudice to any other rights either party may have under this Agreement or at law or in equity, either party may terminate this Agreement with immediate effect, in whole or in part, upon:
 - a. the other party becoming subject to any form of insolvency administration (whether voluntary or otherwise).
 - b. the other party being in breach, including multiple small breaches, of any clause of this Agreement and such breach not being remedied with 30 days of written notice by the party of that breach: or
 - c. a party purporting to or proposing to assign this Agreement or its rights or interests in any relevant Intellectual Property, without the other party's prior written consent.
- ii. Either party may terminate this Agreement for convenience with 180 days of written notice to the other party at any time.
- iii. Mediasphere reserves the right to discontinue a Product or version of a Product at any time. In this event, Mediasphere will announce an End-of-Life date on the Product website and provide email communication to the Customer. The End-of-Life date will apply 12 months after the announcement date. The Customer will provide bug fixes, maintenance releases, work arounds, or patches for critical bugs during the 12-month period. At the end of the period End-of-Support will apply and Customers will be required to upgrade to the supported version of the software or terminate the agreement. When the End-of-Life applies to a critical security issue, upgrades dates may be reduced to protect Customer data.
- iv. Upon termination of this Agreement:
 - a. the Customer agrees to use all reasonable endeavours to assist the transfer of Mediasphere Tools and Templates to Mediasphere.
 - b. Any transfer or migration that occurs under this clause must be carried out at the Customers expense; and
 - c. The Customer agrees to use existing platform functions to extract any data required for their records or auditing purposes i.e., Export user functionality and the Reporting modules. If any custom exports are required these will incur a fee for service determined by Mediasphere.

21. Further assurance

- i. Each party must promptly at its own cost do all things (including executing all documents) necessary or desirable to give full effect to this Agreement.

22. Severability

- i. If anything in this Agreement is unenforceable, illegal or void then it is severed, and the rest of this Agreement remains in force.

23. Variation

- i. An amendment or variation to this Agreement is not effective unless it is in writing and signed by the parties.

24. Assignment

- ii. Mediasphere may not assign or novate its rights and obligations under this Agreement without the prior written consent of the Customer.
- iii. The Customer may assign or novate its rights and obligations under this Agreement without Mediasphere's consent.

25. Waiver

- i. A party's failure or delay to exercise a power or right does not operate as a waiver of that power or right.
- ii. The exercise of a power or right does not preclude either its exercise in the future or the exercise of any other power or right.
- iii. A waiver is not effective unless it is in writing.
- iv. Waiver of a power or right is effective only in respect of the specific instance to which it relates and for the specific purpose for which it is given.

26. Costs and disbursements

- i. Each party must pay its own costs and outlays connected with the negotiation, preparation and execution of this Agreement.
- ii. The Customer as the purchaser of goods and services pursuant to this Agreement, must pay all stamp duty and other government imposts payable in connection with this Agreement and all other documents and matters referred to in this Agreement when due or earlier if requested in writing by Mediasphere.

27. Notices

- i. A notice or other communication connected with this Agreement (**Notice**) has no legal effect unless it is in writing.
- ii. In addition to any other method of service provided by law, the Notice may be:
 - a. sent by prepaid post to the address of the addressee set out in this Agreement or subsequently notified.
 - b. sent by email of the addressee sent by electronic mail to the electronic mail address of the addressee; or
 - c. delivered at the address of the addressee set out in this Agreement or subsequently notified.
- iii. A Notice must be treated as given and received:
 - a. if sent by post, on the 2nd Business Day (at the address to which it is posted) after posting.
 - b. if sent by email before 5 p.m. on a Business Day at the place of receipt, on the day it is sent and otherwise on the next Business Day at the place of receipt; or
- iv. If otherwise delivered before 5 p.m. on a Business Day at the place of delivery, upon delivery, and otherwise on the next Business Day at the place of delivery.
- v. An email message is not treated as given or received if the sender's computer reports that the message has not been delivered.
- vi. A Notice sent or delivered must be treated as validly given to and received by the party to which it is addressed even if:
 - a. the addressee has been liquidated or deregistered or is absent from the place at which the Notice is delivered or to which it is sent.
 - b. the Notice is returned unclaimed; or

- c. in the case of a Notice sent by electronic mail, the electronic mail message is not delivered or opened (unless the sender's computer reports that it has not been delivered).
- vii. Any Notice by a party may be given and may be signed by its solicitor.
- viii. A party may change its postal address for service or email address by giving Notice of that change to each other party.

28. General

- i. This Agreement:
 - a. is the entire agreement and understanding between the parties on everything connected with the subject matter of this Agreement; and
 - b. supersedes any prior agreement or understanding on anything connected with that subject matter.
- ii. Each party has entered into this Agreement without relying on any representation by any other party or any person purporting to represent that party.

29. Governing law and jurisdiction

- i. The law of Queensland governs this Agreement.
- ii. The parties submit to the non-exclusive jurisdiction of the courts of Queensland and the Federal Court of Australia.





Schedule 1

Products and Pricing

PowerHouse Workforce Platform

The Future of Talent Sourcing, Upskilling and Mobility



PowerHouse Workforce	Integrated Modules
<p>The PowerHouse Workforce SaaS platform is designed for employers to manage their own pre-screening onboarding, upskilling, talent mobility and succession planning, and includes the following modules.</p>	
 <p>WORKFLOWS</p>	<p>Manages pre-screens, onboards, and appraisal workflows, background, suitability and psychology tests, file uploads with expiry dates, inductions, forms with digital signatures and compliance management.</p>
 <p>UPSKILL</p>	<p>Manages continuous job skilling and compliance monitoring, CPD, online courses, skills evidence and verification, course libraries, webinars and event management.</p>
 <p>MOBILITY</p>	<p>Manages job role frameworks, searchable internal talent pools, compliance/skill verification, gap analysis, blockchain credentialing and succession plans.</p>
 <p>COMMUNITIES</p>	<p>Manages job posts, register for work, ranked candidate pipelines, recruiter insights, job matching scores, CV parsing and work ready shields, private communities with talent pools and access to marketplace.</p>

The PowerHouse Workforce license is based on an annual/monthly SaaS Per-User-Per-Month license fee for the Communities, Workflows, Upskill and Mobility package. The pricing has been included in the Works Agreement.

Schedule 2

PowerHouse Hub Products: Upgrades and End of Life Policy

1. Scope

To ensure delivery of innovative and cost-effective products, PowerHouse Hub may periodically discontinue specific products or versions of products and hosted services. At PowerHouse Hub's sole discretion, such products or services may be discontinued regardless of the delivery method, including on-premises Software and Cloud Services.

This policy describes the intended communication and transition plans for discontinued products and versions and provides information required to plan for migration to replacement technologies. Any questions arising in the interpretation of this policy or the application of this policy shall be as determined by PowerHouse Hub in its sole discretion. Any conflict between this policy and the terms of support shall be controlled by the provisions of this policy. This policy is effective from the effective date set forth above.

2. Software

Releases

- **Major (Upgrade - Major) Release:** Major releases encompass new products, major architecture changes, major user interface (UI) changes, significant new features or capabilities/functionality additions, new solutions, and substantial innovation.
- **Minor Release:** Minor releases include updates or enhancements/features to existing products, moderate administration or UI changes, and major bug fixes.
- **Update (Patch) Release:** Update releases incorporate minor bug fixes, security fixes, and service packs and Update releases should be incorporated into the next Minor Software release.
- The Software product version numbering scheme is defined as follows:

(Major). (Minor). (Update). Example: 7.03.02 Where Major release is 7, Minor release is 3, Update release is 2.

- PowerHouse Hub will make commercially reasonable efforts to adhere to the following guidelines:
 1. The End-of-Life Period for a Major or Minor Software release, "N," starts when the N+2 release becomes Generally Available.
 2. The maximum total support life of a Software release is the lesser of: (a) three (3) years from the date it first became Generally Available or (b) one (1) year after the N+2 version becomes Generally Available.

3. Products

- PowerHouse Hub will make commercially reasonable efforts to provide six (6) months' notice of an affected product's End of Sale Date and, after the effective End of Sale Date, provide Full-Service Software Support for a maximum of 1 year.
- PowerHouse Hub will not provide Full-Service Software Support past the specified End of Life date.

4. Cloud Services

- PowerHouse Hub will support only the current release of Cloud Services.

5. Extension of Support Terms - Custom Software Support

In rare instances, and at our sole discretion, PowerHouse Hub may offer extended support, beyond the standard support lifecycle. Custom Software Support may be available at an additional cost to the customer based on a current support subscription that is not impacted by an End-of-Life Date.

Custom Software Support will provide commercially reasonable workaround solutions under the following conditions:

- The technology remains supportable per PowerHouse Hub, including being free from unsupported dependencies on components provided by independent Software vendors (ISVs) that are outside PowerHouse Hub's control; and
- The platform it operates on is supported by our original equipment manufacturer (OEM) technology partner (where applicable); and
- Technical support for issue resolution will be provided on a commercially reasonable basis; and

Custom Software Support does not include:

- Product Enhancement Requests (PER)
- Hotfixes or Engineering-related support
- New Operating System support
- SLA commitments related to defects in the supported product.

6. Definitions

Cloud Services - means Software or platform services offered on servers that are owned or managed by PowerHouse Hub and provided to customer as specified in one or more grant letters, or as further defined by the relevant customer agreement. Access to the Cloud Services 4 Corporate Products End of Life Policy requires either an active support agreement or an active subscription, as required by the specific offering.

Custom Software Support - Is an individually negotiated Software support contract requiring a PowerHouse Hub-approved quote for product where the customer requests Support beyond the published End of Life Date.

Defect Severity – References to bug or defect severity reflect a qualitative appraisal of the problem's extent.

End of Life (EOL) Period - Refers to the timeframe beginning with the day PowerHouse Hub announces a product is no longer available for purchase from current PowerHouse Hub price books until the last date the product is formally supported by PowerHouse Hub. If Software version only, EOL Period refers to the timeframe beginning with the day PowerHouse Hub announces a Software version will no longer be available until it is no longer supported.

End of Sale Date – The date a product is no longer Generally Available for purchase.

End of Life Date – The last day that the product and/or Software version is supported per the terms of the standard Software and Hardware support offerings.

Full-Service Software Support - Means the same maintenance and technical support as you receive under your current support contract for products that are Generally Available. Security updates and maintenance will continue until the end of the Full-Service Software Support period. Full-Service Hardware Support - Full-Service Hardware Support includes hardware warranty, new Software/firmware versions, escalations, update releases, product updates, content updates, and available maintenance and technical support.

Generally Available – Product is generally available for Sale and Support on current PowerHouse Hub price books.

Software - means each PowerHouse Hub Software program in object-code format that is (a) licensed from PowerHouse Hub or its authorized partners, or (b) embedded in or pre-loaded on Hardware provided by PowerHouse Hub's hosting partners, in each case including updates and upgrades that customer installs during any applicable support period.

Schedule 3

The PowerHouse Hub Service Level Agreement (SLA)

1. SUPPORT

- i. **Application:** The service levels are provided in respect of the server used in the provision of the Services.
- ii. **Email Support:** Support consists of responding to queries logged by the Customer's administration users via the portal or via email submission.
- iii. **Extended Support:** The Customer may wish to license an extended support contract which provides access to phone support. This extended support will be included on the Works Agreement.
- iv. **Contact Details:** Email: support@powerhousehub.com
- v. **Telephone Queries and Support Requests:** The Customer may contact Mediasphere on a range of issues including:
 - a. Accounts and Invoicing.
 - b. Database backup, management and restoration.
 - c. Urgent platform related issues affecting all users.
 - d. General enquiries.
- vi. **Logging Support Tickets:** The customer will log all support issues via email to: support@powerhousehub.com. After logging a support issue, the Customer will receive a support ticket number that will be used as a reference for the job.
- vii. **Uptime SLA.** Mediasphere shall use all reasonable commercial efforts, being no less than accepted industrial standards in this regard, to ensure that the PowerHouse Portal Service is available to you 99.9% of the time in any calendar month. If it is not, you may be eligible to receive the Service Credits described below:
 - a. **"Service Credit"** may be provided according to the following schedule:
 - i. **One-week Credit:** Includes **Seven (7)** days of Services added to the end of your billing cycle, at no charge to you, if the Monthly Uptime Percentage for any calendar month is between 99.9% and 97.0%.
 - ii. **Two-week Credit:** Includes **Fourteen (14)** days of Services added to the end of your billing cycle, at no charge to you, if the Monthly Uptime Percentage for any calendar month is between 97.0% and 95.0%.
 - iii. **One-month Credit:** Includes **Thirty (30)** days of Services added to the end of your billing cycle, at no charge to you, if the Monthly Uptime Percentage for any calendar month is less than 95.0%.

Right to terminate: In the event the Monthly Uptime Percentage for any calendar month is less than 90.0%, you will have a right to terminate the PowerHouse Hub agreement with seven (7) days written notice to Mediasphere, or alternatively you can opt to procure the One-month Credit outlined above.
- viii. Scheduled or Planned server upgrades or server maintenance does not include:
 - i. Downtime caused by natural disasters – flood, hurricane, earthquake and so on.
 - ii. Downtime caused by third-party digital software attacks on server.
 - iii. Downtime caused by physical attacks a server or data centres.
 - iv. Direct denial of service (DDoS) attacks or hacking attempts.
 - v. Downtime caused during user's DNS and/or IP address changes.
 - vi. Downtime during technical support upgrades.

- ix. **Mediasphere's Indicative Response and Resolution Times for Internet Support**
- x. Depending on the nature and severity of the error, the majority of response and resolution times for priority 1 issues are typically responded within 2 hours and resolved within 8 hours (if the error occurs during Business Hours). In some cases, however, the response time may reflect the times shown below and in extreme situations exceed these times. Events beyond Mediasphere's control or impact such as Acts of God, data centre disasters (fire, flood), power supply issues, replacement hardware etc. may result in protracted response and resolution times. Mediasphere will keep all relevant stakeholders informed of the status and expected time for resolution. If any such delay continues for a period of more than 30 Business Days, and the issue has been caused by Mediasphere's software, the Customer may terminate the Agreement effective immediately.
- xi. Response times relate directly to the urgency and impact of the issue. Urgency and impact factors will be used to calculate a priority level for all incidents.
- xii. The priority level will be determined by Powerhouse Hub upon reviewing the support ticket and referencing the description below.
- xiii. Resolution times outlined in the below table does not include client review time.
- xiv. If further changes are required relating to the original issue the below resolution times will commence again from the requested date.

Priority Level	Description
1	Affects all platform users
2	Affects large number but not all users
3	Affects several users
4	Affects low number or single user

Nature of Defect/Fault	First Reply in Business Hours	Resolution / Mitigation ETA in Business Hours
Priority 1	2 hours	8 hours or as soon as feasible or practical
Priority 2	4 hours	24 hours or as soon as feasible or practical
Priority 3	8 hours	48 hours or as soon as feasible or practical
Priority 4	10 hours	To be negotiated with the customer depending on the fault.

- xv. Hardware and network errors include monitoring, response and resolution 7 days per week, 24 hours per day by the server service provider. Software errors include monitoring, response and resolution. Cloud infrastructure issues are the responsibility of the Service Provider. (Cloud infrastructure can be categorised as hardware, network and software that are in the Cloud Layer. Cloud infrastructure is covered by the Cloud Provider service level agreements (SLA). AWS SLA: <https://aws.amazon.com/legal/service-level-agreements/> The layer above the Cloud Layer which consists of server instances, Firewalls, IP Addresses, and server software, application software is the responsibility of Powerhouse Hub) and covered by this service level agreement.
- xvi. **Server Back-Up:** A server backup means a complete copy of the website files, content and database. The backup data is only to be used as a non-functional copy of the original website in case the original website becomes corrupt or inaccessible.

- xvii. The Database Back-Up Schedule includes the following:
 - Day 1 to Day 7: Full back-ups are generated daily and stored on-network.
 - Day 8 to Day 30: From the daily backups, the System Administrator generates a weekly back-up each Sunday.
 - Day 31 to Day 365: At the start of the month a full back-up is generated. The System Administrator stores a full year of your back-ups. These back-ups are stored off-network.
- xviii. The User File Back-Up processing is every 24 hours. This is a dynamic update and will be backed up reflecting the platform at that time. User file back-ups does not backup files that have been removed by the administrator i.e. if a file is deleted by the customer administrator it will be removed from the back-ups accordingly. Pop-up messages have been implemented prompting confirmation from the administrator that the file will be permanently deleted.
- xix. In the event of data corruption or server fault, the backup will be restored to a functional server which in effect will reinstate the website back to its previous state before the error occurred, minimizing data loss and downtime. The System Administrator may issue a service fee for the data recovery operation if not the fault of Powerhouse Hub.
- xx. **Scheduled Maintenance:** The System Administrator will provide accurate and timely information in order to notify the Customer of all Scheduled Maintenance. Mediasphere will work with any third parties to ensure that Scheduled Maintenance is only to occur during Off-peak Times.

2. PENETRATION TESTING POLICY

- i. Before conducting an external Penetration Test (also known as "pen testing"), at your own cost, you must seek written permission from Mediasphere before proceeding. As many of the tests may use scripts and automated systems which use brute force or multiple attacks to test, these appear as malicious attacks and are prohibited without permission.
- ii. To request permission, please send an email to support@powerhousehub.com with the following information.
 - Site or server being tested.
 - Date and time of the testing.
 - A copy of the test plan, including the range of tests being conducted.
 - Contact information (including direct email address and phone number) of the person conducting the test.
 - IP addresses or IP ranges from where the testing is originating.
- iii. Mediasphere reserves the right to cancel any testing, without notice if the testing is having any adverse impact on any system or service. Mediasphere also runs dedicated firewall systems, which include an Intrusion Prevention System (IPS) and this cannot be disabled for testing.
- iv. We do not permit and DoS, DDoS or black-hat testing to occur, nor any testing against upstream infrastructure.
- v. If you or your testing company have any questions, please don't hesitate to contact our support team. We request that you share the Penetration Testing Report to allow our team to address any vulnerabilities or issues discovered during the test. A re-test can be completed by your testing provider after Mediasphere provide advice that issues discovered in the Penetration Test have been resolved or clarified.

Schedule 4

Data Management and GDPR.

Written Arrangements

1. Context: with regard to common processing operations for purposes as set out in a direct contract between controllers, or indirectly through them with other controllers that provide services, including a memorandum of understanding or similar agreement, the parties in their legitimate interests acknowledge the joint processing of personal data, including determining the purpose and means of processing. In order to preserve the integrity of the personal data and manner processed, each controller (“parties” or “party”) acknowledges their part in ensuring the system, processes and organisational set-up are fit-for-purpose, and accepts their respective roles and responsibilities, as laid out here, to minimise the likelihood of any unauthorised or unlawful processing of the personal data,
2. These written arrangements are referred to in information sharing agreements between joint controllers and reflect the duties and tasks of parties involved. They are a technical and organisational measure to address the varying likelihood and severity of risks to the rights, freedoms, and interests of affected individuals with respect to the joint processing of their personal data for the stated purposes. They cover obligations to address data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, international transfers of personal data, and contacts for individuals and the regulator. The roles and responsibilities of the involved parties are the service and system management, support, and provision of collecting, processing, sharing, storing, and deleting personal data.

GENERAL

3. Each party shall be accountable for their respective data protection obligations.
4. Each party shall define their respective data protection obligations precisely.
5. At the time of the determination of the means and at the time of the joint processing itself, each party shall be responsible for demonstrating compliance with data protection by design by implementing appropriate technical and organisational measures designed to support the data protection principles effectively and maintain an appropriate level of security proportionate to the risks presented by the processing.
6. The pre- and post-processing shall be separate from the joint processing and subject to other arrangements and legal bases where applicable.

CONTACT AND COMMUNICATIONS BETWEEN PARTIES

7. Each party shall notify other parties of their designated contact, who shall through agreed channels manage any communications relating to data protection matters, such as rights requests by individuals, personal data breaches or other incidents, and enquiries from supervisory or competent authorities.
8. Where individuals bypass their designated contact, and contact another party, they shall be referred back to the designated contact without undue delay, and in any case within 24 hours.

GENERAL PRINCIPLES OF DATA PROTECTION

9. In relation to the joint processing and for the state purposes, each party shall observe the general principles of data protection.
10. Regarding the principle of lawfulness, fairness and transparency, each party shall:

- a. have in place adequate policies and training outlining the principles to be followed by its employees and workers to ensure personal data is processed fairly, lawfully, transparently and in a manner consistent with its legitimate business interests.
 - b. provide in its privacy notice the essence of these arrangements including at least that:
 - i. personal data is jointly processed with other parties in our legitimate interests for the stated purposes including profiling;
 - ii. individuals may exercise their right to request further details at any time; and
 - iii. contact details to correspond with regarding data protection matters.
11. Regarding the principle of purpose limitation, each party shall:
- a. process personal data for the stated purposes, including profiling;
 - b. respect the limitations of processing such personal data for further processing activities and purpose(s) after the joint processing, including conducting a compatibility test for any new purpose(s) and
 - i. where not compatible with current purposes, undertake not to process personal data for that new purpose without authority to do so;
 - ii. where compatible, further consider additional technical and organisational measures as required, and inform the other parties of the intention to do so.
 - c. respect the limitations of any prior purpose(s) and associated processing before the joint processing.
12. Regarding the principle of data minimisation, each party shall only process personal data that is adequate, relevant and limited to what is necessary for the stated purposes or as obligated to do so by law.
13. Regarding the principle of accuracy, each party shall:
- a. ensure that processing remains accurate, and, where necessary, kept up to date; and
 - b. take every reasonable step to ensure that any inaccurate personal data, having regard to the stated purposes, are erased or rectified without delay.
14. Regarding the principle of storage limitation, each party shall:
- a. keep such personal data in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed.
 - b. specify in its policy documentation procedures for the tracking and deletion of personal data according to their retention schedules.
 - c. retain personal data for the duration of the business relationship between the parties or until instructed to delete personal data under the terms of a contract, except where lawfully required to retain the personal data for longer.
15. Regarding the principle of integrity and confidentiality, each party shall:
- a. process in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
 - b. have in place adequate documentation including policies and employee or worker contracts, clearly designating any personal data as confidential to allow its legitimate, authorised processing of personal data.
 - c. in relation to introducing new parties to the common processing activities, a party wishing to introduce a new party to the processing in any capacity shall do so based on the appropriate authority.

- d. in relation to transferring personal data to third countries or international organisations, any transfer shall be subject to a transfer test and where applicable appropriate technical, contractual and organisation measures shall be applied, such as encryption, at least to meet to the four 'essential guarantees'.
16. Regarding the principle of accountability, each party shall:
- a. manage risk adequately including necessity, proportionality and legitimacy tests, data protection impact assessments, legitimate interest assessments, and transfers tests, as required.
 - b. make any risk assessment available to the other parties upon reasonable request.
 - c. maintain a record of processing activities including in particular a list of recipients of the personal data, which must be provided to the other parties upon reasonable request as required without undue delay.
 - d. log all individuals rights request as per data protection obligations.

LEGAL BASIS OF PROCESSING

17. Each party acknowledge that personal data is shared and processed in relation to the stated purposes including profiling based on:
- a. legitimate interests for general processing, whilst
 - b. for special categories of personal data, the processing is necessary for
 - i. the purposes of carrying out the obligations and exercising specific rights of the party or of the individual in the field of employment and social security and social protection law, or
 - ii. if applicable, reasons of substantial public interest as laid down by legislation.
18. Each party shall state the legal bases it relies upon for any additional specified, explicit and legitimate purposes that it processes personal data for, which shall be proportionate to the legitimate aim pursued, and, in particular, refer to:
- a. the types of data which are subject to the processing;
 - b. the individuals concerned;
 - c. the entities to, and the purposes for which, the personal data may be disclosed;
 - d. purpose limitation;
 - e. storage periods; and
 - f. processing activities and processing procedures, including measures to ensure lawful and fair processing.
19. Each party shall be responsible for undertaking its own necessity, proportionality and legitimacy tests to justify further processing, taking utmost account that such purposes are not incompatible with the stated purposes by undertaking a compatibility test taking into account, inter alia:
- a. any link between the stated purpose and the intended further purposes;
 - b. the context in which the personal data have been collected, in particular regarding the relationship between individuals and the respective party as well as other parties that may be involved with the processing activities;
 - c. the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed;
 - d. the possible consequences of the intended further processing for individuals;
 - e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

20. The legal basis for all processing, including general processing as well as processing of special categories of personal data, shall be documented appropriately and made available upon reasonable request to other parties involved with the joint processing.

DATA PROTECTION IMPACT ASSESSMENTS

21. Each party shall undertake its own data protection impact assessment (“DPIA”) with regards to the joint processing to set out which party is responsible for the various measures designed to manage or mitigate any identified risks and to protect the rights, freedoms, and interests of individuals, in particular regarding automated decision-making, special categories of personal data, or where the individual is a child.
22. Each party shall provide practical assistance upon reasonable request to another party undertaking its DPIA.
23. Each party shall consider completing a DPIA for any further planned processing activities that is large scale; involves profiling or monitoring; decides on access to services or opportunities; or involves sensitive data or vulnerable individuals.
24. Unless the party has already conducted a substantially similar DPIA, each party shall undertake DPIAs for any further planned processing activities and associated purpose(s) which in particular are likely to result in a high risk or as identified by the regulator.
25. When undertaking a DPIA, the party shall take utmost account of applicable statutory data protection and other relevant codes including the age-appropriate design code (also known as the Children’s code) or Data Sharing code.
26. When undertaking a DPIA, the party shall take utmost account of risks to the rights and freedoms of individuals caused by the nature, scope, context and intended purpose(s).
27. When undertaking a DPIA, the party shall take utmost account of any:
- a. concerns affected individuals may have.
 - b. impact that stakeholders may have including on other parties involved with the processing activities such as processors, controllers, and joint controllers.
 - c. any concerns the data protection officer may have, if appointed.

SECURITY MEASURES

28. For personal data that is processed for the stated purposes or any further processing activities and associated purpose(s), each party shall have in place appropriate technical and organisational measures so that personal data shall be processed in a manner that ensures a level of security appropriate to the personal data being processed, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
29. Each party shall be able to demonstrate the ability to:
- a. manage their respective security risk
 - i. taking appropriate steps to identify, assess and understand security risks to personal data and the systems that process such data;
 - ii. implement appropriate organisational structures, policies, and processes to systematically manage security risks to personal data;
 - iii. in particular risks relating to processing activities that may arise as a result of engaging other parties such as controllers, joint controllers, and / or processors, including ensuring that they employ appropriate security measures, such as, in the case of processors, requiring sufficient guarantees about their technical and organisational measures.

- b. protect personal data against cyber-attack with proportionate security measures which cover the personal data processed as well as the systems that process such data, these measures to include compliance with any Information Security policies:
 - i. the security of data by implementing technical controls (such as appropriate encryption) to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest or accessing data that might remain in memory when technology is sent for repair or disposal.
 - ii. training staff by giving appropriate support to help them manage personal data securely, including the technology they use;
 - iii. monitoring authorised user access to that data, including anomalous user activity, recording user access to personal data.
 - iv. having processes in place, where unexpected events or indications of a personal data breach are detected, to act upon those events as necessary in an appropriate timeframe.
- c. minimise the impact of a personal data breach, restore systems and services, including the availability and access to personal data in a timely manner in the event of a physical or technical incident, manage incidents appropriately, and learn lessons for the future, by:
 - i. effective response and recovery planning;
 - ii. taking steps, when a personal data breach occurs, to understand the root cause, take appropriate action, including, documenting lessons learned, and, where required, reporting the breach to the ICO, the National Cyber Security Centre, other relevant bodies, and affected individuals.

PERSONAL DATA BREACH NOTIFICATIONS

- 30. For personal data that is processed for the stated purposes or any further processing activities and associated purpose(s), when identifying a personal data breach referred to in the sub-paragraph of this clause, each party shall without undue delay, and in any case within 24 hours of becoming aware of the personal data breach, inform other parties about the nature, scope and context of the personal data breach where required, and
 - a. agree which party is the source of the personal data breach, and
 - b. that party shall take the lead in managing the personal data breach including investigating it, undertaking appropriate risk assessments, and managing any remediation, including providing any required notifications.
- 31. A personal data breach is as defined by the UK GDPR, including that in particular 'unauthorised or unlawful processing may include disclosure of personal data to recipients who are not authorised to receive (or access) the data, or *any other form of processing which violates the UK GDPR* – the consequence of such a breach being that the parties will be unable to ensure compliance with the principles relating to the processing of personal data.'
- 32. Where a party is required to inform the other party of a personal data breach, such notification should include the likely consequences of the breach, as well as the measures taken or proposed to be taken by the party if applicable to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects, such consequences including:
 - a. the inability to comply with data protection obligations; and
 - b. the realistic identification of the potential range of significant adverse effects on individuals, which can result in physical, material, or non-material damage, such as loss of control over

their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy, as well as any other significant economic or social disadvantage to those individuals, in particular where such adverse effects on individuals may wholly or partially, directly or indirectly, lead to a further event or incident because of or as well as, for example, a further breach of legal obligations which the parties are beholden to – e.g. Health and Safety at Work Act 1974, etc.

33. Each party shall ensure for their respective part that a description of the nature, scope and context of the personal data breach are recorded and logged, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records.
34. Each party shall assist the other party in notifying the personal data breach to the ICO where required, including providing the information in 7.2 and 7.3 upon reasonable request. The parties shall define all the elements to be provided by the party identifying a personal data breach when assisting each other in the notification of a personal data breach to the ICO.

THE USE OF PROCESSORS

35. For personal data that is processed for the stated purposes or any further processing activities and associated purpose(s), each party shall ensure, in order to satisfy the accountability principle and demonstrate due diligence, by way of a binding contract or other legal act, that any processors it relies upon:
36. only process personal data in line with the party's written instructions within the terms (unless it is required to do otherwise by law), which set out the extent of the processing that the processor is contracted, including:
 - a. the subject matter and duration of the processing;
 - b. the nature and purpose of the processing;
 - c. the type of personal data and categories of affected individuals; and
 - d. the party's obligations and rights.
37. provide sufficient guarantees, in particular in terms of its expert knowledge, resources and reliability, that they will implement appropriate technical and organisational measures to ensure the security of personal data, such as using encryption and pseudonymisation.
38. ensure their processing meets data protection obligations, including:
 - a. protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, through:
 - i. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - ii. the ability to restore access to personal data in the event of an incident; and
 - iii. processes for regularly testing and assessing the effectiveness of the measures.
 - b. demonstrating they are competent to process the personal data in line with those data protection obligations, such as maintaining records, appointing a data protection officer, and allowing the party to conduct timely audits, inspections or assessments, to demonstrate the processor's data protection obligations have been met, taking into account the nature of the processing and the risks to the data subjects.
 - c. obtaining a commitment of confidentiality from anyone it allows to process the personal data, unless that person is already under such a duty by statute, covering their employees

as well as any temporary workers and agency workers who have access to the personal data.

39. shall not engage another processor (i.e. a sub-processor)
 - a. without the party's prior specific or general written authorisation
 - b. where such authorisation is given, the processor shall demonstrate it has in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between the processor and the party.
40. inform the party without undue delay if:
 - a. any of party's instructions would lead to a breach of data protection obligations; or
 - b. they become aware of a personal data breach, taking utmost care to notify, the party within 24 hours, and assist the party in complying with its obligations regarding personal data breaches.
41. only transfer outside the UK when authorised to do so and ensure that such transfers comply with the transfer provisions as laid down by data protection obligations
42. assist the party where required in meeting its obligations to keep personal data secure, notify, where required, the ICO and affected individuals, and carry out DPIAs.
43. cooperate with supervisory authorities (such as the ICO) to help them perform their duties as required.
44. take appropriate technical and organisational measures to help the party respond to requests from individuals to exercise their rights.
45. at the end of the contract, in a secure manner, and, at the party's choice, delete or return to the party all the personal data it has been processing for it unless UK law requires it to be stored.

INTERNATIONAL TRANSFERS OF PERSONAL DATA

46. In relation to a party exporting personal data to a third country or international organisation {recipient), and including onward transfers by that recipient, in relation to the stated purposes or any further processing activities and associated purpose(s), where the recipient is not covered by an adequacy decision, the party shall check that enforceable data subject rights and effective legal remedies for data subjects are available, in addition to documenting (and making available to the other party upon reasonable request) one of the required appropriate safeguards or exceptions as data protection obligations, where:
 47. any routine restricted international personal data transfer that relies on an international data transfer agreement is subject to an international transfer risk assessment (TRA) prior to the transfer.
 48. any more complex restricted international personal data transfer (such as where the recipient is based in more than one country) is, in addition to completing a TRA, subject to a DPIA, and the implementation of any necessary further contractual, technical and organisational measures to sufficiently mitigate risks, including relying on another appropriate safeguard or exception or not proceeding where there is an enhanced risk.
 49. any unrestricted international personal data transfer is subject to contractual clauses that commit the recipient to their data protection obligations to facilitate the exercising of data subject rights as well as the ability of data subjects to seek administrative and judicial redress and to claim compensation in the UK and the destination country, including where the recipient is a:
 - a. controller, their responsibilities, DPIAs, security measures, and transfers or disclosures not authorised by UK law.
 - b. processor (or sub-processor), their processor contract, security measures, and transfers or disclosures not authorised by UK law.

INDIVIDUALS' RIGHT TO EXERCISE THEIR RIGHTS

50. Each party shall provide any individual wishing to exercise their rights directly with the other party the details of other party's designated single point of contact.
51. Each party shall handle any rights requests without prejudice and act to respond or otherwise provide for these requests without undue delay, and in any case within 1 month, or as required by data protection obligations.
52. Each party shall validate any rights request against their record of processing activities.
53. Each party shall fulfil any rights requests in a secure manner, including, security of communications and transmission of personal data.
54. In relation to right of access, each party shall
 - a. respond as to whether or not personal data is being processed; and
 - b. provide the individual with information as laid down by data protection legislation including with regards to the purpose(s) and legal basis for the processing; and
 - c. provide a copy of the personal data being processed.
55. In relation to right to data portability, where relevant, each party shall
 - a. refer the individual for any data portability requests received directly from individuals concerning personal data entered by the other party, who shall resolve any referred or direct data portability requests with the individual.
56. In relation to right to rectification, each party shall
 - a. rectify any inaccurate personal data upon request by individual; and
 - b. refer the individual to the other party for any data rectification requests concerning personal data entered by the other party, and the other party shall resolve any referred or direct right to data rectification requests.
57. In relation to right to erasure, each party shall
 - a. determine if any of the applicable grounds for erasure as laid out by the data protection legislation apply;
 - b. if grounds do not apply inform individual that the request may not be fulfilled.
 - c. if grounds apply immediately erase any personal data as per data protection obligation; and
 - d. inform any recipient of the valid erasure request; and
 - e. inform the individual of these recipients if requested by the individual.
58. In relation to right to restriction of processing,
 - a. if the relevant party no longer needs the personal data for the purposes of the processing, but they are required by the individual for the establishment, exercise or defence of legal claims restrict processing immediately, then the party shall inform the other party without undue delay, and in any case within 24 hours.
 - b. if the individual requests restriction pending the verification of the legitimate grounds of either party overriding those of the individual in connection to a right to object request, then the party shall
 - i. restrict processing immediately, and
 - ii. inform the other party without undue delay, and in any case within 24 hours.
59. In relation to right to object, if the individual objects to the legitimate interest of either party in processing or sharing their personal data the respective party shall demonstrate compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims, and, if unable to do so, cease

processing immediately and notify the other party of valid objection request without undue delay, and in any case within 24 hours.

Designated Points of Contact

Responsibility	Party A	Party B
Matters relating to these written arrangements		
Requests by individuals exercising their rights		
Personal data breaches and similar security incidents		
Authorisation of designated points of contact		
Date of authorisation		

